Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1042

(01/2019)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Seguridad de la información y de las redes – Seguridad de las redes

Servicios de seguridad que utilizan las redes definidas por *software*

Recomendación UIT-T X.1042

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	**X.1030–X.1049**
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD (1)	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad (1)	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD (2)	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
Seguridad de las redes eléctricas inteligentes	X.1330–X.1339
Recomendaciones relacionadas con la PKI	X.1340–X.1349
Seguridad en la Internet de las cosas (IoT)	X.1360–X.1369
Seguridad en los sistemas de transporte inteligente (ITS)	X.1370–X.1379
Seguridad de tecnología de libro mayor distribuido	X.1400–X.1429
Seguridad de tecnología de libro mayor distribuido	X.1430–X.1449
Protocolos de seguridad (2)	X.1450–X.1459
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/heurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1042

Servicios de seguridad que utilizan las redes definidas por *software*

Resumen

La Recomendación UIT-T X.1042 permite la protección de los recursos de red mediante la utilización de servicios de seguridad basados en las redes definidas por *software* (SDN). En la presente Recomendación se procede, en primer lugar, a la clasificación de los recursos de red para los servicios de seguridad basados en las redes SDN, a saber, la aplicación SDN, el controlador SDN, el conmutador SDN y el administrador de seguridad (SM). Después, la Recomendación UIT-T X.1042 define los servicios de seguridad basados en las SDN.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	UIT-T X.1042	30-01-2019	17	11.1002/1000/13803

Palabras clave

Control de acceso, ataques DDoS, cortafuegos, señuelo (tarro de miel), redes definidas por *software* (SDN), escenarios de seguridad.

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Recomendación UIT-T X.1042

Servicios de seguridad que utilizan las redes definidas por *software*

1 Alcance

La presente Recomendación permite la protección de los recursos de red mediante servicios de seguridad basados en las redes definidas por *software* (SDN) y abarca las siguientes cuestiones:

– la clasificación de los recursos de red que podrían protegerse mediante servicios de seguridad basados en la SDN;

– la definición de los servicios de seguridad basados en la SDN;

– la descripción de la manera de implementar los servicios de seguridad basados en la SDN.

La protección de los recursos de red (encaminador, conmutador, sistemas cortafuegos y de detección de intrusión, entre otros) mediante los servicios de seguridad basados en la SDN supone:

– la reacción inmediata ante nuevos ataques a la red (por ejemplo, ataques basados en gusanos y ataques de denegación de servicio distribuido (DDoS));

– la construcción de redes privadas para mitigar los ataques sofisticados a la red;

– la protección automática contra los ataques a la red sin la intervención de los administradores de red;

– la asignación dinámica de recursos adaptada a la carga de la red.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se alienta a los usuarios de esta Recomendación a que investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En la presente Recomendación, la referencia a un documento no confiere a este último, como documento autónomo, la categoría de una Recomendación.

[UIT-T Y.3300] Recomendación UIT-T Y.3300 (2014), *Marco para las redes definidas por software.*

[UIT-T Y.3301] Recomendación UIT-T Y.3301 (2016), *Requisitos funcionales de la conexión en red definida por software*.

[UIT-T Y.3302] Recomendación UIT-T Y.3302 (2017), *Arquitectura funcional de la conexión en red definida por software*.

3 Definiciones

3.1 Términos definidos en otros textos

La presente Recomendación utiliza los siguientes términos que han sido definidos en otros textos:

3.1.1 redes definidas por *software* [UIT-T Y.3300]: conjunto de técnicas que permiten programar, orquestar, controlar y gestionar directamente recursos de red, facilitando así la concepción, suministro y explotación de servicios de red de forma dinámica y evolutiva.

3.1.2 control de acceso [b-UIT-T X.1252]: procedimiento utilizado para determinar si se debe conceder a una entidad acceso a recursos, instalaciones, servicios o información sobre la base de normas preestablecidas, derechos específicos o autoridad que ostente la parte solicitante.

