(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 687 351**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **26.11.2014 PCT/CN2014/092235**

(87) Fecha y número de publicación internacional: **02.07.2015 WO15096580**

(96) Fecha de presentación y número de la solicitud europea: **26.11.2014 E 14875870 (9)**

(97) Fecha y número de publicación de la concesión europea: **04.07.2018 EP 3057282**

(54) Título: **Dispositivo de control de flujo de red y método de configuración de estrategia de seguridad y dispositivo del mismo**

(30) Prioridad:

26.12.2013 CN 201310733490

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.10.2018

(73) Titular/es:

HUAWEI TECHNOLOGIES CO., LTD. (100.0%)
Huawei Administration Building, Bantian Longgang District
Shenzhen, Guangdong 518129, CN

(72) Inventor/es:

WANG, XIANGGUANG

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Dispositivo de control de flujo de red y método de configuración de estrategia de seguridad y dispositivo del mismo

Campo técnico

La presente invención se refiere al campo de la seguridad de red y, en particular, a un dispositivo de control de tráfico de red y a un método de configuración de política de seguridad y a un aparato del mismo.

Antecedentes

Una política de seguridad es una política que está configurada en un dispositivo de control de tráfico de red, por ejemplo, un cortafuegos de red, una pasarela de seguridad o un dispositivo de detección de intrusión, y se utiliza para reenviar un flujo de datos y detectar la seguridad de contenido. La política de seguridad, generalmente, incluye una condición de coincidencia y una acción de política. La condición de coincidencia se refiere a una condición determinante utilizada para determinar si un flujo de datos coincide con la política de seguridad; la acción de política se refiere a una acción que debe realizarse en el flujo de datos cuando se determina, de acuerdo con la condición de coincidencia, que el flujo de datos coincide con la política de seguridad, incluidos el permiso (permit) y la denegación (deny).

El dispositivo de control de tráfico de red puede identificar un atributo de un flujo de datos y realizar la coincidencia entre el atributo del flujo de datos y las condiciones de coincidencia de la política de seguridad. Si todas las condiciones coinciden, el flujo de datos coincide satisfactoriamente con la política de seguridad. Una vez que el flujo de datos coincide con la política de seguridad, el dispositivo ejecuta la acción de política de la política de seguridad.

Hay muchos parámetros configurables en la condición de coincidencia de la política de seguridad, incluidas las zonas de seguridad de origen y de destino, las direcciones de origen y de destino, un usuario, un servicio, una aplicación, un segmento de tiempo y similares. Estos parámetros pueden definir, en diferentes maneras de combinación, flujos de datos que tienen una misma naturaleza. Por ejemplo, si un empleado de un departamento de recursos humanos puede usar una aplicación QQ, la política de seguridad puede estar configurada de la siguiente manera: origen = "departamento de recursos humanos"; destino = cualquier red (any); aplicación = "QQ"; acción = "permitir".

En general, una política de seguridad se configura y se mantiene manualmente por un administrador de acuerdo con la experiencia del administrador y la respuesta de un usuario, lo que ocasiona un problema de gran dificultad de configuración y propenso a error. Este problema es particularmente agudo para las empresas medianas y pequeñas en las cuales los administradores tienen habilidades relativamente bajas.

El documento US 2010/235880 A1 da a conocer un sistema y un método para aplicar una política de tráfico de red a una sesión de aplicación. El método implementado por una pasarela de seguridad incluye: reconocer la sesión de aplicación entre una red y un servidor de aplicaciones a través de la pasarela de seguridad; determinar una identidad de usuario de la sesión de aplicación de acuerdo con un paquete que se transmite a través de la sesión de aplicación; consultar en el directorio corporativo una política de seguridad que incluya la identidad del usuario; aplicar la política de seguridad a la sesión de la aplicación.

Resumen

En vista de esto, un problema técnico que necesita ser resuelto por la presente invención es cómo reducir la dificultad y una probabilidad de error de configuración de una política de seguridad en un dispositivo de control de tráfico de red.

De acuerdo con un primer aspecto, se proporciona un método de configuración de política de seguridad implementado por un dispositivo de control de tráfico de red, que incluye:

identificar un origen, un destino y un tipo de aplicación de un flujo de datos de entrada, donde el origen indica un usuario que envía el flujo de datos o una dirección de usuario desde la cual se envía el flujo de datos, el destino del flujo de datos indica una dirección de usuario, una dirección de servidor o una dirección de red pública en la cual se recibe el flujo de datos y, el tipo de aplicación, indica qué tipo de aplicación cuyos datos están incluidos en el flujo de datos;

si el flujo de datos no coincide con una política existente, hacer coincidir el flujo de datos con una política de permitir cualquiera que permita el acceso de todos los usuarios

ejecutar, en base a una estructura organizativa de empresa predeterminada, en primer lugar, procesamiento de rastreo ascendente para obtener un primer punto de rastreo ascendente de origen y un primer

punto de rastreo ascendente de destino cuando el flujo de datos coincide con la política de permitir cualquiera, en donde el primer punto de rastreo ascendente de origen es un departamento al cual pertenece el usuario indicado por el origen cuando el origen indica un usuario, el primer punto de rastreo ascendente de origen es un primer segmento de red al cual pertenece la dirección de usuario indicada por el origen del flujo de datos cuando el origen indica una dirección de usuario desde la cual se envía el flujo de datos, el primer segmento de red comprende varias direcciones IP (Protocolo de Internet) y el primer punto de rastreo ascendente de destino se establece en cualquier dirección cuando el destino indica una dirección de red pública, el primer punto de rastreo ascendente se establece en un servidor cuando el destino indica una dirección de servidor, el primer punto de rastreo ascendente de destino es un segundo segmento de red en el que la dirección de usuario en la cual se recibe el flujo de datos pertenece cuando el destino indica una dirección de usuario en la cual se recibe el flujo de datos, el segundo segmento de red comprende múltiples direcciones IP; y

generar una primera política de seguridad, donde un origen en una condición de coincidencia de la primera política de seguridad se configura para el primer punto de rastreo ascendente de origen, un destino en la condición de coincidencia de la primera política de seguridad se configura al primer punto de rastreo ascendente de destino y una aplicación en la condición de coincidencia de la primera política de seguridad se configura al tipo de aplicación del flujo de datos, la primera política de seguridad se utiliza para coincidir con un flujo de datos posterior.

En una primera manera posible de implementación del primer aspecto, después de generar una primera política de seguridad, el método incluye además:

determinar si existe una segunda política de seguridad en el dispositivo de control de tráfico de red, donde una condición de coincidencia de la segunda política de seguridad difiere de la condición de coincidencia de la primera política de seguridad solo en orígenes y una acción de política de la segunda política de seguridad es la misma que una acción de política de la primera política de seguridad;

cuando se determina que existe la segunda política de seguridad, ejecutar, en base a la estructura organizativa de empresa, el segundo procesamiento de rastreo ascendente para obtener un segundo punto de rastreo ascendente de origen, donde el segundo punto ascendente de origen es un departamento de nivel superior al que pertenecen un departamento indicado por el origen de la primera política de seguridad y un departamento indicado por un origen de la segunda política de seguridad, o un segmento de red de nivel superior al que pertenecen un segmento de red indicado por el origen de la primera política de seguridad y un segmento de red indicado por un origen de la segunda política de seguridad; y

actualizar el origen de la primera política de seguridad al segundo punto de rastreo ascendente de origen y eliminar la segunda política de seguridad.

Con referencia al primer aspecto o a la primera manera posible de implementación del primer aspecto, en una segunda manera posible de implementación del primer aspecto, después de generar una primera política de seguridad, el método incluye además:

determinar si existe una tercera política de seguridad en el dispositivo de control de tráfico de red, donde una condición de coincidencia de la tercera política de seguridad difiere de la condición de coincidencia de la primera política de seguridad solo en destinos y una acción de política de la tercera política de seguridad es la misma que la acción de política de la primera política de seguridad;

cuando se determina que existe la tercera política de seguridad, ejecutar, en base a la estructura organizativa de empresa, el tercer procesamiento de rastreo ascendente para obtener un segundo punto de rastreo ascendente de destino, donde el segundo punto de rastreo ascendente de destino es un segmento de red de nivel superior al que pertenecen un segmento de red indicado por el destino de la primera política de seguridad y un segmento de red indicado por un destino de la tercera política de seguridad; y

actualizar el destino de la primera política de seguridad al segundo punto de rastreo ascendente de destino y eliminar la tercera política de seguridad.

Con referencia al primer aspecto o cualquiera de las maneras posibles de implementación anteriores del primer aspecto, en una tercera manera posible de implementación del primer aspecto, después de la ejecución, en base a una estructura organizativa de empresa predeterminada, del primer procesamiento de rastreo ascendente, el método incluye además: almacenar el primer punto de rastreo ascendente de origen, el primer punto de rastreo ascendente de destino y el tipo de aplicación del flujo de datos en una memoria del dispositivo de control de tráfico de red como una parte de información de triplete;

después de generar una primera política de seguridad, el método incluye además: eliminar la información de triplete que incluye el primer punto de rastreo ascendente de origen, el primer punto de rastreo ascendente de destino y el tipo de aplicación del flujo de datos de la memoria; y

antes de la ejecución, en base a una estructura organizativa de empresa predeterminada, del primer procesamiento de rastreo ascendente para obtener un primer punto de rastreo ascendente de origen y un primer punto de rastreo ascendente de destino, el método incluye además: determinar si la información de triplete que coincide con el origen, con el destino y con el tipo de aplicación del flujo de datos existe en la memoria; y

cuando se determina que la información de triplete que coincide con el origen, con el destino y con el tipo de aplicación del flujo de datos no existe en la memoria, ejecutar el primer procesamiento de rastreo ascendente.

De acuerdo con un segundo aspecto, se proporciona un aparato de configuración de política de seguridad implementado por un dispositivo de control de tráfico de red, que incluye:

un módulo de identificación, configurado para identificar un origen, un destino y un tipo de aplicación de un flujo de datos de entrada, donde el origen indica un usuario que envía el flujo de datos o una dirección de usuario desde la cual se envía el flujo de datos, el destino del flujo de datos indica una dirección de usuario, una dirección de servidor o una dirección de red pública en la cual se recibe el flujo de datos y el tipo de aplicación indica qué tipo de aplicación cuyos datos están incluidos en el flujo de datos;

un primer módulo de procesamiento de rastreo ascendente, conectado al módulo de identificación y configurado para coincidir con el flujo de datos con una política de permitir cualquier que permita el acceso de todos los usuarios cuando el flujo de datos no coincida con una política existente; ejecutar, en base a una estructura organizativa de empresa predeterminada, el primer procesamiento de rastreo ascendente para obtener un primer punto de rastreo ascendente y un primer punto de rastreo ascendente de destino cuando el flujo de datos coincide con la política de permitir cualquiera, donde el primer punto de rastreo ascendente de origen es un departamento al cual pertenece el usuario indicado por el origen cuando el origen indica un usuario, el primer punto de rastreo ascendente de origen es un primer segmento de red al cual pertenece la dirección de usuario indicada por el origen del flujo de datos cuando el origen indica una dirección de usuario desde la cual se envía el flujo de datos, el primer segmento de red comprende varias direcciones IP (Protocolo de Internet) y el primer punto de rastreo ascendente de destino se establece en cualquier dirección cuando el destino indica una dirección de red pública, el primer punto de rastreo ascendente de destino se establece en un servidor cuando el destino indica una dirección de servidor, el primer punto de rastreo ascendente de destino es un segundo segmento de red al cual pertenece la dirección de usuario en la cual se recibe el flujo de datos cuando el destino indica una dirección de usuario en la cual se recibe el flujo de datos, el segundo segmento de red comprende múltiples direcciones IP; y

un módulo de generación, conectado al primer módulo de procesamiento de rastreo ascendente y configurado para generar una primera política de seguridad, donde un origen en una condición de coincidencia de la primera política de seguridad está configurado al primer punto de rastreo ascendente de origen, un destino en la condición de coincidencia de la primera política de seguridad está configurado al primer punto de rastreo ascendente de destino y una aplicación en la condición de coincidencia de la primera política de seguridad está configurada al tipo de aplicación del flujo de datos; la primera política de seguridad se utiliza para coincidir con un flujo de datos posterior.

