(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 627 755**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 12/715 (2013.01)
H04L 12/721 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **08.12.2014 E 14196841 (2)**

(97) Fecha y número de publicación de la concesión europea: **22.03.2017 EP 2882162**

(54) Título: **Método y equipo de procesamiento de seguridad de flujos de datos**

(30) Prioridad:

09.12.2013 CN 201310661766

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
31.07.2017

(73) Titular/es:

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

(72) Inventor/es:

WANG, DONGHUI y
LI, JINMING

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método y equipo de procesamiento de seguridad de flujos de datos

Campo técnico

Los modos de realización de la presente invención están relacionados con las tecnologías de las comunicaciones y, en particular, con un método y un equipo de procesamiento de seguridad de flujos de datos.

Antecedentes

Una red definida mediante software (software defined network, SDN para abreviar) es una arquitectura de red emergente en la que se separa el control y el reenvío. Los dos principales dispositivos en la tecnología SDN son un controlador central (que también se denomina controlador) y un dispositivo de red.

Basándose en la tecnología SDN, en un método de procesamiento de seguridad de flujos de datos, un flujo de datos pasa en primer lugar a través de un módulo software dentro del controlador para someterse a una detección de seguridad y, a continuación, el controlador transmite una ruta de reenvío que pasa únicamente por el dispositivo de reenvío, esto es el controlador transmite información que indica una ruta de reenvío que pasa únicamente por un dispositivo de reenvío.

En el método de procesamiento de seguridad de flujos de datos existente anterior, el rendimiento de seguridad de la detección de seguridad realizada por el módulo software no es bueno. Además, el controlador no sólo necesita determinar una ruta de transmisión para el flujo de datos, sino que también necesita realizar una detección de seguridad sobre el flujo de datos. Como resultado, la carga del controlador es alta.

El documento "A software-defined networking for inline service chaining (Una red definida por software para enlazar servicios en línea)" de Ying Zhang y otros, Conferencia Internacional del IEEE sobre Protocolos de Red (ICNP), 7 de octubre de 2013, divulga operadores de red enfrentados al reto de desplegar y gestionar bloques intermedios (también denominados servicios en línea) como, por ejemplo, cortafuegos dentro de su acceso de banda ancha, centro de datos o redes de empresa. Debido a la ausencia de protocolos disponibles para encaminar tráfico mediante bloques intermedios, los operadores siguen dependiendo de configuraciones de bajo nivel propensas a errores y complejas para forzar el tráfico a través del conjunto deseado de bloques intermedios. Escrito teniendo en cuenta la arquitectura de red definida por software (SDN) y el protocolo OpenFlow actuales, este artículo propone StEERING, abreviatura de SDN inlinE sERvices and forwardING (servicios en línea SDN y reenvío). Es un marco escalable para encaminar tráfico de forma dinámica mediante cualquier secuencia de bloques intermedios. Con una configuración centralizada simple, StEERING puede guiar explícitamente diferentes tipos de flujos a través del conjunto de bloques intermedios deseados, subiendo al nivel de políticas por abonado y por aplicación. Con su capacidad de soportar encaminamiento flexible, proponemos además un algoritmo para seleccionar las mejores localizaciones para situar servicios, de modo que se optimiza el rendimiento.

El documento WO 2006029399 A2 divulga un método de y un sistema que monitoriza un recurso de red de una red y el rendimiento de una aplicación. El método clasifica un primer subconjunto de tráfico de red en las categorías de confianza, conocido como malo y sospechoso. El método determina una acción para un segundo subconjunto de tráfico basado en la clasificación. Algunos modos de realización proporcionan un sistema para una conexión adaptativa con un primer dispositivo y tráfico que tiene un primer subconjunto y un segundo subconjunto. El sistema también incluye un primer recurso y un segundo recurso para la transmisión del tráfico. El primer dispositivo recibe el tráfico y clasifica el tráfico en el primer y segundo subconjuntos. El primer dispositivo asigna le primer subconjunto al primer recurso. Algunos modos de realización proporcionan un módulo de clasificación que clasifica el tráfico de entrada, y un módulo de asignación de recursos que asigna el tráfico clasificado a un recurso concreto. Una categoría de tráfico para el dispositivo incluye el tráfico sospechoso.

Resumen

Los modos de realización de la presente invención proporcionan un método y un equipo de procesamiento de seguridad de flujos de datos, con el fin de resolver un problema en la técnica anterior de que el rendimiento de seguridad de la detección de seguridad realizada por un módulo de software no es bueno y la carga es relativamente alta.

Un primer aspecto de la invención proporciona un método de procesamiento de seguridad de los flujos de datos de acuerdo con la reivindicación 1. Un segundo aspecto de la invención proporciona un equipo de procesamiento de seguridad de flujos de datos de acuerdo con la reivindicación 5. Los modos de realización preferidos de la invención se definen en las reivindicaciones dependientes.

La presente invención proporciona un método y un equipo de procesamiento de seguridad de flujos de datos. En un método de procesamiento de flujos de datos existente, un flujo de datos pasa en primer lugar a través de un módulo software dentro de un controlador para someterse a una detección de seguridad y, a continuación, el controlador transmite una ruta de reenvío que pasa únicamente por un dispositivo de reenvío, esto es, el controlador transmite información que indica una ruta de reenvío que pasa únicamente por un dispositivo de reenvío. El método de procesamiento de flujos de datos de la presente invención determina los niveles de seguridad de los flujos de datos de acuerdo con diferentes informaciones de características de los flujos de datos y determina, de acuerdo con los niveles de seguridad de los flujos de datos, las rutas de reenvío correspondientes a los flujos de datos. Comparado con que en la técnica anterior una ruta de reenvío pasa únicamente por un dispositivo de reenvío pero no pasa por un dispositivo de seguridad, una ruta de reenvío determinada en los modos de realización de la presente invención puede probablemente pasar por un dispositivo de seguridad, porque el método de procesamiento de flujos de datos de la presente invención determina los niveles de seguridad de los flujos de datos en función de la información de diferentes características de los flujos de datos y determina, en función de los niveles de seguridad de los flujos de datos, las rutas de reenvío correspondientes a los flujos de datos. De este modo, una ruta de reenvío puede pasar por un dispositivo de seguridad para implementar una función de seguridad correspondiente de la ruta de reenvío, mejorando de este modo la seguridad de reenvío de los flujos de datos y aligerando la carga del controlador.

Breve descripción de los dibujos

Con el fin de describir con más claridad las soluciones técnicas de los modos de realización de la presente invención o de la técnica anterior, a continuación, se introducen brevemente los dibujos adjuntos necesarios para describir los modos de realización o la técnica anterior. Evidentemente, los dibujos adjuntos en la siguiente descripción muestran únicamente algunos modos de realización de la presente invención, y una persona con un conocimiento normal en la técnica pueden derivar, además, otros dibujos a partir de estos dibujos adjuntos sin esfuerzos creativos.

La FIG. 1A es un diagrama de flujo de un método de procesamiento de seguridad de flujos de datos de acuerdo con el Modo de realización 1 de la presente invención;

la FIG. 1B es un diagrama esquemático de la estructura de una red de reenvío de acuerdo con el Modo de realización 1 de la presente invención;

la FIG. 2A es un diagrama de flujo de un método del mecanismo para encontrar la ruta de seguridad más corta de acuerdo con el Modo de realización 2 de la presente invención;

la FIG. 2B es un diagrama esquemático de una topología de red de acuerdo con el Modo de realización 2 de la presente invención;

la FIG. 2C es un diagrama esquemático de una topología de red de una red completa de división del nodo de seguridad de acuerdo con el Modo de realización 2 de la presente invención;

la FIG. 2D es un diagrama de flujo de un método del mecanismo para encontrar la ruta de detección más rápida de acuerdo con el Modo de realización 2 de la presente invención;

la FIG. 3 es un diagrama de flujo de un método de procesamiento de seguridad de flujos de datos de acuerdo con el Modo de realización 3 de la presente invención; y

la FIG. 4 es un diagrama esquemático de la estructura de un equipo de procesamiento de seguridad de flujos de datos de acuerdo con el Modo de realización 4 de la presente invención.

Descripción de los modos de realización

Con el fin de hacer más claros los objetivos, las soluciones técnicas y las ventajas de los modos de realización de la presente invención, a continuación, se describen de forma clara y completa las soluciones técnicas de los modos de realización de la presente invención haciendo referencia a los dibujos adjuntos en los modos de realización de la presente invención. Evidentemente, los modos de realización descritos son una parte y no todos los modos de realización de la presente invención.

Los siguientes modos de realización de la presente invención son modos de realización de un método y un equipo de procesamiento de seguridad de flujos de datos basados en una tecnología SDN y una red OpenFlow (flujo abierto, OF para abreviar). Los dispositivos de red de los siguientes modos de realización de la presente invención incluyen un dispositivo de reenvío y un dispositivo de seguridad. El dispositivo de seguridad puede ser un cortafuegos o puede ser un dispositivo de seguridad de tipo sistema de prevención de intrusiones (Intrusion Prevention System, IPS para abreviar) o un sistema de detección de intrusiones (Intrusion Detection System, IDS para abreviar); y la presente invención no establece ninguna limitación en la presente solicitud. El dispositivo de

reenvío puede ser un conmutador, o puede ser un router; y la presente invención no establece ninguna limitación en la presente solicitud.

