(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 663 410**

(51) Int. CI.:

H04L 12/715 (2013.01)
H04L 29/12 (2006.01)
H04L 29/06 (2006.01)
H04L 12/717 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **14.11.2014 E 14382453 (0)**

(97) Fecha y número de publicación de la concesión europea: **10.01.2018 EP 3021534**

(54) Título: **Un controlador de red y un método informático implementado para definir automáticamente reglas de reenvío para configurar un dispositivo de interconexión de red informático**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
12.04.2018

(73) Titular/es:

TELEFÓNICA S.A. (100.0%)
C/ Gran Vía 28
28013 Madrid, ES

(72) Inventor/es:

CONTRERAS, LUIS MIGUEL;
LÓPEZ, DIEGO R. y
PASTOR, ANTONIO AGUSTÍN

(74) Agente/Representante:

ARIZTI ACHA, Monica

Un controlador de red y un método informático implementado para definir automáticamente reglas de reenvío para configurar un dispositivo de interconexión de red informático

DESCRIPCIÓN

Campo de la invención

La presente invención se refiere en general a redes de datos. En particular, la invención se refiere a un controlador de red y a un método informático implementado para definir automáticamente reglas de reenvío para configurar un dispositivo de interconexión de red informático de una red de comunicación. El controlador de red propuesto, o controlador de una Red Definida por Software (SDN) mejorado, configura automáticamente y de manera proactiva bajo demanda las reglas necesarias en la red de comunicación para una comunicación eficaz y hace uso de las capacidades de DNS para identificar con antelación los nuevos flujos que pasarán a través de la red de comunicación.

Antecedentes de la invención

El comportamiento convencional de un controlador de red de SDN implica la configuración reactiva de reglas de reenvío para cualquier nuevo flujo que no coincida con ninguna entrada existente en una tabla de flujos. El proceso de configuración para cualquier regla nueva se inicia una vez que llega un nuevo paquete en un dispositivo de interconexión de red informático tal como un conmutador en caso de que dicho conmutador no contenga ninguna entrada específica en la tabla de flujos. En ese caso, el conmutador envía una petición de flujo al controlador de SDN que analiza el paquete para definir una regla aplicable que se configura finalmente en el conmutador. Las reglas consisten en una acción (por ejemplo, reenviar a un cierto puerto, suprimir, enviar al controlador de red, etc.) determinada mediante unos bits de coincidencia o arbitrarios en el encabezamiento del paquete (por ejemplo, dirección MAC, dirección IP, etiqueta VLAN, puerto TCP, etc.).

El rendimiento de este proceso depende del conmutador y de los recursos del controlador de SDN (CPU, memoria, etc.) y puede conducir a un problema de escalabilidad grave, puesto que el número potencial de peticiones al controlador de red para una nueva regla es directamente proporcional al número de distintos flujos activos en la red de comunicación.

El paradigma de SDN se concibió originalmente para la comunicación eficaz entre máquinas virtuales (o físicas) que residen en entornos de centros de datos. En este entorno las aplicaciones alojadas en diferentes dispositivos se comunican entre sí para proporcionar un cierto servicio.

Hoy en día el concepto de SDN está ganando impulso progresivamente y se prevé su aplicación a las redes de comunicación convencionales. Es necesario entonces resolver los problemas de escalabilidad potenciales que pudieran sufrir los elementos centrales en una red de comunicación (en este caso, un controlador de SDN) debido al uso masivo de la red de comunicación mediante los usuarios finales.

Además de eso, el Servicio de Nombre de Dominio (DNS) es un protocolo estandarizado y uno de los servicios básicos necesarios en el internet de hoy. Además del servicio de resolución de nombres, el DNS se ha extendido a varios usos. Uno es el DSN-SD o descubrimiento del Servicio de DNS [1] que se definió con el objetivo de simplificar que los clientes de red descubran y usen servicios ofrecidos mediante la red como la exploración o impresión. Otro uso común es un enrutamiento de petición basada en DNS mediante las Redes de Distribución de Contenido (CDN) que resuelven una dirección IP diferente del Servidor de CDN basada en sus propios criterios. Un escenario típico es usar la geolocalización de la fuente IP para resolver diferentes direcciones IP del Servidor de contenido, intentando ofrecer contenidos físicamente tan cerrados como sea posible a la fuente que resuelve la dirección IP.

Los Servicios de Seguridad basados en DNS son otra práctica común. Luchar contra el correo basura y el software maligno a través de una Lista de Agujeros Negros basada en DNS (DNSBL) es una práctica común.

Como se ha mencionado antes, la configuración reactiva del conmutador mediante el controlador de red es el comportamiento común de una red de SDN (como puede observarse, por ejemplo, en la especificación de OpenFlow [2]), que puede conducir a problemas de escalabilidad graves. Un ejemplo de una solución evolucionada a partir de la especificación de OpenFlow es el proyecto OpenDayLight [3]. Proporciona una API REST para su plataforma del controlador que puede configurar los servidores de DNS para un nodo controlador. Otro ejemplo de una solución evolucionada es el HP Sentinel [4] que únicamente usa la tecnología de SDN para recibir tráfico de DNS y permitir o no dicho tráfico de DNS avanzando la petición de DNS basándose en reglas locales. Por lo tanto, dicha solución únicamente permite avanzar o no una petición de usuario después de haberla comparado con una lista de reglas predefinida.

Por otro lado, las configuraciones proactivas se implementan mediante los administradores de red especificando