En una primera manera posible de implementación del segundo aspecto, el aparato incluye además:

un primer módulo de determinación, conectado al módulo de generación y configurado para determinar si existe una segunda política de seguridad en el dispositivo de control de tráfico de red, donde una condición de coincidencia de la segunda política de seguridad difiere de la condición de coincidencia de la primera política de seguridad solo en orígenes y una acción de política de la segunda política de seguridad es la misma que una acción de política de la primera política de seguridad;

un segundo módulo de procesamiento de rastreo ascendente, conectado al primer módulo de determinación y configurado para: cuando se determina que existe la segunda política de seguridad, ejecutar, en base a la estructura organizativa de empresa, el segundo procesamiento de rastreo ascendente para obtener un segundo punto de rastreo ascendente de origen, donde el segundo punto de rastreo ascendente de origen es un departamento de nivel superior al que pertenecen un departamento indicado por el origen de la primera política de seguridad y un departamento indicado por un origen de la segunda política de seguridad, o un segmento de red de nivel superior al que pertenecen un segmento de red indicado por el origen de la primera política de seguridad y un segmento de red indicado por un origen de la segunda política de red; y

un módulo de actualización, conectado al segundo módulo de procesamiento de rastreo ascendente y configurado para actualizar el origen de la primera política de seguridad al segundo punto de rastreo ascendente de origen y eliminar la segunda política de seguridad.

Con referencia al segundo aspecto o la primera manera posible de implementación del segundo aspecto, en una segunda manera posible de implementación del segundo aspecto, el aparato incluye además:

un segundo módulo de determinación conectado al módulo de generación y configurado para determinar si existe una tercera política de seguridad en el dispositivo de control de tráfico de red, donde una condición de coincidencia de la tercera política de seguridad difiere de la condición de coincidencia de la primera política de seguridad solo en los destinos y una acción de política de la tercera política de seguridad es la misma que la acción de política de la primera política de seguridad; y

un tercer módulo de procesamiento de rastreo ascendente, conectado al segundo módulo de determinación y al módulo de actualización, y configurado para: cuando se determina que existe la tercera política de seguridad, ejecutar, en base a la estructura organizativa de empresa, el tercer procesamiento de rastreo ascendente para obtener un segundo punto de rastreo ascendente de destino, donde el segundo punto de rastreo ascendente de

destino es un segmento de red de nivel superior al que pertenecen un segmento de red indicado por el destino de la primera política de seguridad y un segmento de red indicado por un destino de la tercera política de seguridad, donde

el módulo de actualización está configurado además para actualizar el destino de la primera política de seguridad al segundo punto de rastreo ascendente de destino y eliminar la tercera política de seguridad.

Con referencia al segundo aspecto o a cualquiera de las maneras posibles de implementación anteriores del segundo aspecto, en una tercera manera posible de implementación del segundo aspecto, el aparato incluye además:

un módulo de generación de triplete conectado al primer módulo de procesamiento de rastreo ascendente y a una memoria del aparato de configuración de políticas de seguridad, y configurado para: enviar una instrucción a la memoria; después de ejecutar el primer procesamiento de rastreo ascendente, en base a la estructura organizativa de empresa predeterminada, almacenar el primer punto de rastreo ascendente de origen, el primer punto de rastreo ascendente de destino y el tipo de aplicación del flujo de datos en la memoria como una parte de la información de triplete; y después de generarse la primera política de seguridad, eliminar de la memoria la información de triplete que incluye el primer punto de rastreo ascendente de origen, el primer punto de rastreo ascendente de destino y el tipo de aplicación del flujo de datos; y

un módulo de determinación de triplete, conectado al módulo de identificación, al primer módulo de procesamiento de rastreo ascendente y a la memoria, y configurado para: antes de que se ejecute el primer procesamiento de rastreo ascendente en base a la estructura organizativa de empresa predeterminada para obtener el primer punto de rastreo ascendente de origen y el primer punto de rastreo ascendente de destino, determinar si la información de triplete que coincide con el origen, con el destino y con el tipo de aplicación del flujo de datos existe en la memoria, donde cuando se determina que la información de triplete que coincide con el origen, con el destino y con el tipo de aplicación del flujo de datos no existe en la memoria, se ejecuta el primer procesamiento de rastreo ascendente.

De acuerdo con un tercer aspecto, se proporciona un dispositivo de control de tráfico de red que incluye una memoria, una interfaz de comunicaciones y un procesador, donde

la memoria está configurada para almacenar código de programa; y

el procesador lee el código de programa almacenado en la memoria y ejecuta las siguientes operaciones:

identificar un origen, un destino y un tipo de aplicación de un flujo de datos obtenido utilizando la interfaz de comunicaciones, donde el origen indica un usuario que envía el flujo de datos o una dirección de usuario desde la cual se envía el flujo de datos, el destino del flujo de datos indica una dirección de usuario, una dirección de servidor o una dirección de red pública en la cual se recibe el flujo de datos y el tipo de aplicación indica qué tipo de aplicación cuyos datos están incluidos en el flujo de datos;

si el flujo de datos no coincide con una política existente, hacer coincidir el flujo de datos con una política de permitir cualquier que permita el acceso de todos los usuarios;

ejecutar, en base a una estructura organizativa de empresa predeterminada, el primer procesamiento de rastreo ascendente para obtener un primer punto de rastreo ascendente de origen y un primer punto de rastreo ascendente de destino cuando el flujo de datos coincide con la política de permitir cualquiera, en donde el primer punto de rastreo ascendente de origen es un departamento al cual pertenece el usuario indicado por el origen cuando el origen indica un usuario, el primer punto de rastreo ascendente de origen es un primer segmento de red al cual pertenece la dirección de usuario indicada por el origen del flujo de datos cuando el origen indica una dirección de usuario desde la cual se envía el flujo de datos, el primer segmento de red comprende múltiples direcciones IP (Protocolo de Internet), y el primer punto de rastreo ascendente de destino se establece en cualquier dirección cuando el destino indica una dirección de red pública; el primer punto de rastreo ascendente de destino se establece en un servidor cuando el destino indica una dirección de servidor; el primer punto de rastreo ascendente de destino es un segundo segmento de red al cual pertenece la dirección de usuario en la cual se recibe el flujo de datos cuando el destino indica una dirección de usuario en la cual se recibe el flujo de datos, el segundo segmento de red comprende múltiples direcciones IP; y

generar una primera política de seguridad, donde un origen en una condición de coincidencia de la primera política de seguridad se configura al primer punto de rastreo ascendente de origen, un destino en la condición de coincidencia de la primera política de seguridad se configura al primer punto de rastreo ascendente de destino y una aplicación en la condición de coincidencia de la primera política de seguridad se configura al tipo de aplicación del flujo de datos, la primera política de seguridad se utiliza para coincidir con un flujo de datos posterior.

El primer procesamiento de rastreo ascendente se ejecuta en base a una estructura organizativa de empresa predeterminada para obtener un primer punto de rastreo ascendente de origen y un primer punto de rastreo ascendente de destino, y se genera una primera política de seguridad. De acuerdo con el método de configuración de política de seguridad y con el aparato implementado por un dispositivo de control de tráfico de red, en las realizaciones de la presente invención, se puede generar automáticamente una política de seguridad que reduce la dificultad de configuración de la política de seguridad y aumenta la tasa de éxito de configuración.

Antes de que se ejecute el primer procesamiento de rastreo ascendente, en base a la estructura organizativa de empresa predeterminada, se determina si existe información de triplete que coincida con un flujo de datos en una memoria. De acuerdo con el método de configuración de política de seguridad y con el aparato implementado por un dispositivo de control de tráfico de red, en las realizaciones de la presente invención, el filtrado puede realizarse en un flujo de datos que se está procesando, lo que impide que el flujo de datos ingrese repetidamente en un proceso y mejora la eficiencia de configuración de una política de seguridad.

Se determina si existe una segunda política de seguridad y una tercera política de seguridad en el dispositivo de control de tráfico de red y se realiza un segundo procesamiento de rastreo ascendente en una primera política de seguridad y en la segunda política de seguridad cuando existe la segunda política de seguridad y se realiza un tercer procesamiento de rastreo ascendente en la primera política de seguridad y en la tercera política de seguridad cuando existe la tercera política de seguridad. De acuerdo con el método de configuración de política de seguridad y con el aparato implementado por un dispositivo de control de tráfico de red, en las realizaciones de la presente invención, las políticas de seguridad generadas pueden fusionarse aún más, lo que reduce una cantidad de políticas de seguridad generadas y logra un efecto de simplificación de políticas de seguridad en el dispositivo de control de tráfico de red.

De acuerdo con las siguientes descripciones detalladas de las realizaciones a modo de ejemplo con referencia a los dibujos adjuntos, otras características y aspectos de la presente invención se vuelven más evidentes.

Breve descripción de los dibujos

Los dibujos adjuntos que están incluidos en la memoria descriptiva y que constituyen una parte de la memoria descriptiva muestran, junto con la memoria descriptiva, realizaciones ejemplares, características y aspectos de la presente invención, y se utilizan para explicar un principio de la presente invención.

La FIG. 1 muestra un diagrama de flujo de un método de configuración de política de seguridad implementado por un dispositivo de control de tráfico de red de acuerdo con una realización de la presente invención;

la FIG. 2 muestra un diagrama esquemático de una estructura organizativa de un modelo 1 de usuario de acuerdo con una realización de la presente invención;

la FIG. 3 muestra un diagrama esquemático de una estructura organizativa de un modelo 2 de usuario de acuerdo con una realización de la presente invención;

la FIG. 4 muestra un diagrama esquemático de una estructura organizativa de un modelo 3 de usuario de acuerdo con una realización de la presente invención;

la FIG. 5 muestra un diagrama esquemático de la ejecución del primer procesamiento de rastreo ascendente cuando un origen de un flujo de datos indica una dirección de usuario de acuerdo con una realización de la presente invención;

la FIG. 6 muestra un diagrama de flujo de un método para identificar una dirección de red privada como una dirección de red pública o una dirección de red privada, de acuerdo con una realización de la presente invención;

la FIG. 7 muestra un diagrama de flujo de otro método de configuración de política de seguridad implementado por un dispositivo de control de tráfico de red de acuerdo con una realización de la presente invención;

la FIG. 8 muestra un diagrama esquemático de una estructura organizativa de un modelo 4 de usuario de acuerdo con una realización de la presente invención;

la FIG. 9a y la FIG. 9b muestran diagramas esquemáticos de estructuras organizativas de un modelo 5 de usuario de acuerdo con una realización de la presente invención;

la FIG. 10 muestra un diagrama esquemático de una estructura de un aparato de configuración de política de seguridad implementado por un dispositivo de control de tráfico de red de acuerdo con una realización de la presente invención;

la FIG. 11 muestra un diagrama esquemático de una estructura de otro aparato de configuración de política de seguridad implementado por un dispositivo de control de tráfico de red de acuerdo con una realización de la presente invención; y

la FIG. 12 muestra un diagrama esquemático de una estructura de un dispositivo de control de tráfico de red de acuerdo con una realización de la presente invención.

Descripción de las realizaciones

Lo siguiente describe en detalle varias realizaciones ejemplares, características y aspectos de la presente invención con referencia a los dibujos adjuntos. Los símbolos de referencia iguales en los dibujos adjuntos indican elementos que tienen una función igual o similar. Diversos aspectos de las realizaciones ilustradas en los dibujos adjuntos pueden no dibujarse necesariamente a escala, a menos que se especifique lo contrario.

La palabra "ejemplar" para uso exclusivo en el presente documento significa "utilizado como ejemplo o realización o para un propósito descriptivo". Cualquier realización descrita en el presente documento para un fin "ejemplar" no debe interpretarse como preferida antes o mejor que otras realizaciones.

Además, muchos detalles específicos se exponen en las siguientes maneras de implementación específicas con el fin de describir mejor la presente invención. Una persona experta en la técnica debe entender que la presente invención todavía puede implementarse sin algunos detalles específicos. En algunos ejemplos, los métodos, medios, elementos y circuitos bien conocidos por una persona experta en la técnica no se describen en detalle, de modo que se resalta un propósito principal de la presente invención.

Realización 1

La FIG. 1 muestra un diagrama de flujo de un método de configuración de política de seguridad implementado por un dispositivo de control de tráfico de red de acuerdo con una realización de la presente invención. El dispositivo de control de tráfico de red en esta realización de la presente invención incluye, pero no está limitado a, un dispositivo de red tal como un cortafuegos, un enrutador y un dispositivo de detección de intrusión. Como se muestra en la FIG. 1, el método incluye principalmente:

Paso S101. Identificar un origen, un destino y un tipo de aplicación de un flujo de datos de entrada.