Modo de realización 1

La FIG. 1A es un diagrama de flujo de un método de procesamiento de seguridad de flujos de datos de acuerdo con el Modo de realización 1 de la presente invención. Tal como se muestra en la FIG. 1A, el método incluye, específicamente, los siguientes pasos:

Paso 101: obtener información de las características de un flujo de datos, en donde la información de las características incluye información del origen e información del destino del flujo de datos.

Paso 102: determinar un nivel de seguridad del flujo de datos en función de la información de las características.

Cuando es necesario reenviar un flujo de datos, un controlador puede obtener la información de las características del flujo de datos y una condición del enlace (por ejemplo, una condición de congestión de puertos y una velocidad de línea de reenvío) de un dispositivo de red actual, y determina el nivel de seguridad del flujo de datos considerando tanto la condición del enlace como la información de las características del flujo de datos. La presente invención no establece ninguna limitación sobre el método para determinar el nivel de seguridad.

Paso 103: determinar, en función del nivel de seguridad, una ruta de reenvío para transmitir el flujo de datos.

Paso 104: enviar a los dispositivos en la ruta de reenvío la información utilizada para indicar la ruta de reenvío.

En concreto, cuando es necesario transmitir un flujo de datos en una red OF, un controlador obtiene la información de las características del flujo de datos, determina un nivel de seguridad del flujo de datos en función de la información de las características, determina, en función del nivel de seguridad correspondiente al flujo de datos, una ruta de reenvío para el flujo de datos, y envía a los dispositivos en la ruta la información determinada utilizada para indicar la ruta de reenvío, en donde diferentes niveles de seguridad pueden corresponderse con diferentes rutas de reenvío, diferentes rutas de reenvío pasan a través de un dispositivo de reenvío o un dispositivo de seguridad de diferentes formas, y los dispositivos pueden incluir el dispositivo de reenvío y el dispositivo de seguridad, o pueden incluir únicamente el dispositivo de reenvío.

La presente invención proporciona un método de procesamiento de seguridad de flujos de datos. En un método existente de procesamiento de flujos de datos, un flujo de datos pasa en primer lugar a través de un módulo software dentro de un controlador para someterse a una detección de seguridad y, a continuación, el controlador envía una ruta de reenvío que pasa únicamente por un dispositivo de reenvío, esto es, el controlador envía la información que indica una ruta de reenvío que pasa únicamente por un dispositivo de reenvío. El método de procesamiento de flujos de datos de la presente invención determina los niveles de seguridad de los flujos de datos en función de una información de diferentes características de los flujos de datos y determina, en función de los niveles de seguridad de los flujos de datos, las rutas de reenvío correspondientes a los flujos de datos. En comparación con una ruta de reenvío que pasa únicamente por un dispositivo de reenvío pero que no pasa por un dispositivo de seguridad en la técnica anterior, una ruta de reenvío determinada en este modo de realización de la presente invención puede probablemente pasar por un dispositivo de seguridad, porque el método de procesamiento de flujos de datos de la presente invención determina los niveles de seguridad de los flujos de datos en función de una información de diferentes características de los flujos de datos y determina, en función de los niveles de seguridad de los flujos de datos, las rutas de reenvío correspondientes a los flujos de datos. De este modo, una ruta de reenvío puede pasar por un dispositivo de seguridad para implementar una función de seguridad correspondiente de la ruta de reenvío, mejorando de este modo la seguridad de reenvío de los flujos de datos y aligerando la carga del controlador.

Además, el modo de realización anterior puede también incluir:

obtener una información de topología de red, en donde la información de topología de red es una información de topología de una red que incluye un dispositivo de reenvío y un dispositivo de seguridad, y la información de topología incluye una información de las capacidades de seguridad del dispositivo de seguridad.

En correspondencia, el paso 103 anterior puede ser específicamente:

determinar, en función del nivel de seguridad y la información de las capacidades de seguridad del dispositivo de seguridad, la ruta de reenvío para transmitir el flujo de datos.

Opcionalmente, la información de las capacidades de seguridad incluye al menos un elemento de información de la siguiente información:

información de las capacidades de seguridad de las capas 2 a 3, y la información de las capacidades de seguridad de las capas 2 a 7.

En concreto, antes de determinar una ruta de reenvío para un flujo de datos en función de un nivel de seguridad del flujo de datos, un controlador puede obtener la información de topología de red de las siguientes tres formas:

Forma uno: obtenerla mediante una interacción de mensajes de tipo handshake (establecimiento de comunicación). Un dispositivo de red en una red OF le envía una petición al controlador para establecer una conexión. Ambas partes establecen una conexión del Protocolo de Control de Transmisión (Transmission Control Protocol, TCP para abreviar). El dispositivo de red puede transferir un identificador de dispositivo del dispositivo de red utilizando la conexión TCP. Al mismo tiempo, el controlador y el dispositivo de red pueden intercambiar entre ambas partes información como, por ejemplo, la versión del protocolo de comunicaciones y, a continuación, seleccionar la versión del protocolo de comunicaciones para establecer la comunicación.

Forma dos: obtenerla mediante una interacción de mensajes de tipo petición del dispositivo de red. Cuando cambia la información de estado de un dispositivo de red de una red OF, el dispositivo de red puede notificarle al controlador de forma activa la información del estado cambiada del dispositivo de red. En consecuencia, el controlador cambia la información de topología de red de acuerdo con la nueva información de estado. La información de estado incluye, pero no se limita a, la siguiente información: información de estado del dispositivo, información de estado del puerto e información de las capacidades de seguridad. La información de las capacidades de seguridad incluye, pero no se limita a, los siguientes dos tipos de información: un campo del paquete de datos que soporta detección como, por ejemplo, el Protocolo de Internet (Internet Protocol, IP para abreviar) que soporta filtrado de paquetes de datos, una red de área local virtual (Virtual Local Area Network, vlan para abreviar) vlan, el número de puntos por pulgada (Deep Packet Inspection, DPI para abreviar); y una forma de ataque que se puede detectar como, por ejemplo, un comando del sistema operativo de disco (Disk Operating System, DOS para abreviar) y un fraude del Protocolo de Resolución de Direcciones (Address Resolution Protocol, ARP para abreviar).

Forma tres: obtenerla mediante una interacción de mensajes de tipo petición del controlador. Un controlador puede pedir y obtener una información de estado de un dispositivo de red en una red OF. El dispositivo de red le envía al controlador la información de estado correspondiente. En consecuencia, el controlador cambia la información de topología de red en función de la información de estado recibida.

Las tres formas anteriores de formas de obtención de información de topología de red se pueden realizar en cualquier momento antes de que el controlador en la red OF realice el paso 103. Una topología de red se puede obtener utilizando una de las tres formas anteriores o una combinación de las tres formas, lo cual no se encuentra limitado por la presente invención.

Por ejemplo, la FIG. 1B es un diagrama esquemático de la estructura de una red de reenvío de acuerdo con el Modo de realización 1 de la presente invención. Tal como se muestra en la FIG. 1B, por ejemplo, una arquitectura física de la red OF incluye, específicamente, tres dispositivos de reenvío y dos dispositivos de seguridad. En la FIG. 1B se muestra una forma de conexión de los tres dispositivos de reenvío y los dos dispositivos de seguridad. Antes de realizar el paso 103, el controlador puede obtener una topología de toda la red utilizando las tres formas anteriores. Por ejemplo, específicamente, el controlador puede obtener en primer lugar, aplicando el método de la forma uno, la información de topología de red, esto es, la información de estado de y una relación de conexión entre los dispositivos de red (los dispositivos de reenvío y los dispositivos de seguridad) que se muestran en la FIG. 1B, en donde un dispositivo de seguridad se corresponde con un nodo de seguridad y un dispositivo de reenvío se corresponde con un nodo de reenvío. Cuando cambia la información de estado de los dispositivos de red en la red, el controlador puede cambiar correspondientemente la nueva información de estado en la información de topología de red aplicando la forma dos. Además, el controlador puede también aplicar la forma tres para solicitar y obtener la información de estado de los dispositivos de red en la red.

Se utiliza un controlador para determinar una ruta de reenvío para un flujo de datos después de haber obtenido la información de topología de una red que incluye un dispositivo de seguridad y un dispositivo de reenvío, mejorando de este modo la seguridad del reenvío de los flujos de datos.

Además, la determinación, en función del nivel de seguridad, de una ruta de reenvío correspondiente al flujo de datos, esto es, el paso 103, puede incluir específicamente:

determinar un mecanismo de búsqueda de ruta correspondiente en función del nivel de seguridad; y

determinar, de acuerdo con el mecanismo de búsqueda de ruta, la ruta de reenvío para transmitir el flujo de datos.

En concreto, después de que el controlador determine el nivel de seguridad del flujo de datos que necesita ser transferido en la red, el controlador puede determinar un mecanismo de búsqueda de ruta correspondiente al nivel de seguridad, y determinar la ruta de reenvío para el flujo de datos utilizando el mecanismo de búsqueda de ruta.

