(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 833 402**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 12/741 (2013.01)
G06F 9/455 (2008.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **06.12.2015 PCT/CN2015/096509**

(87) Fecha y número de publicación internacional: **30.06.2016 WO16101783**

(96) Fecha de presentación y número de la solicitud europea: **06.12.2015 E 15871852 (8)**

(97) Fecha y número de publicación de la concesión europea: **23.09.2020 EP 3226508**

(54) Título: **Método, aparato y sistema de procesamiento de paquete de datos de ataque**

(30) Prioridad:

22.12.2014 CN 201410810857

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
15.06.2021

(73) Titular/es:

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

(72) Inventor/es:

YU, QINGHUA y
YANG, XINHUA

(74) Agente/Representante:

ELZABURU, S.L.P

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Método, aparato y sistema de procesamiento de paquete de datos de ataque

Campo técnico

La presente invención se refiere al campo de las tecnologías de las comunicaciones y, en particular, a un método, un aparato y un sistema de procesamiento de paquetes de datos de ataque.

Antecedentes

Con el rápido desarrollo de las tecnologías en la nube, surgen cantidades cada vez mayores de problemas en la aplicación de las tecnologías en la nube. Por ejemplo, un servidor en un centro de datos en la nube (un servidor en la nube para abreviar) puede ser atacado por varios paquetes de datos de ataque durante la comunicación del Protocolo de Internet (IP), por ejemplo, por un ataque de denegación de servicio distribuido (DDoS) y un ataque de mensaje fraudulento. Por lo tanto, el procesamiento de un paquete de datos de ataque para asegurar una comunicación segura para el servidor en la nube se convierte en una de las tecnologías centrales de las tecnologías en la nube.

Actualmente, una forma común de procesamiento de paquetes de datos de ataque es la siguiente: mediante el despliegue de un firewall físico en un servidor en la nube de entrada en un centro de datos en la nube o al desplegar un firewall virtual en un hipervisor que se ejecuta en cada servidor en la nube en un centro de datos en la nube, se asegura que todos los paquetes de datos que esperan entrar al servidor en la nube se someten a filtrados y reenvíos por el firewall físico/virtual; por lo tanto, se filtra un paquete de datos de ataque y se impide que el paquete de datos de ataque entre al servidor en la nube, asegurando por ello que el servidor en la nube pueda realizar una comunicación segura. Específicamente, según una política de seguridad configurada para el firewall físico/virtual por el personal de trabajo, el firewall físico/virtual identifica la señalización de la capa IP transportada por un paquete de datos que espera entrar a una capa IP. Cuando la señalización de la capa IP no cumple con la política de seguridad, el firewall físico/virtual filtra el paquete de datos, lo que impide que un paquete de datos de ataque, ataque el servidor en la nube, y además asegura que el servidor en la nube pueda realizar una comunicación segura. El documento de la técnica anterior “Building secure telco clouds Achieving resilience with your trusted partner Nokia Networks”, 18 de octubre de 2014, http://networks.nokia.com/sites/default/files/document/nokia_telco_security_white_paper_0.pdf como por la versión del 18 de octubre de 2014, describe que una solución de seguridad implementada por una aplicación SDN. Esta solución pretende proporcionar protección contra ataques DDoS. El documento de la técnica anterior US 2013/311675 A1 describe un sistema informático capaz de proporcionar realimentación a un controlador en una red definida por software. El documento de la técnica anterior WO 2016/000160 A1 describe una solución de la que al menos se tiene una política de seguridad de un creador de políticas en un controlador en una red SDN.

Sin embargo, en el método anterior para impedir, mediante el uso de un firewall, que un paquete de datos de ataque entre a un servidor en la nube, solamente se puede usar el firewall para impedir que el paquete de datos de ataque entre al servidor de la nube, y un conmutador responsable del reenvío de un paquete de datos al firewall aún puede reenviar el paquete de datos de ataque al firewall, es decir, el paquete de datos de ataque todavía se transmite en una red. Por lo tanto, el paquete de datos anormal ocupa una gran cantidad de ancho de banda de la red y afecta la transmisión de un paquete de datos normal.

Compendio

La presente invención se define mediante las reivindicaciones independientes adjuntas, en donde se definen realizaciones adicionales en las reivindicaciones dependientes. Proporciona un método, un aparato y un sistema de procesamiento de paquetes de datos de ataque, que puede limitar el ancho de banda de la red ocupado por un paquete de datos de ataque cuando el paquete de datos de ataque se transmite en una red y asegurar la transmisión de un paquete de datos normal.

Las realizaciones de la presente invención proporcionan el método, aparato y sistema de procesamiento de paquetes de datos de ataque, donde el método es específicamente: la recepción, por un nodo de gestión, de información de descripción de un paquete de datos de ataque y un tipo de ataque del paquete de datos de ataque, donde el la información de descripción y el tipo de ataque son enviados por un nodo de conocimiento; la determinación de una política de procesamiento en el paquete de datos de ataque del tipo de ataque según el tipo de ataque; y el envío de la información de descripción y la política de procesamiento a un conmutador usando un controlador SDN, de manera que el conmutador realice una operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción, donde la política de procesamiento se utiliza para indicarle al conmutador que realice la operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción. Según el método, aparato y sistema de procesamiento de paquetes de datos de ataque, proporcionados en la presente invención, después de que el nodo de conocimiento identifique un paquete de datos recibido por el nodo de conocimiento como el paquete de datos de ataque y envíe la información de descripción del paquete de datos de ataque y el tipo de ataque del paquete de datos de ataque al nodo de gestión, el nodo de gestión puede determinar la política de procesamiento en el paquete de datos de ataque del tipo de ataque según el tipo de ataque y envíe la información de descripción y la política de procesamiento al conmutador utilizando el controlador SDN, de manera que el conmutador realice la operación indicada por la política de procesamiento en el paquete de datos de ataque con la

información de descripción. Por lo tanto, se limita el ancho de banda de la red ocupado por el paquete de datos de ataque con la información de descripción cuando el paquete de datos de ataque con la información de descripción se transmite en una red y se asegura la transmisión de un paquete de datos normal; además, un nodo de conocimiento en un centro de datos en la nube evita ser atacado continuamente por el paquete de datos de ataque con la información de descripción, asegurando por ello que el nodo de conocimiento en el centro de datos en la nube pueda realizar una comunicación segura.

Breve descripción de los dibujos

Para describir las soluciones técnicas en las realizaciones de la presente invención más claramente, a continuación se introducen brevemente los dibujos adjuntos requeridos para describir las realizaciones o la técnica anterior. Aparentemente, los dibujos adjuntos en la siguiente descripción son simplemente algunos, pero no todos, los dibujos adjuntos de las realizaciones de la presente invención.

La fig. 1 es un diagrama de bloques 1 de un sistema de comunicaciones según una realización de la presente invención;

La fig. 2 es un diagrama de flujo 1 de un método de procesamiento de paquetes de datos de ataque según una realización de la presente invención;

La fig. 3 es un diagrama de flujo 2 de un método de procesamiento de paquetes de datos de ataque según una realización de la presente invención;

La fig. 4 es un diagrama esquemático de una tabla de flujo de un primer conmutador según una realización de la presente invención;

La fig. 5 es un diagrama de flujo 3 de un método de procesamiento de paquetes de datos de ataque según una realización de la presente invención;

La fig. 6 es un diagrama de interacción 1 de un método de procesamiento de paquetes de datos de ataque según una realización de la presente invención;

La fig. 7 es un diagrama de interacción 2 de un método de procesamiento de paquetes de datos de ataque según una realización de la presente invención;

La fig. 8A y la fig. 8B son un diagrama de interacción 3 de un método de procesamiento de paquetes de datos de ataque según una realización de la presente invención;

La fig. 9 es un diagrama de bloques 2 de un sistema de comunicaciones según una realización de la presente invención;

La fig. 10 es un diagrama de bloques 3 de un sistema de comunicaciones según una realización de la presente invención;

La fig. 11 es un diagrama estructural esquemático de un nodo de gestión según una realización de la presente invención;

La fig. 12 es un diagrama estructural esquemático de un controlador SDN según una realización de la presente invención;

La fig. 13 es un diagrama estructural esquemático de un nodo de conocimiento según una realización de la presente invención;

La fig. 14 es un diagrama estructural de hardware esquemático de un nodo de gestión según una realización de la presente invención;

La fig. 15 es un diagrama estructural de hardware esquemático de un controlador SDN según una realización de la presente invención;

La fig. 16 es un diagrama estructural de hardware esquemático de un nodo de conocimiento según una realización de la presente invención;

La fig. 17 es un diagrama de bloques 4 de un sistema de comunicaciones según una realización de la presente invención; y

La fig. 18 es un diagrama de bloques 5 de un sistema de comunicaciones según una realización de la presente invención.

Descripción de las realizaciones

A continuación se describen claramente las soluciones técnicas en las realizaciones de la presente invención con referencia a los dibujos adjuntos en las realizaciones de la presente invención. Aparentemente, las realizaciones descritas son simplemente algunas, pero no todas, las realizaciones de la presente invención.

En las realizaciones de la presente invención, un nodo de conocimiento puede ser cualquier servidor en la nube que esté en un centro de datos en la nube y pueda identificar un paquete de datos de ataque, por ejemplo, varias máquinas virtuales (VM) de procesamiento de servicios, un hipervisor, un firewall, un balanceador de carga o una puerta de enlace. Un nodo de gestión puede ser cualquier nodo de gestión de servicios o nodo de gestión de políticas en un centro de datos en la nube, por ejemplo, un administrador de VM, un administrador de infraestructura virtualizada (VIM) o una unidad de función de políticas y cobros (PCRF).

Un método de procesamiento de paquetes de datos de ataque proporcionado en las realizaciones de la presente invención puede aplicarse a una arquitectura de red que se basa en una tecnología de redes definidas por software (SDN). La arquitectura de red que se basa en la tecnología SDN es una arquitectura de red directamente programable que desacopla el control del reenvío. En la arquitectura de red que se basa en la tecnología SDN, un trayecto de reenvío específico y una política de reenvío de cada paquete de datos en una red son controladas ambos por un controlador SDN, el controlador SDN envía el trayecto de reenvío y la política de reenvío del paquete de datos a un grupo de conmutadores en la arquitectura SDN utilizando un protocolo OpenFlow, y un conmutador en el grupo de conmutadores reenvía el paquete de datos a un servidor en la nube en un centro de datos en la nube. El conmutador en la arquitectura de red que se basa en la tecnología SDN solamente es responsable del reenvío del paquete de datos según la política de reenvío y el trayecto de reenvío del paquete de datos.

A modo de ejemplo, la fig. 1 muestra un diagrama de bloques de un sistema de comunicaciones según una realización de la presente invención. Como se muestra en la fig. 1, un centro de datos tiene tres VM y un administrador de VM. En la arquitectura de red que se basa en la tecnología SDN, tanto para la transmisión de paquetes de datos realizada entre las tres VM en el centro de datos y un servidor fuera del centro de datos como para la transmisión de paquetes de datos realizada entre las tres VM, un trayecto de reenvío y una política de reenvío de un paquete de datos son controlados por un controlador SDN, y un conmutador implementa el reenvío del paquete de datos.

Las realizaciones de la presente invención proporcionan un método de procesamiento de paquetes de datos de ataque. Controlando un conmutador para procesar un paquete de datos de ataque, el reenvío del paquete de datos de ataque por el conmutador puede limitarse y, por lo tanto, se limita el ancho de banda de la red ocupado por el paquete de datos de ataque cuando el paquete de datos de ataque se transmite en una red, asegurando por ello la transmisión de un paquete de datos normal, y además asegurando que un servidor en la nube en un centro de datos en la nube pueda realizar una comunicación segura.

Realización 1

Una realización de la presente invención proporciona un método de procesamiento de paquetes de datos de ataque. Como se muestra en la fig. 2, el método puede incluir las siguientes etapas.

S101. Un nodo de gestión recibe información de descripción de un paquete de datos de ataque y un tipo de ataque del paquete de datos de ataque, donde la información de descripción y el tipo de ataque se envían mediante un nodo de conocimiento.

El paquete de datos de ataque puede comprenderse como un paquete de datos que representa una amenaza para el nodo de conocimiento, por ejemplo, un paquete de datos con formato incorrecto, un paquete de datos con una excepción de fragmentación de paquetes, un paquete de datos que utiliza una conexión inválida de Protocolo de control de Transmisión (TCP), y un paquete de datos con un volumen de datos extra grande.

Opcionalmente, la información de descripción del paquete de datos de ataque puede ser información obtenida por el nodo de conocimiento a partir de un encabezado de paquete del paquete de datos de ataque, y puede ser específicamente una dirección IP de origen del paquete de datos de ataque, una dirección IP de destino del paquete de datos de ataque, un número de puerto de origen del paquete de datos de ataque, un número de puerto de destino del paquete de datos de ataque y un número de protocolo del paquete de datos de ataque. El número de puerto de origen del paquete de datos de ataque puede ser específicamente un número de puerto de origen del protocolo de datagramas de usuario (UDP), y el número de puerto de destino del paquete de datos de ataque puede ser específicamente un número de puerto de destino UDP; o el número de puerto de origen del paquete de datos de ataque puede ser específicamente un número de puerto de origen TCP, y el número de puerto de destino del paquete de datos de ataque puede ser específicamente un número de puerto de destino TCP. Utilizando la información de descripción, un conmutador puede procesar el paquete de datos de ataque con la información de descripción.

El tipo de ataque del paquete de datos de ataque puede incluir, pero no está limitado a, un ataque DDoS, un ataque basado en el Protocolo de Inicio de Sesión (SIP), una conexión TCP inválida, un volumen de datos extra grande, un ataque de mensaje fraudulento y similares.

S102. El nodo de gestión determina una política de procesamiento en el paquete de datos de ataque del tipo de ataque según el tipo de ataque, donde la política de procesamiento se utiliza para indicarle a un conmutador que realice una operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción.

La política de procesamiento puede incluir una acción de procesamiento en el paquete de datos de ataque, por ejemplo, caída, tasa de acceso comprometida (CAR) o redirección. Alternativamente, la política de procesamiento puede incluir una acción de procesamiento en el paquete de datos de ataque y un momento para realizar la acción de procesamiento. El momento para la realización de la acción de procesamiento puede ser específicamente: la realización inmediata de la acción de procesamiento, la realización de la acción de procesamiento después de un retraso, la realización de la acción de procesamiento para una cierta duración, o similares.

Además, en esta realización de la presente invención, existen múltiples formas en las que el nodo de gestión determina la política de procesamiento del paquete de datos de ataque del tipo de ataque según el tipo de ataque. El hecho de que el nodo de gestión determina la política de procesamiento en el paquete de datos de ataque del tipo de ataque según el tipo de ataque se describe a modo de ejemplo utilizando las siguientes dos formas de implementación posibles (Modo 1 y Modo 2). El Modo 2 no se ha reivindicado y representa información de contexto.

Modo 1: En esta realización de la presente invención, el nodo de gestión puede obtener una política de procesamiento predeterminada en el paquete de datos de ataque del tipo de ataque según el tipo de ataque. Específicamente, se puede predeterminar una relación de correspondencia entre un tipo de ataque y una política de procesamiento en el nodo de gestión. Cuando se recibe un tipo de ataque, el nodo de gestión puede determinar, a partir de la relación de correspondencia predeterminada según el tipo de ataque, una política de procesamiento correspondiente al tipo de ataque, es decir, se determina la política de procesamiento en el paquete de datos de ataque del tipo de ataque.

Por ejemplo, se supone que la relación de correspondencia, predeterminada en el nodo de gestión, entre un tipo de ataque y una política de procesamiento se puede mostrar en la Tabla 1. La política de procesamiento en la Tabla 1 incluye una acción de procesamiento en un paquete de datos de ataque. "Car + 1 Mbps" indica la realización de una operación de velocidad de acceso comprometida en un paquete de datos de ataque con un volumen de datos extra grande, de manera que el ancho de banda máximo utilizado por el paquete de datos después de la operación de velocidad de acceso comprometida es de 1 Mbps. "Redirect + null0" indica la realización de una operación de redireccionamiento en un paquete de datos de ataque de un tipo de ataque basado en SIP, de manera que el paquete de datos de ataque se reenvía a una interfaz null0, donde la interfaz null0 indica una interfaz de enrutamiento de agujero negro, todos los paquetes de datos reenviados a la interfaz null0 se eliminan, y el reenvío del paquete de datos de ataque a la interfaz null0 tiene poco impacto en la carga de la red. Específicamente, por ejemplo, cuando el tipo de ataque recibido por el nodo de gestión es el ataque DDoS, una política de procesamiento en un paquete de datos de ataque de un tipo de ataque DDoS puede determinarse como "drop" ("descartar") según la Tabla 1.

Tabla 1

Tipo de ataque	Política de procesamiento
Ataque DDoS	Descartar
Volumen de datos extra grande	Car+1 Mbps
Ataque basado en SIP	Redirect+null0

Opcionalmente, la política de procesamiento en la Tabla 1 precedente puede incluir una acción de procesamiento y un momento para realizar la acción de procesamiento. Por ejemplo, una política de procesamiento correspondiente al ataque DDoS puede estar predeterminada para "Drop+immediately" ("Descartar+inmediatamente"), lo que indica la realización inmediata de una operación de descarte de un paquete de datos de ataque del tipo de ataque DDoS; y una política de procesamiento correspondiente al ataque basado en SIP puede ser "Redirect+null0+immediately+duration180", lo que indica la realización inmediata de una operación de redireccionamiento en un paquete de datos de ataque del tipo de ataque basado en SIP, de manera que el paquete de datos de ataque se reenvíe inmediatamente a la interfaz null0, y el reenvío se realiza continuamente durante 180 minutos.