directamente en el controlador de red políticas de flujo sin un conocimiento real de qué flujos se crearán mediante el usuario final, siendo entonces genéricos, y no basándose en el tráfico real que pasará a través de la red.
Además de eso, las reglas pueden cambiar con el tiempo de acuerdo con las necesidades de la red, y la memoria en los conmutadores es limitada, por lo que no pueden pre-configurarse reglas afinadas para todos los flujos potenciales en la red.
Finalmente, en un entorno de telecomunicación es más que probable que más de un dominio de red (sub-red) deba pasarse a través del flujo para ajuste y comunicación de extremo a extremo. Entonces es necesario establecer una comunicación entre controladores de SDN a través de toda la red para preconfigurar la regla de flujo con antelación de extremo a extremo.
El documento WO2014142278 proporciona una función de NAT doble que puede usarse incluso en una única red. Un dispositivo de control comprende: una unidad de gestión de información de mapeo para gestionar información de mapeo en la que se ha asociado información de localización de anfitrión, direcciones IP mapeadas, direcciones IP reales y nombres de anfitrión; y una unidad de generación de instrucción para dar instrucciones a un nodo de reenvío en la ruta de reenvío de un paquete desde el anfitrión para traducir la dirección IP mapeada y la dirección real indicada en la dirección de IP de origen de transmisión y la dirección de IP de destino de transmisión, respectivamente, a la dirección real y dirección de IP mapeada correspondientes basándose en la información de mapeo.
El documento científico ‘Internet Research Task Force SDNi: A Message Exchange Protocol for Software Defined Networks (SDNS)’ desvela una SDNi de protocolo para la interfaz entre dominios de Interconexión de Red Definida por Software (SDN) para intercambiar información entre los controladores de dominio de SDN. Define el concepto de un dominio de SDN; es necesario, cuáles son sus componentes y cómo ayuda la SDNi en comunicación interdominio.
El informe científico ‘SDN architecture’ por la Fundación de Interconexión de Red Abierta (ONF) especifica la arquitectura de SDN. Basándose en una introducción de ONF a SDN, amplía los principios de SDN y los aplica a componentes e interfaces de arquitectura.

Referencias:

[1] RFC6763. Descubrimiento de Servicio de DNS.
[2] Especificación de Conmutador OpenFlow Versión 1.3.0 (Protocolo de Cable 0x04) 25 de junio de 2012. https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-v1.3.0.pdf
[3] http://www.opendaylight.org/project/technical-overview.
[4] http://h17007.www1.hp.com/docs/interopny/4AA4-3871ENW.pdf
[5] 3GPP TS 33.210. Seguridad de Dominio de Red (NDS).
[6] 3GPP TS 33.401. 3GPP Evolución de Arquitectura de Sistema (SAE); Arquitectura de seguridad.
[7] https://datatracker.ietf.org/wg/sfc/charter/

Descripción de la invención

Las realizaciones de la presente invención tratan estas y/u otras necesidades proporcionando un controlador de red, tal como un controlador de SDN, para definir automáticamente reglas de reenvío para configurar un dispositivo de interconexión de red informático, por ejemplo un conmutador. El controlador de red que cumple con varias especificaciones de Interfaces del Plano de Control a Datos (CDPI) tales como OpenFlow, entre otras, está conectado a una sub-red de una red de comunicación y comprende:

- un gestor de controlador que recibe una petición para un servicio dado, y define, ejecutando un algoritmo, reglas de reenvío relacionadas con dicho servicio, e instala las reglas de reenvío definidas en un dispositivo de interconexión de red informático de la sub-red de la red de comunicación para configurar el dispositivo de interconexión de red informático para dicho servicio dado;
- un módulo de decisión configurado para comunicarse con el gestor de controlador y configurado para interactuar con un servidor de DNS para recibir una resolución determinada para una petición de DNS de dicha petición para dicho servicio dado, y con una base de datos para recuperar información complementaria para la petición de DNS, para ayudar al gestor de controlador a realizar la definición de las reglas de reenvío; y
- una pluralidad de interfaces para permitir respectivamente la comunicación del módulo de decisión con el gestor de controlador, el servidor de DNS y la base de datos.

En una realización el gestor de controlador está conectado a al menos otro dispositivo de interconexión de red informático (por ejemplo otro conmutador) de dicha sub-red de la red de comunicación para instalar las reglas de reenvío definidas en dicho otro dispositivo de interconexión de red informático.

En otra realización, el primer controlador de red está conectado a al menos un segundo controlador de red de una sub-red diferente y adyacente de la red de comunicación para que el módulo de decisión de dicho primer controlador de red envíe, a través de una interfaz correspondiente, la información relevante acerca de la petición entrante, o

flujo, en particular, la resolución determinada recibida desde el servidor de DNS y la información recuperada desde la base de datos a al menos otro módulo de decisión incluido en dicho segundo controlador de red.

De acuerdo con la invención, la base de datos incluye: un módulo de información para permitir la recuperación de dicha información complementaria para la petición de DNS a través de dicha interfaz mediante el módulo de decisión; un módulo colector para recoger dicha información complementaria para la petición de DNS desde diferentes fuentes de información a través de una interfaz correspondiente; y un módulo gestor de base de datos para almacenar la información complementaria recogida para la petición de DNS, teniendo dicho gestor de base de datos dos interfaces diferentes, una primera para comunicar con el módulo de información y una segunda para comunicar con el módulo colector.

Las diferentes fuentes de información comprenden información interna a un proveedor de servicios de la red de comunicación e información externa a dicho proveedor de servicios. Preferentemente, la información interna viene desde Sistemas de Soporte a las Operaciones (OSS)/Sistemas de Soporte Empresariales al menos incluyendo bases de datos de topologías de red, herramientas de inventario, supervisión de red y flujos y orquestación de gráfico de servicio, mientras que la información externa al menos incluye información de seguridad, preferencias del usuario y/o información de itinerancia.

Las realizaciones de la presente invención proporcionan también un método informático implementado para definir automáticamente reglas de reenvío para configurar un dispositivo de interconexión de red informático, por ejemplo un conmutador, en el que un gestor de controlador de un controlador de red, tal como un controlador de SDN, conectado a una sub-red de una red de comunicación recibe una petición para un servicio dado y define, ejecutando un algoritmo, reglas de reenvío relacionadas con dicho servicio dado, e instala las reglas de reenvío definidas en un dispositivo de interconexión de red informático de la sub-red de la red de comunicación para configurar el dispositivo de interconexión de red informático para el servicio dado. Además, y característicamente de la presente invención, un módulo de decisión del controlador de red que se comunica con el gestor de controlador, reenvía una petición de DNS de dicha petición para el servicio dado a un servidor de DNS para determinar el último una resolución para la petición de DNS; y recupera, después de haber recibido la resolución determinada desde el servidor de DNS, información complementaria para la petición de DNS desde una base de datos. En consecuencia, el módulo de decisión ayuda al gestor de controlador a realizar la definición de las reglas de reenvío.

De acuerdo con la invención, antes de que se realice dicha recuperación de la información complementaria para la petición de DNS, un módulo colector de la base de datos recoge la información complementaria desde diferentes fuentes de información y almacena adicionalmente la información complementaria recogida en un módulo gestor de base de datos de la base de datos para permitir la recuperación mediante el módulo de decisión.