Diferentes flujos de datos se clasifican en diferentes niveles de seguridad, y diferentes niveles de seguridad se corresponden con diferentes mecanismos de búsqueda de ruta para determinar una ruta de reenvío. Esto hace que los flujos de datos pasen a través de diferentes dispositivos de seguridad o no pasen a través de un dispositivo de seguridad en función de los diferentes niveles de seguridad, mejorando de este modo la eficiencia y la seguridad en el reenvío de flujos de datos.

Modo de realización 2

Basándose en el Modo de realización 1, el Modo de realización 2 describe en detalle cómo determinar diferentes mecanismos de búsqueda de ruta en función de diferentes niveles de seguridad en el Modo de realización 1. En el Modo de realización 1, los mecanismos de búsqueda de ruta pueden ser un mecanismo de búsqueda de la ruta más corta, un mecanismo de búsqueda de la ruta de seguridad más corta, y un mecanismo de búsqueda de la ruta de detección más rápida.

Por ejemplo, la determinación de un nivel de seguridad puede realizarse específicamente de las siguientes dos formas, pero no se encuentra limitada a las siguientes dos formas:

Forma uno: clasificar un nivel de seguridad en función de una fuente del flujo de datos. Por ejemplo, un nivel de seguridad se clasifica específicamente en función de la fiabilidad de una fuente del flujo de datos. Diferentes niveles de seguridad se corresponden con diferentes mecanismos de búsqueda de ruta. Por ejemplo, en la Tabla 1 se describen condiciones de clasificación de niveles de seguridad específicas.

Tabla 1 Condiciones de clasificación de niveles de seguridad de la forma uno

Fiabilidad del origen del flujo de datos	**Nivel de seguridad**	**Mecanismo de búsqueda de ruta correspondiente**
Alta	Bajo	Mecanismo de búsqueda de la ruta más corta
Media	Medio	Mecanismo de búsqueda de la ruta de seguridad más corta
Baja	Alto	Mecanismo de búsqueda de la ruta de detección más rápida

Forma dos: calcular la información de las características de un flujo de datos de acuerdo con una de las formas, y clasificar el nivel de seguridad en función del resultado del cálculo. La información de las características del flujo de datos puede ser la información del origen y la información del destino del flujo de datos, la cual puede ser específicamente un puerto de conmutación al que llega el paquete de datos, un puerto Ethernet de origen, un puerto IP de origen, una etiqueta VLAN, un puerto Ethernet de destino o un puerto IP de destino, y muchas otras características del paquete de datos. Por ejemplo, la forma de cálculo puede ser tal que: Level_packet = (k1*Level_vlan ID + k2*Level_MAC)/2, en donde Level_packet es el nivel de un flujo de datos, Level_vlan ID es el nivel de seguridad de una red virtual, Level_MAC es el nivel de una tarjeta de interfaz de red física, y k1 y k2 son unas constantes predefinidas. Los valores de las características del flujo de datos mencionados en la presente solicitud no están limitados a los distintos valores de ejemplo de las características. En concreto, en una red SDN, los valores de características que representan características del flujo de datos anterior se pueden obtener desde un campo "match (de correspondencia)" en un mensaje de flujo abierto. Las áreas se pueden dividir en función de los resultados del cálculo. Cada área se corresponde con un nivel de seguridad. En la Tabla 2 se describen ejemplos específicos, en donde a, b, c y d son valores límite de las áreas de resultado del cálculo. El resultado del cálculo de la información de las características de un flujo de datos pertenece a dicha área en la Tabla 2, y el nivel de seguridad correspondiente al área es un nivel de seguridad del flujo de datos. Por ejemplo, específicamente, tal como se describe en la Tabla 2, se pueden clasificar tres niveles de seguridad.

Tabla 2 Condiciones de clasificación de niveles de seguridad de la forma dos

Área de información de las características	**Nivel de seguridad**	**Mecanismo de búsqueda de ruta correspondiente**
[a,b)	Bajo	Mecanismo de búsqueda de la ruta más corta
[b,c)	Medio	Mecanismo de búsqueda de la ruta de seguridad más corta
[c,d)	Alto	Mecanismo de búsqueda de la ruta de detección más rápida

Las formas de implementación de los tres mecanismos de búsqueda de ruta anteriores son del siguiente modo:

Uno: mecanismo de búsqueda de la ruta más corta

La determinación de una ruta de reenvío de acuerdo con el mecanismo de búsqueda de la ruta más corta incluye: determinar, de acuerdo con el mecanismo de búsqueda de la ruta más corta, que la ruta de reenvío es la ruta más corta desde un nodo de origen a un nodo de destino, en donde la ruta más corta no pasa por un dispositivo de seguridad.

En concreto, en el caso en el que un flujo de datos, en una red OF, que necesite ser transferido tenga un relativamente bajo requisito de garantía de seguridad o no tenga ningún requisito de seguridad, el nivel de seguridad del flujo de datos es relativamente bajo, y, con el fin de determinar una ruta de reenvío, se puede seleccionar el mecanismo de búsqueda de la ruta más corta, en función del relativamente bajo nivel de seguridad. Un proceso de implementación del mecanismo de búsqueda de la ruta más corta es: determinar la ruta más corta desde un nodo de origen a un nodo de destino del flujo de datos que necesita ser transferido, en donde la ruta más corta no pasa por un dispositivo de seguridad con el fin de mejorar la velocidad de reenvío.

Dos: mecanismo de búsqueda de la ruta de seguridad más corta

La FIG. 2A es un diagrama de flujo de un método de un mecanismo de búsqueda de la ruta de seguridad más corta de acuerdo con el Modo de realización 2 de la presente invención. Tal como se muestra en la FIG. 2A, la determinación de una ruta de reenvío correspondiente de acuerdo con el mecanismo de búsqueda de la ruta de seguridad más corta incluye, específicamente, los siguientes pasos:

Paso 210: dividir un nodo de seguridad en nodos split (resultantes de la división) en función de un grado del nodo de seguridad, en donde el nodo de seguridad se corresponde con un dispositivo de seguridad, y el número de nodos split es igual al número de grados.

Paso 211: obtener rutas desde un nodo de origen a los nodos split.

Paso 212: obtener rutas desde un nodo de destino a los nodos split.

Paso 213: determinar que una ruta de reenvío para transmitir un flujo de datos es la ruta más corta de las rutas que pasan por el mismo nodo de seguridad pero diferentes nodos split, en donde las rutas se encuentran entre las rutas desde el nodo de origen a los nodos split y las rutas desde el nodo de destino a los nodos split.

En concreto, en el caso en el que un flujo de datos, en una red OF, que necesita ser transferido tenga un requisito relativamente alto de garantía de seguridad y de velocidad de reenvío, el nivel de seguridad del flujo de datos es relativamente alto, y se puede seleccionar el mecanismo de búsqueda de la ruta de seguridad más corta, en función del relativamente alto nivel de seguridad, con el fin de determinar una ruta de reenvío. Una forma de implementación del mecanismo de búsqueda de la ruta de seguridad más corta es: dividir un nodo de seguridad correspondiente a un dispositivo de seguridad en nodos split, en donde el número de los nodos split es igual al número de grados, y obtener las rutas desde el nodo de origen, que se corresponde con el flujo de datos que necesita ser transferido, a cada uno de los nodos split, esto es, se ejecuta el paso 211, en donde el "grado" es tal que un nodo se puede conectar a otro nodo utilizando múltiples enlaces, y el número de enlaces conectados al nodo es el número de grados; y además, obtener las rutas desde el nodo de origen, que se corresponde con los datos que necesitan ser transferido, a cada uno de los nodos split, esto es, se ejecuta el paso 212. Los pasos 211 a 212 se ejecutan para los nodos split de cada nodo de seguridad con el fin de determinar la ruta de reenvío correspondiente al flujo de datos, en donde la ruta de reenvío es la ruta más corta de las rutas que pasan por el mismo nodo de seguridad pero diferentes nodos split, en donde las rutas se encuentran entre las rutas desde el nodo de origen a los nodos split y las rutas desde el nodo de destino a los nodos split.

Por ejemplo, la FIG. 2B es un diagrama esquemático de una topología de red de acuerdo con el Modo de realización 2 de la presente invención, y la FIG. 2C es un diagrama esquemático de una topología de toda la red de división de nodos de seguridad de acuerdo con el Modo de realización 2 de la presente invención. Por ejemplo, tal como se muestra en la FIG. 2B, la topología de toda la red incluye, específicamente, cuatro nodos de reenvío V1 a V4, y dos nodos de seguridad S1 y S2. El grado del nodo de seguridad S1 es 3, y el grado del nodo de seguridad S2 es 2. Un valor ponderado entre un nodo de seguridad y un nodo de reenvío representa una longitud de una ruta entre dos nodos, un valor ponderado mayor indica una mayor longitud de una ruta, y un menor valor ponderado indica una menor longitud de una ruta. Tal como se muestra en la FIG. 2C, la FIG. 2C es un diagrama esquemático de la topología de toda la red que se muestra en la FIG. 2B después de haber dividido los nodos de seguridad en la topología de toda la red. El nodo de seguridad S1 se divide en tres nodos split en función del grado, y el nodo de seguridad S2 se divide en dos nodos split en función del grado.