El origen indica un usuario que envía el flujo de datos o una dirección de usuario desde la cual se envía el flujo de datos, por ejemplo, un usuario A o una dirección de Protocolo de Internet (inglés: Internet Protocol Address, dirección IP para abreviar) de un usuario. El destino del flujo de datos indica una dirección de usuario, una dirección de servidor o una dirección de red pública en la cual se recibe el flujo de datos. El tipo de aplicación indica qué tipo de aplicación cuyos datos están incluidos en el flujo de datos, por ejemplo, el tipo de aplicación es QQ.

En una manera posible de implementación, después del paso S101, el método puede incluir además crear una nueva política de permitir cualquiera (inglés: permit any) para permitir el acceso de todos los usuarios. Si el flujo de datos coincide con una política existente, el procesamiento se realiza de acuerdo con la política existente. Si el flujo de datos no coincide con una política existente, se realiza la coincidencia con la política de permitir cualquiera. Cuando un flujo de datos coincide con la política de permitir cualquiera, se ejecuta el paso S102.

Paso S102. Ejecutar, en base a una estructura organizativa de empresa predeterminada, el primer procesamiento de rastreo ascendente para obtener un primer punto de rastreo ascendente de origen y un primer punto de rastreo ascendente de destino.

El primer punto de rastreo ascendente de origen es un departamento al cual pertenece el usuario indicado por el origen del flujo de datos, o un segmento de red al cual pertenece la dirección de usuario indicada por el origen del flujo de datos.

Cuando el origen indica un usuario, el primer punto de rastreo ascendente de origen es un departamento al cual pertenece el usuario indicado por el origen; cuando el origen indica un departamento al cual pertenecen un usuario, se establece un punto de rastreo ascendente correspondiente al origen en el departamento o en un departamento de nivel superior. A continuación, se detalla por separado, de acuerdo con diferentes modelos de usuario, un principio del primer procesamiento de rastreo ascendente con referencia a los dibujos adjuntos. La FIG. 2 muestra un diagrama esquemático de una estructura organizativa de un modelo 1 de usuario. La FIG. 3 muestra un diagrama esquemático de una estructura organizativa de un modelo 2 de usuario. Como se muestra en la FIG. 2 y en la FIG. 3, en una manera posible de implementación, un departamento puede incluir solo un subdepartamento o un empleado; en los dos modelos de usuario, este tipo de usuario se puede rastrear ascendente directamente a un departamento de nivel superior. La FIG. 4 muestra un diagrama esquemático de una estructura organizativa de un modelo 3 de usuario. Como se muestra en la FIG. 4, un departamento de usuario incluye múltiples usuarios. En este caso, los usuarios se pueden rastrear ascendentes directamente a un departamento de nivel superior, o se pueden

configurar para rastrearse ascendentes a un departamento de nivel superior solo bajo una política que al menos varios usuarios en este departamento tienen un mismo destino y un mismo tipo de aplicación.

Cuando el origen indica una dirección de usuario, el primer punto de rastreo ascendente de origen es un segmento de red al cual pertenece la dirección de usuario indicada por el origen del flujo de datos. La FIG. 5 muestra un diagrama esquemático de la ejecución del primer procesamiento de rastreo ascendente cuando un origen de un flujo de datos indica una dirección de usuario. Cuando se utiliza una aplicación mediante el uso de una dirección IP, la dirección IP se puede rastrear ascendente a un segmento de red con una máscara de subred 255.255.255.0. Es imposible que cada una de todas las direcciones IP en un segmento de red IP se utilice por los usuarios. En un caso en el que una política está configurada de acuerdo con una dirección IP, un administrador planifica una red de una empresa de acuerdo con los grupos. Por lo tanto, existe una alta probabilidad de que los usuarios en un mismo segmento de red pertenezcan a un mismo departamento. La máscara de subred 255.255.255.0 pertenece a un criterio de división de segmento de red universal. Un principio de rastreo ascendente basado en una máscara de subred es que cuando existen segmentos de red con una máscara de subred 255.255.254.0, se realiza un rastreo ascendente a un segmento de red con la máscara de subred 255.255.254.0.

El primer punto de rastreo ascendente de destino puede ser un segmento de red al cual pertenece la dirección de usuario indicada por el destino del flujo de datos. El primer punto de rastreo ascendente de destino también puede ser un servidor correspondiente a la dirección de servidor indicada por el destino del flujo de datos, o cualquier dirección (any) correspondiente a la dirección de red pública indicada por el destino del flujo de datos.

Una dirección indicada por el destino se clasifica en una dirección de red pública o una dirección de red privada, donde la dirección de red privada debe clasificarse además en una dirección de servidor y una dirección de usuario de empresa. Cuando el destino indica una dirección de red pública, el primer punto de rastreo ascendente de destino se establece en cualquier dirección (any); cuando el destino indica una dirección de servidor, el primer punto de rastreo ascendente de destino se establece en un servidor; cuando el destino indica una dirección de usuario, el primer punto de rastreo ascendente de destino se establece en un segmento de red al cual pertenece la dirección de usuario.

La dirección IP pública se identifica utilizando un segmento de red IP. Todas las direcciones IP privadas se concentran en tres grupos de direcciones de red privadas: 10.0.0.0-10.255.255.255, 172.16.0.0-172.31.0.0 y 192.168.0.0-192.168.255.255. Todas las direcciones excluidas de los grupos de direcciones de red privada son direcciones IP públicas y las direcciones IP públicas se rastrean ascendentes directamente a cualquier dirección.

La dirección de red privada debe clasificarse además en una dirección de servidor y en una dirección de usuario de empresa. La FIG. 6 muestra un diagrama de flujo de un método para identificar una dirección de red privada como una dirección de red pública o una dirección de red privada. En primer lugar, es necesario cumplir con la condición previa de que una dirección de destino es una dirección de red privada. Los pasos específicos son como sigue:

Paso S601. Determinar si una dirección de origen de un flujo de datos es una dirección de red pública.

Si la dirección de origen es una dirección de red pública, el paso S606 se ejecuta para identificar una dirección de destino del flujo de datos como una dirección de servidor.

Si la dirección de origen no es una dirección de red pública, se ejecuta el paso S602.

Paso S602. Determinar si la dirección de destino pertenece a una zona desmilitarizada (inglés: Demilitarized Zone, DMZ para abreviar).

Si la dirección de destino pertenece a una DMZ, se ejecuta el paso S606; si la dirección de destino no pertenece a una DMZ, se ejecuta el paso S603.

Un dispositivo de control de tráfico de red, en general, está configurado para mantener múltiples zonas de seguridad por defecto: una zona de seguridad confiable, una red relativamente confiable y una zona de seguridad no confiable, donde la zona de seguridad confiable utilizada generalmente para el despliegue de una red interna de una compañía, la zona de seguridad no confiable utilizada generalmente para desplegar una red desconocida. La zona de seguridad DMZ generalmente utilizada para el despliegue de un servidor. El servidor se utiliza para proporcionar servicio de forma externa. Por lo tanto, para una red interna de una compañía, es relativamente seguro desplegar el servidor en la zona de seguridad DMZ.

Paso S603. Determinar si la dirección de destino es una dirección para balanceo de carga del servidor (inglés: Server Load Balancing, SLB para abreviar) o una dirección de un servidor de traducción de direcciones de red (inglés: Network Address Translation Server, servidor NAT para abreviar).

Si la dirección de destino es una dirección para SLB o una dirección de una NAT, se ejecuta el paso S606; si la dirección de destino no es una dirección para SLB o una dirección de una NAT, se ejecuta el paso S604.

El SLB y el servidor NAT se utilizan en un escenario en el que una empresa proporciona el servicio para una red externa, y una dirección IP privada del servidor se asigna a una dirección IP pública virtual para que acceda un usuario externo. Una diferencia entre el SLB y el servidor NAT radica en una cantidad de servidores, tal como uno o más servidores. El SLB corresponde a un escenario en el que hay varios servidores y se utiliza un algoritmo de planificación para balancear la carga de tráfico de acceso desde una red externa entre los servidores múltiples. El servidor NAT corresponde a un escenario en el que solo hay un servidor, no se requiere un algoritmo de planificación y todo el tráfico se asigna al servidor.

Paso S604. Determinar si una dirección de respuesta de un sistema de nombres de dominio (inglés: Domain Name Server, DNS para abreviar) es una dirección de red privada.

Si la dirección de respuesta de la solicitud de DNS es una dirección de red privada, se ejecuta el paso S606; si la dirección de respuesta de la solicitud de DNS no es una dirección de red privada, se ejecuta el paso S605.

Un servidor DNS se utiliza para devolver una dirección IP real de un nombre de dominio específico. Si el servidor existe en una red privada y cuando se debe proporcionar un nombre de dominio del servidor a un usuario interno para acceder al servidor, una dirección IP correspondiente al servidor también puede ser una dirección IP privada. Por lo tanto, en este caso, la dirección IP debe identificarse como una dirección de servidor.

Paso S605. Identificar la dirección de destino como una dirección de usuario de empresa.

Cuando el destino indica una dirección de usuario de empresa, el primer punto de rastreo ascendente de destino se establece en un segmento de red al cual pertenece la dirección de usuario de empresa. En este caso, un método para realizar el primer procesamiento de rastreo ascendente es similar al método mostrado en la FIG. 5 y la correspondiente descripción de los mismos y los detalles no se describen de nuevo en el presente documento.

Paso S103. Generar una primera política de seguridad, donde un origen en una condición de coincidencia de la primera política de seguridad se configura al primer punto de rastreo ascendente de origen, un destino en la condición de coincidencia de la primera política de seguridad se configura al primer punto de rastreo ascendente de destino y una aplicación en la condición de coincidencia de la primera política de seguridad se configura al tipo de aplicación del flujo de datos.

El primer procesamiento de rastreo ascendente se ejecuta en base a una estructura organizativa de empresa predeterminada para obtener un primer punto de rastreo ascendente de origen y un primer punto de rastreo ascendente de destino, y se genera una primera política de seguridad. De acuerdo con el método de configuración de política de seguridad implementado por un dispositivo de control de tráfico de red, en la realización de la presente invención, se puede generar automáticamente una política de seguridad, lo que reduce la dificultad para configurar la política de seguridad y aumenta una tasa de éxito de configuración.

Realización 2

La FIG. 7 muestra un diagrama de flujo de un método de configuración de política de seguridad implementado por un dispositivo de control de tráfico de red de acuerdo con otra realización de la presente invención. En la Fig. 7, los componentes cuyos símbolos de referencia son iguales que los de los componentes en la FIG. 1 tienen las mismas funciones. Para abreviar, se omiten las descripciones detalladas de estos componentes. Como se muestra en la FIG. 7, en una manera posible de implementación, después del paso S101, el método incluye además:

Paso S701. Determinar si la información de triplete que coincide con el origen, con el destino y con el tipo de aplicación del flujo de datos existe en una memoria.

Cuando se determina que la información de triplete que coincide con el origen, con el destino y con el tipo de aplicación del flujo de datos no existe en la memoria, se ejecuta el paso S102.

Cuando se determina que existe la información de triplete que coincide, el proceso termina.

Paso S102. Este paso es similar al paso S102 en la FIG. 1 y los detalles no se describen de nuevo en el presente documento.

Paso S702. Almacenar el primer punto de rastreo ascendente de origen, el primer punto de rastreo ascendente de destino y el tipo de aplicación del flujo de datos en la memoria como una parte de la información de triplete.

En esta realización de la presente invención, si la información de triplete que coincide con el flujo de datos existe en la memoria, se determina antes de que se ejecute el primer procesamiento de rastreo ascendente, en base a la estructura organizativa de empresa predeterminada, y el filtrado se puede realizar en un flujo de datos que está siendo procesado. Esto evita que un mismo flujo de datos ingrese repetidamente en un proceso y mejora la eficiencia de configuración de una política de seguridad.

Paso S103. Este paso es similar al paso S103 en la FIG. 1 y los detalles no se describen de nuevo en el presente documento. Por ejemplo, un usuario A utiliza una dirección de origen 192.168.0.2 para iniciar sesión en QQ accediendo a Internet y se genera una primera política de seguridad: origen = 192.168.0.0/24; destino = cualquiera; aplicación = QQ; acción = permitir.

Paso S703. Determinar si existe una segunda política de seguridad en el dispositivo de control de tráfico de red, donde una condición de coincidencia de la segunda política de seguridad difiere de la condición de coincidencia de la primera política de seguridad solo en orígenes y una acción de política de la segunda política de seguridad es la misma que una acción de política de la primera política de seguridad. Cabe señalar que puede haber una o más segundas políticas de seguridad.