En una realización, la petición para el servicio dado se realiza mediante un usuario conectador al dispositivo de interconexión de red informático por medio de un dispositivo informático tal como una Tableta, un PC, un portátil, un Teléfono inteligente, etc.

En otra realización, la petición para el servicio dado se realiza mediante un centro de datos conectado al dispositivo de interconexión de red informático.

Por lo tanto, la presente invención permite automáticamente y de manera proactiva la configuración de reglas de reenvío bajo demanda en el controlador de SDN proporcionado tomando como entrada el tráfico de DNS como consecuencia de una petición para un servicio dado realizado por un usuario final, por ejemplo, una petición para una función de resolución de nombre de dominio, para identificar con antelación el flujo que puede crearse por el usuario final antes de que tal flujo entre en la red de comunicación.

En una red de comunicación/telecomunicación los usuarios finales acceden a aplicaciones retransmitiendo servicios de DNS, para obtener una dirección IP enrutable en la red desde un URL especificado mediante el usuario o los usuarios cuando acceden a un servicio (por ejemplo, una página web o contenido). Por lo tanto, con la presente invención es posible conocer con antelación el flujo que pasará a través de la red de comunicación, y preparar automáticamente la red de comunicación para manejarlo configurando reglas apropiadas en el controlador de SDN proporcionado.

Puesto que el controlador de SDN proporcionado permite un manejo más rico del flujo, la información mantenida en una base de datos separada (consultada en base a la resolución de DNS) hace posible un manejo afinado del flujo entrante (incorporando información complementaria tal como etiqueta VLAN, dirección MAC, puertos TCP/UDP, etc., o combinación de ellos, que podrían ser de interés para que el dominio maneje los flujos entrantes esperados).

Breve descripción de los dibujos

Las anteriores y otras ventajas y características se entenderán más completamente a partir de la siguiente

descripción detallada de realizaciones, con referencia a los dibujos adjuntos, que deben considerarse en una manera ilustrativa y no limitante, en los que:

La Figura 1 es una ilustración que muestra la estructura e interfaces del controlador de red propuesto o controlador de SDN para definir automáticamente reglas de reenvío para configurar un dispositivo de interconexión de red informático.

La Figura 2 es una ilustración que muestra la estructura de la base de datos y de las interfaces.

La Figura 3 ilustra el proceso de alto nivel realizado mediante la presente invención de acuerdo con algunas realizaciones.

Las Figuras 4 y 5 son dos ejemplos diferentes donde la presente invención es de relevancia particular. La Figura 4 es un ejemplo de aplicación de seguridad y la Figura 5 es un ejemplo de centro de datos virtual en una infraestructura de sistema informático en la nube.

Descripción detallada de varias realizaciones

La Figura 1 ilustra el controlador 100 de red propuesto, o controlador de SDN aumentado como se denominará a partir de ahora. El controlador 100 de SDN aumentado incluye un módulo de controlador de SDN convencional, en esta descripción denominado como el gestor 101 de controlador, y se aumenta incluyendo adicionalmente un módulo 102 de decisión que interactúa con un servidor 150 de DNS y con una base de datos 300.

El módulo 300 de decisión se encarga de: reenviar una petición de DNS al servidor 150 de DNS; recibir la respuesta desde el servidor 150 de DNS; consultar a la base de datos 300 para obtener información complementaria o afinada para la petición de DNS; informar al gestor 101 de controlador de un nuevo flujo que entra a la red de comunicación; y reenviar a otros módulos de decisión en la ruta de comunicación esa información para preparar sus segmentos de red correspondientes. La información recuperada desde el servidor 150 de DNS podría originar nuevas reglas de reenvío o no, dependiendo de la decisión del gestor 101 de controlador (es decir un flujo que entra podría coincidir con una regla existente, no produciendo entonces ninguna regla de flujo nueva).

Las interfaces principales del controlador 100 de SDN aumentado son:

- una interfaz S_A usada para la comunicación entre el gestor 101 de controlador y el módulo 102 de decisión. Desde el gestor 101 de controlador esta interfaz se usa para reenviar las peticiones de DNS desde el usuario 10 final al módulo 102 de decisión, para alcanzar el servidor 150 de DNS. Desde el módulo 102 de decisión, esta interfaz transporta la información recuperada desde el servidor 150 de DNS para informar al gestor 101 de controlador acerca de las características de un flujo entrante a la red de comunicación, para configurar con antelación los dispositivos de interconexión de red informáticos afectados (por ejemplo los conmutadores) en su dominio de red (o sub-red);
- una interfaz S_B usada para la comunicación entre el módulo 102 de decisión y el servidor 150 de DNS. Desde el módulo 102 de decisión esta interfaz se usa para reenviar al usuario final la petición de DNS al servidor 150 de DNS y para pedir los detalles para el nuevo flujo que entra a la red. Desde el servidor 150 de DNS esta interfaz se usa para proporcionar la resolución de nombre de dominio;
- una interfaz S_C usada para la comunicación entre el módulo 102 de decisión en el controlador de SDN aumentado del dominio de red del usuario final y uno o más módulo o módulos de decisión que pertenecen a otro controlador o controladores 100 de SDN aumentados en otros dominios de red en la ruta de extremo a extremo para distribuir los detalles del flujo usados para establecer reglas de flujo a lo largo de la ruta. Desde el módulo 102 de decisión en el dominio del usuario final, esta interfaz transporta los detalles del flujo. Desde el módulo o módulos de decisión en otros dominios de red en la ruta, esta interfaz se usa para realizar acuse de recibo a la información recibida; y
- una interfaz S_D se usa para consultar la base de datos 300 que contiene los detalles afinados para el flujo que pueden usarse para configurar nuevas reglas en los elementos de red a lo largo de la ruta de extremo a extremo. Desde el Controlador 100 de SDN aumentado esta interfaz se usa para obtener detalles de flujo adicionales útiles en un entorno de SDN. Desde la base de datos 300, esta interfaz se usa para suministrar tal información.