Por ejemplo, un proceso algorítmico del mecanismo de búsqueda de la ruta de seguridad más corta en la topología de toda la red que se muestra en la FIG. 2B es específicamente como sigue:

Paso 1: realizar una reconstrucción de la topología para el diagrama de topología que se muestra en la FIG. 2B, y dividir los nodos de seguridad en función de los grados de los nodos de seguridad. En la FIG. 2C se muestra una topología reconstruida.

Paso 2: en el nuevo diagrama de topología, calcular, utilizando el algoritmo de Dijkstra, una suma de valores ponderados de un punto de origen V1 a los nodos split S1-1 a S1-3, respectivamente, y una suma de valores ponderados del punto de origen V1 a los nodos split S2-1 a S2-2, respectivamente, una suma de valores ponderados representa una longitud de una ruta. Mediante el cálculo se obtiene lo siguiente:

se obtiene que: V1->S1-1 = 7;

se obtiene que: V1->S1-2 = 2;

se obtiene que: V1->S1-3 = 13;

se obtiene que: V1->S2-1 = 4; y

se obtiene que: V1->S2-2 = 15.

Paso 3: calcular, utilizando el algoritmo de Dijkstra, una suma de valores ponderados de un punto de origen V2 a los nodos split S1-1 a S1-3, respectivamente, y una suma de valores ponderados del origen V2 a los nodos split S2-1 a S2-2, respectivamente. Mediante el cálculo se obtiene lo siguiente:

se obtiene que: V2->S1-1 = 8;

se obtiene que: V2->S1-2 = 1;

se obtiene que: V2->S1-3 = 14;

se obtiene que: V2->S2-1 = 5; y

se obtiene que: V2->S2-2 = 16.

Paso 4: determinar una ruta final para cada nodo de seguridad.

Para el nodo de seguridad S1: el resultado de las dos rutas de V1 y V2 con la suma más pequeña y de los diferentes nodos split es V1->S1-1 = 7 más V2->S1-2 = 1. Por lo tanto, la ruta más corta que pasa por S1 es 8.

Para el nodo de seguridad S2: el resultado de las dos rutas de V1 y V2 con la suma más pequeña y de los diferentes nodos split es V1->S2-1 = 4 más V2->S2-2 = 16. Por lo tanto, la ruta más corta que pasa por S2 es 20.

Paso 5: en los nodos de seguridad, seleccionar como ruta final la ruta cuya longitud sea la más corta, esto es V1->V4->S1->V2. El algoritmo finaliza.

El proceso anterior calcula la ruta más corta desde V1 a V2. Utilizando el mismo método se puede obtener mediante cálculo la ruta más corta entre dos puntos cualesquiera. El proceso de cálculo es como sigue:

Una suma de valores ponderados desde el nodo V1 a cada nodo split:

se obtiene que: V1->S1-1 = 7;

se obtiene que: V1->S1-2 = 2;

se obtiene que: V1->S1-3 = 13;

se obtiene que: V1->S2-1 = 4; y

se obtiene que: V1->S2-2 = 1.

Una suma de valores ponderados desde el nodo V2 a cada nodo split:

se obtiene que: V2->S1-1 = 8;

se obtiene que: V2->S1-2 = 1;

se obtiene que: V2->S1-3 = 14;

se obtiene que: V2->S2-1 = 5; y

se obtiene que: V2->S2-2 = 16.

Una suma de valores ponderados desde el nodo V3 a cada nodo split:

se obtiene que: V3->S1-1 = 11;

se obtiene que: V3->S1-2 = 10;

se obtiene que: V3->S1-3 = 5;

se obtiene que: V3->S2-1 = 12; y

se obtiene que: V3->S2-2 = 7.

Una suma de valores ponderados desde el nodo V4 a cada nodo split:

se obtiene que: V4->S1-1 = 5;

se obtiene que: V4->S1-2 = 4;

se obtiene que: V4->S1-3 = 1;

se obtiene que: V4->S2-1 = 6; y

se obtiene que: V4->S2-2 = 13.

En resumen, se puede obtener que la ruta más corta entre dos puntos cualesquiera es del siguiente modo:

V1->V2: min(V1->S1->V2) = V1->S1-1 + V2->S1-2 = 8;

min(V1->S2->V2) = V1->S2-1 + V2->S2-2 = 20;

por lo tanto, la longitud de la ruta más corta de V1->V2 es 8, y la ruta es V1->V4->S1->V2.

V1->V3: min(V1->S1->V3) = V1->S1-2 + V3->S1-3 = 7;

min(V1->S2->V3) = V1->S2-1 + V3->S2-2 = 11;

por lo tanto, la longitud de la ruta más corta de V1->V3 es 7, y la ruta es V1->V2->S1->V3.

V1->V4: min(V1->S1->V4) = V1->S1-2 + V4->S1-1 = 7;

min(V1->S2->V4) = V1->S2-1 + V4->S2-2 = 17;

por lo tanto, la longitud de la ruta más corta de V1->V4 es 7, y la ruta es V1->V2->S1->V4.

V2->V3: min(V2->S1->V3) = V2->S1-2 + V3->S1-3 = 6;

min(V2->S2->V3) = V2->S2-1 + V3->S2-2 = 12;

por lo tanto, la longitud de la ruta más corta de V2->V3 es 6, y la ruta es V2->S1->V3.

V2->V4: min(V2->S1->V4) = V2->S1-2 + V4->S1-1 = 6;

min(V2->S2->V4) = V2->S2-1 + V4->S2-2 = 18;

por lo tanto, la longitud de la ruta más corta de V2->V4 es 6, y la ruta es V2->S1->V4.

V3->V4: min(V3->S1->V4) = V3->S1-3 + V4->S1-2 = 9;

min(V3->S2->V4) = V3->S2-2 + V4->S2-1 = 13;

por lo tanto, la longitud de la ruta más corta de V3->V4 es 9, y la ruta es V3->S1->V2->V1->V4.

El algoritmo finaliza.

Tres: mecanismo de búsqueda de la ruta de detección más rápida

La FIG. 2D es un diagrama de flujo de un método de un mecanismo de búsqueda de la ruta de detección más rápida de acuerdo con el Modo de realización 2. Tal como se muestra en la FIG. 2D, la determinación de una ruta

de reenvío de acuerdo con el mecanismo de búsqueda de la ruta de detección más rápida incluye, específicamente, los siguientes pasos:

Paso 220: dividir un nodo de seguridad en nodos split en función del grado del nodo de seguridad, en donde el nodo de seguridad se corresponde con un dispositivo de seguridad, y el número de nodos split es igual al número de grados.

Paso 221: obtener la ruta más corta desde un nodo de origen a los nodos split actuales.

Paso 222: obtener una ruta desde un nodo de destino a otro nodo split del nodo de seguridad, en donde el otro nodo split es un nodo split distinto del nodo split que utiliza la ruta más corta.

Paso 223: determinar una ruta de reenvío para transmitir un flujo de datos, en donde la ruta de reenvío para transmitir el flujo de datos es una ruta tal que en primer lugar la ruta de reenvío pasa por la ruta más corta desde el nodo de origen a los nodos split; a continuación, pasa por el dispositivo de seguridad; y, por último, pasa por el nodo de destino hasta el otro nodo split del nodo de seguridad, esto es, la ruta de reenvío para transmitir el flujo de datos es una ruta tal que en primer lugar la ruta de reenvío pasa por la ruta más corta desde el nodo de origen a los nodos split y, a continuación, pasa por el otro nodo split del nodo de seguridad hasta el nodo de destino.

En concreto, cuando un flujo de datos, en una red OF, que necesita ser transferido tiene un coeficiente de peligro relativamente alto o pertenece a alguien con una credibilidad relativamente baja, el nivel de seguridad correspondiente al flujo de datos es particularmente alto. Entonces, con el fin de determinar una ruta de reenvío, se puede seleccionar el mecanismo de búsqueda de la ruta de detección más rápida, en función del nivel de seguridad particularmente alto. Una forma de implementación del mecanismo de búsqueda de la ruta de detección más rápida es: dividir un nodo de seguridad correspondiente a un dispositivo de seguridad en nodos split, en donde el número de nodos split es igual al número de grados; obtener las rutas desde un nodo de origen, que se corresponden con el flujo de datos que necesita ser transferido, a cada nodo split, y seleccionar la ruta más corta desde el nodo de origen a los nodos split, esto es, se ejecuta el paso 221; y obtener una ruta desde un nodo de destino, del flujo de datos que necesita ser transferido, a otro nodo split en el nodo de seguridad a través del que pasa la ruta seleccionada en el paso 211, en donde el otro nodo split es un nodo split distinto del nodo split a través del cual pasa la ruta seleccionada en el paso 211 pero pertenece al mismo nodo de seguridad que el nodo split a través del cual pasa la ruta seleccionada en el paso 211. Una ruta de reenvío, que se determina de acuerdo con el mecanismo de búsqueda de la ruta de detección más rápida, a través del cual pasa el flujo de datos que necesita ser transferido es una ruta que en primer lugar pasa a través de la ruta más corta desde el nodo de origen correspondiente al flujo de datos a todos los nodos split, y a continuación pasa a través de un dispositivo de seguridad correspondiente al nodo split, y por último pasa a través del nodo de destino correspondiente al flujo de datos hasta otro nodo split del nodo de seguridad, esto es, la ruta de reenvío para transmitir el flujo de datos es una ruta que en primer lugar pasa a través de la ruta más corta desde el nodo de origen a los nodos split, y a continuación pasa a través de otro nodo split del nodo de seguridad hacia el nodo de destino.