3.1.3 política de control de acceso [b-UIT-T X.812]: conjunto de reglas que definen las condiciones bajo las cuales puede tener lugar un acceso.

3.1.4 reglas de política de control de acceso [b-UIT-T X.812]: reglas de política de seguridad relativas a la provisión de servicios de control de acceso.

3.2 Términos definidos en la presente Recomendación

En la presente Recomendación se definen los siguientes términos:

3.2.1 recurso de red: un dispositivo que realiza la transmisión de paquetes en un sistema de red.

NOTA – Entre los recursos de red figuran conmutadores, encaminadores, pasarelas y puntos de acceso Wi-Fi.

3.2.2 cortafuegos: dispositivo o servicio en la unión de dos segmentos de red que inspecciona cada paquete que intenta cruzar el límite entre ambos. También rechaza los paquetes que quedan descalificados con arreglo a determinados criterios como, por ejemplo, la presencia de números de puerto o direcciones IP no permitidos.

NOTA – Los servicios de cortafuegos pueden estar separados de los dispositivos físicos y funcionar como aplicación.

3.2.3 señuelo (tarro de miel): un mecanismo de seguridad informática configurado como cebo para engañar a los ciberatacantes. Se utiliza para detectar o desviar ataques desde un objetivo legítimo y para recopilar datos sobre el ataque. La expresión "tarro de miel" se utiliza para referirse al comportamiento que adopta el sistema, que atrae a los atacantes ("abejas") hacia un lugar determinado (el objetivo del ataque o "miel"), que se utiliza a modo de trampa.

3.2.4 servicio de cortafuegos centralizado: un servicio que puede crear y distribuir reglas de política de control de acceso que se incorporan en los recursos de red para asegurar una gestión de cortafuegos eficaz. Esas reglas son gestionadas dinámicamente por un servidor centralizado. Las redes definidas por *software* (SDN) pueden funcionar como servicio de cortafuegos centralizado mediante una interfaz normalizada entre las aplicaciones cortafuegos y los recursos de red.

3.2.5 servicio de mitigación de ataques DDoS centralizado: un servicio que puede crear y distribuir reglas de política de control de acceso que se incorporan en los recursos de red para mitigar eficazmente los ataques de denegación de servicio distribuido (DDoS). Esas reglas son gestionadas dinámicamente por un servidor centralizado. Las redes definidas por *software* (SDN) pueden funcionar como servicio centralizado de mitigación de ataques DDoS mediante una interfaz normalizada entre las aplicaciones de mitigación de los ataques DDoS y los recursos de red.

3.2.6 servicio de señuelo centralizado: un servicio que puede crear y distribuir reglas de política de control de acceso que se incorporan en los recursos de red para configurar dinámicamente el método del señuelo. Esas reglas son gestionadas dinámicamente por un servidor centralizado. Las redes definidas por *software* (SDN) pueden funcionar como servicio de señuelo centralizado mediante una interfaz normalizada entre las aplicaciones de señuelo y los recursos de red.

3.2.7 servicio de gestión de dispositivos ilícitos centralizado: un servicio que puede crear y distribuir reglas de política de control de acceso que se incorporan en los recursos de red para confeccionar una lista negra de dispositivos ilícitos. Esas reglas pueden gestionarse dinámicamente y de manera global por un servidor centralizado. La red definida por *software* (SDN) puede funcionar como un gestor de dispositivos ilícitos basado en la red mediante una interfaz normalizada entre las aplicaciones de gestión de los dispositivos ilícitos y los recursos de red.

NOTA – Queda fuera del alcance de la presente Recomendación el establecimiento de un criterio para definir un dispositivo como ilícito. La gestión de dispositivos ilícitos se puede determinar, por ejemplo, mediante el uso del sistema de identificación único mundial.