La Figura 2 ilustra la estructura de base de datos e interfaces propuestas. La base de datos 300 es el módulo específico encargado de recoger y almacenar información relevante del proveedor de servicios (o propietario de la red) de la red de comunicación para mejorar la información ofrecida mediante el servidor 150 de DNS. Varias fuentes de información pueden alimentar a la base de datos 300, como listas de reputación de Dominios externos, o dominios de interés del Proveedor para optimizar el tráfico, como dominios propios o dominios del cliente. Esta información se recupera mediante un módulo 303 colector y se procesa (incluyendo cualquier algoritmo de análisis y extracción de datos relevante) y finalmente se almacena en un módulo 302 gestor de base de datos. La indexación de la información de la base de datos se organiza para combinar datos de registros de DNS con la topología e

información contextual del proveedor de servicios, de esta manera, informar datos al controlador 100 de SDN aumentado optimizará el tiempo de proceso y reducirá el retardo. Esta última tarea se hace mediante un módulo 301 de información que podrá suministrar información de flujos afinada para construir reglas y políticas en el controlador 100 de SDN aumentado.

Las interfaces de la base de datos 300 son:

- una interfaz S_E usada para la comunicación con las diferentes fuentes de información. Esta interfaz transporta dos tipos diferentes de datos: uno interno para el proveedor de servicios y uno externo. Preferentemente las fuentes internas de datos vendrán de OSS/BSS, incluyendo bases de datos de topologías de Red, Herramientas de Inventario, Supervisión de Red, Flujos y orquestación de gráfico de servicio. Las fuentes de datos externas incluirán preferentemente información de seguridad, preferencias de clientes o información de itinerancia. Todos estos datos alimentan al módulo 303 colector con información relevante para adaptar dinámicamente la red de comunicación. Esta es la fuente principal de información usada mediante el módulo 303 colector para llevar a cabo el análisis y almacenamiento de subsecuencia;
- una interfaz S_G que usa un formato normalizado para tener un almacenamiento persistente de la información recogida mediante el módulo 303 colector en el módulo 302 gestor de base de datos;
- una interfaz S_F que permite la comunicación entre el módulo 301 de información y el módulo 302 gestor de base de datos. Esta interfaz intercambia información de consultas y respuestas al módulo 302 gestor de base de datos. Además, en modelos distribuidos podría también permitir escalabilidad y equilibrio de carga frente a varias bases de datos; y
- la interfaz previamente descrita S_D.

Con referencia ahora a la Figura 3 se ilustra una realización de la presente invención. En este caso, (1) cuando un usuario 10 final desea realizar un servicio dado tal como el (ella) desea recuperar alguna información de internet; por ejemplo una página web o contenido de medios, que se hace típicamente accediendo a tal información por medio de un URL, el (ella) realiza una petición para dicho servicio que genera un paquete para resolución de DNS. Tal paquete se intercepta e identifica como una petición de DNS mediante el gestor 101 de controlador del controlador 100 de SDN aumentado. La intercepción del paquete mediante el gestor 101 de controlador podría ser posible por varias razones. Por ejemplo, el controlador 100 de SDN aumentado puede incorporar funcionalidades de DNS intermediario. Otra posibilidad es que la petición de DNS alcance al controlador 100 de SDN aumentado como un primer paquete de un flujo sin flujo no configurado que maneje la entrada en la tabla de flujo, o que exista una entrada de flujo pre-configurada específica en la tabla de flujo que redirija todas las peticiones de DNS al controlador 100 de SDN aumentado.

A continuación, el módulo 102 de decisión reenvía (2) la petición del usuario final al servidor 150 de DNS para resolución de nombre que determina el dominio detrás del URL y reenvía la información determinada al módulo 102 de decisión. El nombre determinado mediante el servidor 150 de DNS puede reenviarse al usuario 10 final, directamente mediante el servidor 150 de DNS, o mediante el controlador 100 de SDN aumentado si está actuando como DNS intermediario. En cualquier caso, la resolución de nombre proporcionada al usuario 10 final es una resolución de DNS convencional.

El módulo 102 de decisión, después de recibir la información desde el servidor 150 de DNS, (3) consulta la base de datos 300 para recuperar la información complementaria o afinada para la petición de DNS (complementada con nuevos campos) para preparar la red de comunicación para el flujo entrante. Finalmente, después de que el gestor 101 de controlador procese, ejecutando un algoritmo, la información determinada proporcionada mediante el servidor 150 de DNS y la información afinada recuperada desde la base de datos 300, el gestor 101 de controlador establece (4) las entradas de reenvío requeridas en las tablas de flujo del dispositivo 120a de interconexión de red informático, en esta realización particular un conmutador, en su dominio o sub-red A, si fuera necesario.

El controlador 100 de SDN aumentado (en particular el módulo 102 de decisión del controlador 100 de SDN aumentado) puede transferir (5) también la información relevante acerca del flujo entrante a otros controladores 100a de SDN aumentados (a otros módulos de decisión) en la ruta de extremo a extremo donde otro usuario o usuarios finales 20 pueden conectarse. Esto puede hacerse por ejemplo basándose en una interfaz ascendente con un orquestador para ayudarles a preparar los segmentos de red correspondientes para el tráfico entrante. Por lo tanto, otros controladores 100a de SDN aumentados en otros dominios de red B de la red de comunicación pueden preconfigurar (6) los conmutadores 120b, 120c implicados en la ruta de extremo a extremo, si fuera necesario, de acuerdo con la información recibida mediante el controlador 100 de SDN aumentado del dominio de red A del usuario 10 final.

Finalmente el flujo (7) del usuario final hacia el destino deseado pasa a través de la red de comunicación sin desencadenar ninguna configuración de regla de flujo reactiva.

A continuación se detallan dos ejemplos diferentes en los que la presente invención es de particular relevancia.

Debe observarse que cada uno de los siguientes ejemplos tiene entidad en su totalidad por ellos mismos puesto que son aplicaciones específicas de la invención, pero pueden entenderse también como un mecanismo para definir la ruta y el orden entre los nodos de red de comunicación que ofrecen funciones de servicio en lo que se conoce como Concatenación de Función de Servicio (SFC), es decir la visión abstracta de las funciones de servicio requeridas y el orden en el que se han de aplicar (la Descripción detallada está disponible en el IETF WG SFC [7]).