Diferentes niveles de seguridad se corresponden a diferentes mecanismos de búsqueda de ruta para determinar una ruta de reenvío. Esto hace que los flujos de datos pasen por diferentes dispositivos de seguridad o no pasen por ningún dispositivo de seguridad en función de diferentes niveles de seguridad, mejorando de este modo la eficiencia del reenvío y la seguridad de los flujos de datos.

Modo de realización 3

El Modo de realización 3 combina el Modo de realización 1 y el Modo de realización 2 y describe en detalle un método de procesamiento de seguridad de flujos de datos. La FIG. 3 es un diagrama de flujo del método de procesamiento de seguridad de flujos de datos de acuerdo con el Modo de realización 3 de la presente invención. Tal como se muestra en la FIG. 3, el método incluye, específicamente, los siguientes pasos:

Paso 301: obtener la información de topología de red.

La información de topología de red incluye información de estado de un dispositivo de seguridad y la de un dispositivo de reenvío, y una relación de conexión entre el dispositivo de seguridad y el dispositivo de reenvío. Al mismo tiempo, también se puede obtener la información de las capacidades de seguridad del dispositivo de seguridad. La información de las capacidades de seguridad incluye la información de las capacidades de seguridad de las capas 2 a 3 y la información de las capacidades de seguridad de las capas 2 a 7.

Paso 302: obtener la información de las características de un flujo de datos y determinar un nivel de seguridad del flujo de datos.

Paso 303: determinar un mecanismo de búsqueda de ruta correspondiente en función del nivel de seguridad.

Paso 304: determinar una ruta de reenvío para el flujo de datos de acuerdo con el mecanismo de búsqueda de ruta determinado.

Paso 305: enviar la ruta de reenvío a los dispositivos en la ruta de reenvío de acuerdo con la ruta de reenvío determinada.

La obtención de la información de topología de red en el paso 301 es un proceso dinámico, esto es, en una red, cuando cambia la información de estado del dispositivo de seguridad o la del dispositivo de reenvío, o cambia la información de las capacidades de seguridad del dispositivo de seguridad, un controlador se actualiza síncronamente. Un método de actualización puede realizarse de las tres formas del Modo de realización 1, las cuales no se vuelven a describir en la presente solicitud.

En el método de procesamiento de seguridad de flujos de datos de este modo de realización, se obtiene la información de topología de una red que incluye un dispositivo de reenvío y un dispositivo de seguridad, se determinan los niveles de seguridad de los flujos de datos en función de la información de las características de los flujos de datos; y se seleccionan diferentes mecanismos de búsqueda de ruta, en función de los niveles de seguridad de los flujos de datos, con el fin de determinar las rutas de reenvío para los flujos de datos, aligerando de este modo la carga de un controlador y mejorando la seguridad de reenvío de los flujos de datos.

Modo de realización 4

La FIG. 4 es un diagrama esquemático de la estructura de un equipo de procesamiento de seguridad de flujos de datos de acuerdo con el Modo de realización 4 de la presente invención. Tal como se muestra en la FIG. 4, el equipo 40 de procesamiento de seguridad de flujos de datos de este modo de realización incluye: un módulo 41 de obtención de características, un módulo 42 de determinación de nivel, un módulo 43 de determinación de ruta, y un módulo 44 de envío de ruta. El módulo 41 de obtención de características está configurado para obtener información de las características de un flujo de datos, en donde la información de las características incluye información del origen e información del destino del flujo de datos. El módulo 42 de determinación de nivel está configurado para determinar un nivel de seguridad del flujo de datos en función de la información de las características. El módulo 43 de determinación de ruta está configurado para determinar, en función del nivel de seguridad, una ruta de reenvío para transmitir el flujo de datos. El módulo 44 de envío de ruta está configurado para enviar la información utilizada para indicar la ruta de reenvío a los dispositivos en la ruta de reenvío.

Además, el módulo 42 de determinación de nivel está configurado específicamente para:

determinar una regla de búsqueda de ruta correspondiente en función del nivel de seguridad; y

determinar, en función de la regla de búsqueda de ruta, la ruta de reenvío para transmitir el flujo de datos.

Además, la regla de búsqueda de ruta es una regla de búsqueda de la ruta más corta.

En correspondencia, el módulo 43 de determinación de ruta está configurado específicamente, para:

determinar, de acuerdo con la regla de búsqueda de ruta más corta, que la ruta de reenvío es la ruta más corta desde un nodo de origen a un nodo de destino, en donde la ruta más corta no pasa por un dispositivo de seguridad.

Además, la regla de búsqueda de ruta es una regla de búsqueda de ruta de seguridad más corta.

En correspondencia, el módulo 43 de determinación de ruta está configurado específicamente, para:

dividir un nodo de seguridad en nodos split en función del grado del nodo de seguridad, en donde el nodo de seguridad se corresponde con el dispositivo de seguridad, y el número de nodos split es igual al número de grados;

obtener rutas desde el nodo de origen a los nodos split;

obtener rutas desde el nodo de destino a los nodos split; y

determinar que la ruta de reenvío para transmitir el flujo de datos es la ruta más corta entre las rutas que pasan por el mismo nodo de seguridad pero diferentes nodos split, en donde las rutas se encuentran dentro de las rutas que van desde el nodo de origen a los nodos split y las rutas que van desde el nodo de destino a los nodos split.

Alternativamente, la regla de búsqueda de ruta es una regla de búsqueda de ruta de detección más rápida.

En correspondencia, el módulo 43 de determinación de ruta está configurado específicamente para:

dividir un nodo de seguridad en nodos split en función del grado del nodo de seguridad, en donde el nodo de seguridad se corresponde con el dispositivo de seguridad, y el número de nodos split es igual al número de grados;

obtener la ruta más corta desde el nodo de origen a los nodos split actuales;

obtener rutas desde el nodo de destino a otro nodo split del nodo de seguridad, en donde el otro nodo split es un nodo split distinto del nodo split actual por el que pasa la ruta más corta; y

determinar la ruta de reenvío para transmitir el flujo de datos, en donde la ruta de reenvío para transmitir el flujo de datos es una ruta tal que la ruta de reenvío pasa en primer lugar por la ruta más corta que va desde el nodo de origen a los nodos split; a continuación pasa por el dispositivo de seguridad; y por último va desde el nodo de destino a otro nodo split del nodo de seguridad, esto es, la ruta de reenvío para transmitir el flujo de datos es una ruta que pasa en primer lugar por la ruta más corta desde el nodo de origen a los nodos split, y a continuación pasa por otro nodo split del nodo de seguridad hasta el nodo de destino.

Además, el equipo 40 de procesamiento de seguridad de flujos de datos del modo de realización también puede incluir: un módulo 45 de obtención de topología, el cual está configurado para obtener la información de topología de red. La información de topología de red es información de topología de una red que incluye un dispositivo de reenvío y el dispositivo de seguridad. La información de topología incluye información de las capacidades de seguridad del dispositivo de seguridad. En correspondencia, el módulo 43 de determinación de ruta está configurado específicamente para determinar, en función del nivel de seguridad y la información de las capacidades de seguridad del dispositivo de seguridad, la ruta de reenvío para transmitir el flujo de datos.

Preferiblemente, la información de las capacidades de seguridad incluye al menos un elemento de información de la siguiente información: información de las capacidades de seguridad de las capas 2 a 3, e información de las capacidades de seguridad de las capas 2 a 7.

El equipo de procesamiento de seguridad de flujos de datos de este modo de realización se puede utilizar para aplicar las soluciones técnicas de los modos de realización del método del Modo de realización 1, Modo de realización 2 y Modo de realización 3. Los principios de implementación y los efectos técnicos son parecidos, y no se vuelven a describir en la presente solicitud. Para los detalles, consúltense las descripciones correspondientes en los modos de realización.

Por último, se debería observar que los modos de realización anteriores únicamente pretenden describir las soluciones técnicas de la presente invención, pero no limitar la presente invención. Aunque la presente invención se ha descrito detalladamente haciendo referencia a los modos de realización anteriores, las personas con un conocimiento normal en la técnica deberían entender que se pueden seguir haciendo modificaciones a las soluciones técnicas descritas en los modos de realización anteriores sin apartarse del alcance de la invención tal como está definido por las reivindicaciones.