Debería observarse que en un proceso de implementación específico, se puede establecer una relación de correspondencia adecuada entre un tipo de ataque y una política de procesamiento en el nodo de gestión según un requisito de ingeniería real, que no está limitado en la presente invención.

Modo 2: el nodo de gestión genera una política de procesamiento en el paquete de datos de ataque del tipo de ataque según el tipo de ataque y un algoritmo predeterminado. Específicamente, puede predeterminarse un algoritmo en el nodo de gestión. Cuando se recibe un tipo de ataque, el nodo de gestión genera la política de procesamiento en el paquete de datos de ataque del tipo de ataque realizando el procedimiento de algoritmo predeterminado para el tipo de ataque.

De manera ejemplar, cuando el tipo de ataque recibido por el nodo de gestión es el ataque DDoS, el nodo de gestión

calcula el código del tipo de ataque utilizando el algoritmo predeterminado y genera una política de procesamiento "drop" (“descarte”) en el paquete de datos de ataque del tipo de ataque; o cuando el tipo de ataque recibido por el nodo de gestión es el ataque basado en SIP, el nodo de gestión calcula el código del tipo de ataque utilizando el algoritmo predeterminado y genera una política de procesamiento "Redirect + null0" en el paquete de datos de ataque del tipo de ataque.

Debería observarse que en un proceso de implementación específico, se puede establecer un algoritmo adecuado en el nodo de gestión según un requisito de ingeniería real.

S103. El nodo de gestión envía la información de descripción y la política de procesamiento a un conmutador utilizando un controlador SDN, de manera que el conmutador realice una operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción.

A modo de ejemplo, se supone que la información de descripción, recibida por el nodo de gestión, del paquete de datos de ataque es específicamente "[10.11.100.100,10.22.200.200,6,1234,4321]", donde 10.11.100.100 indica una dirección IP de origen del paquete de datos de ataque, 10.22.200.200 indica una dirección IP de destino del paquete de datos de ataque, 1234 indica un número de puerto de origen del paquete de datos de ataque, 4321 indica un número de puerto de destino del paquete de datos de ataque y un número de protocolo del paquete de datos de ataque es 6. El tipo de ataque, recibido por el nodo de gestión, del paquete de datos de ataque es el ataque DDoS, y una política de procesamiento que está en el paquete de datos de ataque y se determina según el tipo de ataque es "Drop+imediately" (“Descartar+inmediatamente”). El nodo de gestión puede envíe la información de descripción y la política de procesamiento al controlador SDN en un formato "[10.11.100.100,10.22.200.200,6,1234,4321] + Drop + immediately". El controlador SDN reenvía el "[10.11.100.100,10.22.200.200,6,1234,4321] + Drop + immediately" recibido al conmutador en un formato especificado por un protocolo Open Flow.

Después de la recepción de la información de descripción y la política de procesamiento, el conmutador descarta inmediatamente los datos de ataque con la información de descripción según la política de procesamiento. De esta manera, el conmutador ya no reenvía el paquete de datos de ataque, de manera que el paquete de datos de ataque no se transmite en una red, es decir, el paquete de datos de ataque con la información de descripción no ocupa ancho de banda de red, asegurando por ello la transmisión de un paquete de datos normal.

Se puede comprender que si la política de procesamiento que está en el paquete de datos de ataque y se determina por el nodo de gestión según el tipo de ataque es "Car+1 Mbps", después de que el nodo de gestión envía la información de descripción y la política de procesamiento al conmutador utilizando el controlador SDN, el conmutador realiza una operación de velocidad de acceso comprometida en el paquete de datos de ataque con la información de descripción, de manera que cuando se transmite en una red, el paquete de datos de ataque con la información de descripción ocupa un ancho de banda máximo de 1 Mbps. Es decir, incluso aunque el conmutador todavía reenvía el paquete de datos de ataque, el paquete de datos de ataque ocupa un ancho de banda máximo de 1 Mbps cuando se transmite en la red. Por lo tanto, se limita el ancho de banda de la red ocupado por el paquete de datos de ataque con la información de descripción cuando el paquete de datos de ataque con la información de descripción se transmite en una red y se asegura la transmisión de un paquete de datos normal.

Además, un proceso en el que el conmutador realiza la operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción se describe en detalle en la siguiente realización, y los detalles no se describen adicionalmente en la presente memoria.

Esta realización de la presente invención proporciona un método de procesamiento de paquetes de datos de ataque, que es específicamente: la recepción, mediante un nodo de gestión, de información de descripción de un paquete de datos de ataque y un tipo de ataque del paquete de datos de ataque, donde la información de descripción y el tipo de ataque se envían mediante un nodo de conocimiento; la determinación de una política de procesamiento en el paquete de datos de ataque del tipo de ataque según el tipo de ataque; y el envío de la información de descripción y la política de procesamiento a un conmutador utilizando un controlador SDN, de manera que el conmutador realice una operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción, donde la política de procesamiento se utiliza para indicarle al conmutador que realice la operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción. Según el método, después de que el nodo de conocimiento identifique un paquete de datos recibido por el nodo de conocimiento como el paquete de datos de ataque y envíe la información de descripción del paquete de datos de ataque y el tipo de ataque del paquete de datos de ataque al nodo de gestión, el nodo de gestión puede determinar la política de procesamiento en el paquete de datos de ataque del tipo de ataque según el tipo de ataque y envíe la información de descripción y la política de procesamiento al conmutador utilizando el controlador SDN, de manera que el conmutador realice la operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción. Por lo tanto, se limita el ancho de banda de la red ocupado por el paquete de datos de ataque con la información de descripción cuando el paquete de datos de ataque con la información de descripción se transmite en una red y se asegura la transmisión de un paquete de datos normal; además, un nodo de conocimiento en un centro de datos en la nube evita ser atacado continuamente por el paquete de datos de ataque con la información de descripción, asegurando por ello que el nodo de conocimiento en el centro de datos en la nube pueda realizar una comunicación segura.

Una realización de la presente invención proporciona un método de procesamiento de paquetes de datos de ataque. Como se muestra en la fig. 3, el método puede incluir las siguientes etapas.

S201. Un controlador SDN recibe información de descripción de un paquete de datos de ataque y una política de procesamiento en el paquete de datos de ataque con la información de descripción, donde la información de descripción y la política de procesamiento se envían mediante un nodo de gestión.

Para la información de descripción del paquete de datos de ataque y la política de procesamiento en el paquete de datos de ataque con la información de descripción, se puede hacer referencia específicamente a una descripción relacionada en la realización mostrada en la fig. 2, y los detalles no se describen adicionalmente en la presente memoria.

S202. El controlador SDN envía la información de descripción y la política de procesamiento a un primer conmutador, de manera que el primer conmutador realiza una operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción.

El primer conmutador es cualquier conmutador en un grupo de conmutadores controlado por el controlador SDN.

Específicamente, el controlador SDN puede convertir la información de descripción y la política de procesamiento en un mensaje de controlador a conmutador y enviar el mensaje de controlador a conmutador al primer conmutador. El mensaje de controlador a conmutador es un tipo de mensaje que se especifica mediante un protocolo de Open Flow y el controlador SDN lo envía al conmutador para indicarle al conmutador que modifique o descarte la información registrada en una tabla de flujo del conmutador.

Después de que el controlador SDN convierta la información de descripción y la política de procesamiento en el mensaje de controlador a conmutador y envíe el mensaje de controlador a conmutador al primer conmutador, el primer conmutador busca, según la información de descripción incluida en el mensaje de controlador a conmutador, una tabla de flujo del primer conmutador para un flujo de datos de ataque que coincide con la información de descripción, y a continuación realiza la operación indicada por la política de procesamiento en un paquete de datos de ataque en el flujo de datos de ataque según la política de procesamiento incluida en el mensaje de controlador a conmutador, es decir, el controlador SDN realiza la operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción según la política de procesamiento.

La fig. 4 muestra un diagrama esquemático de una tabla de flujo de un primer conmutador según una realización de la presente invención. En la Fig. 4, la tabla de flujo del primer conmutador incluye un campo de encabezado de paquete, un contador y una acción realizada en un paquete de datos. El campo de encabezado de paquete puede incluir específicamente una dirección IP de origen, una dirección IP de destino, una dirección de control de acceso a medios (MAC) de origen, una dirección MAC de destino, un número de protocolo, un número de puerto de origen, un número de puerto de destino y similares, que son del flujo de datos recibido por el primer conmutador. El contador está configurado para recoger estadísticas en una cantidad de paquetes de datos, una cantidad de bytes, la duración de la transmisión y similares que son del flujo de datos recibido por el primer conmutador. La acción realizada en el paquete de datos puede incluir el reenvío del paquete de datos, el descarte del paquete de datos, la modificación de la información en un encabezado de paquete de un paquete de datos en la tabla de flujo y similares.

A modo de ejemplo, suponiendo que la información de descripción y la política de procesamiento que se reciben por el controlador SDN son "[10.11.100.100,10.22.200.200,6,1234,4321] + Drop + immediately", después de que el controlador SDN envía el "[10.11 .100.100,10.22.200.200,6,1234,4321] + Drop + immediately" al primer conmutador en un formato especificado por un protocolo Open Flow, el primer conmutador busca en la tabla de flujo del primer conmutador un flujo de datos de ataque cuya dirección IP de origen es 10.11.100.100, la dirección IP de destino es 10.22.200.200, el número de puerto de origen es 1234, el número de puerto de destino es 4321 y el número de protocolo es 6. Después de que el primer conmutador encuentre el flujo de datos de ataque, según la política de procesamiento, una acción realizada en un paquete de datos de ataque del flujo de datos de ataque se descarta específicamente de inmediato. Es decir, el primer conmutador realiza la operación de descartar inmediatamente en un paquete de datos de ataque con la información de descripción "[10.11.100.100,10.22.200.200,6,1234,4321]".

Debería observarse que cada flujo de datos almacenado en la tabla de flujo del primer conmutador tiene información de descripción única y una acción realizada en un paquete de datos en cada flujo de datos. Después de que se complete la transmisión de todos los paquetes de datos en un flujo de datos, la tabla de flujo elimina un registro del flujo de datos. Por lo tanto, en el método de procesamiento de paquetes de datos de ataque proporcionado en esta realización de la presente invención, un primer conmutador puede buscar, según la información de descripción y una política de procesamiento que son enviadas por un controlador SDN, una tabla de flujo para un flujo de datos de ataque con la información de descripción, y cambiar una acción realizada en un paquete de datos de ataque en el flujo de datos de ataque a una operación indicada por la política de procesamiento, con el objetivo de realizar la operación indicada por la política de procesamiento en un paquete de datos de ataque que no se transmite en los paquetes de datos de ataque en el flujo de datos de ataque. Además, un nodo de conocimiento en un centro de datos en la nube evita ser atacado continuamente por el paquete de datos de ataque en el flujo de datos de ataque.

Esta realización de la presente invención proporciona un método de procesamiento de paquetes de datos de ataque,

que es específicamente: la recepción, mediante un controlador SDN, de información de descripción de un paquete de datos de ataque y una política de procesamiento en el paquete de datos de ataque con la información de descripción, donde la información de descripción y la política de procesamiento se envían mediante un nodo de gestión; y el envío de la información de descripción y la política de procesamiento a un primer conmutador, de manera que el primer conmutador realice una operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción. Según el método, después de que un nodo de conocimiento identifique un paquete de datos recibido por el nodo de conocimiento como un paquete de datos de ataque y envíe información de descripción del paquete de datos de ataque y un tipo de ataque del paquete de datos de ataque a un nodo de gestión, el nodo de gestión determina una política de procesamiento en el paquete de datos de ataque del tipo de ataque según el tipo de ataque y envía la información de descripción y la política de procesamiento a un conmutador utilizando un controlador SDN, de manera que el conmutador realice una operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción. Por lo tanto, se limita el ancho de banda de la red ocupado por el paquete de datos de ataque con la información de descripción cuando el paquete de datos de ataque con la información de descripción se transmite en una red y se asegura la transmisión de un paquete de datos normal; Además, un nodo de conocimiento en un centro de datos en la nube evita ser atacado continuamente por el paquete de datos de ataque con la información de descripción, asegurando por ello que un servidor en la nube en el centro de datos en la nube pueda realizar una comunicación segura.

Una realización de la presente invención proporciona un método de procesamiento de paquetes de datos de ataque. Como se muestra en la fig. 5, el método puede incluir las siguientes etapas.

S301. Un nodo de conocimiento identifica un paquete de datos recibido por el nodo de conocimiento como un paquete de datos de ataque.

Existen múltiples formas en las que el nodo de conocimiento identifica el paquete de datos recibido por el nodo de conocimiento como el paquete de datos de ataque, y un método para identificar, por el nodo de conocimiento, el paquete de datos de ataque se describe a modo de ejemplo utilizando los siguientes tres ejemplos.

Ejemplo 1: después de la recepción de un paquete de datos, el nodo de conocimiento identifica un paquete del paquete de datos recibido por el nodo de conocimiento, y si el nodo de conocimiento determina que una dirección IP de origen y una dirección IP de destino que son del paquete de datos son la misma, el nodo de conocimiento determina que el paquete del paquete de datos es un paquete con formato incorrecto y determina que el paquete de datos es un paquete de datos de ataque.

Ejemplo 2: Después de que el nodo de conocimiento reciba un paquete de datos, si el nodo de conocimiento determina dentro de un momento predeterminado que un volumen de tráfico de paquetes del paquete de datos recibido por el nodo de conocimiento excede un umbral predeterminado, el nodo de conocimiento determina que el paquete de datos es un paquete de datos de ataque.

Ejemplo 3: Después de la recepción de un paquete de datos, el nodo de conocimiento identifica la señalización SIP en el paquete de datos y determina si un proceso de sesión SIP del paquete de datos es el mismo que un proceso de sesión SIP en un estándar conocido. Si el nodo de conocimiento determina que el proceso de sesión SIP del paquete de datos es diferente del proceso de sesión SIP en el estándar conocido, el nodo de conocimiento determina que el paquete de datos es un paquete de datos de ataque.

Además, otras formas en las que un nodo de conocimiento identifica un paquete de datos recibido por el nodo de conocimiento como un paquete de datos de ataque son las mismas formas que en la técnica anterior en las que el nodo de conocimiento identifica un paquete de datos recibido por el nodo de conocimiento como un paquete de datos de ataque, y no se enumeran uno por uno en la presente memoria.

Debería observarse que en esta realización de la presente invención, un nodo de conocimiento puede ser cualquier nodo de servicio que esté en un centro de datos en la nube y pueda identificar un paquete de datos de ataque, por ejemplo, una VM, un hipervisor, un firewall, un balanceador de carga, o una puerta de enlace. Por lo tanto, en comparación con la técnica anterior en la que un paquete de datos de ataque se identifica mediante la identificación de la señalización de la capa IP utilizando un firewall, esta realización de la presente invención proporciona el método de procesamiento de paquetes de datos de ataque en el que un nodo de conocimiento no solamente puede identificar un paquete de datos de ataque mediante la identificación de la señalización de la capa IP (por ejemplo, identifica un paquete de datos de ataque mediante la identificación de un paquete con formato incorrecto), sino que también identifica un paquete de datos de ataque mediante la identificación de la señalización de la capa de servicio (por ejemplo, identifica un paquete de datos de ataque de un tipo de ataque basado en SIP mediante identificación de señalización SIP). De esta manera, se mejora la precisión de identificación del paquete de datos de ataque y, además, se impide de manera más completa un ataque del paquete de datos de ataque al nodo de conocimiento.

S302. El nodo de conocimiento determina la información de descripción del paquete de datos de ataque y un tipo de ataque del paquete de datos de ataque.

A modo de ejemplo, si el nodo de conocimiento identifica que el paquete del paquete de datos recibido por el nodo de conocimiento es el paquete con formato incorrecto, y ya que un ataque de paquete con formato incorrecto pertenece

a un tipo de ataque DDoS, el nodo de conocimiento puede determinar que el tipo de ataque del paquete de datos de ataque es el ataque DDoS; o si el nodo de conocimiento identifica, mediante la identificación de información SIP, el paquete de datos recibido por el nodo de conocimiento como el paquete de datos de ataque, el nodo de conocimiento puede determinar que un tipo de ataque del paquete de datos es un ataque basado en SIP; o si el nodo de conocimiento determina que un volumen de tráfico de paquetes del paquete de datos recibido por el nodo de conocimiento excede un umbral predeterminado, el nodo de conocimiento identifica el paquete de datos como el paquete de datos de ataque, de manera que el nodo de conocimiento puede determinar que el tipo de ataque del paquete de datos es un ataque de gran volumen de datos.

Además, después de que el nodo de conocimiento determine que el paquete de datos recibido por el nodo de conocimiento es el paquete de datos de ataque, el nodo de conocimiento obtiene la información de descripción del paquete de datos de ataque del paquete de datos de ataque. Opcionalmente, la información de descripción del paquete de datos de ataque puede ser específicamente una dirección IP de origen del paquete de datos de ataque, una dirección IP de destino del paquete de datos de ataque, un número de puerto de origen del paquete de datos de ataque, un número de puerto de destino del paquete de datos de ataque y un número de protocolo del paquete de datos de ataque.