Con referencia a la Figura 4 se ilustra un primer ejemplo para un sistema de seguridad, por ejemplo para un sistema de protección de Software Maligno que podría detectar y tratar tráfico malicioso. En particular, este sistema de seguridad incluirá en la base de datos 300 la información relevante acerca de la seguridad basada en la información de DNS. Podría añadirse diferente tipo de información:

I. Dominios de la lista negra, incluyendo dominios de contenido malicioso conocidos para correo basura, suplantación de identidad, descarga de software maligno, comando y control de controladores de redes robot;
II. Comportamiento de tráfico de DNS anormal, algunos ejemplos son la velocidad de consultas de DNS por origen y excesivas (la dirección MAC será la mejor identificación de origen único, pero no la única) que identifican un robot basado en algoritmo de generación de Dominio (DGA) o unas consultas de tipo MX masivas que indican generación de tráfico de CORREO BASURA;
III. Nombres de dominios raros, que incluyen palabras ininteligibles o sin sentido, generadas automáticamente y usadas para alojamiento de software maligno.

Toda esta información no forma parte de la invención, y puede obtenerse a partir de las fuentes externas o detectarse internamente y almacenarse en el módulo 302 gestor de base de datos.

Los datos de seguridad relacionados con los dominios se incluyen (1) en la base de datos 300, por lo que siempre que el Controlador 100 de SDN aumentado reciba un dispositivo o un flujo de tráfico de DNS de usuario, pedirá (2) a la base de datos 300 la información de seguridad complementada entorno a la petición de dominio. Cuando la información recuperada desde la base de datos 300 confirma un riesgo de seguridad (presencia relacionada con software maligno en el Dominio), el controlador 100 de SDN aumentado puede ejecutar (3) diferentes acciones basándose en la información complementaria. Por lo tanto, el controlador 100 de SDN aumentado puede redirigir con antelación (4) todo el tráfico desde esa fuente a una zona de red específica para tratar el tráfico (sensores de sumideros, remediación de usuario de portales cautivos, etc.), limpiar el tráfico en la red y proteger la fuente.

Otro tipo de caso de aplicación adicional para esta realización de seguridad es direccionamiento de tráfico de seguridad basado en información pre-programada. En este caso la base de datos 300 incluye (1) una información sensible como una lista de dominios sensibles o una lista de direcciones IP de fuente que debe tratarse diferente desde el punto de vista de seguridad (servicio en línea de bancos, servicios transaccionales de empresas, acceso de VPN de compañías, etc.). El proveedor de servicios o incluso los usuarios pueden definir estos dominios e incluirlos en la base de datos 300. El controlador 100 de SDN aumentado, basándose en la información complementaria (2) recibida desde la base de datos 300 preparará (3) la red con diferentes acciones: redirigir el tráfico de acceso que venga a la red desde el usuario para asegurar puntos de entrada (SecGW para el acceso móvil de 3G o 4G, o terminador de VPN, etc.) si el acceso físico no es seguro; y redirigir (5) el tráfico hacia el destino a los dispositivos o dominios de red que se encargarán de inspeccionar (DPI, IDS) y supervisar el tráfico desde el punto de vista de seguridad. Por lo tanto, la presente invención permite la combinación de las capacidades de SDN y la información de DNS para preparar y optimizar la redirección de tráfico evitando técnicas complejas (protocolos de enrutamiento, políticas de filtrado, etc.).

Debe observarse que SecGW se define en 3GPP TS 33.210 [5] en un modelo general para conectar dos dominios no seguros, pero en 3GPP TS 33.401 Sección 11, [6] se aplica a LTE móvil para proteger el acceso físico entre eNB, MME y S-GW.

La Figura 5 ilustra un segundo ejemplo para un centro de datos virtual en una infraestructura de sistema informático en la nube genérica (pública, privada y/o híbrida). El Sistema Informático en la Nube permite la compartición de la infraestructura física de una manera multi-abonado, gracias a las capacidades de virtualización de sistemas operativos existentes y tecnologías de IT en general. Los recursos asignados a un usuario pueden asignarse en diferentes centros de datos e incluso cambian en el tiempo, sin impacto para el usuario final. Existen varias ofertas comerciales basándose en infraestructuras en la nube donde se permite a los usuarios de estos sistemas desarrollar máquinas virtuales VM_A, VM_B en centros de datos separados DC_a, DC_b. Estas Máquinas Virtuales VM_A, VM_B se pretenden para proporcionar servicios, internos o externos a la red del usuario final. Debido a la flexibilidad proporcionada mediante estos sistemas, las máquinas virtuales VM_A, VM_B pueden migrarse entre centros de datos DC_a, DC_b sin impacto adicional.

El acceso más común y fácil a un servicio dado que se ejecuta en una máquina virtual VM_A será mediante una consulta de DNS, para ocultar la IP específica de la máquina virtual VM_A. A continuación, como una manera común de procedimiento, el centro de datos virtual DC_a desarrollará un servicio de DNS donde la resolución entre los

nombres de la máquina virtual y se proporciona la correspondiente IP, tanto para fines de comunicación interna como externa. Adicionalmente estos entornos en la nube empiezan a integrarse con soluciones basadas en SDN para provisión de conectividad. Las capacidades de SDN pueden extenderse más allá de los límites del centro de datos, incluyendo también las conexiones en una WAN, para una solución de conectividad de extremo a extremo uniforme.

En esta situación, la invención propuesta se hace beneficiosa puesto que la combinación de tanto SDN como DNS para establecer con antelación los enlaces de transporte requeridos en el entorno del centro de datos virtual DC_a. Todavía más, esta conectividad puede re-adaptarse de acuerdo con la asignación de nuevos recursos en un centro de datos diferente DC_b como en el caso de movilidad de máquina virtual. Cualquier nueva comunicación a una máquina virtual VM_A que necesite una consulta de DNS en un entorno de SDN permitirá identificar con antelación los flujos que cruzarán tanto el centro de datos DC_a como la red WAN.

Gracias a las tecnologías de Virtualización de Funciones de Red (NFV), se hace posible crear instancias de funciones de red virtual (VNF) en recursos informáticos de centros de datos. En consecuencia la realización presentada en este punto puede usarse como un mecanismo para definir concatenación de función de servicio entre tales VNF.

El alcance de la presente invención se determina mediante las reivindicaciones que siguen.