REIVINDICACIONES

1. Un método de procesamiento de seguridad de flujos de datos, que comprende:

obtener (101) información de las características de un flujo de datos, en donde la información de las características comprende información del origen e información del destino del flujo de datos;

obtener información de topología de red;

determinar (102) un nivel de seguridad del flujo de datos de acuerdo con la información de las características;

determinar (103), en función del nivel de seguridad, una ruta de reenvío para transmitir el flujo de datos; y

enviar (104) a los dispositivos en la ruta de reenvío la información utilizada para indicar la ruta de reenvío;

en donde la determinación, en función del nivel de seguridad, de una ruta de reenvío para transmitir el flujo de datos comprende:

determinar una regla de búsqueda de ruta correspondiente en función del nivel de seguridad; y

determinar, de acuerdo con la regla de búsqueda de ruta, la ruta de reenvío para transmitir el flujo de datos;

estando caracterizado el método por que

si la regla de búsqueda de ruta es una regla de búsqueda de ruta de seguridad más corta, entonces

la determinación, de acuerdo con la regla de búsqueda de ruta, de la ruta de reenvío para transmitir el flujo de datos comprende:

dividir un nodo de seguridad en nodos split (resultantes de la división) en función del grado del nodo de seguridad, en donde el nodo de seguridad es la representación de un dispositivo de seguridad en la información de topología de red, y el número de nodos split es igual al número de grados; en donde, el grado es tal que un nodo está conectado a otro nodo utilizando múltiples enlaces, y el número de enlaces conectados al nodo es el número de grados;

obtener rutas desde el nodo de origen a los nodos split;

obtener rutas desde el nodo de destino a los nodos split; y

determinar que la ruta de reenvío para transmitir el flujo de datos es la ruta más corta entre las rutas que pasan por el mismo nodo de seguridad pero diferentes nodos split, en donde las rutas se encuentran entre las rutas desde el nodo de origen a los nodos split y las rutas desde el nodo de destino a los nodos split.

2. El método de acuerdo con la reivindicación 1, en donde si la regla de búsqueda de ruta es una regla de búsqueda de ruta más corta, entonces

la determinación, de acuerdo con la regla de búsqueda de ruta, de la ruta de reenvío para transmitir el flujo de datos comprende:

determinar, de acuerdo con la regla de búsqueda de ruta más corta, que la ruta más corta desde un nodo de origen a un nodo de destino es la ruta de reenvío, en donde la ruta más corta no pasa por un dispositivo de seguridad.

3. El método de acuerdo con la reivindicación 1, que comprende, además:

en donde la información de topología de red es una información de topología de una red que comprende un dispositivo de reenvío y un dispositivo de seguridad, y la información de topología comprende una información de las capacidades de seguridad del dispositivo de seguridad; y

la determinación, en función del nivel de seguridad, de una ruta de reenvío para transmitir el flujo de datos comprende:

determinar, en función del nivel de seguridad y la información de las capacidades de seguridad del dispositivo de seguridad, la ruta de reenvío para transmitir el flujo de datos.

4. El método de acuerdo con la reivindicación 3, en donde la información de las capacidades de seguridad comprende al menos un elemento de información entre la siguiente información:

información de las capacidades de seguridad de las capas 2 a 3, e información de las capacidades de seguridad de las capas 2 a 7.

5. Un equipo de procesamiento de seguridad de flujos de datos, que comprende:

un módulo (41) de obtención de características, configurado para obtener una información de las características de un flujo de datos, en donde la información de las características comprende información del origen e información del destino del flujo de datos;

un módulo (42) de determinación de nivel, configurado para determinar un nivel de seguridad del flujo de datos de acuerdo con la información de las características;

un módulo (43) de determinación de ruta, configurado para determinar, en función del nivel de seguridad, una ruta de reenvío para transmitir el flujo de datos; y

un módulo (44) de envío de ruta, configurado para enviarle a los dispositivos en la ruta de reenvío la información utilizada para indicar la ruta de reenvío;

un módulo (45) de obtención de topología, configurado para obtener la información de topología de la red;

en donde el módulo de determinación de nivel está configurado específicamente para:

determinar una regla de búsqueda de ruta correspondiente en función del nivel de seguridad; y

determinar, de acuerdo con la regla de búsqueda de ruta, la ruta de reenvío para transmitir el flujo de datos;

estando caracterizado el equipo por que

si la regla de búsqueda de ruta es una regla de búsqueda de ruta de seguridad más corta, entonces

el módulo de determinación de ruta está configurado específicamente para:

dividir un nodo de seguridad en nodos split en función del grado del nodo de seguridad, en donde el nodo de seguridad es la representación de un dispositivo de seguridad en la información de topología de red, y el número de nodos split es igual al número de grados; en donde, el grado es tal que un nodo está conectado a otro nodo utilizando múltiples enlaces, y el número de enlaces conectados al nodo es el número de grados;

obtener rutas desde el nodo de origen a los nodos split;

obtener rutas desde el nodo de destino a los nodos split; y

determinar que la ruta de reenvío para transmitir el flujo de datos es la ruta más corta entre las rutas que pasan por el mismo nodo de seguridad pero diferentes nodos split, en donde las rutas se encuentran entre las rutas desde el nodo de origen a los nodos split y las rutas desde el nodo de destino a los nodos split.

6. El equipo de procesamiento de seguridad de flujos de datos de acuerdo con la reivindicación 9, en donde si la regla de búsqueda de ruta es una regla de búsqueda de ruta más corta, entonces

el módulo de determinación de ruta está configurado específicamente para:

determinar, de acuerdo con la regla de búsqueda de ruta más corta, que la ruta de reenvío es la ruta más corta desde un nodo de origen a un nodo de destino, en donde la ruta más corta no pasa por un dispositivo de seguridad.

7. El equipo de procesamiento de seguridad de flujos de datos de acuerdo con la reivindicación 5, que comprende, además:

en donde la información de topología de red es una información de topología de una red que comprende un dispositivo de reenvío y un dispositivo de seguridad, y la información de topología comprende una información de las capacidades de seguridad del dispositivo de seguridad; y

el módulo de determinación de ruta está configurado específicamente para:

determinar, en función del nivel de seguridad y la información de las capacidades de seguridad del dispositivo de seguridad, la ruta de reenvío para transmitir el flujo de datos.

8. El equipo de procesamiento de seguridad de flujos de datos de acuerdo con la reivindicación 7, en donde la información de las capacidades de seguridad comprende al menos un elemento de información entre la siguiente información:

información de las capacidades de seguridad de las capas 2 a 3, e información de las capacidades de seguridad de las capas 2 a 7.

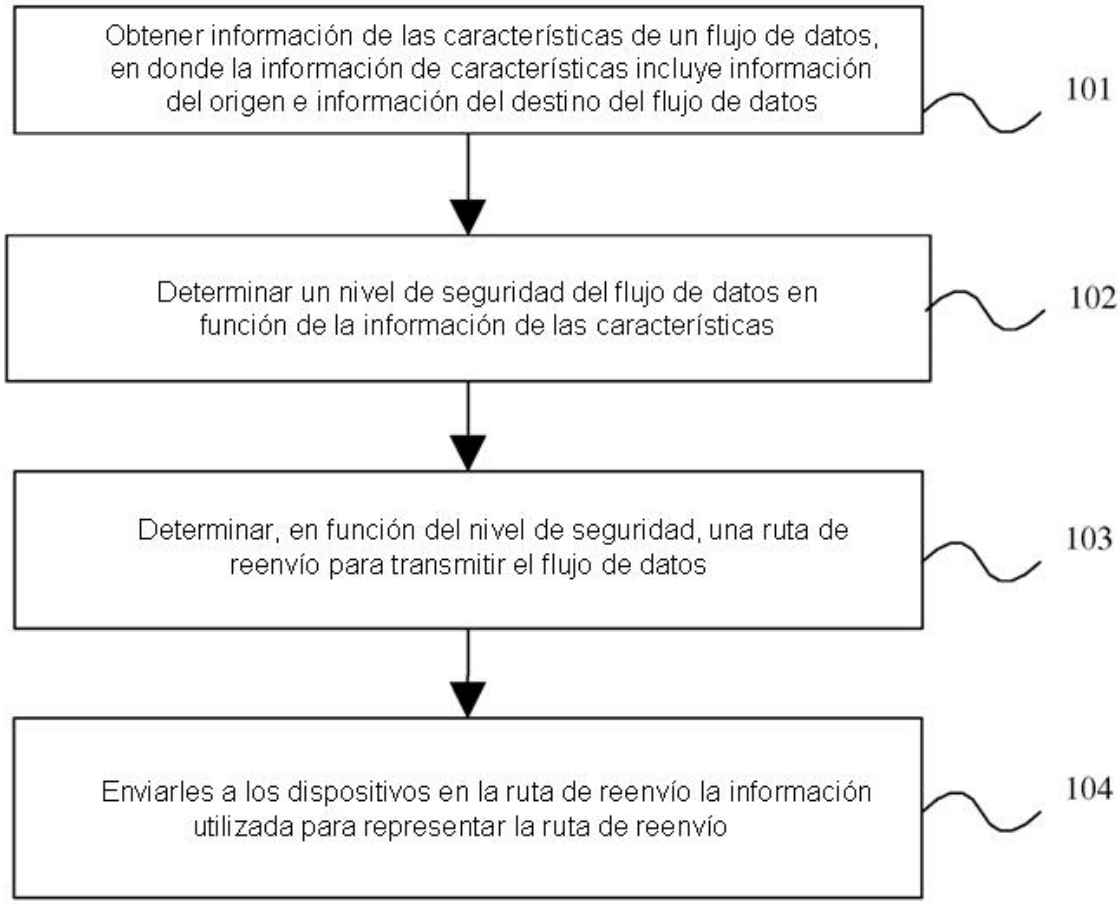
Obtener información de las características de un flujo de datos, en donde la información de características incluye información del origen e información del destino del flujo de datos
101
Determinar un nivel de seguridad del flujo de datos en función de la información de las características
102
Determinar, en función del nivel de seguridad, una ruta de reenvío para transmitir el flujo de datos
103
Enviarles a los dispositivos en la ruta de reenvío la información utilizada para representar la ruta de reenvío
104