S303. El nodo de conocimiento envía la información de descripción y el tipo de ataque a un nodo de gestión, donde el nodo de gestión utiliza el tipo de ataque para determinar una política de procesamiento en el paquete de datos de ataque del tipo de ataque, y la política de procesamiento se utiliza para indicarle a un conmutador que reenvíe un paquete de datos para realizar una operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción.

Para un proceso en el que el nodo de gestión determina la política de procesamiento en el paquete de datos de ataque del tipo de ataque, se puede hacer referencia específicamente a una descripción relacionada en la realización mostrada en la fig. 2; para un proceso en el que el conmutador realiza la operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción según la política de procesamiento, se puede hacer referencia específicamente a una descripción relacionada en la realización mostrada en la fig. 3, y los detalles no se describen adicionalmente en la presente memoria.

Esta realización de la presente invención proporciona un método de procesamiento de paquetes de datos de ataque, que es específicamente: la identificación, mediante un nodo de conocimiento, de un paquete de datos recibido por el nodo de conocimiento como un paquete de datos de ataque; la determinación de la información de descripción del paquete de datos de ataque y un tipo de ataque del paquete de datos de ataque; y el envío de la información de descripción y el tipo de ataque a un nodo de gestión, donde el nodo de gestión utiliza el tipo de ataque para determinar una política de procesamiento en el paquete de datos de ataque del tipo de ataque, y la política de procesamiento se utiliza para indicarle a un conmutador que reenvíe un paquete de datos para realizar una operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción. Según el método, después de que el nodo de conocimiento identifique el paquete de datos recibido por el nodo de conocimiento como el paquete de datos de ataque y envíe la información de descripción del paquete de datos de ataque y el tipo de ataque del paquete de datos de ataque con la información de descripción al nodo de gestión, el nodo de gestión determina la política de procesamiento en el paquete de datos de ataque del tipo de ataque según el tipo de ataque y envía la información de descripción y la política de procesamiento al conmutador utilizando un controlador SDN, de manera que el conmutador realiza una operación indicada por la política de procesamiento del paquete de datos del ataque con la información de descripción. Por lo tanto, se limita el ancho de banda de la red ocupado por el paquete de datos de ataque con la información de descripción cuando el paquete de datos de ataque con la información de descripción se transmite en una red y se asegura la transmisión de un paquete de datos normal; se resuelve un problema en la técnica anterior de que el paquete de datos de ataque ocupa una gran cantidad de ancho de banda de la red y afecta a la transmisión de un paquete de datos normal; además, un nodo de conocimiento en un centro de datos en la nube evita ser atacado continuamente por el paquete de datos de ataque con la información de descripción, asegurando por ello que el nodo de conocimiento en el centro de datos en la nube pueda realizar una comunicación segura.

Realización 2

Una realización de la presente invención proporciona un método de procesamiento de paquetes de datos de ataque. Como se muestra en la fig. 6, el método puede incluir las siguientes etapas.

S401. Un nodo de conocimiento recibe un paquete de datos.

S402. El nodo de conocimiento identifica el paquete de datos como un paquete de datos de ataque.

S403. El nodo de conocimiento determina la información de descripción del paquete de datos de ataque y un tipo de ataque del paquete de datos de ataque.

S404. El nodo de conocimiento envía la información de descripción y el tipo de ataque a un nodo de gestión.

Específicamente, para una forma de implementación específica de las etapas S401 a S404 precedentes, se puede hacer referencia a una descripción relacionada en la realización mostrada en la fig. 5, y los detalles no se describen

adicionalmente en la presente memoria.

S405. Después de la recepción de la información de descripción y el tipo de ataque que envían mediante un nodo de conocimiento, el nodo de gestión determina una política de procesamiento en el paquete de datos de ataque del tipo de ataque según el tipo de ataque.

S406. El nodo de gestión envía la información de descripción y la política de procesamiento a un controlador SDN.

Debería observarse que en esta realización de la presente invención, una interfaz de comunicaciones está preestablecida en el nodo de gestión, y la interfaz de comunicaciones se utiliza por el nodo de gestión para enviar la información de descripción y el tipo de ataque al controlador SDN. Además, una interfaz de comunicaciones está preestablecida en el controlador SDN y se utiliza por el controlador SDN para recibir la información de descripción y el tipo de ataque que envía el nodo de gestión.

Específicamente, si el nodo de gestión y el controlador SDN realizan la interacción de la información utilizando un protocolo UDP, la interfaz de comunicaciones por separado en el nodo de gestión y el controlador SDN se pueden configurar basándose en el protocolo UDP. Cuando se envía la información de descripción y el tipo de ataque al controlador SDN, el nodo de gestión no necesita establecer un enlace de comunicaciones con el controlador SDN y puede enviar directamente la información de descripción y el tipo de ataque al controlador SDN utilizando una dirección de la interfaz de comunicaciones predeterminada en el nodo de gestión y una dirección de la interfaz de comunicaciones predeterminada en el controlador SDN.

Si el nodo de gestión y el controlador SDN realizan la interacción de la información utilizando un protocolo TCP, la interfaz de comunicaciones por separado en el nodo de gestión y el controlador SDN se pueden configurar basándose en el protocolo TCP. Cuando el nodo de gestión envía la información de descripción y el tipo de ataque al controlador SDN, es necesario establecer una conexión TCP entre el nodo de gestión y el controlador SDN para establecer un enlace de comunicaciones entre dos interfaces de comunicaciones predeterminadas, y el nodo de gestión envía la información de descripción y el tipo de ataque al controlador SDN utilizando el enlace de comunicaciones.

S407. El controlador SDN envía la información de descripción y la política de procesamiento a un primer conmutador.

S408. El primer conmutador realiza una operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción.

Específicamente, para una forma de implementación específica de las etapas S407 a S408 precedentes, se puede hacer referencia a una descripción relacionada en la realización mostrada en la fig. 3, y los detalles no se describen adicionalmente en la presente memoria.

Opcionalmente, en la etapa S405 precedente, si el nodo de gestión recibe información de descripción de múltiples paquetes de datos de ataque y tipos de ataque de los múltiples paquetes de datos de ataque, donde la información de descripción y los tipos de ataque se envían mediante múltiples nodos de conocimiento, con referencia a la fig. 6, como se muestra en la fig. 7, la etapa S405 precedente puede incluir específicamente las siguientes etapas:

S405a. El nodo de gestión determina al menos dos tipos de ataque iguales según los tipos de ataque de los múltiples paquetes de datos de ataque.

S405b. El nodo de gestión determina, según uno de los al menos dos tipos de ataque, una política de procesamiento en el paquete de datos de ataque del tipo de ataque.

Específicamente, si el nodo de gestión recibe la información de descripción de los múltiples paquetes de datos de ataque y los tipos de ataque de los múltiples paquetes de datos de ataque, donde la información de descripción y los tipos de ataque se envían mediante múltiples nodos de conocimiento, el nodo de gestión determina, según los tipos de ataque de los múltiples paquetes de datos de ataque, si existen al menos dos tipos de ataque iguales en los tipos de ataque de los múltiples paquetes de datos de ataque. Si el nodo de gestión determina que existen al menos dos tipos de ataque iguales en los tipos de ataque de los múltiples paquetes de datos de ataque, el nodo de gestión determina, según uno de los al menos dos tipos de ataque, una política de procesamiento en el paquete de datos de ataque del tipo de ataque. Es decir, ya que los al menos dos tipos de ataque son iguales, el nodo de gestión determina, según cualquiera de los al menos dos tipos de ataque, una política de procesamiento en el paquete de datos de ataque del tipo de ataque.

Además, el nodo de gestión envía la política de procesamiento con información de descripción de cada uno de al menos dos paquetes de datos de ataque al controlador SDN, es decir, una política de procesamiento correspondiente a la información de descripción de cada uno de los al menos dos paquetes de datos de ataque del mismo tipo de ataque es la política de procesamiento.

Además, después de la etapa S406 precedente, con referencia a la fig. 6, como se muestra en la fig. 8A y en la fig. 8B, el método incluye además las siguientes etapas:

S409. El controlador SDN envía la información de descripción y la política de procesamiento a un controlador SDN

maestro conectado al controlador SDN.

S410. El controlador SDN maestro envía la información de descripción y la política de procesamiento a un segundo conmutador.

S411. El segundo conmutador realiza la operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción.

Debería observarse que una secuencia para las etapas S407 y S409 precedentes no está limitada en esta realización de la presente invención.

Específicamente, si tanto una red interna como una red externa de un centro de datos utilizan una arquitectura de red que se basa en una tecnología SDN, después de que un controlador SDN dentro del centro de datos recibe la información de descripción y la política de procesamiento que se envían mediante el nodo de gestión, el controlador SDN reenvía directamente la información de descripción y la política de procesamiento a un controlador SDN maestro. El controlador SDN maestro es un controlador SDN que está fuera del centro de datos y está conectado al controlador SDN, es decir, el controlador SDN maestro es un controlador SDN que está en una red troncal y está conectado al centro de datos. El controlador SDN maestro envía la información de descripción y la política de procesamiento al segundo conmutador en un formato especificado por un protocolo Open Flow. El segundo conmutador es cualquier conmutador en un grupo de conmutadores controlado por el controlador SDN maestro. Después de la recepción de la información de descripción y la política de procesamiento, el segundo conmutador realiza la operación indicada por la política de procesamiento en el paquete de datos con la información de descripción, de manera que el ancho de banda de la red ocupado por el paquete de datos de ataque cuando se transmite el paquete de datos de ataque está limitado una red completa y se asegura la transmisión de un paquete de datos normal.

Para un proceso específico en el que el segundo conmutador realiza la operación indicada por la política de procesamiento en el paquete de datos de ataque, se puede hacer referencia a un proceso específico, en la realización mostrada en la fig. 3, en la que el primer conmutador realiza la operación indicada por la política de procesamiento en el paquete de datos de ataque, y los detalles no se describen adicionalmente en la presente memoria.

Además, a continuación se enumeran dos posibles escenarios de aplicación para describir de manera ejemplar el método de procesamiento de paquetes de datos de ataque proporcionado en esta realización de la presente invención. La fig. 9 muestra un diagrama de bloques de un sistema de comunicaciones según una realización de la presente invención. Cuando el nodo de conocimiento es específicamente una VM en una capa de sistema operativo invitado en un centro de datos en la nube, por ejemplo, una VM en un conmutador virtual (vSwitch), el nodo de conocimiento puede ser una VM2 en un conmutador de VM 2, y cuando el nodo de gestión es específicamente un administrador de VM en el centro de datos en la nube, porque la VM2 puede identificar la señalización de la capa IP en un paquete de datos, la VM2 puede identificar un paquete de datos de ataque cuando la VM2 recibe el paquete de datos de ataque de un tipo de ataque DDoS de capa IP (tal como como un ataque de paquete con formato incorrecto). Por lo tanto, la VM2, el administrador de VM, el controlador SDN y el conmutador que se encuentran en el sistema de comunicaciones mostrado en la fig. 9 pueden procesar un paquete de datos de ataque mediante la realización del método precedente mostrado en la fig. 6 o fig. 7.

La fig. 10 muestra un diagrama de bloques de otro sistema de comunicaciones según una realización de la presente invención. Cuando el nodo de conocimiento es específicamente un hipervisor, por ejemplo, un hipervisor 2, en un centro de datos en la nube, y el nodo de gestión es específicamente un PCRF en el centro de datos en la nube, y ya que el hipervisor 2 puede identificar un paquete de datos de ataque mediante la identificación de la señalización de capa de servicio en un paquete de datos, por ejemplo, identificar un paquete de datos de ataque de un tipo de ataque basado en SIP mediante la identificación de la señalización de SIP, el hipervisor 2 puede identificar el paquete de datos de ataque cuando el hipervisor 2 recibe el paquete de datos de ataque del tipo de ataque basado en SIP. Por lo tanto, el hipervisor 2, el PCRF, el controlador SDN y el conmutador pueden procesar un paquete de datos de ataque mediante la realización del método precedente mostrado en la fig. 6 o fig. 7.

Esta realización de la presente invención proporciona un método de procesamiento de paquetes de datos de ataque, que incluye específicamente: la identificación, mediante un nodo de conocimiento, de un paquete de datos recibido por el nodo de conocimiento como un paquete de datos de ataque; la determinación de la información de descripción del paquete de datos de ataque y un tipo de ataque del paquete de datos de ataque, y el envío de la información de descripción y el tipo de ataque a un nodo de gestión; la determinación, mediante el nodo de gestión según el tipo de ataque, de una política de procesamiento en el paquete de datos de ataque del tipo de ataque; y el envío de la información de descripción y la política de procesamiento a un conmutador utilizando un controlador SDN, de manera que el conmutador realice una operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción, donde la política de procesamiento se utiliza para indicarle al conmutador que realice la operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción. Según el método, puede limitarse el ancho de banda de la red ocupado por el paquete de datos de ataque cuando el paquete de datos de ataque se transmite en una red, y se asegura la transmisión de un paquete de datos normal; se resuelve un problema en la técnica anterior de que el paquete de datos de ataque ocupa una gran cantidad de ancho de banda de la red y afecta a la transmisión de un paquete de datos normal; Además, un nodo de

conocimiento en un centro de datos en la nube evita ser atacado continuamente por el paquete de datos de ataque con la información de descripción, asegurando por ello que un servidor en la nube en el centro de datos en la nube pueda realizar una comunicación segura.

Realización 3

Como se muestra en la fig. 11, esta realización de la presente invención proporciona un nodo de gestión, y el nodo de gestión puede incluir:

una unidad 10 de recepción, configurada para recibir información de descripción de un paquete de datos de ataque y un tipo de ataque del paquete de datos de ataque, donde la información de descripción y el tipo de ataque se envían mediante un nodo de conocimiento;

una unidad 11 de determinación, configurada para determinar una política de procesamiento en el paquete de datos de ataque del tipo de ataque según el tipo de ataque recibido por la unidad 10 de recepción, donde la política de procesamiento se utiliza para indicarle a un conmutador que realice una operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción; y

una unidad 12 de envío, configurada para enviar la información de descripción recibida por la unidad 10 de recepción y la política de procesamiento determinada por la unidad 11 de determinación al conmutador utilizando un controlador SDN de red definido por software, de manera que el conmutador realice la operación indicada por la política de procesamiento del paquete de datos del ataque con la información de descripción.

Opcionalmente, la unidad 11 de determinación está configurada específicamente para obtener una política de procesamiento predeterminada en el paquete de datos de ataque del tipo de ataque según el tipo de ataque recibido por la unidad 10 de recepción.

Opcionalmente, la unidad 11 de determinación está configurada específicamente para generar una política de procesamiento en el paquete de datos de ataque del tipo de ataque según el tipo de ataque recibido por la unidad 10 de recepción y un algoritmo predeterminado.

Opcionalmente, la operación indicada por la política de procesamiento determinada por la unidad 11 de determinación incluye: una acción de procesamiento en el paquete de datos de ataque con la información de descripción, o una acción de procesamiento en el paquete de datos de ataque con la información de descripción y un momento para realizar la acción de procesamiento.

Opcionalmente, la unidad 11 de determinación está configurada específicamente para: cuando la unidad 10 de recepción recibe información de descripción de múltiples paquetes de datos de ataque y tipos de ataque de los paquetes de datos de ataque, donde la información de descripción y los tipos de ataque se envían por múltiples nodos de conocimiento, determinar al menos dos tipos de ataque iguales según los tipos de ataque de los múltiples paquetes de datos de ataque, y determinar, según uno de los al menos dos tipos de ataque, una política de procesamiento en el paquete de datos de ataque del tipo de ataque.

Opcionalmente, la unidad 12 de envío está configurada específicamente para enviar la información de descripción recibida por la unidad 10 de recepción y la política de procesamiento determinada por la unidad 11 de determinación al controlador SDN utilizando una interfaz de comunicaciones predeterminada, de manera que el controlador SDN reenvíe la información de descripción y la política de procesamiento al conmutador.

Opcionalmente, la información de descripción recibida por la unidad 10 de recepción incluye: una dirección IP de Protocolo de Internet de origen del paquete de datos de ataque, un número de puerto de origen del paquete de datos de ataque, una dirección IP de destino del paquete de datos de ataque, un número de puerto de destino del paquete de datos de ataque y un número de protocolo del paquete de datos de ataque.

Debería observarse que el nodo de gestión proporcionado en esta realización de la presente invención puede ser cualquier nodo de gestión de servicios o nodo de gestión de políticas en un centro de datos en la nube, por ejemplo, un administrador de VM, un VIM, un PCRF, o similar.