REIVINDICACIONES

1. Un controlador de red para definir automáticamente reglas de reenvío para configurar un dispositivo de interconexión de red, mediante el cual dicho controlador de red (100) está conectado a una sub-red (A) de una red de comunicación y comprende:

- un gestor de controlador (101) que recibe una petición para un servicio dado y define, ejecutando un algoritmo, reglas de reenvío relacionadas con dicho servicio e instala las reglas de reenvío definidas en un dispositivo de interconexión de red informático (120a) de la sub-red (A) de la red de comunicación para configurar el dispositivo de interconexión de red informático (120a) para dicho servicio dado,

caracterizado porque el controlador de red (100) comprende adicionalmente:

- un módulo de decisión (102) configurado para comunicar con el gestor de controlador (101) y configurado para interactuar con un servidor de DNS (150) para recibir una resolución determinada para una petición de DNS de dicha petición para dicho servicio dado, y con una base de datos (300) para recuperar información complementaria para la petición de DNS, para ayudar al gestor de controlador (101) a realizar la definición de las reglas de reenvío, alimentándose dicha base de datos (300) por diferentes fuentes de información; y
- una pluralidad de interfaces (S_A, S_B, S_D) para permitir la comunicación del módulo de decisión (102) con el gestor de controlador (101), el servidor de DNS (150) y la base de datos (300),

en el que la indexación de la información de la base de datos está organizada para combinar datos de registros de DNS con información de topología y contextual de un proveedor de servicios de la red de comunicación, y
en el que las diferentes fuentes de información comprenden información interna para dicho proveedor de servicios de la red de comunicación e información externa para dicho proveedor de servicios, en el que la información interna viene de Sistemas de Soporte a las Operaciones u OSS/Sistemas de Soporte Empresariales o BSS al menos incluyendo bases de datos de topologías de red, herramientas de inventario, supervisión de red y flujos y orquestación de gráfico de servicio; y la información externa al menos incluye información de seguridad, preferencias del usuario y/o información de itinerancia.

2. El dispositivo de la reivindicación 1, en el que el gestor de controlador (101) está conectado a al menos otro dispositivo de interconexión de red informático (120b) de dicha sub-red (A) de la red de comunicación para instalar las reglas de reenvío definidas en dicho otro dispositivo de interconexión de red informático (120b).

3. El dispositivo de cualquier reivindicación anterior, en el que el primer controlador de red (100) está conectado a al menos un segundo controlador de red (100a) de una sub-red (B) de la red de comunicación adyacente a la sub-red (A) para que el módulo de decisión (102) del primer controlador de red (100) envíe, a través de una interfaz correspondiente (S_c), la resolución determinada recibida desde el servidor de DNS (150) y recuperada desde la base de datos (300) a al menos otro módulo de decisión (102a) incluido en dicho segundo controlador de red (100a).

4. El dispositivo de la reivindicación 1, en el que dicha base de datos (300) comprende:

- un módulo de generación de información (301) para permitir la recuperación de dicha información complementaria para la petición de DNS a través de dicha interfaz (S_D) por el módulo de decisión (102);
- un módulo colector (303) para recoger dicha información complementaria para la petición de DNS desde dichas diferentes fuentes de información a través de una interfaz correspondiente (S_E); y
- un módulo gestor de base de datos (302) para almacenar la información complementaria recogida para la petición de DNS, teniendo dicho gestor de base de datos (302) dos interfaces diferentes, una primera (S_F) para comunicar con el módulo de generación de información (301) y una segunda (S_G) para comunicar con el módulo colector (303).

5. El dispositivo de las reivindicaciones anteriores, en el que el dispositivo de interconexión de red informático (120a, 120b) comprende un conmutador.

6. El controlador de red de las reivindicaciones anteriores, en el que el gestor de controlador (101) cumple con las especificaciones de la de la Interfaz del Plano de Control a Datos o CDPI.

7. Un método implementado por ordenador para definir automáticamente reglas de reenvío para configurar un dispositivo de interconexión de red informático, comprendiendo el método:

- recibir, mediante un gestor de controlador (101) de un controlador de red (100) conectado a una sub-red (A) de una red de comunicación, una petición para un servicio dado; y
- definir, por dicho gestor de controlador (101), ejecutando un algoritmo, reglas de reenvío relacionadas con dicho servicio dado, e instalar las reglas de reenvío definidas en un dispositivo de interconexión de red informático

(120a) de la sub-red (A) de la red de comunicación para configurar el dispositivo de interconexión de red informático (120a) para el servicio dado,
caracterizado porque el método comprende:

- reenviar, mediante un módulo de decisión (102) del controlador de red (100) en comunicación con el gestor de controlador (101), una petición de DNS de dicha petición para el servicio dado a un servidor de DNS (150), determinando el último una resolución para la petición de DNS y reenviando adicionalmente la resolución determinada al módulo de decisión (102); y
- recuperar, mediante el módulo de decisión (102), después de recibir la resolución determinada desde el servidor de DNS (150), información complementaria para la petición de DNS desde una base de datos (300), alimentándose la base de datos (300) por diferentes fuentes de información,
de modo que el módulo de decisión (102) ayuda al gestor de controlador (101) a realizar la definición de las reglas de reenvío,
en el que la indexación de la información de base de datos está organizada para combinar datos de registros de DNS con información de topología y contextual de un proveedor de servicios de la red de comunicación, y
en el que las diferentes fuentes de información comprenden información interna para dicho proveedor de servicios de la red de comunicación e información externa para dicho proveedor de servicios, en el que la información interna viene de Sistemas de Soporte a las Operaciones u OSS/Sistemas de Soporte Empresariales o BSS al menos incluyendo bases de datos de topologías de red, herramientas de inventario, supervisión de red y flujos y orquestación de gráfico de servicio; y la información externa al menos incluye información de seguridad, preferencias del usuario y/o información de itinerancia.

8. El método de la reivindicación 7, que comprende adicionalmente instalar, por el gestor de controlador (101), las reglas de reenvío definidas en al menos otro dispositivo de interconexión de red informático (120b) de dicha sub-red (A) de la red de comunicación.

9. El método de la reivindicación anterior 7 u 8, que comprende adicionalmente enviar, por el módulo de decisión (102), la resolución determinada recibida desde el servidor de DNS (150) y la información complementaria recuperada desde la base de datos (300) a al menos otro módulo de decisión (102a) incluido en otro controlador de red (100a) de una sub-red (B) de la red de comunicación adyacente a la sub-red (A).