3.2.8 servicio de gestión del control de acceso: un servicio que puede establecer y distribuir políticas de derechos de acceso en los recursos de red para la lista blanca de dispositivos de Internet de las cosas (IoT). Esas políticas pueden gestionarse dinámicamente y de manera global por un servidor centralizado. La red definida por *software* (SDN) puede funcionar como un gestor de dispositivos de IoT basado en la red mediante una interfaz normalizada entre las aplicaciones de gestión del control de acceso y los recursos de red.

NOTA – La especificación de una composición jerárquica de las políticas de acceso queda fuera del ámbito de aplicación de la presente Recomendación. Estas políticas de acceso pueden componerse y dividirse en función del nivel de seguridad de los recursos de la red y distribuirse en el sistema de red.

4 Abreviaturas y acrónimos

Esta Recomendación hace uso de las siguientes abreviaturas y acrónimos:

ACI Interfaz de control de aplicaciones (*application control interface*)

ACM Gestión del control de acceso (*access control management*)

AL-MSO Capa de aplicación – soporte de la gestión y orquestación (*application layer management support and orchestration*)

ALM Gestión de la capa de aplicación (*application layer management*)

BSS Sistema de apoyo empresarial (*business support system*)

CL-AS Capa de control – soporte de la aplicación (*control layer application support*)

CL-CLS Capa de control – servicio de la capa de control (*control layer control layer services*)

CL-MSO Capa de control – soporte de la gestión y orquestación (*control layer management support and orchestration*)

CL-RA Capa de control – abstracción de los recursos (*control layer resource abstraction*)

CLM Gestión de la capa de control (*control layer management*)

DDoS Denegación de servicio distribuido (*distributed denial-of-service*)

DNS Sistema de nombre de dominio (*domain name service*)

I2NSF Interfaz con la función de seguridad de red (*interface to network security function*)

IDP Inspección detallada de paquetes

IoT Internet de las cosas (*Internet of things*)

IP Protocolo Internet (*Internet protocol*)

MAC Control de acceso a los medios (*media access control*)

MMF Función de gestión multicapa (*multi-layer management function*)

MMFA Función de gestión multicapa – capa de aplicación (*multi-layer management function application layer*)

MMFC Función de gestión multicapa – capa de control (*multi-layer management function control layer*)

MMFO Función de gestión multicapa – sistemas OSS/BSS (*multi-layer management function OSS/BSS*)

MMFR Función de gestión multicapa – capa de recursos (*multi-layer management function resource layer*)

NSF Función de seguridad de red (*network security function*)

OSS Sistema de soporte de operaciones (*operation support system*)

RCI Interfaz de control de recursos (*resource control interface*)

RLM Gestión de la capa de recursos (*resource layer management*)

RL-MS Capa de recursos – soporte de la gestión (*resource layer management support*)

SDN Redes definidas por *software* (*software-defined networking*)

SDN-AL Capa de aplicación de las redes definidas por *software* (*software-defined networking – application layer*)

SDN-CL Capa de control de las redes definidas por *software* (*software-defined networking – control laye*r)

SDN-RL Capa de recursos de las redes definidas por *software* (*software-defined networking – resource layer*)

SIP Protocolo de iniciación de sesión (*session initiation protocol*)

SM Administrador de seguridad (*security manager*)

TCP Protocolo de control de transmisión (*transmission control protocol*)

VoIP Voz por el protocolo de Internet (*voice over Internet protocol*)

VoLTE Voz por el sistema de evolución a largo plazo (*voice over long-term evolution*)

5 Convenios

En la presente Recomendación:

La expresión "se requiere" indica que el requisito es absolutamente obligatorio y debe aplicarse sin excepción si se pretende declarar la conformidad con la presente Recomendación.

La expresión "se recomienda" indica que se trata de un requisito recomendado y que, por ende, no es absolutamente obligatorio. El cumplimiento de ese requisito no es necesario para acreditar la conformidad.

La expresión "se prohíbe" indica un requisito que debe cumplirse estrictamente, sin permitirse desviación alguna si la Recomendación pretende ser conforme.