Esta realización de la presente invención proporciona un nodo de gestión, donde el nodo de gestión puede recibir información de descripción de un paquete de datos de ataque y un tipo de ataque del paquete de datos de ataque, donde la información de descripción y el tipo de ataque se envían mediante un nodo de conocimiento, determinar una política de procesamiento en el paquete de datos de ataque del tipo de ataque según el tipo de ataque y enviar la información de descripción y la política de procesamiento a un conmutador utilizando un controlador SDN, de manera que el conmutador realice una operación indicada por la política de procesamiento en el ataque paquete de datos con la información de descripción, donde la política de procesamiento se utiliza para indicarle al conmutador que realice la operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción. Por lo tanto, después de que el nodo de conocimiento identifique un paquete de datos recibido por el nodo de conocimiento como el paquete de datos de ataque y envíe la información de descripción del paquete de datos de ataque y el tipo de ataque del paquete de datos de ataque al nodo de gestión, el nodo de gestión proporcionado en

este realización de la presente invención puede determinar la política de procesamiento del paquete de datos de ataque del tipo de ataque según el tipo de ataque y enviar la información de descripción y la política de procesamiento al conmutador utilizando el controlador SDN, de manera que el conmutador realice la operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción. Por lo tanto, se limita el ancho de banda de la red ocupado por el paquete de datos de ataque con la información de descripción cuando el paquete de datos de ataque con la información de descripción se transmite en una red y se asegura la transmisión de un paquete de datos normal; además, un nodo de conocimiento en un centro de datos en la nube evita ser atacado continuamente por el paquete de datos de ataque con la información de descripción, asegurando por ello que el nodo de conocimiento en el centro de datos en la nube pueda realizar una comunicación segura.

Como se muestra en la FIG. 12, esta realización de la presente invención proporciona un controlador SDN, y el controlador SDN puede incluir:

una unidad 20 de recepción, configurada para recibir información de descripción de un paquete de datos de ataque y una política de procesamiento en el paquete de datos de ataque con la información de descripción, donde la información de descripción y la política de procesamiento se envían mediante un nodo de gestión; y

una unidad 21 de envío, configurada para enviar la información de descripción y la política de procesamiento que son recibidas por la unidad 20 de recepción a un primer conmutador, de manera que el primer conmutador realiza una operación indicada por la política de procesamiento en el paquete de datos de ataque con la descripción información.

Opcionalmente, la unidad 20 de recepción está configurada específicamente para recibir, utilizando una interfaz de comunicaciones predeterminada, la información de descripción y la política de procesamiento que se envían mediante el nodo de gestión.

Opcionalmente, la unidad 21 de envío está configurada además para enviar la información de descripción y la política de procesamiento que son recibidas por la unidad 20 de recepción a un controlador SDN maestro, de manera que el controlador SDN maestro reenvía la información de descripción y la política de procesamiento a un segundo conmutador, y el segundo conmutador realiza la operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción.

Esta realización de la presente invención proporciona un controlador SDN, donde el controlador SDN puede recibir información de descripción de un paquete de datos de ataque y una política de procesamiento en el paquete de datos de ataque con la información de descripción, donde la información de descripción y la política de procesamiento se envían mediante un nodo de gestión, y enviar la información de descripción y la política de procesamiento a un primer conmutador, de manera que el primer conmutador realice una operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción. Por lo tanto, después de que un nodo de conocimiento identifique un paquete de datos recibido por el nodo de conocimiento como un paquete de datos de ataque y envíe información de descripción del paquete de datos de ataque y un tipo de ataque del paquete de datos de ataque al nodo de gestión, el nodo de gestión determina una política de procesamiento en el paquete de datos de ataque del tipo de ataque según el tipo de ataque y envía la información de descripción y la política de procesamiento a un conmutador utilizando el controlador SDN proporcionado en esta realización de la presente invención, de manera que el conmutador realice una operación indicada por la política de procesamiento del paquete de datos del ataque con la información de descripción. Por lo tanto, se limita el ancho de banda de la red ocupado por el paquete de datos de ataque con la información de descripción cuando el paquete de datos de ataque con la información de descripción se transmite en una red y se asegura la transmisión de un paquete de datos normal; además, un nodo de conocimiento en un centro de datos en la nube evita ser atacado continuamente por el paquete de datos de ataque con la información de descripción, asegurando por ello que el nodo de conocimiento en el centro de datos en la nube pueda realizar una comunicación segura.

Como se muestra en la FIG. 13, esta realización de la presente invención proporciona un nodo de conocimiento, y el nodo de conocimiento puede incluir:

una unidad 30 de identificación, configurada para identificar un paquete de datos recibido por el nodo de conocimiento como un paquete de datos de ataque;

una unidad 31 de determinación, configurada para determinar la información de descripción del paquete de datos de ataque identificado por la unidad 30 de identificación y un tipo de ataque del paquete de datos de ataque; y

una unidad 32 de envío, configurada para enviar la información de descripción y el tipo de ataque que son determinados por la unidad 31 de determinación a un nodo de gestión, donde el tipo de ataque se utiliza por el nodo de gestión para determinar una política de procesamiento en el paquete de datos de ataque del tipo de ataque y la política de procesamiento se utiliza para indicarle a un conmutador que reenvíe un paquete de datos para que realice una operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción.

Opcionalmente, la información de descripción determinada por la unidad 31 de determinación incluye: una dirección IP de Protocolo de Internet de origen del paquete de datos de ataque, un número de puerto de origen del paquete de

datos de ataque, una dirección IP de destino del paquete de datos de ataque, un número de puerto de destino del paquete de datos de ataque y un número de protocolo del paquete de datos de ataque.

Debería observarse que el nodo de conocimiento proporcionado en esta realización de la presente invención puede ser cualquier servidor en la nube que esté en un centro de datos en la nube y pueda identificar un paquete de datos de ataque, por ejemplo, varias VM de procesamiento de servicios, un hipervisor, un firewall, un balanceador de carga o una puerta de enlace.

Esta realización de la presente invención proporciona un nodo de conocimiento, donde el nodo de conocimiento puede identificar un paquete de datos recibido por el nodo de conocimiento como un paquete de datos de ataque, determinar información de descripción del paquete de datos de ataque y un tipo de ataque del paquete de datos de ataque, y enviar la información de descripción y el tipo de ataque a un nodo de gestión, donde el nodo de gestión utiliza el tipo de ataque para determinar una política de procesamiento en el paquete de datos de ataque del tipo de ataque, y la política de procesamiento se utiliza para indicarle a un conmutador que reenvíe un paquete de datos para que realice una operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción. Por lo tanto, después de que el nodo de conocimiento proporcionado en esta realización de la presente invención identifique el paquete de datos recibido por el nodo de conocimiento como el paquete de datos de ataque y envíe la información de descripción del paquete de datos de ataque y el tipo de ataque del paquete de datos de ataque con la información de descripción al nodo de gestión, el nodo de gestión determina la política de procesamiento en el paquete de datos de ataque del tipo de ataque según el tipo de ataque y envía la información de descripción y la política de procesamiento al conmutador utilizando un controlador SDN, de manera que el conmutador realiza una operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción. Por lo tanto, se limita el ancho de banda de la red ocupado por el paquete de datos de ataque con la información de descripción cuando el paquete de datos de ataque con la información de descripción se transmite en una red y se asegura la transmisión de un paquete de datos normal; además, un nodo de conocimiento en un centro de datos en la nube evita ser atacado continuamente por el paquete de datos de ataque con la información de descripción, asegurando por ello que el nodo de conocimiento en el centro de datos en la nube pueda realizar una comunicación segura.

Realización 4

Como se muestra en la fig. 14, esta realización de la presente invención proporciona un nodo de gestión, y el nodo de gestión puede incluir: un procesador 40, una interfaz 41 de comunicaciones, una memoria 42 y un bus 43 de sistema. El procesador 40, la interfaz 41 de comunicaciones y la memoria 42 están conectados y completan la comunicación entre sí utilizando el bus 43 de sistema.

El procesador 40 puede ser una unidad central de procesamiento (CPU) o un circuito integrado específico de aplicación (ASIC), o uno o más circuitos integrados configurados para implementar esta realización de la presente invención.

La interfaz 41 de comunicaciones está configurada para interactuar con otro dispositivo, por ejemplo, interactuar con un nodo de conocimiento o interactuar con un controlador SDN.

La memoria 42 puede incluir una memoria volátil, por ejemplo, una memoria de acceso aleatorio (RAM); o la memoria 42 puede incluir una memoria no volátil, por ejemplo, una memoria de sólo lectura (ROM), una memoria flash, una unidad de disco duro (HDD) o una unidad de estado sólido (SSD); o la memoria 42 puede incluir una combinación de los tipos de memorias precedentes.

Cuando se ejecuta el nodo de gestión, el procesador 40, la interfaz 41 de comunicaciones y la memoria 42 pueden realizar un procedimiento del método descrito en la fig. 2 o cualquiera de las figs. 6 a la fig. 8A y fig. 8B, que incluye específicamente:

El procesador 40 está configurado para: utilizando la interfaz 41 de comunicaciones, recibir información de descripción de un paquete de datos de ataque y un tipo de ataque del paquete de datos de ataque, donde la información de descripción y el tipo de ataque se envían mediante un nodo de conocimiento, determinar una política de procesamiento en el paquete de datos de ataque del tipo de ataque según el tipo de ataque, y enviar la información de descripción y la política de procesamiento a un conmutador utilizando un controlador SDN, de manera que el conmutador realice una operación indicada por la política de procesamiento en los datos del ataque paquete con la información de descripción, donde la política de procesamiento se utiliza para indicarle al conmutador que realice la operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción. La memoria 42 está configurada para almacenar el código de la información de descripción, el código del tipo de ataque y el código de la política de procesamiento, y un programa de software que controla el procesador 40 para completar el proceso precedente, de manera que el procesador 40 completa el proceso precedente ejecutando el programa de software e invocando el código de la información de descripción, el código del tipo de ataque y el código de la política de procesamiento.

Opcionalmente, el procesador 40 está configurado específicamente para obtener una política de procesamiento predeterminada en el paquete de datos de ataque del tipo de ataque según el tipo de ataque.

Opcionalmente, el procesador 40 está configurado específicamente para generar una política de procesamiento en el paquete de datos de ataque del tipo de ataque según el tipo de ataque y un algoritmo predeterminado.

Opcionalmente, la operación indicada por la política de procesamiento determinada por el procesador 40 incluye:

una acción de procesamiento en el paquete de datos de ataque con la información de descripción, o una acción de procesamiento en el paquete de datos de ataque con la información de descripción y un momento para realizar la acción de procesamiento.

Opcionalmente, el procesador 40 está configurado específicamente para: cuando la interfaz 41 de comunicaciones recibe información de descripción de múltiples paquetes de datos de ataque y tipos de ataque de los múltiples paquetes de datos de ataque, donde la información de descripción y los tipos de ataque se envían mediante múltiples nodos de conocimiento, determinar al menos dos tipos de ataque iguales según los tipos de ataque de los múltiples paquetes de datos de ataque, y determinar, según uno de los al menos dos tipos de ataque, una política de procesamiento en el paquete de datos de ataque del tipo de ataque.

Opcionalmente, el procesador 40 está configurado específicamente para enviar la información de descripción y la política de procesamiento al controlador SDN utilizando una interfaz de comunicaciones predeterminada, de manera que el controlador SDN reenvía la información de descripción y la política de procesamiento al conmutador.

Opcionalmente, la información de descripción recibida por el procesador 40 utilizando la interfaz 41 de comunicaciones incluye: una dirección IP de Protocolo de Internet de origen del paquete de datos de ataque, un número de puerto de origen del paquete de datos de ataque, una dirección IP de destino del paquete de datos de ataque, un número de puerto de destino del paquete de datos de ataque y un número de protocolo del paquete de datos de ataque.

Esta realización de la presente invención proporciona un nodo de gestión, donde el nodo de gestión puede recibir información de descripción de un paquete de datos de ataque y un tipo de ataque del paquete de datos de ataque, donde la información de descripción y el tipo de ataque se envían mediante un nodo de conocimiento, determinar una política de procesamiento en el paquete de datos de ataque del tipo de ataque según el tipo de ataque y enviar la información de descripción y la política de procesamiento a un conmutador utilizando un controlador SDN, de manera que el conmutador realice una operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción, donde la política de procesamiento se utiliza para indicarle al conmutador que realice la operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción. Por lo tanto, después de que el nodo de conocimiento identifique un paquete de datos recibido por el nodo de conocimiento como el paquete de datos de ataque y envíe la información de descripción del paquete de datos de ataque y el tipo de ataque del paquete de datos de ataque al nodo de gestión, el nodo de gestión proporcionado en esta realización de la presente invención puede determinar la política de procesamiento del paquete de datos de ataque del tipo de ataque según el tipo de ataque y enviar la información de descripción y la política de procesamiento al conmutador utilizando el controlador SDN, de manera que el conmutador realice la operación indicada por la política de procesamiento del paquete de datos de ataque con la información de descripción. Por lo tanto, se limita el ancho de banda de la red ocupado por el paquete de datos de ataque con la información de descripción cuando el paquete de datos de ataque con la información de descripción se transmite en una red y se asegura la transmisión de un paquete de datos normal; además, un nodo de conocimiento en un centro de datos en la nube evita ser atacado continuamente por el paquete de datos de ataque con la información de descripción, asegurando por ello que el nodo de conocimiento en el centro de datos en la nube pueda realizar una comunicación segura.

Como se muestra en la FIG. 15, esta realización de la presente invención proporciona un controlador SDN, y el controlador SDN puede incluir: un procesador 50, una interfaz 51 de comunicaciones, una memoria 52 y un bus 53 de sistema. El procesador 50, la interfaz 51 de comunicaciones y la memoria 52 están conectados y completan la comunicación entre sí utilizando el bus 53 de sistema.

El procesador 50 puede ser una CPU o un ASIC, o uno o más circuitos integrados configurados para implementar esta realización de la presente invención.

La interfaz 51 de comunicaciones está configurada para interactuar con otro dispositivo, por ejemplo, interactuar con un nodo de gestión o interactuar con un conmutador.

La memoria 52 puede incluir una memoria volátil, por ejemplo, una RAM; o la memoria 52 puede incluir una memoria no volátil, por ejemplo, una ROM, una memoria flash, un HDD o un SSD; o la memoria 52 puede incluir una combinación de los tipos de memorias precedentes.

Cuando se ejecuta el controlador SDN, el procesador 50, la interfaz 51 de comunicaciones y la memoria 52 pueden realizar un procedimiento del método descrito en la fig. 3 o cualquiera de la fig. 6 a la fig. 8A y fig. 8B, que incluye específicamente:

El procesador 50 está configurado para: utilizando la interfaz 51 de comunicaciones, recibir información de descripción de un paquete de datos de ataque y una política de procesamiento en el paquete de datos de ataque con la información de descripción, donde la información de descripción y la política de procesamiento se envían mediante un nodo de

gestión y enviar la información de descripción y la política de procesamiento a un primer conmutador, de manera que el primer conmutador realice una operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción. La memoria 52 está configurada para almacenar el código de la información de descripción, el código de la política de procesamiento y un programa de software que controla el procesador 50 para completar el proceso precedente, de manera que el procesador 50 completa el proceso precedente ejecutando el programa de software e invocando el código de la información de descripción y el código de la política de procesamiento.

Opcionalmente, el procesador 50 está configurado específicamente para recibir, utilizando una interfaz de comunicaciones predeterminada, la información de descripción y la política de procesamiento que se envían mediante el nodo de gestión.

Opcionalmente, el procesador 50 está configurado además para enviar la información de descripción y la política de procesamiento a un controlador SDN maestro utilizando la interfaz 51 de comunicaciones, de manera que el controlador SDN maestro reenvíe la información de descripción y la política de procesamiento a un segundo conmutador, y el segundo conmutador realiza la operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción.

Esta realización de la presente invención proporciona un controlador SDN, donde el controlador SDN puede recibir información de descripción de un paquete de datos de ataque y una política de procesamiento en el paquete de datos de ataque con la información de descripción, donde la información de descripción y la política de procesamiento se envían mediante un nodo de gestión, y enviar la información de descripción y la política de procesamiento a un primer conmutador, de manera que el primer conmutador realice una operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción. Por lo tanto, después de que un nodo de conocimiento identifique un paquete de datos recibido por el nodo de conocimiento como un paquete de datos de ataque y envíe información de descripción del paquete de datos de ataque y un tipo de ataque del paquete de datos de ataque al nodo de gestión, el nodo de gestión determina una política de procesamiento en el paquete de datos de ataque del tipo de ataque según el tipo de ataque y envía la información de descripción y la política de procesamiento a un conmutador utilizando el controlador SDN proporcionado en esta realización de la presente invención, de manera que el conmutador realice una operación indicada por el política de procesamiento del paquete de datos del ataque con la información de descripción. Por lo tanto, se limita el ancho de banda de la red ocupado por el paquete de datos de ataque con la información de descripción cuando el paquete de datos de ataque con la información de descripción se transmite en una red y se asegura la transmisión de un paquete de datos normal; además, un nodo de conocimiento en un centro de datos en la nube evita ser atacado continuamente por el paquete de datos de ataque con la información de descripción, asegurando por ello que el nodo de conocimiento en el centro de datos en la nube pueda realizar una comunicación segura.

Como se muestra en la fig. 16, esta realización de la presente invención proporciona un nodo de conocimiento, y el nodo de conocimiento puede incluir: un procesador 60, una interfaz 61 de comunicaciones, una memoria 62 y un bus 63 de sistema. El procesador 60, la interfaz 61 de comunicaciones y la memoria 62 están conectados y completan la comunicación entre sí utilizando el bus 63 de sistema.

El procesador 60 puede ser una CPU, un ASIC o uno o más circuitos integrados configurados para implementar esta realización de la presente invención.