10. El método de cualquiera de las reivindicaciones anteriores 7 a 9, en el que la petición para el servicio dado se realiza por un usuario (10) conectado al dispositivo de interconexión de red informático (120a) por medio de un dispositivo informático.

11. El método de cualquiera de las reivindicaciones anteriores 7 a 9, en el que la petición para el servicio dado se realiza por al menos un centro de datos conectado al dispositivo de interconexión de red informático (120a).

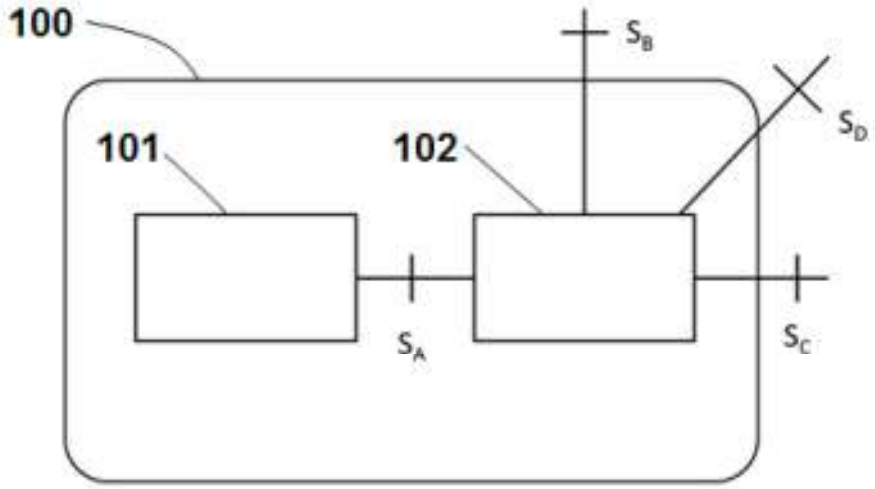