La expresión "se tiene la opción de" u "opcionalmente" indica que el requisito se permite, sin que ello signifique que se recomienda. El uso de este término no implica que el fabricante deba ofrecer esta opción y que el operador de red/proveedor de servicio tenga la posibilidad de activarla. Significa, más bien, que el fabricante tiene la opción de proporcionar esta función sin que ello afecte a la conformidad con la presente especificación.

6 Visión general de la arquitectura funcional de la SDN

En esta cláusula se describe la arquitectura de referencia de alto nivel relativa a los servicios de seguridad (por ejemplo, cortafuegos y mitigación de los ataques DDoS) mediante la arquitectura de alto nivel SDN [UIT-T Y.3300], como el servicio de cortafuegos centralizado y el servicio de mitigación de los ataques DDoS centralizado.

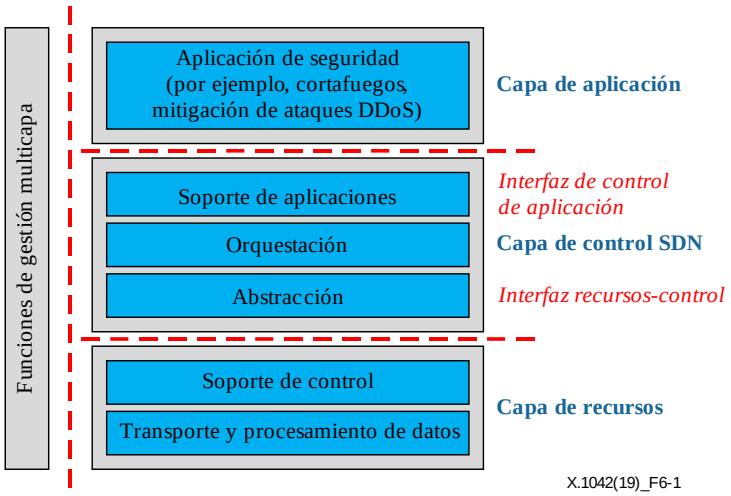


Figura 6-1 – Arquitectura de alto nivel de los servicios de seguridad basados en la SDN

Como se puede apreciar en la Figura 6-1, las aplicaciones para los servicios de seguridad (por ejemplo, los servicios de cortafuegos, mitigación de los ataques de DDoS y señuelo) se ejecutan por encima de la arquitectura SDN. Cuando un usuario o administrador (por ejemplo, la gestión de la capa de aplicación (ALM) de la Figura 6-2) implanta políticas de seguridad para los servicios de seguridad a través de una interfaz de aplicación, el controlador SDN genera las reglas de control de acceso correspondientes para la ejecución rápida y autónoma de esas políticas de seguridad. Según las reglas de control de acceso, los recursos de red generados como los conmutadores SDN actúan para mitigar los ataques a la red, por ejemplo, suprimiendo los paquetes con patrones sospechosos.