La interfaz 61 de comunicaciones está configurada para interactuar con otro dispositivo, por ejemplo, interactuar con otro nodo de conocimiento o interactuar con un nodo de gestión.

La memoria 62 puede incluir una memoria volátil, por ejemplo, una RAM; o la memoria 62 puede incluir una memoria no volátil, por ejemplo, una ROM, una memoria flash, un HDD o un SSD; o la memoria 62 puede incluir una combinación de los tipos de memorias precedentes.

Cuando se ejecuta el nodo de conocimiento, el procesador 60, la interfaz 61 de comunicaciones y la memoria 62 pueden realizar un procedimiento de método descrito en cualquiera de la fig. 5 a la fig. 8A y fig. 8B, que incluye específicamente:

El procesador 60 está configurado para: identificar un paquete de datos recibido por la interfaz 61 de comunicaciones como un paquete de datos de ataque, determinar la información de descripción del paquete de datos de ataque y un tipo de ataque del paquete de datos de ataque, y enviar la información de descripción y el tipo de ataque a un nodo de gestión, donde el tipo de ataque se utiliza por el nodo de gestión para determinar una política de procesamiento en el paquete de datos de ataque del tipo de ataque, y la política de procesamiento se utiliza para indicarle a un conmutador que reenvíe un paquete de datos para realizar una operación indicada por la política de procesamiento del paquete de datos de ataque con la información de descripción. La memoria 62 está configurada para almacenar el código del paquete de datos de ataque, la información de descripción, el tipo de ataque y un programa de software que controla el procesador 60 para completar el proceso precedente, de manera que el procesador 60 completa el proceso precedente ejecutando el programa de software e invocando el código del paquete de datos de ataque, la información de descripción y el tipo de ataque.

Opcionalmente, la información de descripción determinada por el procesador 60 incluye: una dirección IP de Protocolo de Internet de origen del paquete de datos de ataque, un número de puerto de origen del paquete de datos de ataque, una dirección IP de destino del paquete de datos de ataque, un número de puerto de destino del paquete de datos de ataque y un número de protocolo del paquete de datos de ataque.

Esta realización de la presente invención proporciona un nodo de conocimiento, donde el nodo de conocimiento puede identificar un paquete de datos recibido por el nodo de conocimiento como un paquete de datos de ataque, determinar información de descripción del paquete de datos de ataque y un tipo de ataque del paquete de datos de ataque, y enviar la información de descripción y el tipo de ataque a un nodo de gestión, donde el nodo de gestión utiliza el tipo de ataque para determinar una política de procesamiento en el paquete de datos de ataque del tipo de ataque, y la política de procesamiento se utiliza para indicarle a un conmutador que reenvíe un paquete de datos para realizar una operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción. Por lo tanto, después de que el nodo de conocimiento proporcionado en esta realización de la presente invención identifique el paquete de datos recibido por el nodo de conocimiento como el paquete de datos de ataque y envíe la información de descripción del paquete de datos de ataque y el tipo de ataque del paquete de datos de ataque con la información de descripción al nodo de gestión, el nodo de gestión determina la política de procesamiento en el paquete de datos de ataque del tipo de ataque según el tipo de ataque y envíe la información de descripción y la política de procesamiento al conmutador utilizando un controlador SDN, de manera que el conmutador realice una operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción. Por lo tanto, se limita el ancho de banda de la red ocupado por el paquete de datos de ataque con la información de descripción cuando el paquete de datos de ataque con la información de descripción se transmite en una red y se asegura la transmisión de un paquete de datos normal; además, un nodo de conocimiento en un centro de datos en la nube evita ser atacado continuamente por el paquete de datos de ataque con la información de descripción, asegurando por ello que el nodo de conocimiento en el centro de datos en la nube pueda realizar una comunicación segura.

Realización 5

Como se muestra en la fig. 17, esta realización de la presente invención proporciona un sistema de comunicaciones, y el sistema de comunicaciones puede incluir: el nodo de gestión mostrado en la fig. 11, el controlador SDN mostrado en la fig. 12, el nodo de conocimiento mostrado en la fig. 13 y un conmutador; o el sistema de comunicaciones proporcionado en esta realización de la presente invención también puede incluir: el nodo de gestión mostrado en la fig. 14, el controlador SDN mostrado en la fig. 15, el nodo de conocimiento mostrado en la fig. 16 y un conmutador. El conmutador es un conmutador que se encuentra en una arquitectura de red basada en una tecnología SDN y está controlado por un controlador SDN.

En el sistema de comunicaciones proporcionado en esta realización de la presente invención, el nodo de conocimiento puede identificar un paquete de datos recibido por el nodo de conocimiento como un paquete de datos de ataque, determinar información de descripción del paquete de datos de ataque y un tipo de ataque del paquete de datos de ataque, y enviar la información de descripción y el tipo de ataque al nodo de gestión. Después de la recepción de la información de descripción y el tipo de ataque, el nodo de gestión puede determinar una política de procesamiento en el paquete de datos de ataque del tipo de ataque según el tipo de ataque, y enviar la información de descripción y la política de procesamiento al controlador SDN. Después de la recepción de la política de procesamiento y la información de descripción que se envían mediante el nodo de gestión, el controlador SDN envía la información de descripción y la política de procesamiento al conmutador, de manera que el conmutador realiza una operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción.

Opcionalmente, como se muestra en la fig. 18, el sistema de comunicaciones proporcionado en esta realización de la presente invención puede incluir además un controlador SDN maestro y un conmutador que es controlado por el controlador SDN maestro. El controlador SDN maestro es un controlador SDN que está fuera de un centro de datos y está conectado al controlador SDN.

En el sistema de comunicaciones proporcionado en esta realización de la presente invención, después de que el controlador SDN reciba la información de descripción y la política de procesamiento que se envían mediante el nodo de gestión, el controlador SDN reenvía la información de descripción y la política de procesamiento al controlador SDN maestro, el controlador SDN maestro envía la información de descripción y la política de procesamiento al conmutador controlado por el controlador SDN maestro, de manera que el conmutador realice una operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción.

Según el sistema de comunicaciones proporcionado en esta realización de la presente invención, después de que un nodo de conocimiento identifique un paquete de datos recibido por el nodo de conocimiento como un paquete de datos de ataque y envíe información de descripción del paquete de datos de ataque y un tipo de ataque del paquete de datos de ataque a un nodo de gestión, el nodo de gestión puede determinar una política de procesamiento en el paquete de datos de ataque del tipo de ataque según el tipo de ataque y enviar la información de descripción y la política de procesamiento a un conmutador utilizando un controlador SDN, de manera que el conmutador realice una operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción. Por lo tanto, se limita el ancho de banda de la red ocupado por el paquete de datos de ataque con la información de

descripción cuando el paquete de datos de ataque con la información de descripción se transmite en una red y se asegura la transmisión de un paquete de datos normal; además, un nodo de conocimiento en un centro de datos en la nube evita ser atacado continuamente por el paquete de datos de ataque con la información de descripción, asegurando por ello que el nodo de conocimiento en el centro de datos en la nube pueda realizar una comunicación segura.

Un experto en la técnica puede comprender claramente que, con el propósito de una descripción breve y conveniente, la división de los módulos de función precedentes se toma como ejemplo a modo de ilustración. En la aplicación real, las funciones precedentes pueden asignarse a diferentes módulos de función e implementarse según un requisito, es decir, una estructura interna de un aparato se divide en diferentes módulos de función para implementar todas o algunas de las funciones descritas anteriormente. Para un proceso de trabajo específico del sistema, aparato y unidad precedentes, se puede hacer referencia a un proceso correspondiente en las realizaciones del método precedentes, y los detalles no se describen en la presente memoria nuevamente.

En las diversas realizaciones proporcionadas en esta solicitud, debería comprenderse que el sistema, el aparato y el método descritos pueden implementarse de otras maneras. Por ejemplo, la realización del aparato descrito es simplemente ejemplar. Por ejemplo, la división de módulo o unidad es simplemente una división de función lógica y puede ser otra división en la implementación real. Por ejemplo, una pluralidad de unidades o componentes pueden combinarse o integrarse en otro sistema, o algunas características pueden ignorarse o no realizarse. Además, los acoplamientos mutuos mostrados o descritos o acoplamientos directos o conexiones de comunicaciones pueden implementarse utilizando algunas interfaces. Los acoplamientos indirectos o conexiones de comunicaciones entre los aparatos o unidades pueden implementarse en manera electrónica, mecánica o de otra forma.

Las unidades descritas como partes separadas pueden estar o no físicamente separadas, y las partes mostradas como unidades pueden o no ser unidades físicas, pueden estar ubicadas en una posición o pueden estar distribuidas en una pluralidad de unidades de red. Algunas o todas las unidades pueden seleccionarse según las necesidades reales para lograr los objetivos de las soluciones de las realizaciones.

Además, las unidades funcionales en las realizaciones de la presente invención pueden integrarse en una unidad de procesamiento, o cada una de las unidades puede existir sola físicamente, o dos o más unidades están integradas en una unidad. La unidad integrada puede implementarse en forma de hardware o puede implementarse en forma de unidad funcional de software.

Cuando la unidad integrada se implementa en forma de una unidad funcional de software y se vende o se utiliza como un producto independiente, la unidad integrada puede almacenarse en un medio de almacenamiento legible por ordenador. Basándose en tal comprensión, las soluciones técnicas de la presente invención esencialmente, o la parte que contribuye a la técnica anterior, o todas o algunas de las soluciones técnicas pueden implementarse en forma de un producto de software. Un producto de software informático se almacena en un medio de almacenamiento e incluye varias instrucciones para indicarle a un dispositivo informático (que puede ser un ordenador personal, un servidor o un dispositivo de red) o un procesador que realice todos o algunas de los etapas de los métodos descritos en las realizaciones de la presente invención. El medio de almacenamiento precedente incluye: cualquier medio que pueda almacenar código de programa, tal como una unidad flash USB, un disco duro extraíble, una memoria de solo lectura (ROM), una memoria de acceso aleatorio (RAM), un disco magnético o un dispositivo óptico.

Las descripciones precedentes son simplemente formas de implementación específicas de la presente invención, pero no pretenden limitar el 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 procesamiento de paquetes de datos de ataque, que comprende:

la recepción (S101), mediante una interfaz (41) de comunicaciones de un nodo de gestión, interactuando la interfaz (41) de comunicaciones con una interfaz (61) de comunicaciones de un nodo de conocimiento, la información de descripción de un paquete de datos de ataque y un tipo de ataque del paquete de datos de ataque, en donde la información de descripción y el tipo de ataque se envían mediante el nodo de conocimiento.

la determinación (S102), mediante el nodo de gestión, de una política de procesamiento en el paquete de datos de ataque del tipo de ataque según el tipo de ataque, en donde la política de procesamiento se utiliza para indicarle a un conmutador que realice una operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción; y

el envío (S103), mediante la interfaz (41) de comunicaciones del nodo de gestión, interactuando la interfaz (41) de comunicaciones con una interfaz (51) de comunicaciones del controlador SDN de red definido por software, la información de descripción y la política de procesamiento al conmutador utilizando el controlador SDN de red definido por software, de manera que el conmutador realice la operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción,

en donde la determinación (S102), mediante el nodo de gestión, de una política de procesamiento en el paquete de datos de ataque del tipo de ataque según el tipo de ataque comprende:

la obtención, mediante el nodo de gestión, de una política de procesamiento predeterminada en el paquete de datos de ataque del tipo de ataque según el tipo de ataque.

2.- El método según la reivindicación 1, en donde:

la operación indicada por la política de procesamiento comprende:

una acción de procesamiento en el paquete de datos de ataque con la información de descripción, o una acción de procesamiento en el paquete de datos de ataque con la información de descripción y un momento para realizar la acción de procesamiento.

3.- El método según una cualquiera de las reivindicaciones 1 y 2, en donde cuando el nodo de gestión recibe información de descripción de múltiples paquetes de datos de ataque y tipos de ataque de los múltiples paquetes de datos de ataque, en donde la información de descripción y los tipos de ataque se envían mediante múltiples nodos de conocimiento,

la determinación (S102), mediante el nodo de gestión, de una política de procesamiento en el paquete de datos de ataque del tipo de ataque según el tipo de ataque comprende:

la determinación, mediante el nodo de gestión, al menos dos tipos de ataque iguales según los tipos de ataque de los múltiples paquetes de datos de ataque; y

la determinación, mediante el nodo de gestión según uno de los al menos dos tipos de ataque, de una política de procesamiento en el paquete de datos de ataque del tipo de ataque.

4.- El método según una cualquiera de las reivindicaciones 1 a 3, en donde el envío, mediante el nodo de gestión, de la información de descripción y la política de procesamiento al conmutador utilizando un controlador SDN comprende:

el envío, mediante el nodo de gestión, de la información de descripción y la política de procesamiento al controlador SDN utilizando una interfaz de comunicaciones predeterminada, de manera que el controlador SDN reenvía la información de descripción y la política de procesamiento al conmutador.

5.- Un nodo de gestión, que comprende:

una unidad (10) de recepción, configurada para recibir (S101) información de descripción de un paquete de datos de ataque y un tipo de ataque del paquete de datos de ataque, en donde la información de descripción y el tipo de ataque se envían mediante un nodo de conocimiento, interactuando una interfaz (41) de comunicaciones del nodo de gestión con una interfaz (61) de comunicaciones del nodo de conocimiento;

una unidad (11) de determinación, configurada para determinar (S102) una política de procesamiento en el paquete de datos de ataque del tipo de ataque según el tipo de ataque recibido por la unidad (10) de recepción, en donde la política de procesamiento se utiliza para indicarle a un conmutador que realice una operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción; y

una unidad (12) de envío, configurada para enviar (S103) la información de descripción recibida por la unidad (10) de recepción y la política de procesamiento determinada por la unidad (11) de determinación al conmutador utilizando un

controlador SDN de red definido por software, de manera que el conmutador realice la operación indicada por la política de procesamiento en el paquete de datos del ataque con la información de descripción, interactuando la interfaz (41) de comunicaciones del nodo de gestión con una interfaz (51) de comunicaciones del controlador SDN,

en donde:

la unidad (11) de determinación está configurada específicamente para obtener una política de procesamiento predeterminada en el paquete de datos de ataque del tipo de ataque según el tipo de ataque recibido por la unidad (10) de recepción.

6.- El nodo de gestión según la reivindicación 5, en donde:

la unidad (11) de determinación está configurada específicamente para generar una política de procesamiento en el paquete de datos de ataque del tipo de ataque según el tipo de ataque recibido por la unidad (10) de recepción y un algoritmo predeterminado.

7.- El nodo de gestión según una cualquiera de las reivindicaciones 5 y 6, en donde:

la operación indicada por la política de procesamiento determinada por la unidad (11) de determinación comprende:

una acción de procesamiento en el paquete de datos de ataque con la información de descripción, o una acción de procesamiento en el paquete de datos de ataque con la información de descripción y un momento para realizar la acción de procesamiento.

8.- El nodo de gestión según una cualquiera de las reivindicaciones 5 a 7, en donde:

la unidad (11) de determinación está configurada específicamente para: cuando la unidad (10) de recepción recibe información de descripción de múltiples paquetes de datos de ataque y tipos de ataque de los múltiples paquetes de datos de ataque, en donde la información de descripción y los tipos de ataque se envían mediante múltiples nodos de conocimiento, determinar al menos dos tipos de ataque iguales según los tipos de ataque de los múltiples paquetes de datos de ataque, y determinar, según uno de los al menos dos tipos de ataque, una política de procesamiento en el paquete de datos de ataque del tipo de ataque.

9.- Un sistema de comunicaciones, que comprende:

un nodo de gestión según una cualquiera de las reivindicaciones 5 a 8;

un conmutador;

un controlador de red definido por software, SDN que comprende:

una unidad (20) de recepción, configurada para recibir información de descripción de un paquete de datos de ataque y una política de procesamiento en el paquete de datos de ataque con la información de descripción, donde la información de descripción y la política de procesamiento se envían mediante en nodo de gestión; y

una unidad (21) de envío, configurada para enviar la información de descripción y la política de procesamiento que son recibidas por la unidad de recepción al conmutador, de manera que el conmutador realice una operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción;

un nodo de conocimiento, que comprende:

una unidad (30) de identificación, configurada para identificar un paquete de datos recibido como un paquete de datos de ataque;

una unidad (31) de determinación, configurada para determinar la información de descripción del paquete de datos de ataque identificado por la unidad de identificación y un tipo de ataque del paquete de datos de ataque; y

una unidad (32) de envío, configurada para enviar la información de descripción y el tipo de ataque que se determinan mediante la unidad de determinación al nodo de gestión, donde el tipo de ataque se utiliza por el nodo de gestión para determinar una política de procesamiento en el paquete de datos de ataque del tipo de ataque, y la política de procesamiento se utiliza para indicarle a un conmutador que reenvíe un paquete de datos para realizar una operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción.