Cuando se determina que existe la segunda política de seguridad, se ejecuta el paso S704. Por ejemplo, el paso S704 se ejecuta si existe la siguiente segunda política de seguridad en el dispositivo de control de tráfico de red: origen = 192.168.1.0/24; destino = cualquiera; aplicación = QQ; acción = permitir.

Cuando se determina que no existe la segunda política de seguridad, el proceso termina.

Paso S704. Ejecutar, en base a la estructura organizativa de empresa, el segundo procesamiento de rastreo ascendente para obtener un segundo punto de rastreo ascendente de origen, donde el segundo punto ascendente de origen es un departamento de nivel superior al que pertenecen un departamento indicado por el origen de la primera política de seguridad y un departamento indicado por un origen de la segunda política de seguridad, o un segmento de red de nivel superior al que pertenecen un segmento de red indicado por el origen de la primera política de seguridad y un segmento de red indicado por un origen de la segunda política de seguridad.

El segundo procesamiento de rastreo ascendente incluye: cuando el origen de la primera política de seguridad y el origen de la segunda política de seguridad cada uno indica un departamento, establecer un punto de rastreo ascendente correspondiente al origen de la primera política de seguridad y al origen de la segunda política de seguridad a un departamento de nivel superior común de los departamentos. Por ejemplo, en un diagrama esquemático de una estructura organizativa de un modelo 4 de usuario, el cual se muestra en la FIG. 8, el origen de la primera política de seguridad y el origen de la segunda política de seguridad cada uno indica un subdepartamento en la figura, y el punto de rastreo ascendente correspondiente al origen de la primera política de seguridad y al origen de la segunda política de seguridad se establece en un departamento de nivel superior común de los dos subdepartamentos. La FIG. 9a y la FIG.9b muestran diagramas esquemáticos de estructuras organizativas de un modelo 5 de usuario. Cuando uno o más subdepartamentos y uno o más usuarios existen en un departamento, en el paso S102, los usuarios que están directamente afiliados al departamento pueden formar un subdepartamento 3 virtual (mostrado en la FIG. 9b), y un empleado se rastrea primero ascendente al subdepartamento 3 virtual, es decir, el origen de la primera política de seguridad es el subdepartamento 3 virtual. En este paso, si el origen de la segunda política de seguridad es un subdepartamento 2 y otras condiciones de coincidencia son las mismas que las de la primera política de seguridad, se cumple una condición de rastreo ascendente del departamento y el punto de rastreo ascendente correspondiente al origen de la primera política de seguridad y al origen de la segunda política de seguridad puede establecerse en un departamento de nivel superior común del subdepartamento 2 y del subdepartamento 3. Además, en una manera posible de implementación, un usuario tiene permiso de múltiples departamentos y se realiza el rastreo ascendente para cada uno de los departamentos de acuerdo con un principio de rastreo ascendente del departamento. Se puede hacer referencia a los principios de procesamiento de los modelos 1 a 5.

Cuando el origen de la primera política de seguridad y el origen de la segunda política de seguridad indican cada uno un segmento de red, el punto de rastreo ascendente correspondiente al origen de la primera política de seguridad y al origen de la segunda política de seguridad se establece en un segmento de red de nivel superior al que pertenecen los dos segmentos de red. Por ejemplo, el origen (192.168.0.0/24) de la primera política de seguridad y el origen (192.168.1.0/24) de la segunda política de seguridad se rastrean ascendentes a (192.168.0.0/23).

Paso S705. Actualizar el origen de la primera política de seguridad al segundo punto de rastreo ascendente de origen y eliminar la segunda política de seguridad.

Por ejemplo, la primera política de seguridad se actualiza a: origen = 192.168.0.0/23; destino = cualquiera; aplicación = QQ; acción = permitir. La segunda política de seguridad original (origen = 192.168.1.0/24; destino = cualquiera; aplicación = QQ; acción = permitir) se elimina.

Paso S706. Determinar si existe una tercera política de seguridad en el dispositivo de control de tráfico de red, donde una condición de coincidencia de la tercera política de seguridad difiere de la condición de coincidencia de la primera política de seguridad solo en destinos y una acción de política de la tercera política de seguridad es la misma que la acción de política de la primera política de seguridad.

Cuando se determina que existe la tercera política de seguridad, se ejecuta el paso S707.

Cuando se determina que la tercera política de seguridad no existe, el proceso termina.

Paso S707. Ejecutar, en base a la estructura organizativa de empresa, el tercer procesamiento de rastreo ascendente para obtener un segundo punto de rastreo ascendente de destino, donde el segundo punto de rastreo ascendente de destino es un segmento de red de nivel superior al que pertenecen un segmento de red indicado por el destino de la primera seguridad la política y un segmento de red indicado por un destino de la tercera política de seguridad.

Paso S708. Actualizar el destino de la primera política de seguridad al segundo punto de rastreo ascendente de destino y eliminar la tercera política de seguridad.

Los pasos S706 a S708 son similares a los pasos S703 a S705, y no se describen adicionalmente en el presente documento utilizando un ejemplo. También puede haber una o más terceras políticas de seguridad. En esta realización de la presente invención, se determina si la segunda política de seguridad y la tercera política de seguridad existen en el dispositivo de control de tráfico de red, y el segundo procesamiento de rastreo ascendente se realiza en una primera política de seguridad y en la segunda política de seguridad cuando existe la segunda política de seguridad, y el tercer procesamiento de rastreo ascendente se realiza en la primera política de seguridad y en la tercera política de seguridad cuando existe la tercera política de seguridad. De esta forma, las políticas de seguridad generadas se fusionan aún más, lo que reduce la cantidad de políticas de seguridad generadas y logra un efecto de simplificación de las políticas de seguridad en el dispositivo de control de tráfico de red.

Paso S709. Eliminar la información de triplete que incluye el primer punto de rastreo ascendente de origen, el primer punto de rastreo ascendente de destino y el tipo de aplicación del flujo de datos de la memoria.

Ya se ha generado una política de seguridad. Para un flujo de datos posterior que coincida con el triplete, se alcanza la política de seguridad generada y la política de permitir cualquier ya no se alcanza. Por lo tanto, no es necesario continuar almacenando la información de triplete en la memoria. Un administrador ve las políticas generadas en base a un modelo de tráfico, aplica las políticas en lotes y verifica la idoneidad de las políticas después de que el dispositivo se ejecute durante un período de tiempo. Cuando la política de permitir cualquiera no se alcanza por el nuevo tráfico, se puede considerar que el tráfico de un usuario ha sido estable.

El primer procesamiento de rastreo ascendente se ejecuta en base a una estructura organizativa de empresa predeterminada para obtener un primer punto de rastreo ascendente de origen y un primer punto de rastreo ascendente de destino, y se genera una primera política de seguridad. De acuerdo con el método de configuración de política de seguridad implementado por un dispositivo de control de tráfico de red, en la realización de la presente invención, se puede generar automáticamente una política de seguridad, lo que reduce la dificultad de configurar la política de seguridad y aumenta una tasa de éxito de configuración.

Antes de que se ejecute el primer procesamiento de rastreo ascendente, en base a la estructura organizativa de empresa predeterminada, se determina si la información de triplete que coincide con un flujo de datos existe en una memoria. De acuerdo con el método de configuración de política de seguridad implementado por un dispositivo de control de tráfico de red, en la realización de la presente invención, el filtrado puede realizarse en un flujo de datos que se está procesando, lo que previene que un mismo flujo de datos ingrese repetidamente en un proceso y mejora la eficiencia de configuración de una política de seguridad.

Se determina si existen una segunda política de seguridad y una tercera política de seguridad en el dispositivo de control de tráfico de red, y el segundo procesamiento de rastreo ascendente se realiza en una primera política de seguridad y en la segunda política de seguridad, cuando la segunda política de seguridad existe, y el tercer procesamiento de rastreo ascendente se realiza en la primera política de seguridad y en la tercera política de seguridad, cuando la tercera política de seguridad existe. De acuerdo con el método de configuración de política de seguridad implementado por un dispositivo de control de tráfico de red, en la realización de la presente invención, las

políticas de seguridad generadas pueden fusionarse aún más, lo que reduce una cantidad de políticas de seguridad generadas y logra un efecto de simplificación de políticas de seguridad en el dispositivo de control de tráfico de red.

Realización 3

La FIG. 10 muestra un diagrama esquemático de una estructura de un aparato de configuración de política de seguridad implementado por un dispositivo de control de tráfico de red de acuerdo con una realización de la presente invención. Como se muestra en la FIG. 10, el aparato 10 de configuración de política de seguridad incluye: un módulo 110 de identificación, un primer módulo 120 de procesamiento de rastreo ascendente y un módulo 130 de generación.

El módulo 110 de identificación está configurado para identificar un origen, un destino y un tipo de aplicación de un flujo de datos de entrada, donde el origen indica un usuario que envía el flujo de datos o una dirección de usuario desde la cual se envía el flujo de datos, el destino del flujo de datos indica una dirección de usuario, una dirección de servidor o una dirección de red pública en la cual se recibe el flujo de datos, y el tipo de aplicación indica qué tipo de aplicación cuyos datos están incluidos en el flujo de datos.

El primer módulo 120 de procesamiento de rastreo ascendente está conectado al módulo 110 de identificación y está configurado para ejecutar, en base a una estructura organizativa de empresa predeterminada, el primer procesamiento de rastreo ascendente para obtener un primer punto de rastreo ascendente de origen y un primer punto de rastreo ascendente de destino, donde el primer punto de rastreo ascendente de origen es un departamento al cual pertenece el usuario indicado por el origen del flujo de datos, o un segmento de red al cual pertenece la dirección de usuario indicada por el origen del flujo de datos, y el primer punto de rastreo ascendente de destino es un segmento de red al cual pertenece la dirección de usuario indicada por el destino del flujo de datos, un servidor correspondiente a la dirección de servidor indicado por el destino del flujo de datos, o cualquier dirección correspondiente a la dirección de red pública indicada por el destino del flujo de datos.

El módulo 130 de generación está conectado al módulo 120 de procesamiento de rastreo ascendente y está configurado para generar una primera política de seguridad, donde un origen en una condición de coincidencia de la primera política de seguridad está configurado al primer punto de rastreo ascendente de origen, un destino en la condición de coincidencia de la primera política de seguridad está configurado al primer punto de rastreo ascendente de destino y una aplicación en la condición de coincidencia de la primera política de seguridad está configurada al tipo de aplicación del flujo de datos.

Específicamente, el módulo 110 de identificación identifica el origen, el destino y el tipo de aplicación del flujo de datos, para los cuales puede hacerse referencia al paso S101 en la Realización 1. El primer módulo 120 de procesamiento de rastreo ascendente ejecuta, en base a la estructura organizativa de empresa predeterminada, el primer procesamiento de descubrimiento de punto de rastreo ascendente en el origen y en el destino del flujo de datos para obtener un punto de rastreo ascendente correspondiente al origen del flujo de datos y un punto de rastreo ascendente correspondiente al destino del flujo de datos. Para un proceso específico, se puede hacer referencia a la descripción relacionada del paso S102 en la Realización 1.

Un primer módulo 120 de procesamiento de rastreo ascendente ejecuta, en base a una estructura organizativa de empresa predeterminada, el primero procesamiento de rastreo ascendente para obtener un primer punto de rastreo ascendente de origen y un primer punto de rastreo ascendente de destino, y se genera una primera política de seguridad. De acuerdo con el aparato 10 de configuración de política de seguridad implementado por un dispositivo de control de tráfico de red, en esta realización de la presente invención, se puede generar automáticamente una política de seguridad, lo que reduce la dificultad de configuración de la política de seguridad y aumenta una tasa de éxito de configuración.

Realización 4

La FIG. 11 muestra un diagrama esquemático de una estructura de un aparato de configuración de política de seguridad implementado por un dispositivo de control de tráfico de red de acuerdo con una realización de la presente invención. Como se muestra en la FIG. 11, los componentes cuyos símbolos de referencia son los mismos que los de los componentes en la FIG. 10 tienen las mismas funciones. Para abreviar, se omiten las descripciones detalladas de estos componentes. El aparato 10 incluye además: un primer módulo 210 de determinación, un segundo módulo 220 de procesamiento de rastreo ascendente, un módulo 230 de actualización, un segundo módulo 240 de determinación y un tercer módulo 250 de procesamiento de rastreo ascendente.

El primer módulo 210 de determinación está conectado al módulo 130 de generación y está configurado para determinar si existe una segunda política de seguridad en el dispositivo de control de tráfico de red, donde una

condición de coincidencia de la segunda política de seguridad difiere de la condición de coincidencia de la primera política de seguridad solo en orígenes, y una acción de política de la segunda política de seguridad es la misma que una acción de política de la primera política de seguridad.