FIG. 1A

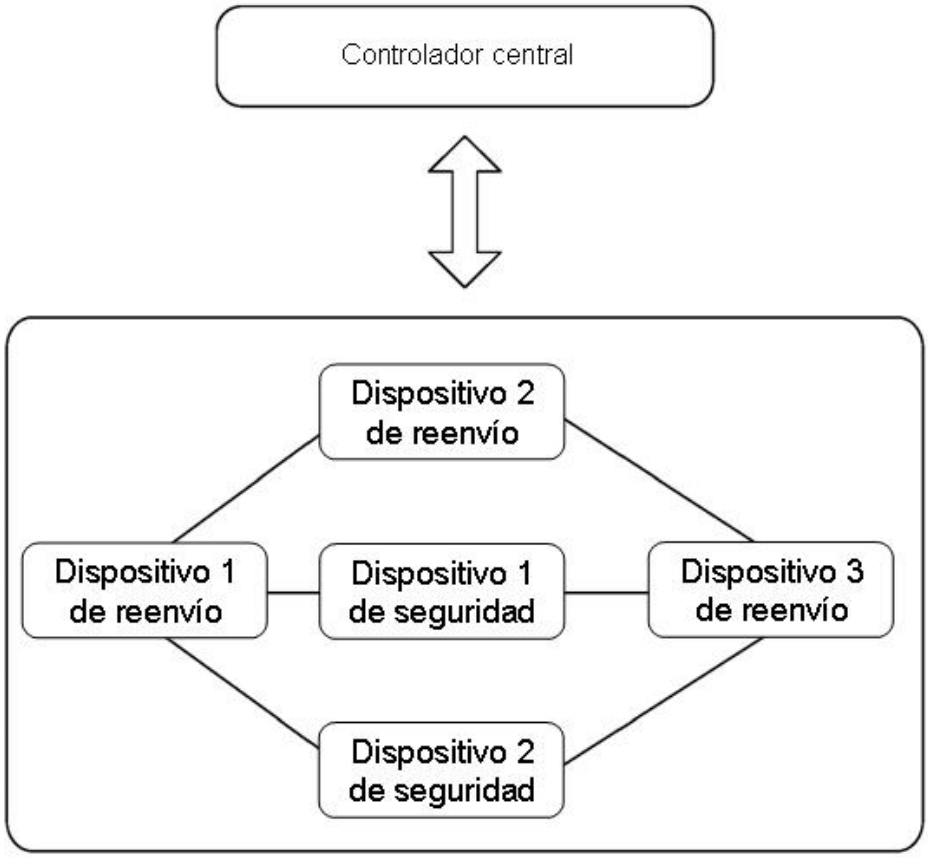
Controlador central
Dispositivo 2 de reenvío
Dispositivo 1 de reenvío
Dispositivo 1 de seguridad
Dispositivo 3 de reenvío
Dispositivo 2 de seguridad

FIG. 1B

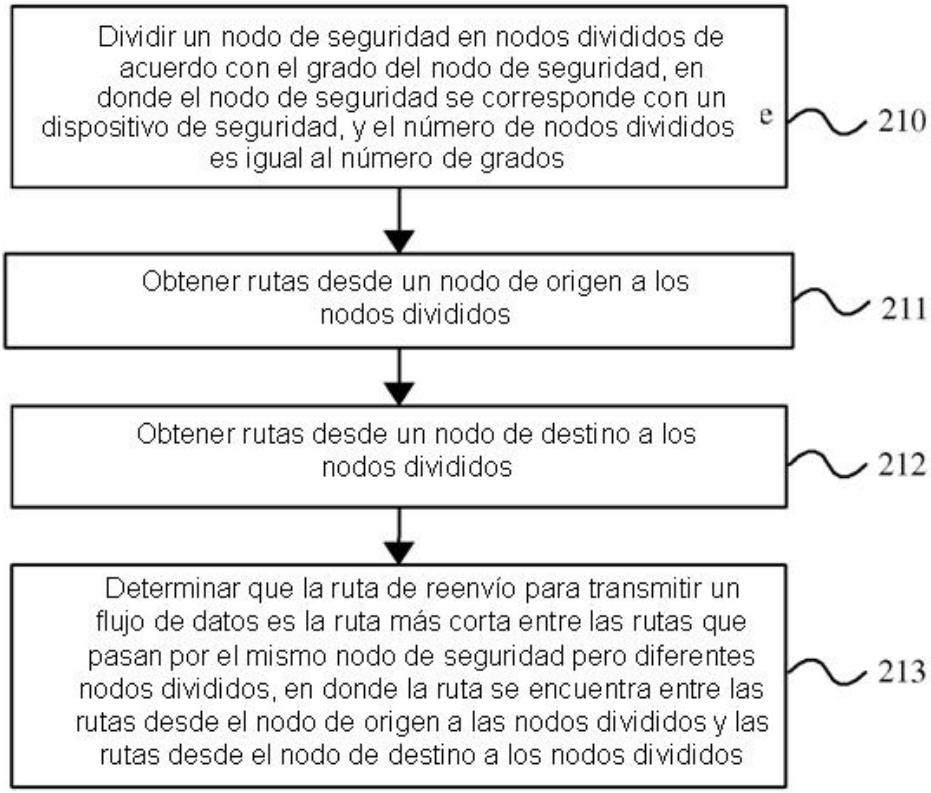
Dividir un nodo de seguridad en nodos divididos de acuerdo con el grado del nodo de seguridad, en donde el nodo de seguridad se corresponde con un dispositivo de seguridad, y el número de nodos divididos es igual al número de grados
e
210
Obtener rutas desde un nodo de origen a los nodos divididos
211
Obtener rutas desde un nodo de destino a los nodos divididos
212
Determinar que la ruta de reenvío para transmitir un flujo de datos es la ruta más corta entre las rutas que pasan por el mismo nodo de seguridad pero diferentes nodos divididos, en donde la ruta se encuentra entre las rutas desde el nodo de origen a las nodos divididos y las rutas desde el nodo de destino a los nodos divididos
213