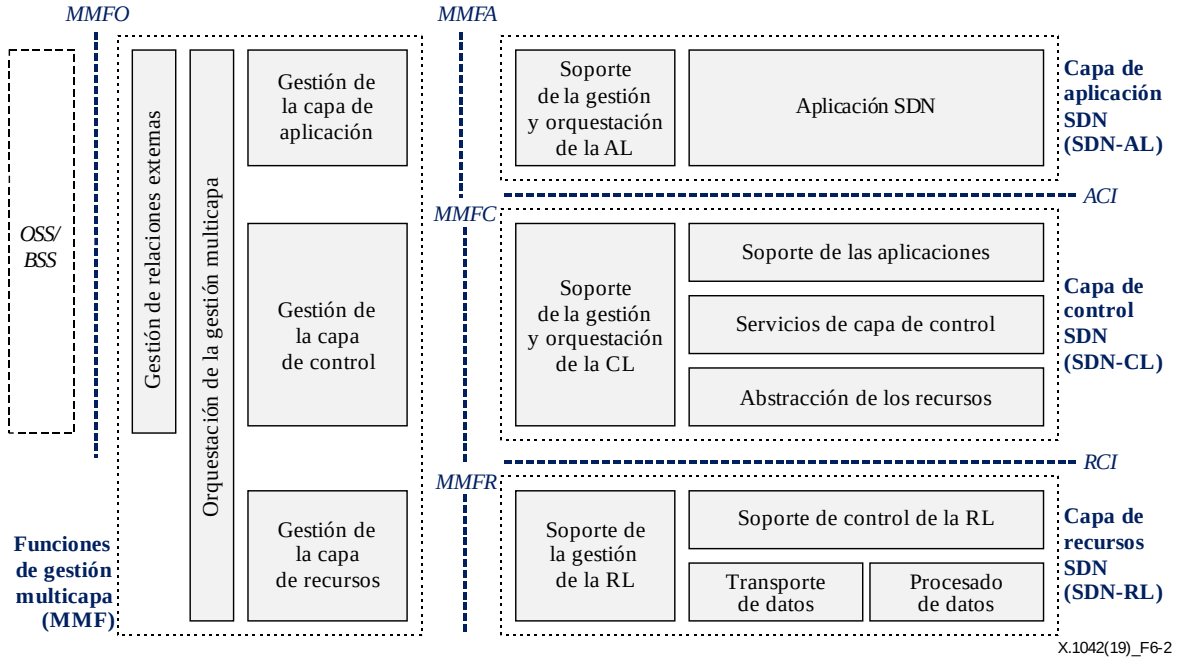
En la Figura 6-2 se muestra la arquitectura funcional de la SDN [UIT-T Y.3302], que se basa en la arquitectura de alto nivel de la SDN.

– Capa de aplicación de las redes definidas por *software* (SDN-AL): la SDN-AL consta del soporte de la gestión y orquestación de la AL (AL-MSO) y de varios componentes funcionales de aplicaciones SDN [UIT-T Y.3302]. El AL-MSO interactúa con el componente funcional de ALM en la función de gestión multicapa (MMF) a través del punto de referencia de la función de gestión multicapa – capa de aplicación (MMFA), con el fin de apoyar la gestión de las aplicaciones SDN y permitir operaciones conjuntas de gestión en todas las subcapas de las SDN. Las aplicaciones SDN interactúan con la capa de control de las redes definidas por *software* (SDN-CL) a través del punto de referencia de la interfaz de control de aplicaciones (ACI), pidiendo que la SDN-CL personalice automáticamente el comportamiento y las propiedades de los recursos de red. Las aplicaciones SDN usan la vista abstracta y el estado de los recursos de red que proporciona la SDN-CL mediante los modelos de información y datos expuestos a través del punto de referencia de la ACI. Opcionalmente, y dependiendo del tipo de uso de la SDN (por ejemplo, en/entre los centros de datos, las redes móviles, las redes de acceso), se pueden definir diferentes ACI. Se da por supuesto que las ACI usan interfaces de programación de aplicaciones abiertas.

– SDN-CL: la SDN-CL consta de la capa de control – soporte de la gestión y orquestación (CL-MSO), la capa de control – soporte de la aplicación (CL-AS), la capa de control – servicio de la capa de control (CL-CLS) y la capa de control – abstracción de los recursos (CL-RA). La SDN-CL ofrece los medios programables para controlar el comportamiento de los recursos SDN (como el transporte de datos y los recursos de procesamiento), en función de las solicitudes de la capa de aplicación SDN (SDN-AL) y las políticas de la MMF. La SDN-CL actúa sobre los recursos suministrados por la capa de recursos de las redes definidas por *software* (SDN-RL) y expone una vista abstracta de la red a la SDN-AL. La SDN-CL interactúa con la SDN-RL mediante un punto de referencia de la interfaz de control de

recursos (RCI), con un componente funcional de la gestión de la capa de control (CLM) en la MMF, utilizando el punto de referencia de la función de gestión multicapa – capa de control (MMFC). También interactúa con la SDN-AL utilizando un punto de referencia de la ACI. El CL-MSO puede solicitar a la MMF que delegue algunas funciones de gestión. La MMF proporciona una serie de funcionalidades para administrar las funcionalidades de SDN-CL a través del punto de referencia de la MMFC.