El segundo módulo 220 de procesamiento de rastreo ascendente está conectado al primer módulo 210 de determinación y está configurado para: cuando se determina que existe la segunda política de seguridad, ejecutar, en base a la estructura organizativa de empresa, el segundo procesamiento de rastreo ascendente para obtener un segundo punto de rastreo ascendente de origen, donde el segundo punto de rastreo ascendente de origen es un departamento de nivel superior al que pertenecen un departamento indicado por el origen de la primera política de seguridad y un departamento indicado por un origen de la segunda política de seguridad, o un segmento de red de nivel superior al que pertenecen un segmento de red indicado por el origen de la primera política de seguridad y un segmento de red indicado por un origen de la segunda política de red.

El módulo 230 de actualización está conectado al segundo módulo 220 de procesamiento de rastreo ascendente y está configurado para actualizar el origen de la primera política de seguridad al segundo punto de rastreo ascendente de origen y eliminar la segunda política de seguridad.

El segundo módulo 240 de determinación está conectado al módulo 130 de generación y está configurado para determinar si existe una tercera política de seguridad en el dispositivo de control de tráfico de red, donde una condición de coincidencia de la tercera política de seguridad difiere de la condición de coincidencia de la primera política de seguridad solo en destinos, y una acción de política de la tercera política de seguridad es la misma que la acción de política de la primera política de seguridad.

El tercer módulo 250 de procesamiento de rastreo ascendente está conectado al segundo módulo 240 de determinación y al módulo 230 de actualización, y está configurado para: cuando se determina que existe la tercera política de seguridad, ejecutar, en base a la estructura organizativa de empresa, el tercer procesamiento de rastreo ascendente para obtener un segundo punto de rastreo ascendente de destino, donde el segundo punto de rastreo ascendente de destino es un segmento de red de nivel superior al que pertenecen un segmento de red indicado por el destino de la primera política de seguridad y un segmento de red indicado por un destino de la tercera política de seguridad.

El módulo 230 de actualización está configurado, además, para actualizar el destino de la primera política de seguridad al segundo punto de rastreo ascendente de destino y eliminar la tercera política de seguridad. Específicamente, se puede hacer referencia a las descripciones relacionadas de los pasos S703 a S708 en la Realización 2 y los detalles no se describen de nuevo en el presente documento.

De acuerdo con el aparato 10 de configuración de política de seguridad para un dispositivo de control de tráfico de red, en esta realización de la presente invención, un primer módulo 210 de determinación y un segundo módulo 240 de determinación determinan si existen una segunda política de seguridad y una tercera política de seguridad en el dispositivo de control de tráfico de red, un segundo módulo 220 de procesamiento de rastreo ascendente realiza el segundo procesamiento de rastreo ascendente en una primera política de seguridad y en la segunda política de seguridad, y un tercer módulo 250 de procesamiento de rastreo ascendente realiza el tercer procesamiento de rastreo ascendente en una primera política de seguridad y en la tercera política de seguridad. De esta forma, las políticas de seguridad generadas se fusionan aún más, lo que reduce la cantidad de políticas de seguridad generadas y logra un efecto de simplificación de las políticas de seguridad en el dispositivo de control de tráfico de red.

En aún otra manera posible de implementación, el aparato 10 incluye además: un módulo 260 de generación de triplete y un módulo 270 de determinación de triplete.

El módulo 260 de generación de triplete está conectado al módulo 120 de procesamiento de rastreo ascendente y a una memoria 300, y está configurado para: enviar una instrucción a la memoria 300; después de que se ejecute el primer procesamiento de rastreo ascendente, en base a la estructura organizativa de empresa predeterminada, almacenar el primer punto de rastreo ascendente de origen, el primer punto de rastreo ascendente de destino y el tipo de aplicación del flujo de datos en la memoria 300 como una parte de información de triplete; y después de que el módulo 130 de generación genere la primera política de seguridad, eliminar la información de triplete que incluye el primer punto de rastreo ascendente de origen, el primer punto de rastreo ascendente de destino y el tipo de aplicación del flujo de datos de la memoria 300.

El módulo 270 de determinación de triplete está conectado por separado al módulo 110 de identificación, al primer módulo 120 de procesamiento de rastreo ascendente y a la memoria 300, y está configurado para: antes de que se ejecute el primer procesamiento de rastreo ascendente, en base a la estructura organizativa de empresa

predeterminada, determinar si la información de triplete que coincide con el origen, con el destino y con el tipo de aplicación del flujo de datos existe en la memoria 300. Cuando se determina que la información de triplete que coincide con el origen, con el destino y con el tipo de aplicación del flujo de datos no existe en el memoria 300, el primer módulo 120 de procesamiento de rastreo ascendente ejecuta el primer procesamiento de rastreo ascendente. Para pasos específicos, se puede hacer referencia a las descripciones detalladas del paso S701, el paso S702 y el paso S709 en la Realización 2, y los detalles no se describen de nuevo en el presente documento. De acuerdo con el aparato 10 de configuración de política de seguridad implementado por un dispositivo de control de tráfico de red, en esta realización de la presente invención, un módulo 260 de generación de triplete y un módulo 270 de determinación de triplete realizan filtrado en un flujo de datos que se está procesando, lo que previene que un flujo de datos que tiene un mismo atributo ingrese repetidamente un proceso y mejora la eficiencia de configuración de una política de seguridad.

Realización 5

La FIG. 12 muestra un diagrama esquemático de una estructura de un dispositivo de control de tráfico de red de acuerdo con una realización de la presente invención. Un aparato 1100 de configuración de política de seguridad en el dispositivo de control de tráfico de red puede ser un servidor host que tiene una capacidad informática, una computadora personal (PC), una computadora o terminal portátil, o similares. La implementación específica de un nodo informático no está limitada en una realización específica de la presente invención.

El aparato 1100 de configuración de política de seguridad en el dispositivo de control de tráfico de red incluye un procesador (processor) 1110, una interfaz 1120 de comunicaciones (Communications Interface), una memoria (memory) 1130 y un bus 1140. El procesador 1110, la interfaz 1120 de comunicaciones y la memoria 1130 se comunican entre sí utilizando el bus 1140.

La interfaz 1120 de comunicaciones está configurada para comunicarse con un dispositivo de red, donde el dispositivo de red incluye, por ejemplo, un centro de gestión de máquina virtual y un dispositivo de almacenamiento compartido. En esta realización, la interfaz 1120 de comunicaciones está configurada para adquirir un flujo de datos.

El procesador 1110 está configurado para leer y ejecutar código de programa almacenado en la memoria 1130. El procesador 1110 puede ser una unidad central de procesamiento CPU o un circuito integrado de aplicación específica ASIC (Application Specific Integrated Circuit), o puede estar configurado como uno o más circuitos integrados para implementar las realizaciones de la presente invención.

La memoria 1130 está configurada para almacenar el código de programa. La memoria 1130 puede incluir una memoria RAM de alta velocidad y también puede incluir una memoria no volátil (non-volatile memory), por ejemplo, al menos una memoria de disco. La memoria 1130 también puede ser una matriz de memoria. La memoria 1130 se puede dividir en bloques y los bloques se pueden combinar en un volumen virtual de acuerdo con una regla.

En una manera posible de implementación, el código de programa anterior puede ser código de programa que incluye una instrucción de operación de computadora. El código de programa se puede utilizar específicamente para:

identificar un origen, un destino y un tipo de aplicación de un flujo de datos de entrada utilizando la interfaz 1120 de comunicaciones, donde el origen indica un usuario que envía el flujo de datos o una dirección de usuario desde la cual se envía el flujo de datos, el destino del flujo de datos indica una dirección de usuario, una dirección de servidor o una dirección de red pública en la cual se recibe el flujo de datos, y el tipo de aplicación indica qué tipo de aplicación cuyos datos están incluidos en el flujo de datos;

ejecutar, en base a una estructura organizativa de empresa predeterminada, el primer procesamiento de rastreo ascendente para obtener un primer punto de rastreo ascendente de origen y un primer punto de rastreo ascendente de destino, donde el primer punto de rastreo ascendente de origen es un departamento al cual pertenece el usuario indicado por el origen del flujo de datos, o un segmento de red al cual pertenece la dirección de usuario indicada por el origen del flujo de datos, y el primer punto de rastreo ascendente de destino es un segmento de red al cual pertenece la dirección de usuario indicada por el destino del flujo de datos, un servidor correspondiente a la dirección de servidor indicada por el destino del flujo de datos, o cualquier dirección correspondiente a la dirección de red pública indicada por el destino del flujo de datos; y

generar una primera política de seguridad, donde un origen en una condición de coincidencia de la primera política de seguridad está configurado al primer punto de rastreo ascendente de origen, un destino en la condición de coincidencia de la primera política de seguridad está configurado al primer punto de rastreo ascendente de destino y una aplicación en la condición de coincidencia de la primera política de seguridad está configurada al tipo de aplicación del flujo de datos.

En una manera posible de implementación, después de la generación de una primera política de seguridad, el código de programa se utiliza además para:

determinar si existe una segunda política de seguridad en el dispositivo de control de tráfico de red, donde una condición de coincidencia de la segunda política de seguridad difiere de la condición de coincidencia de la primera política de seguridad solo en orígenes, y una acción de política de la segunda política de seguridad es la misma que una acción de política de la primera política de seguridad;

cuando se determina que existe la segunda política de seguridad, ejecutar, en base a la estructura organizativa de empresa, el segundo procesamiento de rastreo ascendente para obtener un segundo punto de rastreo ascendente de origen, donde el segundo punto ascendente de origen es un departamento de nivel superior al que pertenecen un departamento indicado por el origen de la primera política de seguridad y un departamento indicado por un origen de la segunda política de seguridad, o un segmento de red de nivel superior al que pertenecen un segmento de red indicado por el origen de la primera política de seguridad y un segmento de red indicado por un origen de la segunda política de seguridad; y

actualizar el origen de la primera política de seguridad al segundo punto de rastreo ascendente de origen y eliminar la segunda política de seguridad.

En una manera posible de implementación, después de la generación de una primera política de seguridad, el código de programa se utiliza además para:

determinar si existe una tercera política de seguridad en el dispositivo de control de tráfico de red, donde una condición de coincidencia de la tercera política de seguridad difiere de la condición de coincidencia de la primera política de seguridad solo en destinos, y una acción de política de la tercera política de seguridad es la misma que la acción de política de la primera política de seguridad;

cuando se determina que existe la tercera política de seguridad, ejecutar, en base a la estructura organizativa de empresa, el tercer procesamiento de rastreo ascendente para obtener un segundo punto de rastreo ascendente de destino, donde el segundo punto de rastreo ascendente de destino es un segmento de red de nivel superior al que pertenecen un segmento de red indicado por el destino de la primera política de seguridad y un segmento de red indicado por un destino de la tercera política de seguridad; y

actualizar el destino de la primera política de seguridad al segundo punto de rastreo ascendente de destino y eliminar la tercera política de seguridad.

En una manera posible de implementación, después de la ejecución, en base a una estructura organizativa de empresa predeterminada, del primer procesamiento de rastreo ascendente, el código de programa se utiliza además para: almacenar el primer punto de rastreo ascendente de origen, el primer punto de rastreo ascendente de destino y el tipo de aplicación del flujo de datos en la memoria como una parte de la información de triplete;

después de la generación de una primera política de seguridad, el código de programa se utiliza además para: eliminar la información de triplete que incluye el primer punto de rastreo ascendente de origen, el primer punto de rastreo ascendente de destino y el tipo de aplicación del flujo de datos de la memoria; y

antes de la ejecución, en base a una estructura organizativa de empresa predeterminada, del primer procesamiento de rastreo ascendente para obtener un primer punto de rastreo ascendente de origen y un primer punto de rastreo ascendente de destino, el código de programa se utiliza además para: determinar si la información de triplete que coincide con el origen, con el destino y con el tipo de aplicación del flujo de datos existe en la memoria; y

cuando se determina que la información de triplete que coincide con el origen, con el destino y con el tipo de aplicación del flujo de datos no existe en la memoria, ejecutar el primer procesamiento de rastreo ascendente.

Una persona con experiencia ordinaria en la técnica puede estar al tanto de que las unidades ejemplares y los pasos de algoritmo en las realizaciones descritas en esta memoria descriptiva pueden implementarse mediante hardware electrónico o una combinación de software informático y hardware electrónico. Si las funciones se implementan mediante hardware o software depende de las aplicaciones particulares y las condiciones de restricción de diseño de las soluciones técnicas. Una persona experta en la técnica puede seleccionar diferentes métodos para implementar las funciones descritas para una aplicación particular, pero no se debe considerar que la implementación va más allá del alcance de la presente invención.