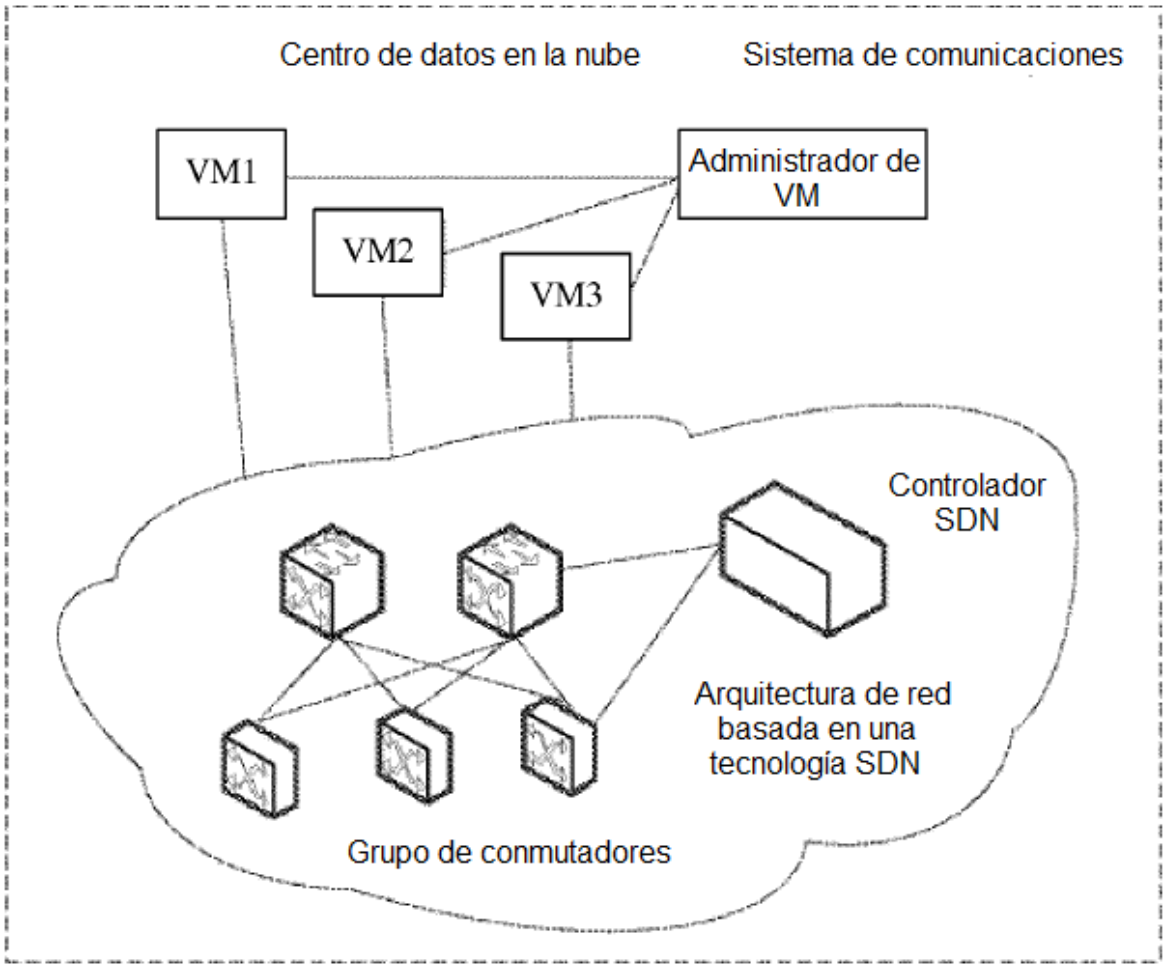
Centro de datos en la nube
Sistema de comunicaciones
VM1
VM2
VM3
Administrador de VM
Controlador SDN
Arquitectura de red basada en una tecnología SDN
Grupo de conmutadores

FIG. 1

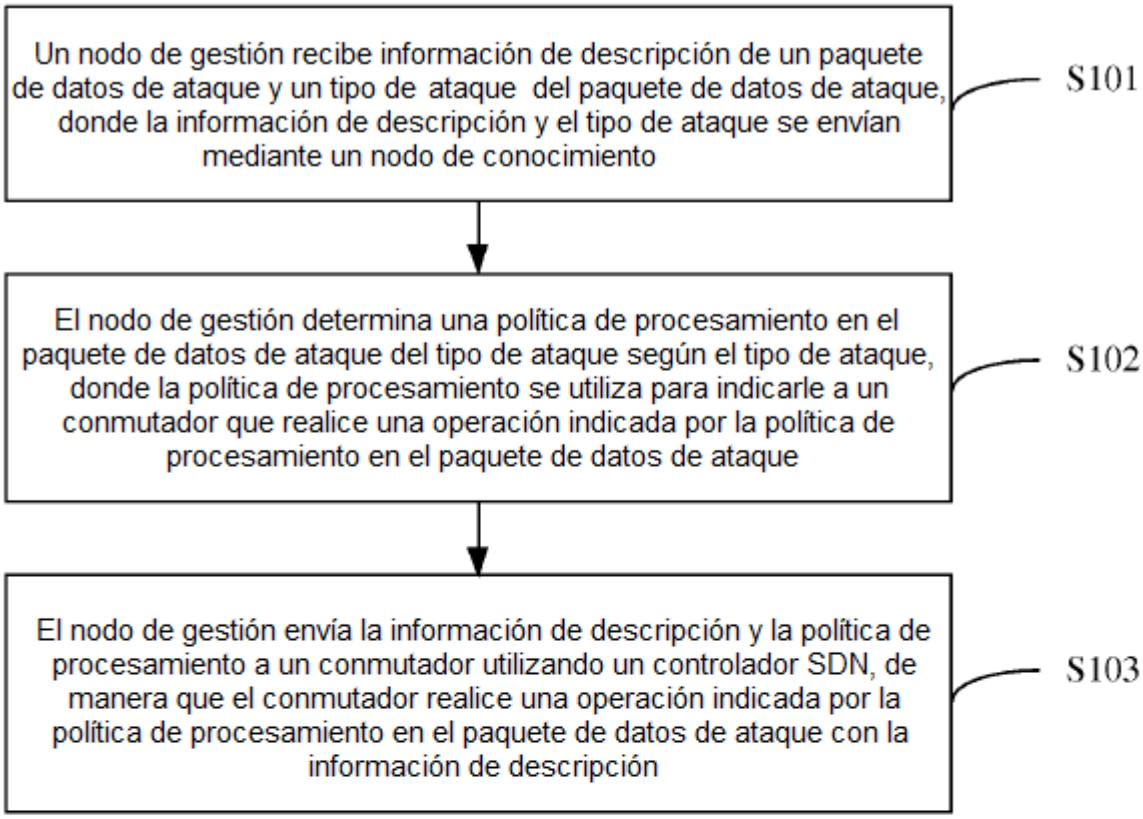
Un nodo de gestión recibe información de descripción de un paquete de datos de ataque y un tipo de ataque del paquete de datos de ataque, donde la información de descripción y el tipo de ataque se envían mediante un nodo de conocimiento
S101
El nodo de gestión determina una política de procesamiento en el paquete de datos de ataque del tipo de ataque según el tipo de ataque, donde la política de procesamiento se utiliza para indicarle a un conmutador que realice una operación indicada por la política de procesamiento en el paquete de datos de ataque
S102
El nodo de gestión envía la información de descripción y la política de procesamiento a un conmutador utilizando un controlador SDN, de manera que el conmutador realice una operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción
S103

FIG. 2

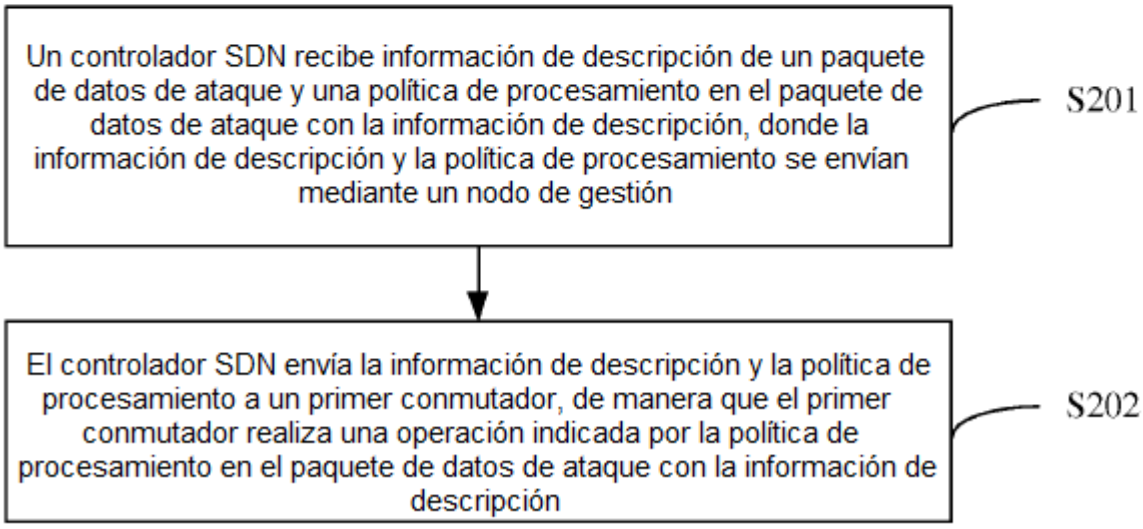
Un controlador SDN recibe información de descripción de un paquete de datos de ataque y una política de procesamiento en el paquete de datos de ataque con la información de descripción, donde la información de descripción y la política de procesamiento se envían mediante un nodo de gestión
S201
El controlador SDN envía la información de descripción y la política de procesamiento a un primer conmutador, de manera que el primer conmutador realiza una operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción
S202

FIG. 3

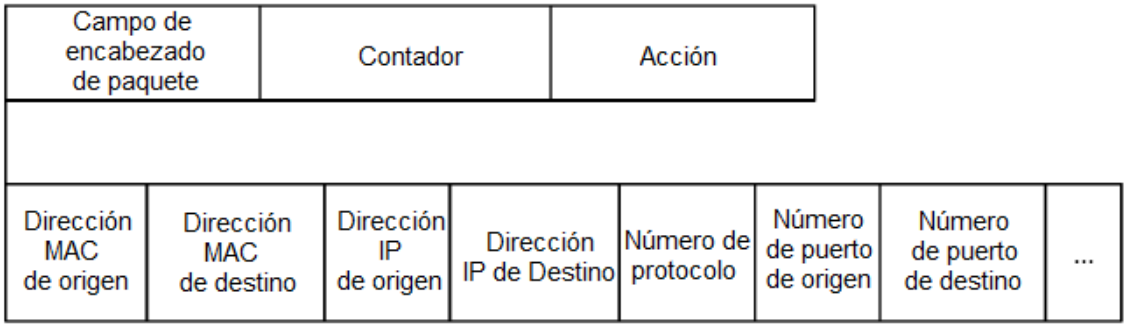
Campo de encabezado de paquete
Contador
Acción
Dirección MAC de origen
Dirección MAC de destino
Dirección IP de origen
Dirección IP de Destino
Número de protocolo
Número de puerto de origen
Número de puerto de destino
...

FIG. 4

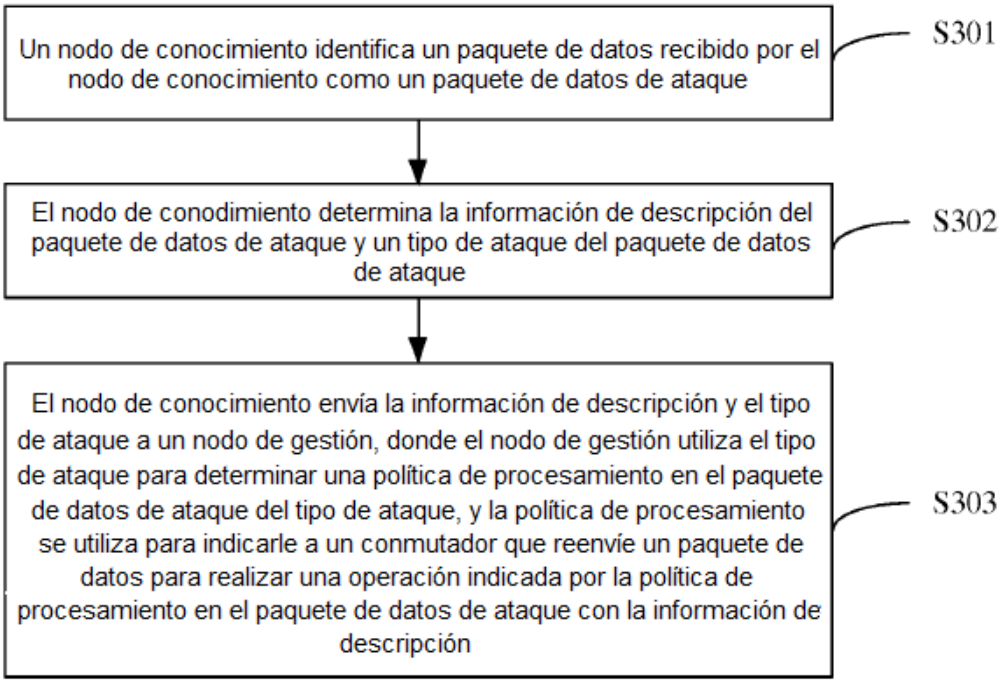
Un nodo de conocimiento identifica un paquete de datos recibido por el nodo de conocimiento como un paquete de datos de ataque
S301
El nodo de conodimiento determina la información de descripción del paquete de datos de ataque y un tipo de ataque del paquete de datos de ataque
S302
El nodo de conocimiento envía la información de descripción y el tipo de ataque a un nodo de gestión, donde el nodo de gestión utiliza el tipo de ataque para determinar una política de procesamiento en el paquete de datos de ataque del tipo de ataque, y la política de procesamiento se utiliza para indicarle a un conmutador que reenvíe un paquete de datos para realizar una operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción
S303

FIG. 5

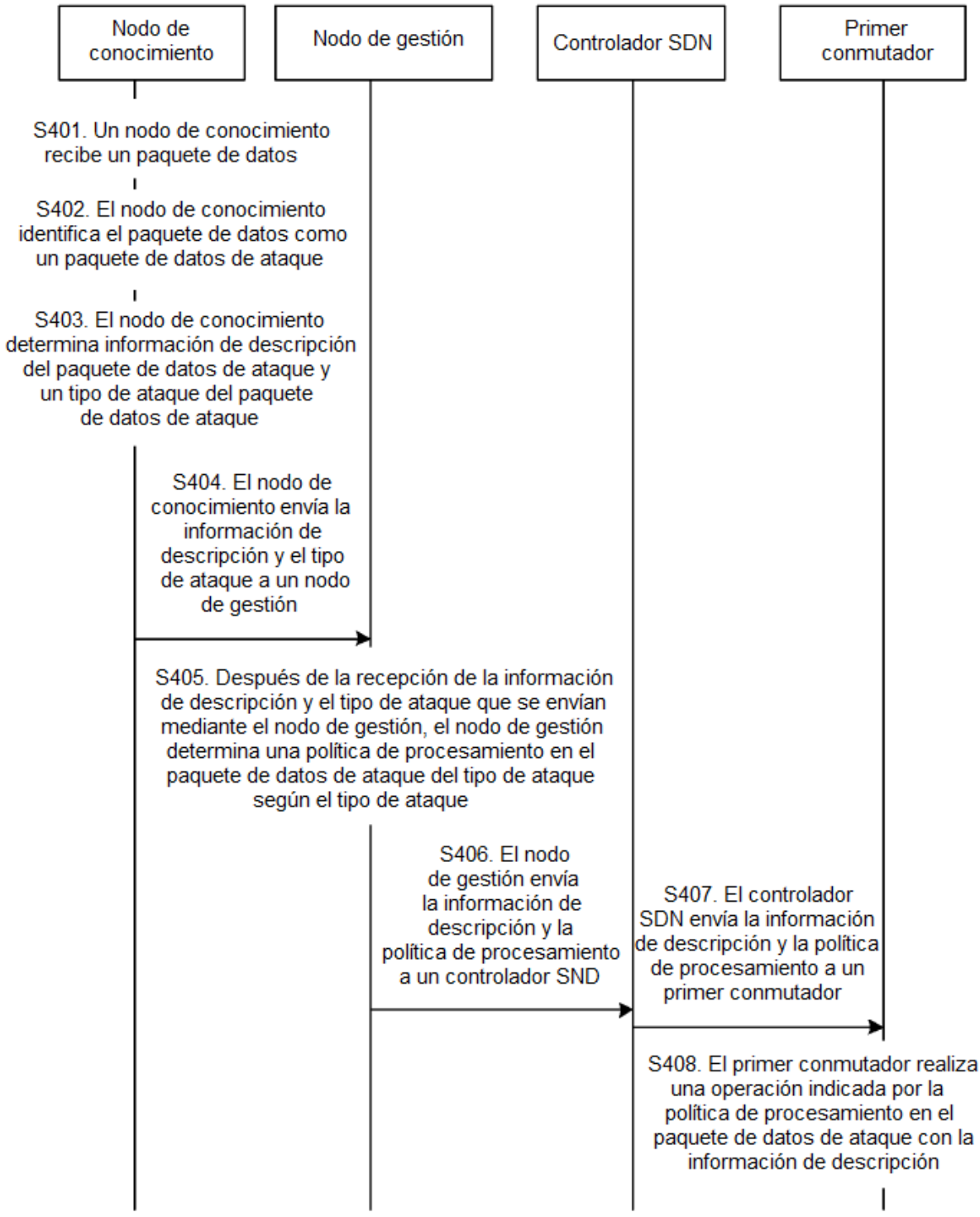
Nodo de conocimiento
Nodo de gestión
Controlador SDN
Primer conmutador
S401. Un nodo de conocimiento recibe un paquete de datos
S402. El nodo de conocimiento identifica el paquete de datos como un paquete de datos de ataque
S403. El nodo de conocimiento determina información de descripción del paquete de datos de ataque y un tipo de ataque del paquete de datos de ataque
S404. El nodo de conocimiento envía la información de descripción y el tipo de ataque a un nodo de gestión
S405. Después de la recepción de la información de descripción y el tipo de ataque que se envían mediante el nodo de gestión, el nodo de gestión determina una política de procesamiento en el paquete de datos de ataque del tipo de ataque según el tipo de ataque
S406. El nodo de gestión envía la información de descripción y la política de procesamiento a un controlador SND
S407. El controlador SDN envía la información de descripción y la política de procesamiento a un primer conmutador
S408. El primer conmutador realiza una operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción

FIG. 6

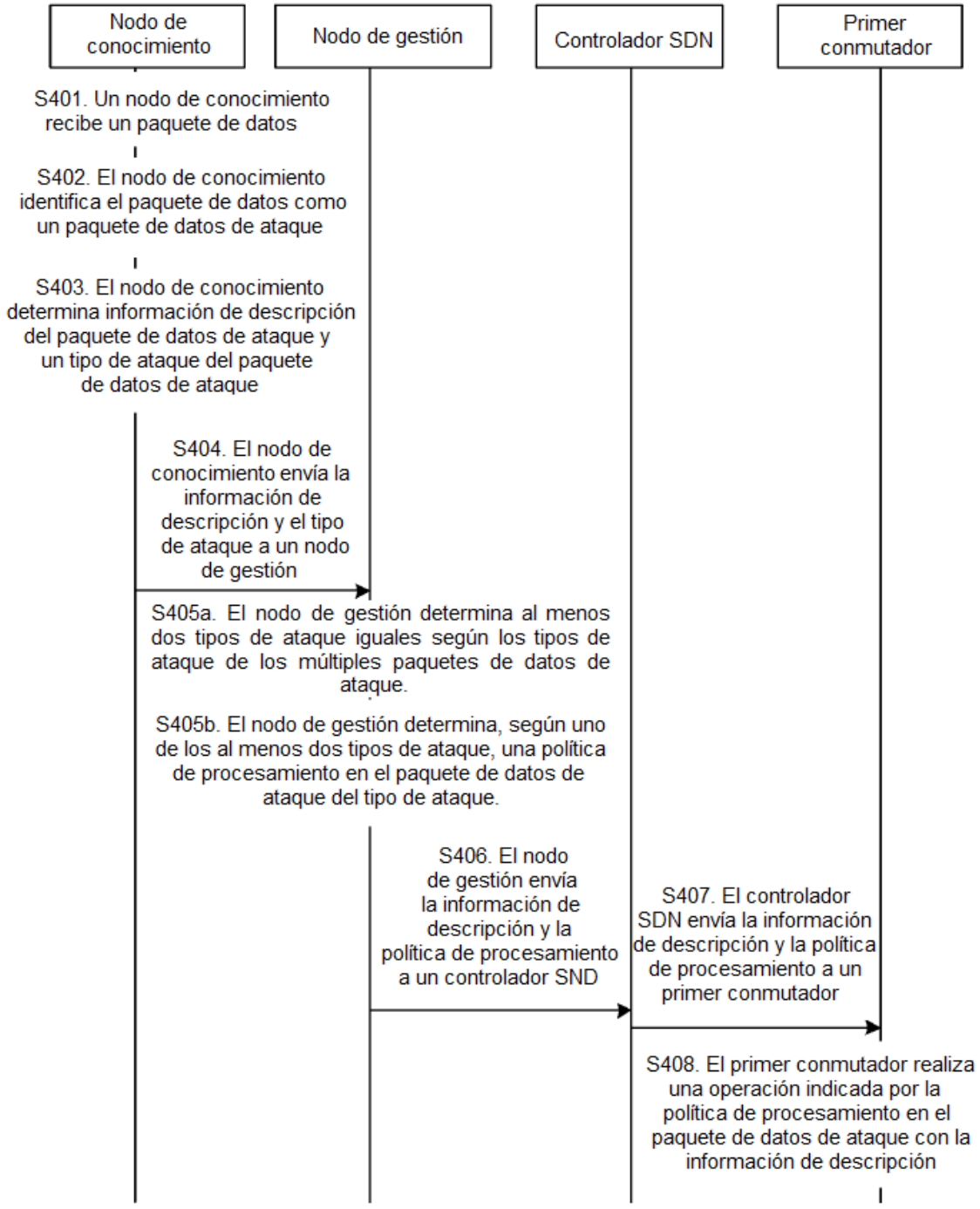
Nodo de conocimiento
Nodo de gestión
Controlador SDN
Primer conmutador
S401. Un nodo de conocimiento recibe un paquete de datos
S402. El nodo de conocimiento identifica el paquete de datos como un paquete de datos de ataque
S403. El nodo de conocimiento determina información de descripción del paquete de datos de ataque y un tipo de ataque del paquete de datos de ataque
S404. El nodo de conocimiento envía la información de descripción y el tipo de ataque a un nodo de gestión
S405a. El nodo de gestión determina al menos dos tipos de ataque iguales según los tipos de ataque de los múltiples paquetes de datos de ataque.
S405b. El nodo de gestión determina, según uno de los al menos dos tipos de ataque, una política de procesamiento en el paquete de datos de ataque del tipo de ataque.
S406. El nodo de gestión envía la información de descripción y la política de procesamiento a un controlador SND
S407. El controlador SDN envía la información de descripción y la política de procesamiento a un primer conmutador
S408. El primer conmutador realiza una operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción

FIG. 7

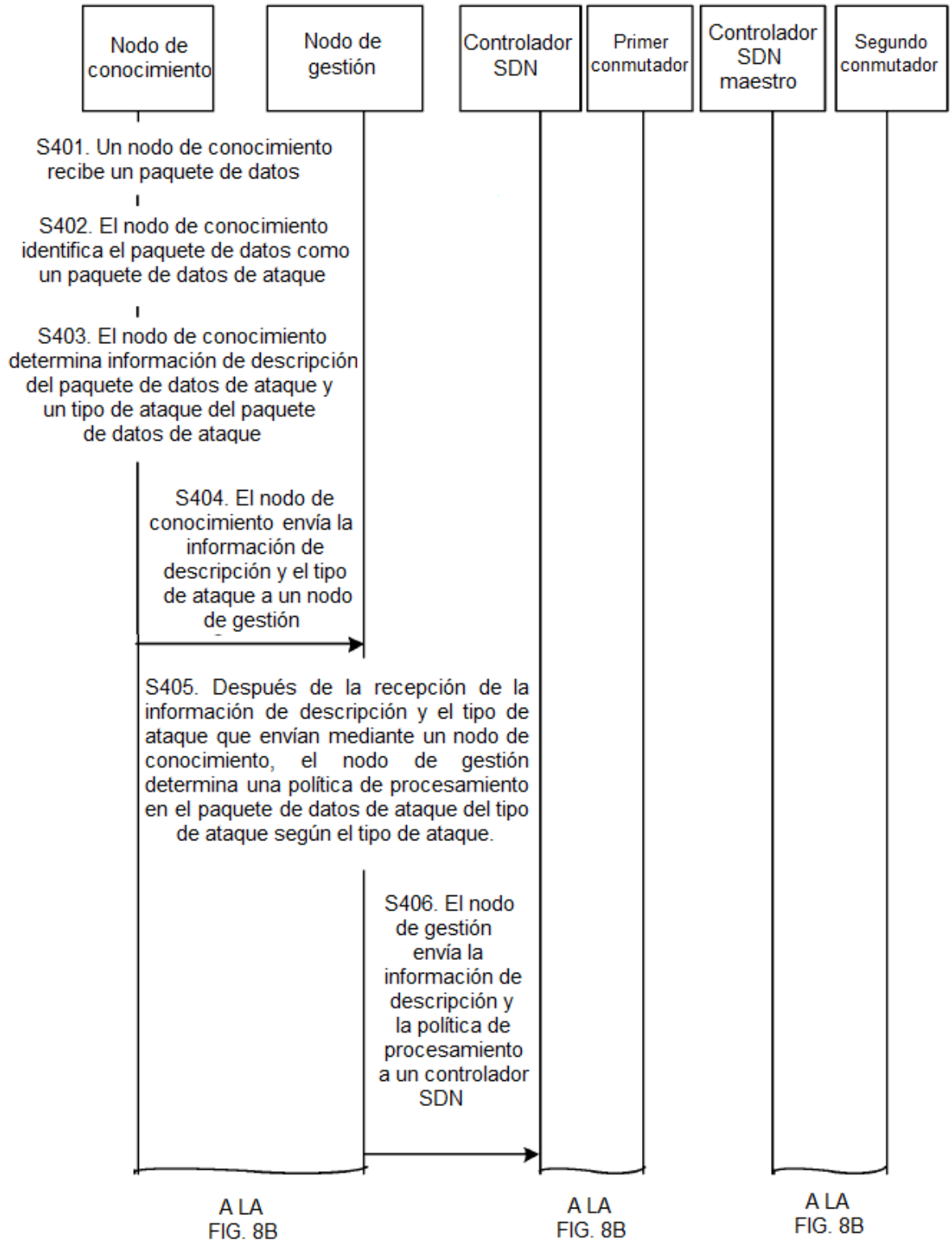
Nodo de conocimiento
Nodo de gestión
Controlador SDN
Primer conmutador
Controlador SDN maestro
Segundo conmutador
S401. Un nodo de conocimiento recibe un paquete de datos
S402. El nodo de conocimiento identifica el paquete de datos como un paquete de datos de ataque
S403. El nodo de conocimiento determina información de descripción del paquete de datos de ataque y un tipo de ataque del paquete de datos de ataque
S404. El nodo de conocimiento envía la información de descripción y el tipo de ataque a un nodo de gestión
S405. Después de la recepción de la información de descripción y el tipo de ataque que envían mediante un nodo de conocimiento, el nodo de gestión determina una política de procesamiento en el paquete de datos de ataque del tipo de ataque según el tipo de ataque.
S406. El nodo de gestión envía la información de descripción y la política de procesamiento a un controlador SDN
A LA FIG. 8B
A LA FIG. 8B
A LA FIG. 8B

FIG. 8A

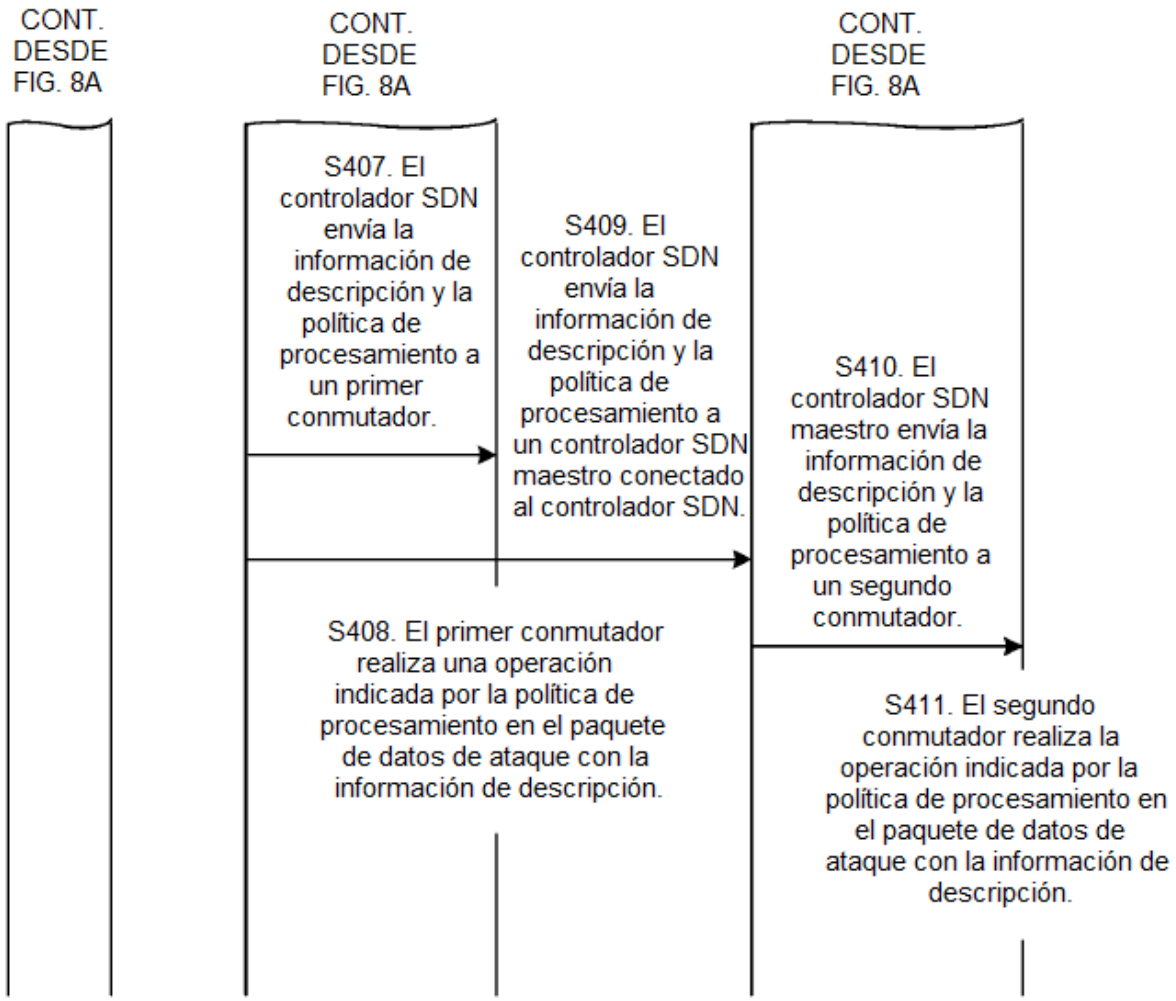
CONT. DESDE FIG. 8A
CONT. DESDE FIG. 8A
CONT. DESDE FIG. 8A
S407. El controlador SDN envía la información de descripción y la política de procesamiento a un primer conmutador.
S409. El controlador SDN envía la información de descripción y la política de procesamiento a un controlador SDN maestro conectado al controlador SDN.
S410. El controlador SDN maestro envía la información de descripción y la política de procesamiento a un segundo conmutador.
S408. El primer conmutador realiza una operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción.
S411. El segundo conmutador realiza la operación indicada por la política de procesamiento en el paquete de datos de ataque con la información de descripción.

FIG. 8B

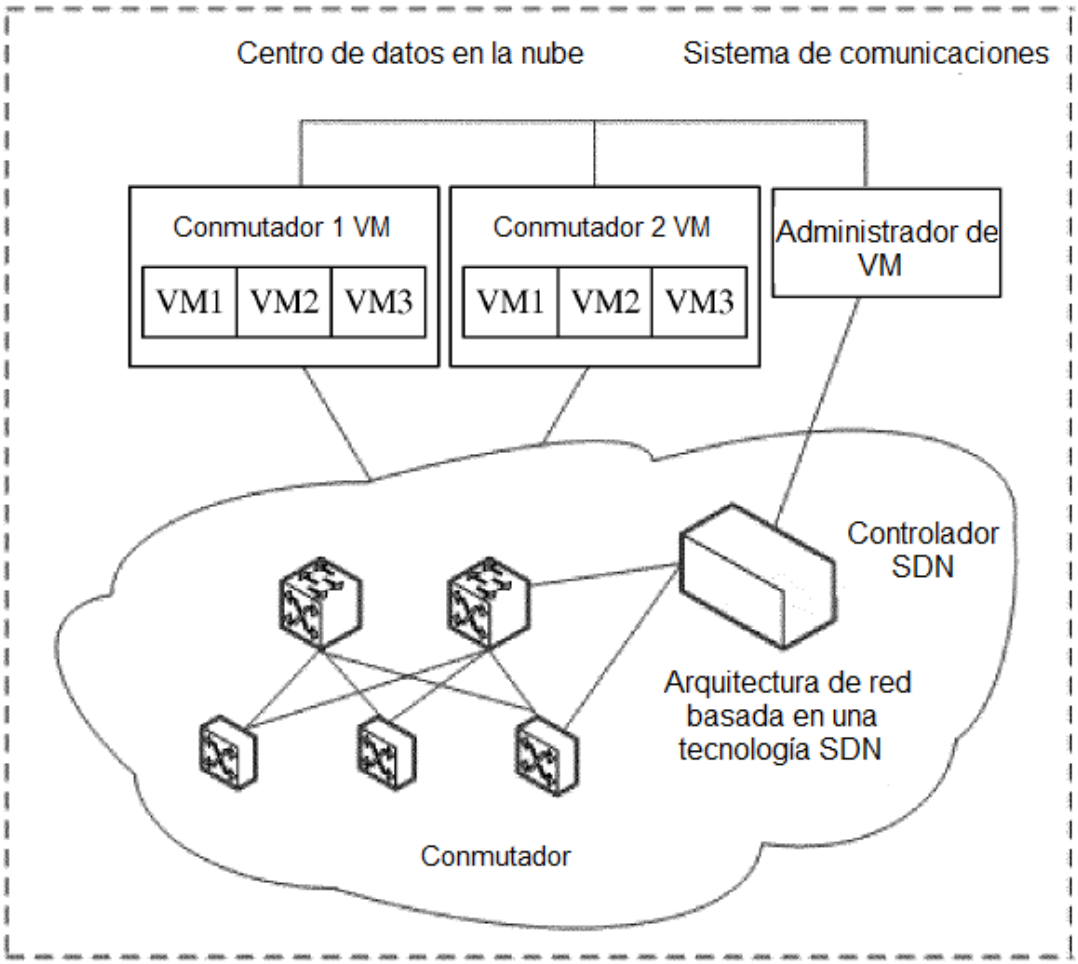
Centro de datos en la nube
Sistema de comunicaciones
Conmutador 1 VM
VM1
VM2
VM3
Conmutador 2 VM
VM1
VM2
VM3
Administrador de VM
Controlador SDN
Arquitectura de red basada en una tecnología SDN
Conmutador