FIG. 2A

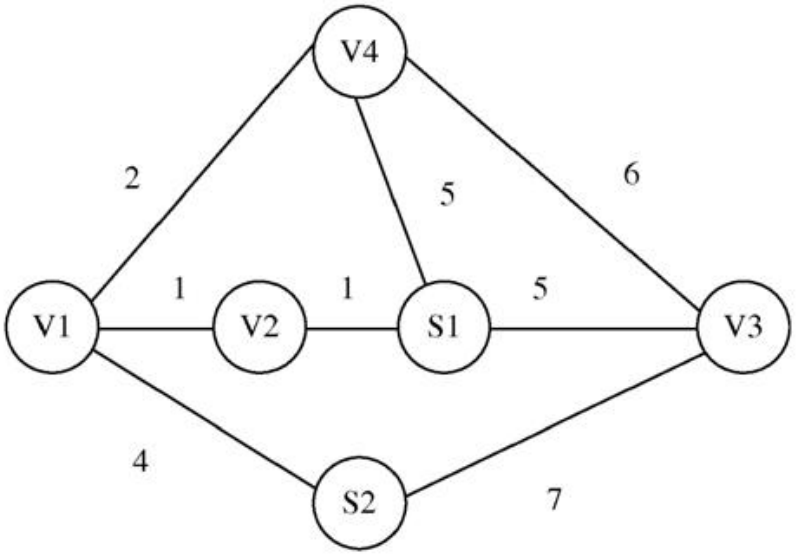
V4
2
5
6
1
1
5
V1
V2
S1
V3
4
S2
7

FIG. 2B

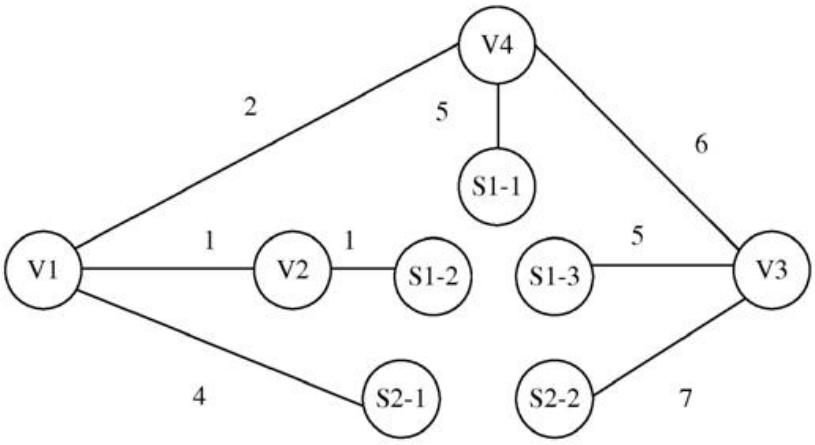

FIG. 2C

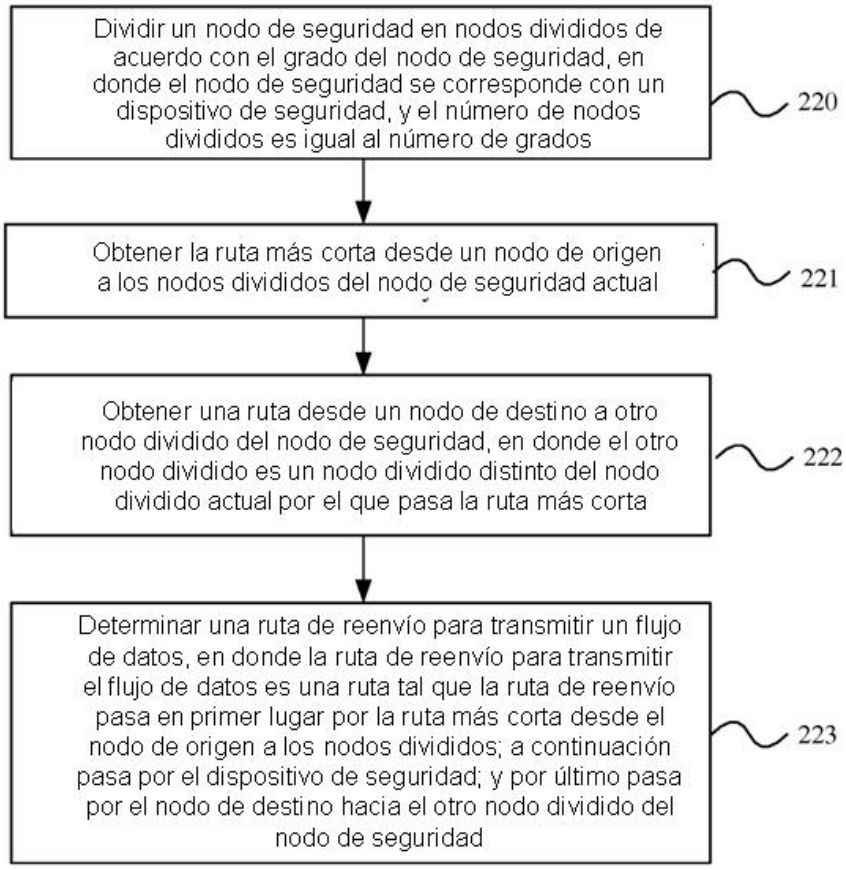
Dividir un nodo de seguridad en nodos divididos de acuerdo con el grado del nodo de seguridad, en donde el nodo de seguridad se corresponde con un dispositivo de seguridad, y el número de nodos divididos es igual al número de grados
220
Obtener la ruta más corta desde un nodo de origen a los nodos divididos del nodo de seguridad actual
221
Obtener una ruta desde un nodo de destino a otro nodo dividido del nodo de seguridad, en donde el otro nodo dividido es un nodo dividido distinto del nodo dividido actual por el que pasa la ruta más corta
222
Determinar una ruta de reenvío para transmitir un flujo de datos, en donde la ruta de reenvío para transmitir el flujo de datos es una ruta tal que la ruta de reenvío pasa en primer lugar por la ruta más corta desde el nodo de origen a los nodos divididos; a continuación pasa por el dispositivo de seguridad; y por último pasa por el nodo de destino hacia el otro nodo dividido del nodo de seguridad
223

FIG. 2D

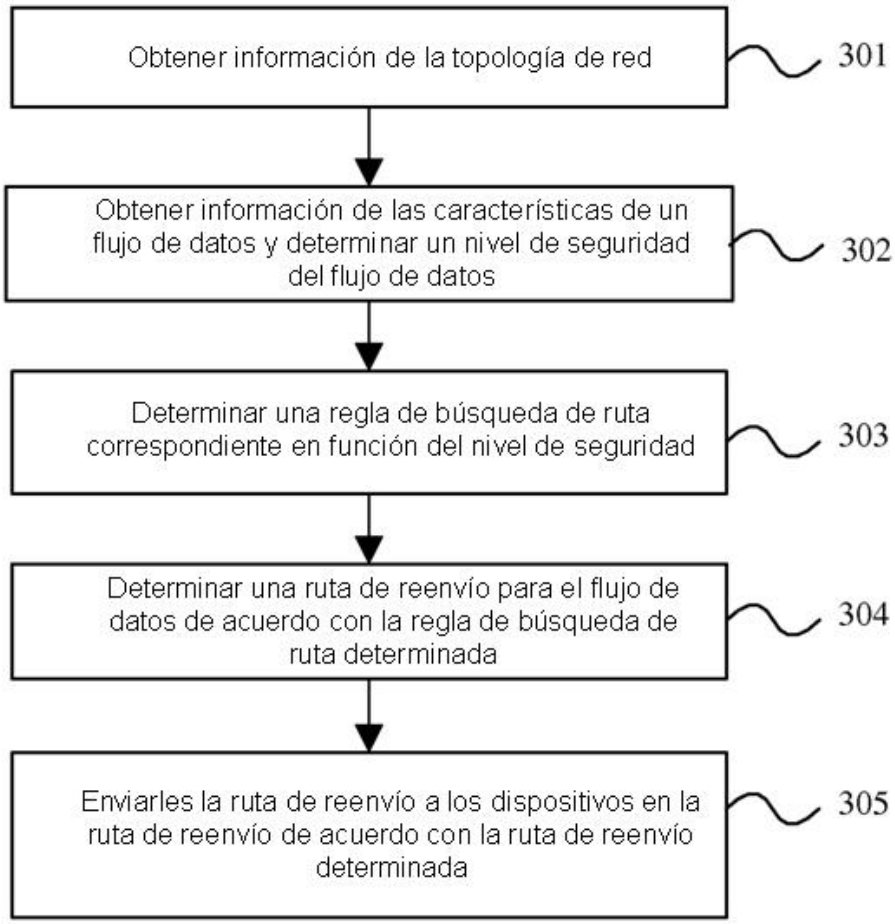
Obtener información de la topología de red
301
Obtener información de las características de un flujo de datos y determinar un nivel de seguridad del flujo de datos
302
Determinar una regla de búsqueda de ruta correspondiente en función del nivel de seguridad
303
Determinar una ruta de reenvío para el flujo de datos de acuerdo con la regla de búsqueda de ruta determinada
304
Enviarles la ruta de reenvío a los dispositivos en la ruta de reenvío de acuerdo con la ruta de reenvío determinada
305

FIG. 3

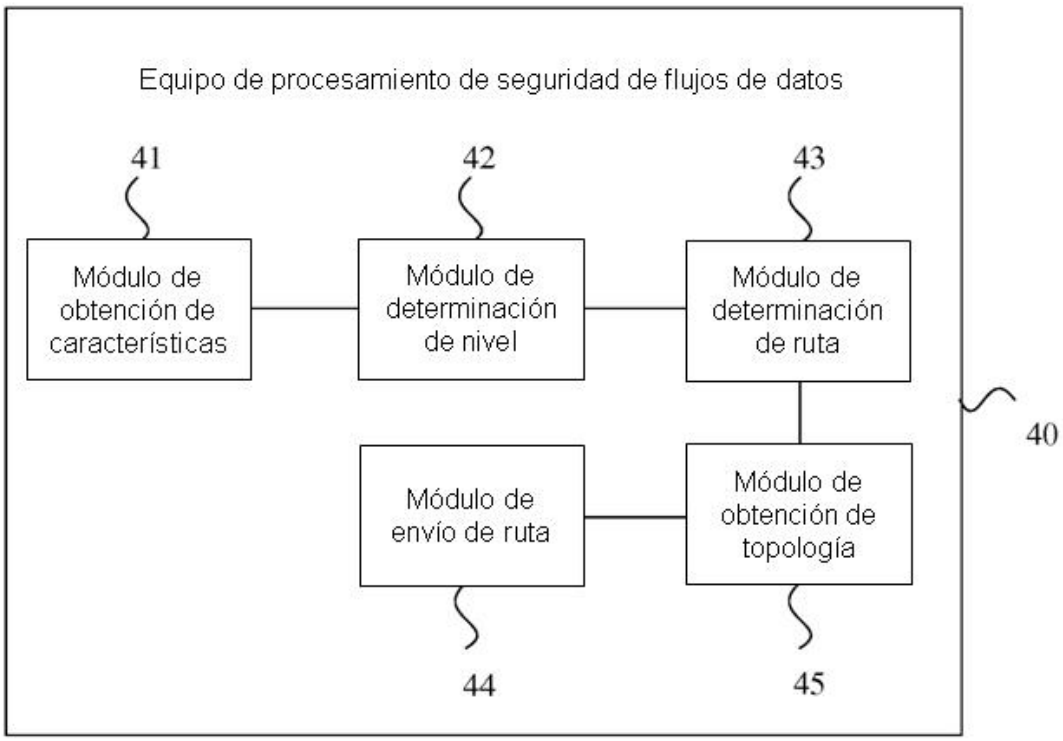
Equipo de procesamiento de seguridad de flujos de datos
41
42
43
Módulo de obtención de características
Módulo de determinación de nivel
Módulo de determinación de ruta
40
Módulo de envío de ruta
Módulo de obtención de topología
44
45

FIG. 4