Si las funciones se implementan en una forma de software informático y se venden o utilizan como un producto independiente, se puede considerar hasta cierto punto que todas o algunas de las soluciones técnicas de la presente invención, por ejemplo, la parte que contribuye a la técnica anterior, se implementan en forma de un producto de software informático. El producto de software informático generalmente se almacena en un medio de almacenamiento no volátil legible por computadora e incluye varias instrucciones para instruir a un dispositivo informático, que puede ser una computadora personal, un servidor, un dispositivo de red o similares, para realizar todos o una parte de los pasos de los métodos descritos en las realizaciones de la presente invención. El medio de almacenamiento anterior incluye cualquier medio que pueda almacenar código de programa, como una unidad flash

USB, un disco duro extraíble, una memoria de solo lectura (ROM, Read-Only Memory), una memoria de acceso aleatorio (RAM, Random Access Memory), un disco magnético o un disco óptico.

Las descripciones anteriores son meramente maneras de implementación específicas de la presente invención, pero no están destinadas a limitar el alcance de protección de la presente invención. Cualquier variación o reemplazo que el experto en la técnica descubra fácilmente dentro del alcance técnico dado a conocer en la presente invención, deberá caer dentro del alcance de protección de la presente invención. Por lo tanto, el alcance de protección de la presente invención estará sujeto al alcance de protección de las reivindicaciones.

REIVINDICACIONES

1. Un método de configuración de política de seguridad implementado por un dispositivo de control de tráfico de red, que comprende:

identificar (S101) un origen, un destino y un tipo de aplicación de un flujo de datos de entrada, en donde el origen indica un usuario que envía el flujo de datos o una dirección de usuario desde la cual se envía el flujo de datos, el destino del flujo de datos indica una dirección de usuario, una dirección de servidor o una dirección de red pública en la cual se recibe el flujo de datos, y el tipo de aplicación indica qué tipo de aplicación cuyos datos están comprendidos en el flujo de datos;

si el flujo de datos no coincide con una política existente, hacer coincidir el flujo de datos con una política de permitir cualquiera que permita el acceso de todos los usuarios;

ejecutar (S102), en base a una estructura organizativa de empresa predeterminada, el primer procesamiento de rastreo ascendente para obtener un primer punto de rastreo ascendente de origen y un primer punto de rastreo ascendente de destino cuando el flujo de datos coincide con la política de permitir cualquiera, en donde el primer punto de rastreo ascendente de origen es un departamento al cual pertenece el usuario indicado por el origen cuando el origen indica un usuario, el primer punto de rastreo ascendente de origen es un primer segmento de red al cual pertenece la dirección de usuario indicada por el origen del flujo de datos cuando el origen indica una dirección de usuario desde la cual se envía el flujo de datos, el primer segmento de red comprende múltiples direcciones IP (Protocolo de Internet), y

el primer punto de rastreo ascendente de destino se establece en cualquier dirección cuando el destino indica una dirección de red pública, el primer punto de rastreo ascendente de destino se establece en un servidor cuando el destino indica una dirección de servidor; el primer punto de rastreo ascendente de destino es un segundo segmento de red al cual pertenece la dirección de usuario en la cual se recibe el flujo de datos cuando el destino indica una dirección de usuario en la cual se recibe el flujo de datos, el segundo segmento de red comprende múltiples direcciones IP; y

generar (S103) una primera política de seguridad, en donde un origen en una condición de coincidencia de la primera política de seguridad se configura al primer punto de rastreo ascendente de origen, un destino en la condición de coincidencia de la primera política de seguridad se configura al primer punto de rastreo ascendente de destino, y una aplicación en la condición de coincidencia de la primera política de seguridad se configura al tipo de aplicación del flujo de datos, la primera política de seguridad se utiliza para coincidir con un flujo de datos posterior.

2. El método de configuración de política de seguridad de acuerdo con la reivindicación 1, después de la generación de una primera política de seguridad, comprende además:

determinar (S703) si existe una segunda política de seguridad en el dispositivo de control de tráfico de red, en donde una condición de coincidencia de la segunda política de seguridad difiere de la condición de coincidencia de la primera política de seguridad solo en orígenes, y una acción de política de la segunda política de seguridad es la misma que una acción de política de la primera política de seguridad;

cuando se determina que existe la segunda política de seguridad, ejecutar (S704), en base a la estructura organizativa de empresa, el segundo procesamiento de rastreo ascendente para obtener un segundo punto de rastreo ascendente de origen, en donde el segundo punto ascendente de origen es un departamento de nivel superior al que pertenecen un departamento indicado por el origen de la primera política de seguridad y un departamento indicado por un origen de la segunda política de seguridad, o un segmento de red de nivel superior al que pertenecen un segmento de red indicado por el origen de la primera política de seguridad y un segmento de red indicado por un origen de la segunda política de seguridad; y

actualizar (S705) el origen de la primera política de seguridad al segundo punto de rastreo ascendente de origen y eliminar la segunda política de seguridad.

3. El método de configuración de política de seguridad de acuerdo con la reivindicación 1 o 2, después de la generación de una primera política de seguridad, comprende además

determinar (S706) si existe una tercera política de seguridad en el dispositivo de control de tráfico de red, donde una condición de coincidencia de la tercera política de seguridad difiere de la condición de coincidencia de la primera política de seguridad solo en destinos, y una acción de política de la tercera política de seguridad es la misma que la acción de política de la primera política de seguridad;

cuando se determina que existe la tercera política de seguridad, ejecutar (S707), en base a la estructura organizativa de empresa, el tercer procesamiento de rastreo ascendente para obtener un segundo punto de rastreo ascendente de destino, en donde el segundo punto de rastreo ascendente de destino es un segmento de red de nivel superior a la que pertenece un segmento de red indicado por el destino de la primera política de seguridad y un segmento de red indicado por un destino de la tercera política de seguridad; y

actualizar (S708) el destino de la primera política de seguridad al segundo punto de rastreo ascendente de destino y eliminar la tercera política de seguridad.

4. El método de configuración de política de seguridad de acuerdo con una cualquiera de las reivindicaciones 1 a 3, en donde:

después de la ejecución, en base a una estructura organizativa de empresa predeterminada, del primer procesamiento de rastreo ascendente, el método comprende además: almacenar (S702) el primer punto de rastreo ascendente de origen, el primer punto de rastreo ascendente de destino y el tipo de aplicación del flujo de datos en una memoria del dispositivo de control de tráfico de red como una parte de la información de triplete;

después de la generación de una primera política de seguridad, el método comprende además: eliminar la información de triplete que comprende el primer punto de rastreo ascendente de origen, el primer punto de rastreo ascendente de destino y el tipo de aplicación del flujo de datos de la memoria; y

antes de la ejecución, en base a una estructura organizativa de empresa predeterminada, del primer procesamiento de rastreo ascendente para obtener un primer punto de rastreo ascendente de origen y un primer punto de rastreo ascendente de destino, el método comprende además: determinar (S701) si la información de triplete que coincide con el origen, con el destino y con el tipo de aplicación del flujo de datos existe en la memoria; y

cuando se determina que la información de triplete que coincide con el origen, con el destino y con el tipo de aplicación del flujo de datos no existe en la memoria, ejecutar el primer procesamiento de rastreo ascendente (S102).

5. Un aparato (10) de configuración de política de seguridad implementado por un dispositivo de control de tráfico de red, que comprende:

un módulo (110) de identificación, configurado para identificar un origen, un destino y un tipo de aplicación de un flujo de datos de entrada, en donde el origen indica un usuario que envía el flujo de datos o una dirección de usuario desde la cual se envía el flujo de datos, el destino del flujo de datos indica una dirección de usuario, una dirección de servidor o una dirección de red pública en la cual se recibe el flujo de datos, y el tipo de aplicación indica qué tipo de aplicación cuyos datos están comprendidos en el flujo de datos;

un primer módulo (120) de procesamiento de rastreo ascendente, conectado al módulo (110) de identificación y configurado para hacer coincidir el flujo de datos con una política de permitir cualquiera que permita el acceso de todos los usuarios cuando el flujo de datos no coincida con una política existente; ejecutar, en base a una estructura organizativa de empresa predeterminada, el primer procesamiento de rastreo ascendente para obtener un primer punto de rastreo ascendente de origen y un primer punto de rastreo ascendente de destino cuando el flujo de datos coincide con la política de permitir cualquiera, en donde el primer punto de rastreo ascendente de origen es un departamento al cual pertenece el usuario indicado por el origen cuando el origen indica un usuario, el primer punto ascendente de origen es un primer segmento de red al cual pertenece la dirección de usuario indicada por el origen del flujo de datos cuando el origen indica una dirección de usuario desde la cual se envía el flujo de datos, el primer segmento de red comprende múltiples direcciones IP (Protocolo de Internet), y

el primer punto de rastreo ascendente se establece en cualquier dirección cuando el destino indica una dirección de red pública, el primer punto de rastreo ascendente se establece en un servidor cuando el destino indica una dirección de servidor, el primer punto de rastreo ascendente es un segundo segmento de red a la que pertenece la dirección de usuario en la cual se recibe el flujo de datos cuando el destino indica una dirección de usuario en la cual se recibe el flujo de datos, el segundo segmento de red comprende múltiples direcciones IP; y

un módulo (130) de generación, conectado al primer módulo (120) de procesamiento de rastreo ascendente y configurado para generar una primera política de seguridad, en donde un origen en una condición de coincidencia de la primera política de seguridad está configurado al primer punto de rastreo ascendente de origen, un destino en la condición de coincidencia de la primera política de seguridad está configurado al primer punto de rastreo ascendente de destino y una aplicación en la condición de coincidencia de la primera política de seguridad está configurada al tipo de aplicación del flujo de datos, la primera política de seguridad se utiliza para hacer coincidir con un flujo de datos posterior.

6. Aparato de configuración de política de seguridad de acuerdo con la reivindicación 5, que comprende además:

un primer módulo (210) de determinación conectado al módulo (130) de generación y configurado para determinar si existe una segunda política de seguridad en el dispositivo de control de tráfico de red, en donde una condición de coincidencia de la segunda política de seguridad difiere de la condición de coincidencia de la primera política de seguridad solo en orígenes, y una acción de política de la segunda política de seguridad es la misma que una acción de política de la primera política de seguridad;

un segundo módulo (220) de procesamiento de rastreo ascendente conectado al primer módulo (210) de determinación y configurado para: cuando se determina que existe la segunda política de seguridad, ejecutar, en base a la estructura organizativa de empresa, el segundo procesamiento de rastreo ascendente para obtener un segundo punto de rastreo ascendente de origen, en donde el segundo punto de rastreo ascendente de origen es un departamento de nivel superior al que pertenecen un departamento indicado por el origen de la primera política de seguridad y un departamento indicado por un origen de la segunda política de seguridad, o un segmento de red de nivel superior al que pertenecen un segmento de red indicado por el origen de la primera política de seguridad y un segmento de red indicado por un origen de la segunda política de red; y

un módulo (230) de actualización conectado al segundo módulo (220) de procesamiento de rastreo ascendente y configurado para actualizar el origen de la primera política de seguridad al segundo punto de rastreo ascendente de origen y eliminar la segunda política de seguridad.

7. El aparato de configuración de política de seguridad de acuerdo con la reivindicación 5 o 6, que comprende además:

un segundo módulo (240) de determinación conectado al módulo (130) de generación y configurado para determinar si existe una tercera política de seguridad en el dispositivo de control de tráfico de red, en donde una condición de coincidencia de la tercera política de seguridad difiere de la condición de coincidencia de la primera política de seguridad solo en destinos, y una acción de política de la tercera política de seguridad es la misma que la acción de política de la primera política de seguridad; y

un tercer módulo (250) de procesamiento de rastreo ascendente conectado al segundo módulo (240) de determinación y al módulo (230) de actualización, y configurado para: cuando se determina que existe la tercera política de seguridad, ejecutar, en base a la estructura organizativa de empresa, el tercer procesamiento de rastreo ascendente para obtener un segundo punto de rastreo ascendente de destino, en donde el segundo punto de rastreo ascendente de destino es un segmento de red de nivel superior al que pertenecen un segmento de red indicado por el destino de la primera política de seguridad y un segmento de red indicado por un destino de la tercera política de seguridad, en donde

el módulo (230) de actualización está configurado además para actualizar el destino de la primera política de seguridad al segundo punto de rastreo ascendente de destino y eliminar la tercera política de seguridad.