Fig. 1

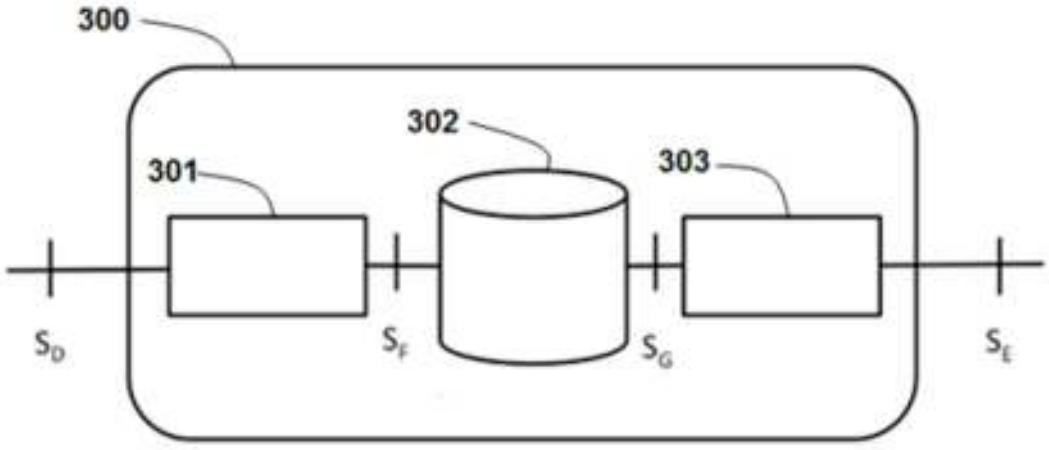


Fig. 2

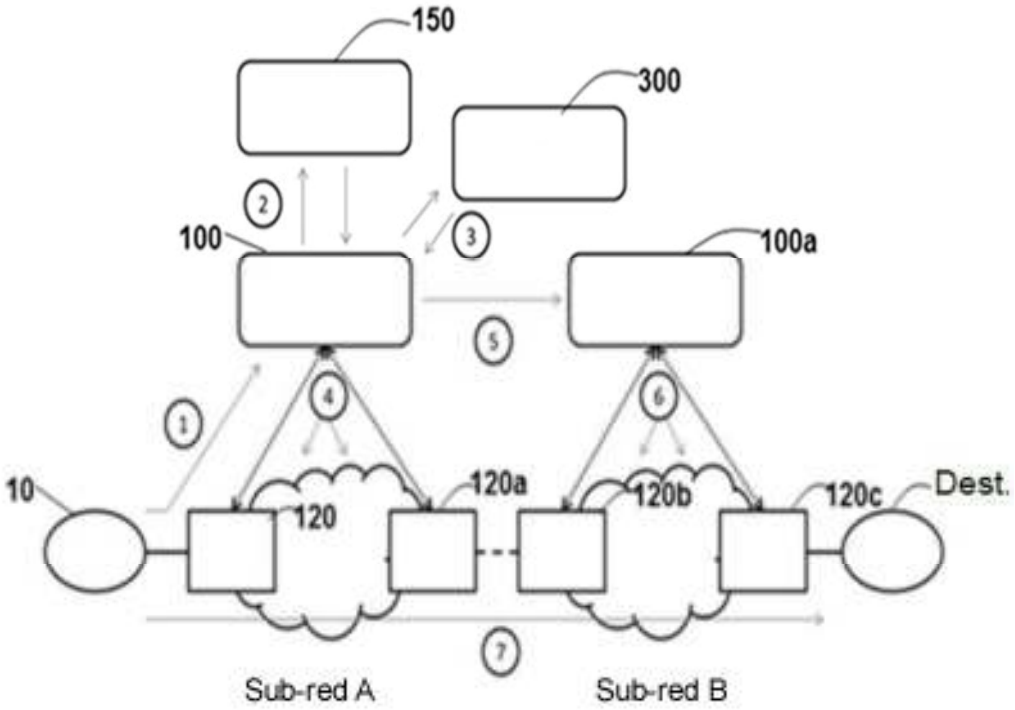

150
300
100
100a
2
3
5
1
4
6
10
120
120a
120b
120c
Dest.
7
Sub-red A
Sub-red B

Fig. 3

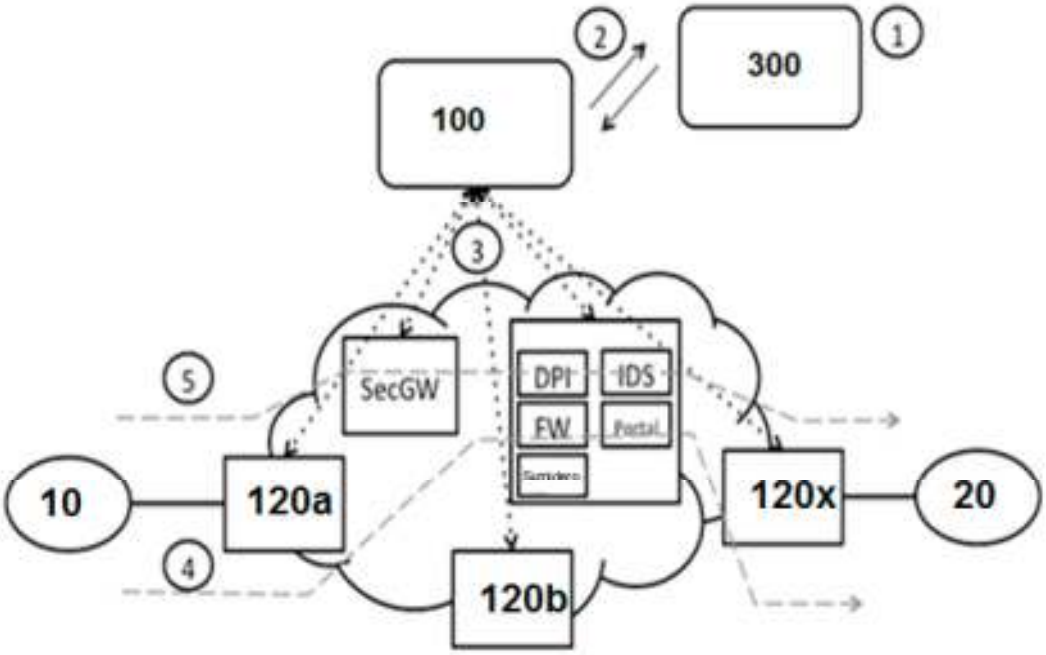
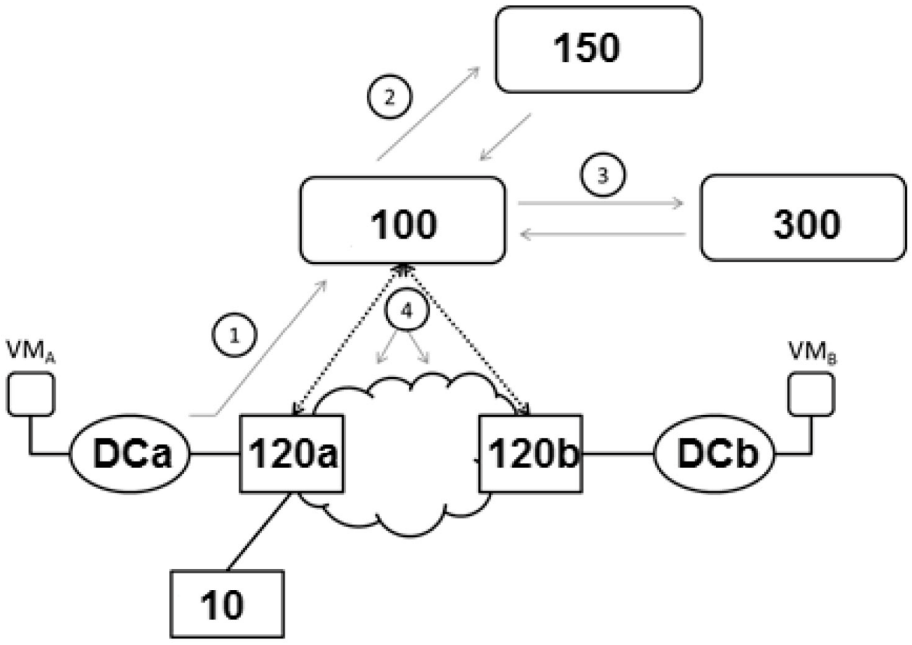
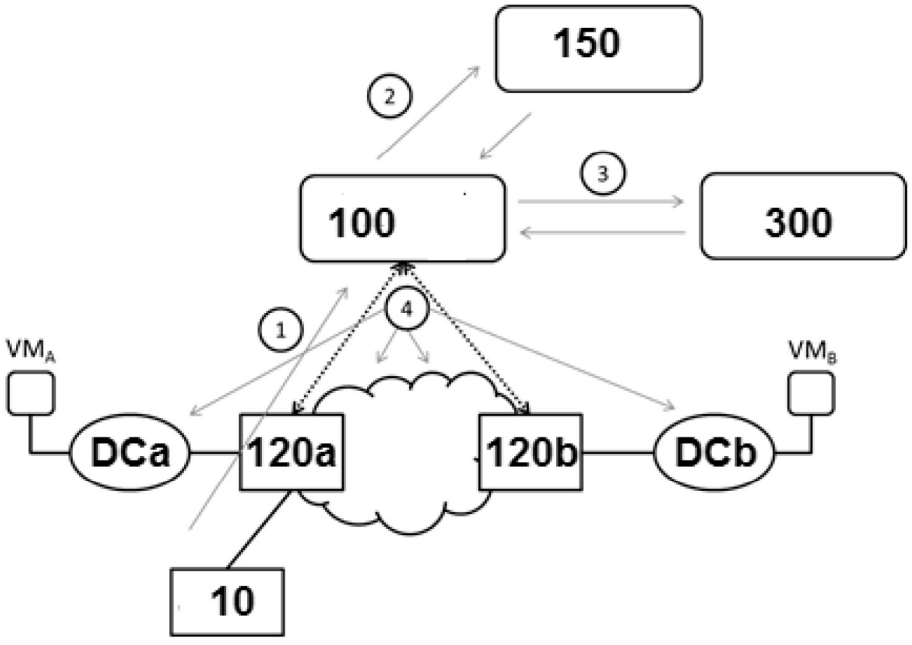

1
2
300
100
3
5
SecGW
DPI
IDS
FW
Portal
Servidores
10
120a
120x
20
4
120b

Fig. 4


150
2
3
100
300
4
1
VMA
VMB
DCa
120a
120b
DCb
10

(a)


150
2
3
100
300
4
1
VMA
VMB
DCa
120a
120b
DCb
10

(b)

Fig. 5