FIG. 9

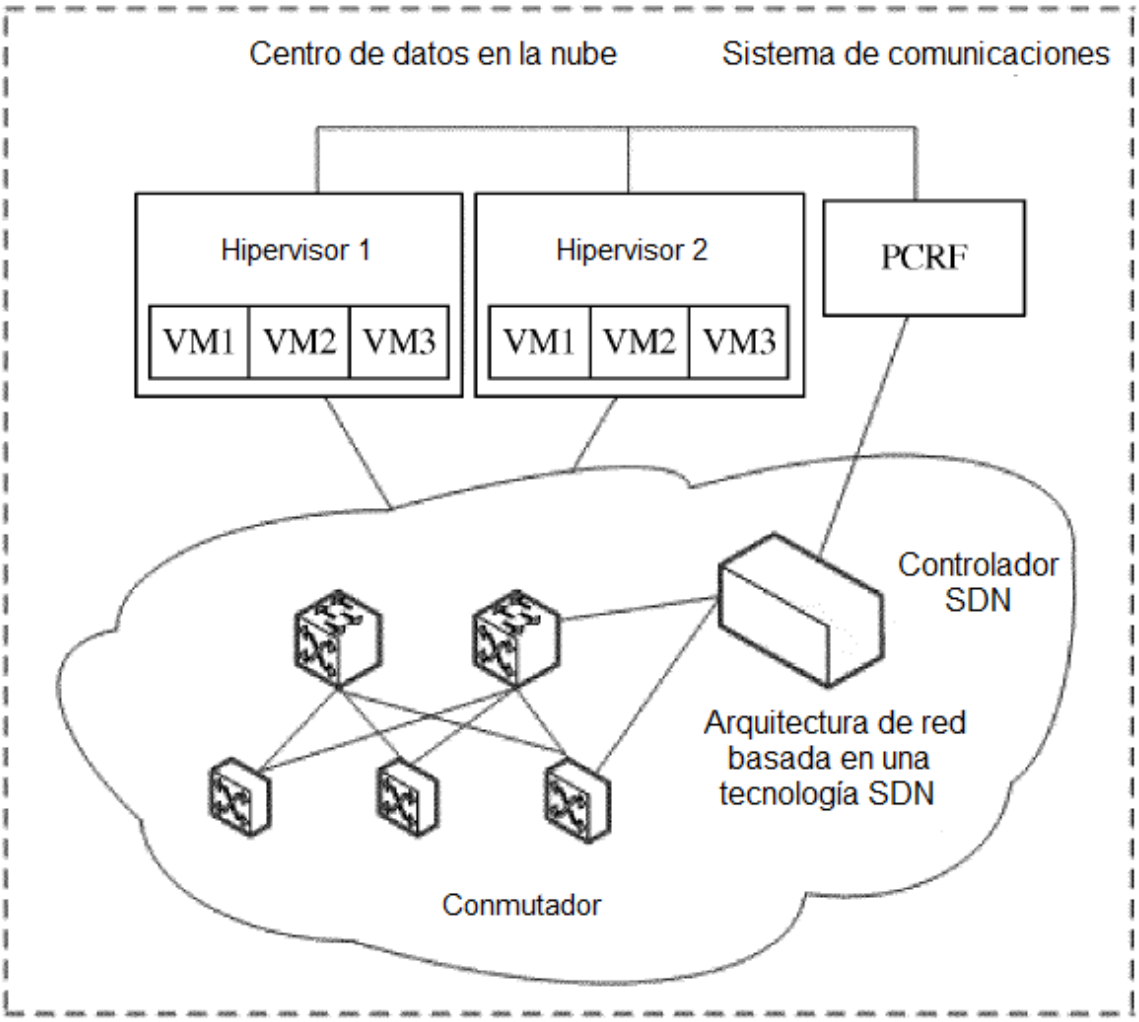
Centro de datos en la nube
Sistema de comunicaciones
Hipervisor 1
VM1
VM2
VM3
Hipervisor 2
VM1
VM2
VM3
PCRF
Controlador SDN
Arquitectura de red basada en una tecnología SDN
Conmutador

FIG. 10

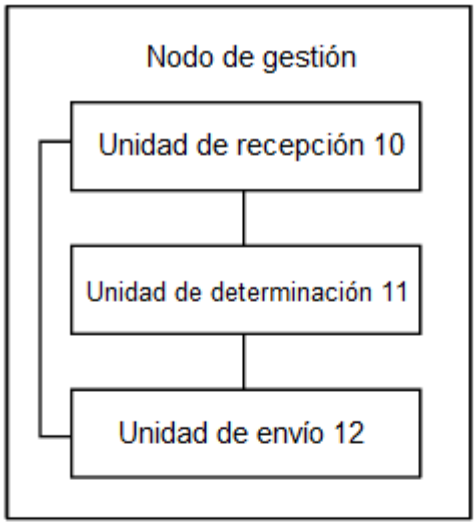

FIG. 11

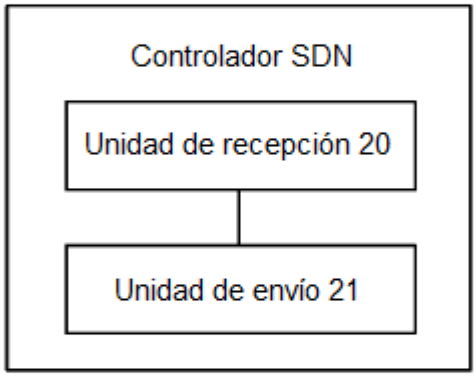

FIG. 12

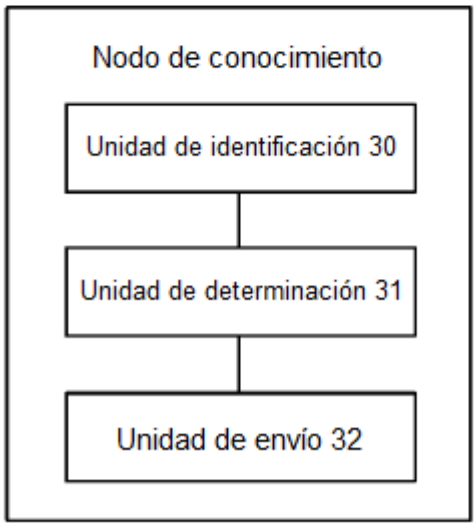

FIG. 13

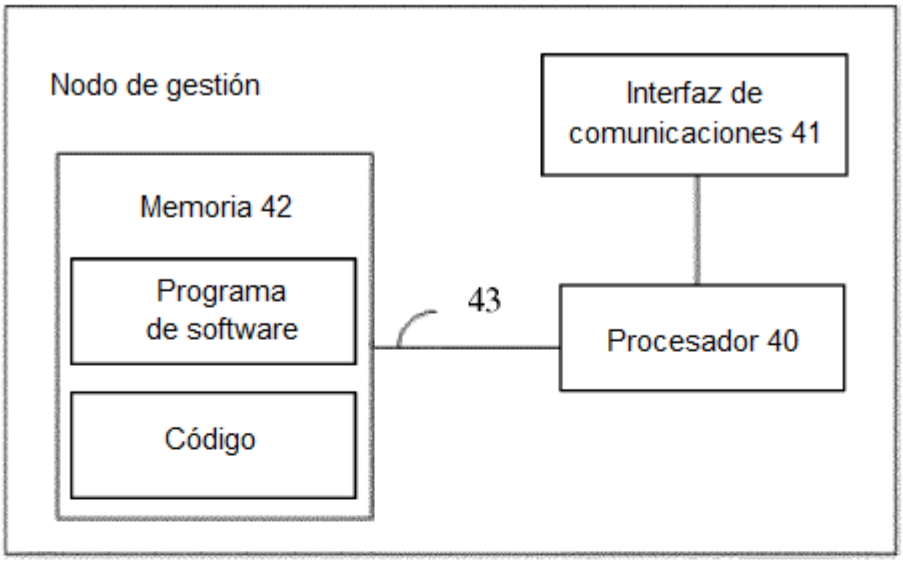
Nodo de gestión
Interfaz de comunicaciones 41
Memoria 42
Programa de software
Código
43
Procesador 40

FIG. 14

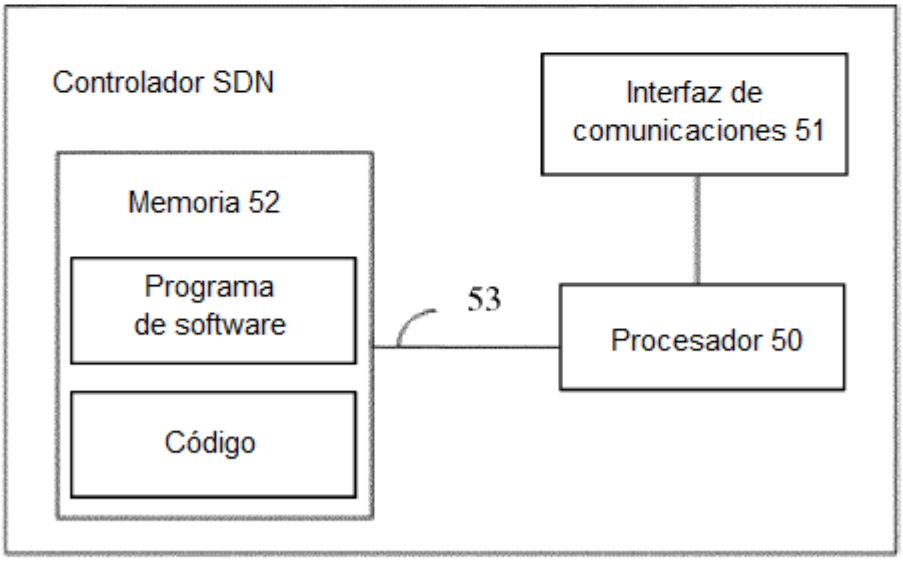
Controlador SDN
Interfaz de comunicaciones 51
Memoria 52
Programa de software
Código
53
Procesador 50

FIG. 15

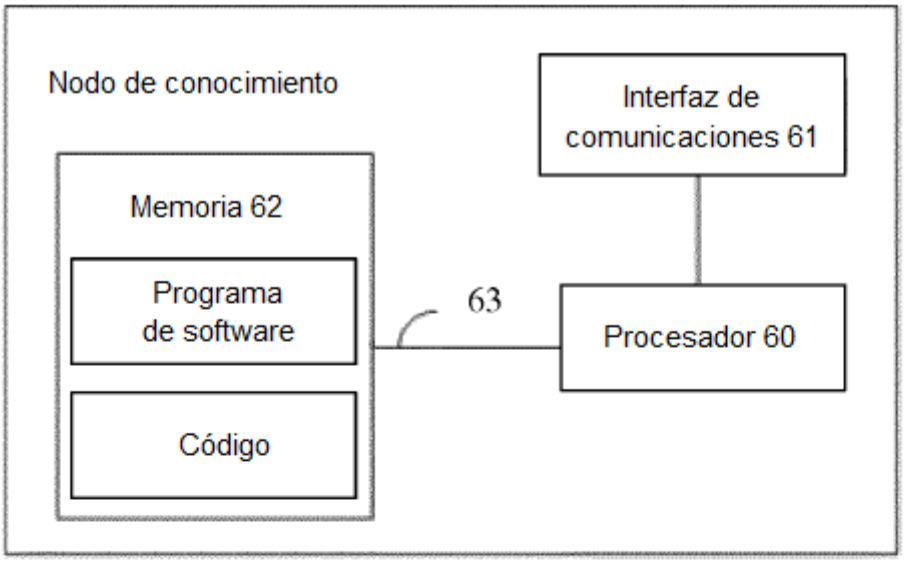
Nodo de conocimiento
Interfaz de comunicaciones 61
Memoria 62
Programa de software
Código
63
Procesador 60

FIG. 16

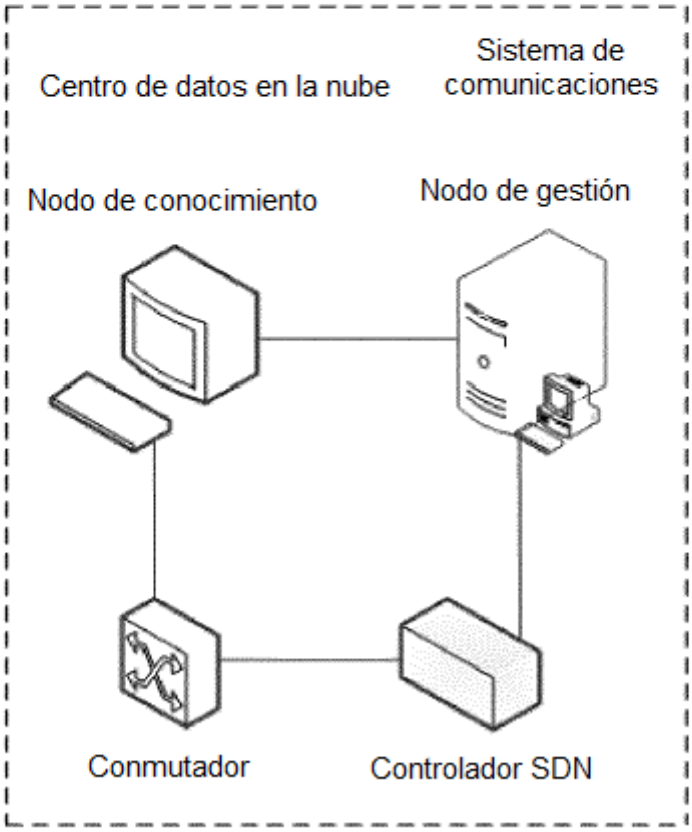
Centro de datos en la nube
Sistema de comunicaciones
Nodo de conocimiento
Nodo de gestión
Conmutador
Controlador SDN

FIG. 17

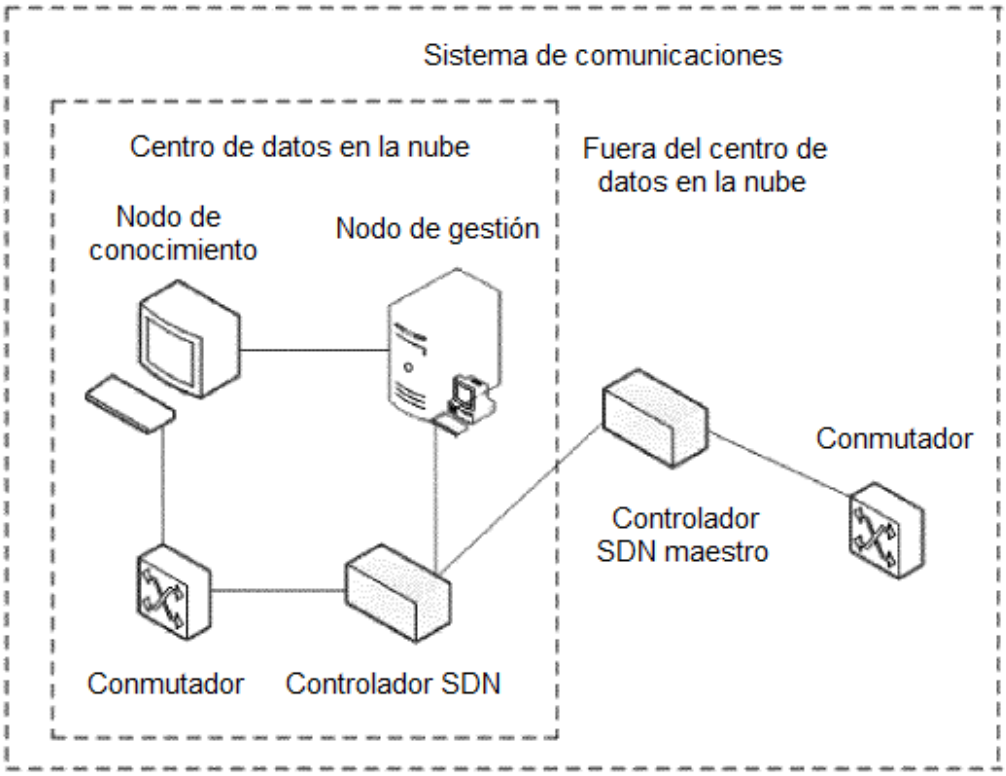
Sistema de comunicaciones
Centro de datos en la nube
Fuera del centro de datos en la nube
Nodo de conocimiento
Nodo de gestión
Conmutador
Controlador SDN maestro
Conmutador
Controlador SDN

FIG. 18