8. El aparato de configuración de política de seguridad de acuerdo con una cualquiera de las reivindicaciones 5 a 7, que comprende además:

un módulo (260) de generación de triplete conectado al primer módulo (120) de procesamiento de rastreo ascendente y a una memoria (300) del aparato de configuración de políticas de seguridad, y configurado para: enviar una instrucción a la memoria; después de ejecutarse el primer procesamiento de rastreo ascendente, en base a la estructura organizativa de empresa predeterminada, almacenar el primer punto de rastreo ascendente de origen, el primer punto de rastreo ascendente de destino y el tipo de aplicación del flujo de datos en la memoria (300) como una parte de la información de triplete; y, después de generarse la primera política de seguridad, eliminar la información de triplete que comprende el primer punto de rastreo ascendente de origen, el primer punto de rastreo ascendente de destino y el tipo de aplicación del flujo de datos de la memoria (300); y

un módulo (270) de determinación de triplete conectado al módulo (110) de identificación, al primer módulo (120) de procesamiento de rastreo ascendente y a la memoria (300), y configurado para: antes de ejecutarse el primer procesamiento de rastreo ascendente, en base a la estructura organizativa de empresa predeterminada, para obtener el primer punto de rastreo ascendente de origen y el primer punto de rastreo ascendente de destino, determinar si la información de triplete que coincida con el origen, con el destino y con el tipo de aplicación del flujo de datos existe en la memoria, en donde, cuando se determina que la información de triplete que coincide con el origen, con el destino y con el tipo de aplicación del flujo de datos no existe en la memoria, se ejecuta el primer procesamiento de rastreo ascendente.

9. Un dispositivo de control de tráfico de red, que comprende una memoria (1130), una interfaz (1120) de comunicaciones y un procesador (1110), en donde

la memoria (1130) está configurada para almacenar código de programa; y

el procesador (1110) lee el código de programa almacenado en la memoria (1130) y ejecuta las siguientes operaciones:

identificar un origen, un destino y un tipo de aplicación de un flujo de datos obtenido utilizando la interfaz de comunicaciones, en donde el origen indica un usuario que envía el flujo de datos o una dirección de usuario desde la cual se envía el flujo de datos, el destino del flujo de datos indica una dirección de usuario, una dirección de servidor o una dirección de red pública en la cual se recibe el flujo de datos, y el tipo de aplicación indica qué tipo de aplicación cuyos datos están comprendidos en el flujo de datos;

si el flujo de datos no coincide con una política existente, hacer coincidir el flujo de datos con una política de permitir cualquiera que permita el acceso de todos los usuarios;

ejecutar, en base a una estructura organizativa de empresa predeterminada, el primer procesamiento de rastreo ascendente para obtener un primer punto de rastreo ascendente de origen y un primer punto de rastreo ascendente de destino cuando el flujo de datos coincide con la política de permitir cualquiera, en donde el primer punto de rastreo ascendente de origen es un departamento al cual pertenece el usuario indicado por el origen cuando el origen indica un usuario, el primer punto de rastreo ascendente de origen es un primer segmento de red al cual pertenece la dirección de usuario indicada por el origen del flujo de datos cuando el origen indica una dirección de usuario desde la cual se envía el flujo de datos, el primer segmento de red comprende múltiples direcciones IP (Protocolo de Internet), y

el primer punto de rastreo ascendente de destino se establece en cualquier dirección cuando el destino indica una dirección de red pública; el primer punto de rastreo ascendente de destino se establece en un servidor

cuando el destino indica una dirección de servidor; el primer punto de rastreo ascendente de destino es un segundo segmento de red al cual pertenece la dirección de usuario en la cual se recibe el flujo de datos cuando el destino indica una dirección de usuario en la cual se recibe el flujo de datos, el segundo segmento de red comprende múltiples direcciones IP; y

generar una primera política de seguridad, en donde un origen en una condición de coincidencia de la primera política de seguridad se configura al primer punto de rastreo ascendente de origen, un destino en la condición de coincidencia de la primera política de seguridad se configura al primer punto de rastreo ascendente de destino y una aplicación en la condición de coincidencia de la primera política de seguridad se configura al tipo de aplicación del flujo de datos, la primera política de seguridad se utiliza para coincidir con un flujo de datos posterior.

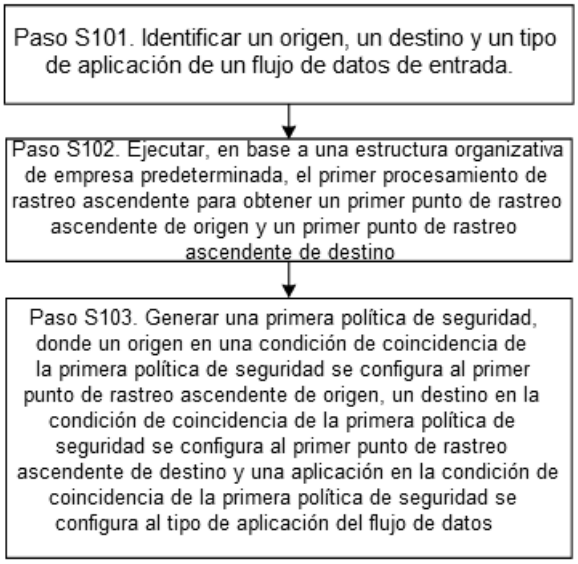
Paso S101. Identificar un origen, un destino y un tipo de aplicación de un flujo de datos de entrada.
Paso S102. Ejecutar, en base a una estructura organizativa de empresa predeterminada, el primer procesamiento de rastreo ascendente para obtener un primer punto de rastreo ascendente de origen y un primer punto de rastreo ascendente de destino
Paso S103. Generar una primera política de seguridad, donde un origen en una condición de coincidencia de la primera política de seguridad se configura al primer punto de rastreo ascendente de origen, un destino en la condición de coincidencia de la primera política de seguridad se configura al primer punto de rastreo ascendente de destino y una aplicación en la condición de coincidencia de la primera política de seguridad se configura al tipo de aplicación del flujo de datos

FIG. 1

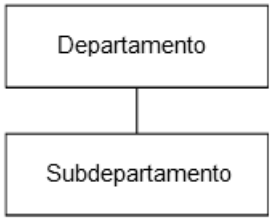
Departamento
Subdepartamento

FIG. 2

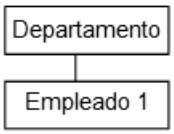

FIG. 3

FIG. 4

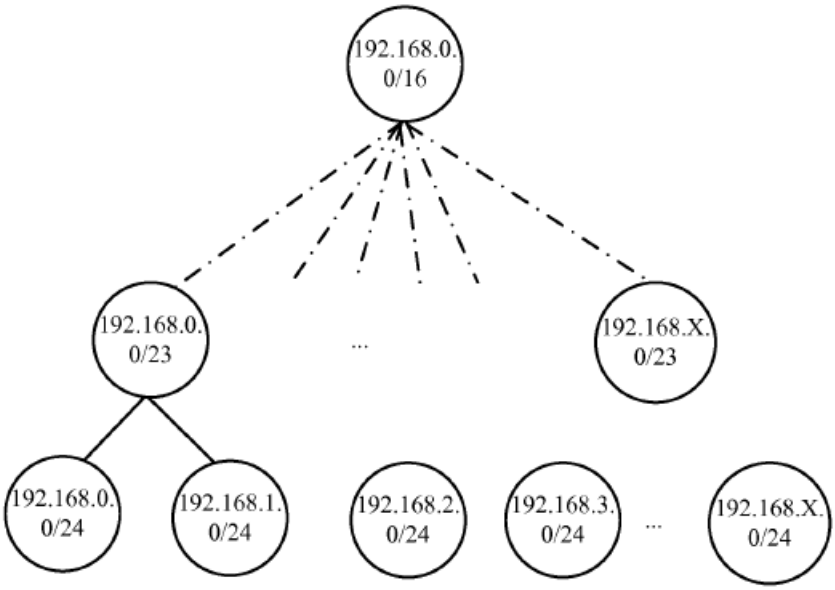

FIG. 5

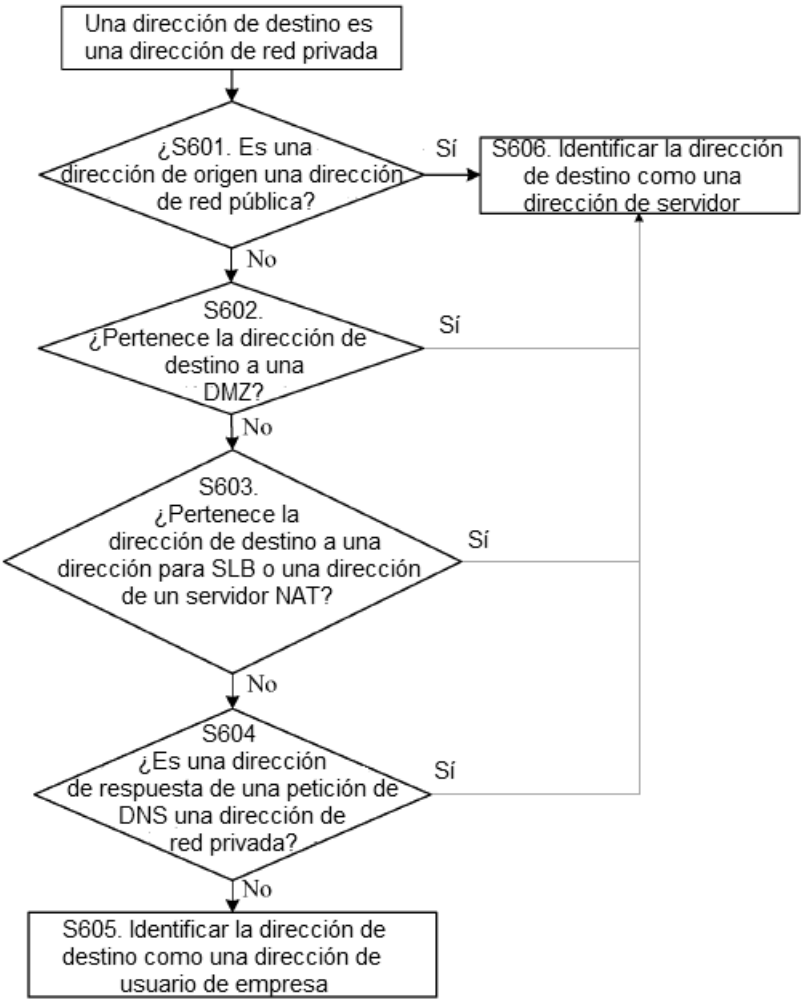
Una dirección de destino es una dirección de red privada
¿S601. Es una dirección de origen una dirección de red pública?
Sí
S606. Identificar la dirección de destino como una dirección de servidor
No
S602. ¿Pertenece la dirección de destino a una DMZ?
Sí
No
S603. ¿Pertenece la dirección de destino a una dirección para SLB o una dirección de un servidor NAT?
Sí
No
S604 ¿Es una dirección de respuesta de una petición de DNS una dirección de red privada?
Sí
No
S605. Identificar la dirección de destino como una dirección de usuario de empresa

FIG. 6

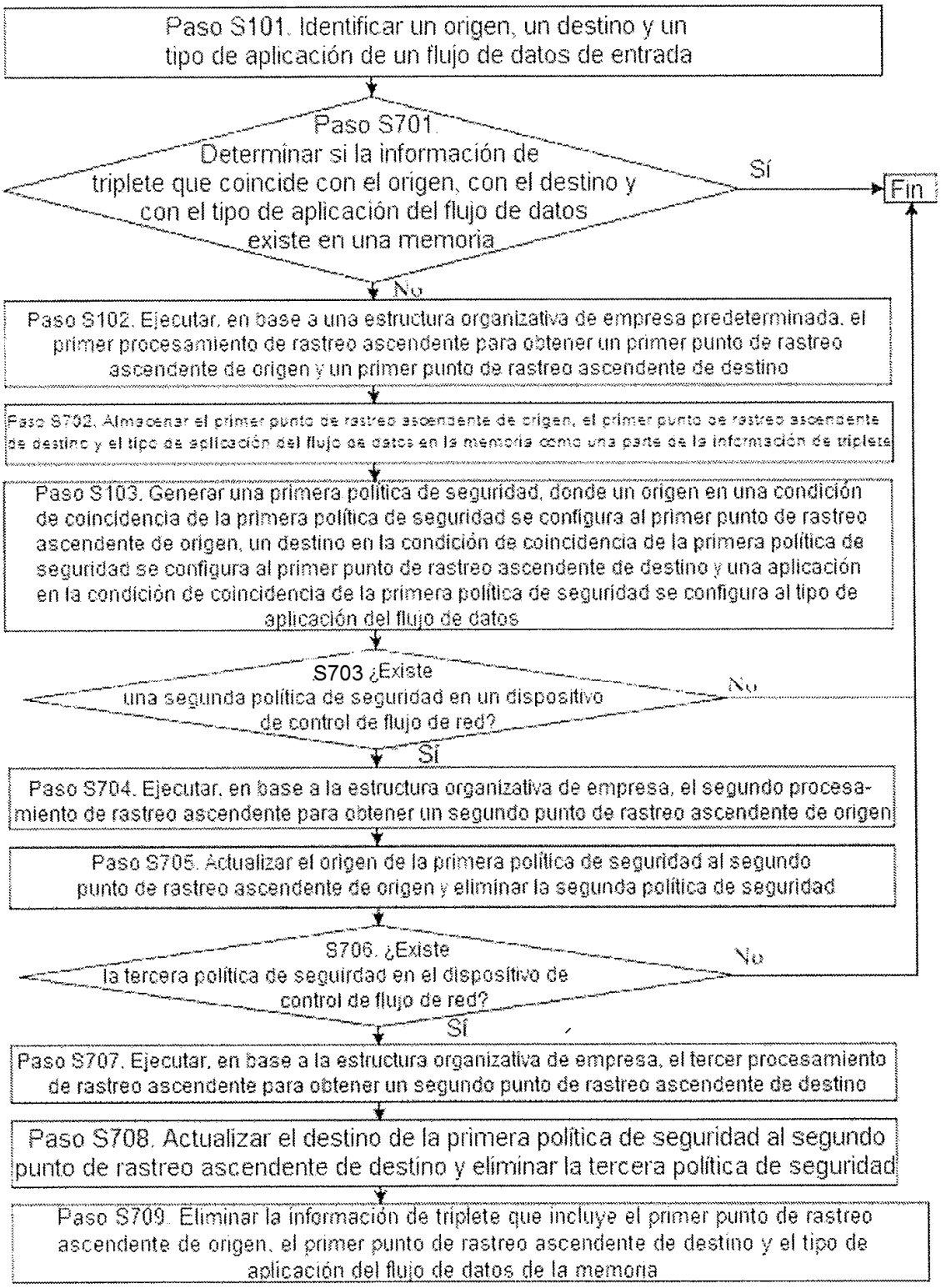
Paso S101. Identificar un origen, un destino y un tipo de aplicación de un flujo de datos de entrada
Paso S701. Determinar si la información de triplete que coincide con el origen, con el destino y con el tipo de aplicación del flujo de datos existe en una memoria
Sí
Fin
No
Paso S102. Ejecutar, en base a una estructura organizativa de empresa predeterminada, el primer procesamiento de rastreo ascendente para obtener un primer punto de rastreo ascendente de origen y un primer punto de rastreo ascendente de destino
Paso S702. Almacenar el primer punto de rastreo ascendente de origen, el primer punto de rastreo ascendente de destino y el tipo de aplicación del flujo de datos en la memoria como una parte de la información de triplete
Paso S103. Generar una primera política de seguridad, donde un origen en una condición de coincidencia de la primera política de seguridad se configura al primer punto de rastreo ascendente de origen, un destino en la condición de coincidencia de la primera política de seguridad se configura al primer punto de rastreo ascendente de destino y una aplicación en la condición de coincidencia de la primera política de seguridad se configura al tipo de aplicación del flujo de datos
S703 ¿Existe una segunda política de seguridad en un dispositivo de control de flujo de red?
No
Sí
Paso S704. Ejecutar, en base a la estructura organizativa de empresa, el segundo procesamiento de rastreo ascendente para obtener un segundo punto de rastreo ascendente de origen
Paso S705. Actualizar el origen de la primera política de seguridad al segundo punto de rastreo ascendente de origen y eliminar la segunda política de seguridad
S706. ¿Existe la tercera política de seguirdad en el dispositivo de control de flujo de red?
No
Sí
Paso S707. Ejecutar, en base a la estructura organizativa de empresa, el tercer procesamiento de rastreo ascendente para obtener un segundo punto de rastreo ascendente de destino
Paso S708. Actualizar el destino de la primera política de seguridad al segundo punto de rastreo ascendente de destino y eliminar la tercera política de seguridad
Paso S709. Eliminar la información de triplete que incluye el primer punto de rastreo ascendente de origen, el primer punto de rastreo ascendente de destino y el tipo de aplicación del flujo de datos de la memoria

FIG. 7

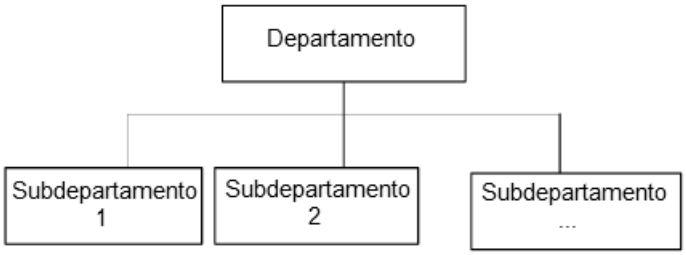

FIG. 8

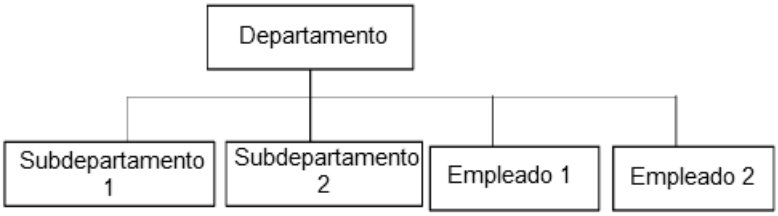

FIG. 9a

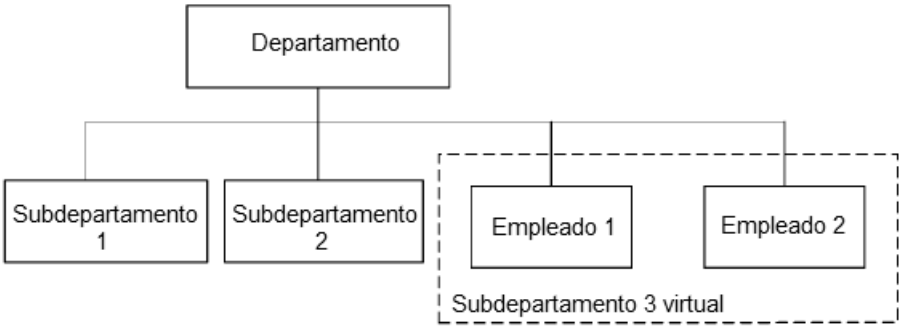

FIG. 9b


Aparato 10 de configuración de política de seguridad implementado por un dispositivo de control de tráfico de red
Módulo de identificación 110
Primer módulo 120 de procesamiento de rastreo ascendente
Módulo 130 de generación

FIG. 10

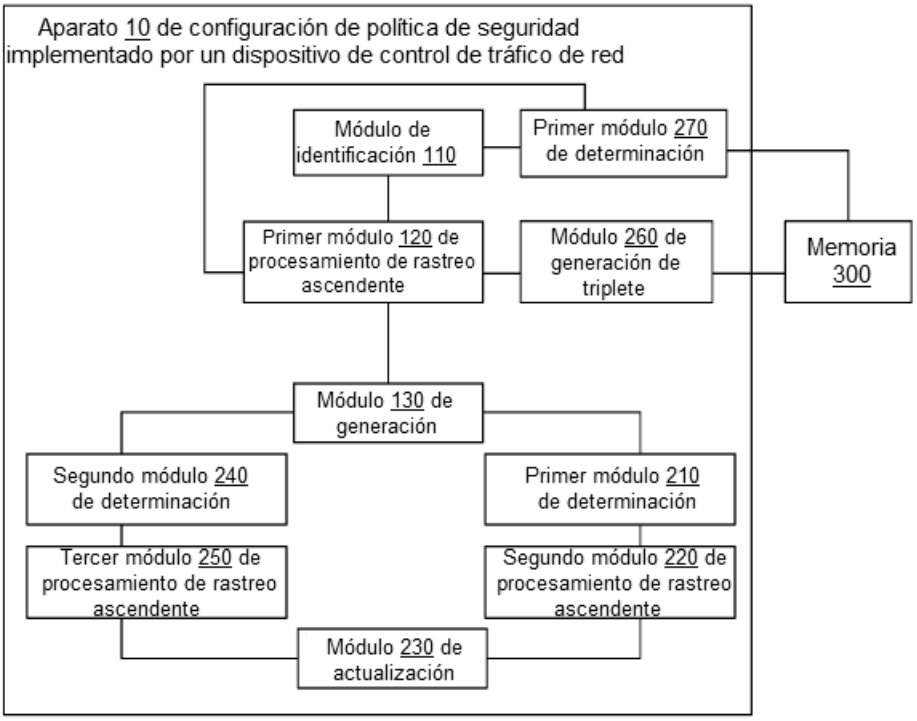
Aparato 10 de configuración de política de seguridad implementado por un dispositivo de control de tráfico de red
Módulo de identificación 110
Primer módulo 270 de determinación
Primer módulo 120 de procesamiento de rastreo ascendente
Módulo 260 de generación de triplete
Memoria 300
Módulo 130 de generación
Segundo módulo 240 de determinación
Primer módulo 210 de determinación
Tercer módulo 250 de procesamiento de rastreo ascendente
Segundo módulo 220 de procesamiento de rastreo ascendente
Módulo 230 de actualización

FIG. 11

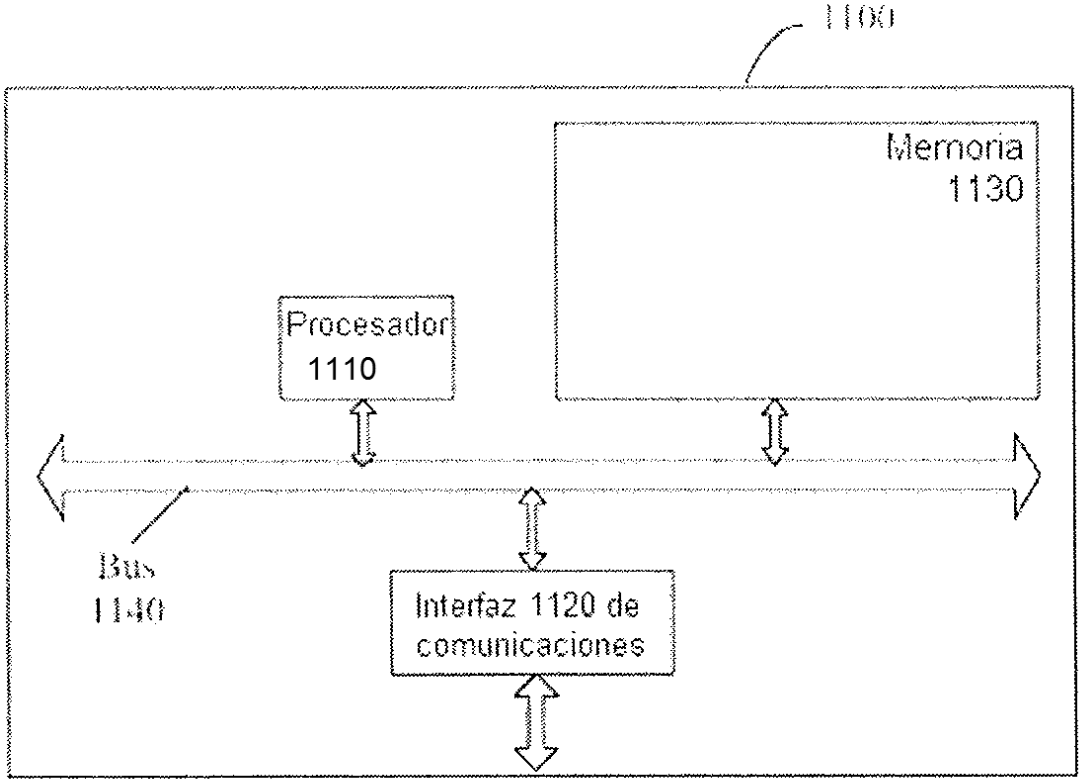
1100
Memoria
1130
Procesador
1110
Bus
1140
Interfaz 1120 de
comunicaciones

FIG. 12