– SDN-RL: la SDN-RL incluye la capa de recursos – soporte de la gestión (RL-MS), el control de la capa de recursos, el procesamiento de datos de la capa de recursos y el transporte de datos de la capa de recursos. La SDN-RL es donde los elementos de la red física o virtual efectúan el transporte y/o procesamiento de los paquetes de datos en función de las decisiones de la SDN-CL. La información sobre la provisión de políticas (incluida la información sobre la configuración), que son consecuencia de decisiones de la SDN-CL así como de información sobre los recursos de red, se intercambia a través del punto de referencia de la RCI. La información intercambiada a través de la interfaz RCI incluye la información de control suministrada por la SDN-CL a la SDN-RL (por ejemplo, para configurar un recurso de red o proporcionar políticas), así como la información relativa a las notificaciones enviadas por la SDN-RL cuando se detecta un cambio en los recursos de la red (siempre que se disponga de esa información). El RL-MS ofrece una descripción del recurso: proveedor, versión del programa informático y estado (por ejemplo, carga de la unidad central de procesamiento (CPU), el almacenamiento o la memoria de acceso aleatorio (RAM) usados). Puede incluir un agente de gestión que realiza algunas operaciones locales de gestión delegadas, en su caso, por la MMF. La MMF ofrece funcionalidades que permiten administrar las funcionalidades de la SDN-RL a través del punto de referencia de la función de gestión multicapa – capa de recursos (MMFR).



BSS: Sistema de apoyo empresarial; MMFO: Función de gestión multicapa – sistemas OSS/BSS; OSS: Sistema de soporte de operaciones.

Figura 6-2 – Arquitectura funcional de una SDN [UIT-T Y.3302]

7 Clasificación de los recursos de red

En esta cláusula se definen cuatro recursos de red para los servicios de seguridad que utilizan las SDN sobre la base de la Figura 6-2:

1) Aplicación SDN: un servicio que comunica al controlador SDN de forma explícita, directa y programática sus requisitos de red y la pauta de comportamiento de red deseada, a través de una interfaz ascendente como la ACI en la Figura 6-2. Además, las aplicaciones de red definida por *software* pueden utilizar una vista abstracta de la red para fines de toma de decisiones interna. Por ejemplo, los servicios como los cortafuegos, el método del señuelo, la mitigación de los ataques de DDoS y la gestión de dispositivos ilícitos se pueden suministrar como aplicaciones. A efectos de la gestión de fallos, la configuración, la contabilidad, el rendimiento y la seguridad, se requiere que estas aplicaciones SDN interactúen con la gestión de la capa de aplicación (ALM) a través del AL-MSO. Además, estas aplicaciones también crean reglas de acceso, por lo que es preciso que interactúen también con la SDN-CL a través de las ACI para asegurar la aplicación de las reglas de acceso.

2) Controlador SDN: una entidad centralizada lógicamente que: i) convierte los requisitos de las aplicaciones SDN en términos comprensibles para los conmutadores SDN; y ii) proporciona vistas abstractas de la red a las aplicaciones que contengan información útil sobre la red, como estadísticas y eventos de tráfico. En otras palabras, el controlador SDN crea entradas de flujos sobre la base de las reglas de acceso que recibe de las aplicaciones SDN. Por lo tanto, se requiere la interacción del controlador SDN con la gestión de la capa de control (CLM), las aplicaciones SDN y la SDN-RL.

3) Conmutador SDN: un programa informático o un dispositivo físico que transmite paquetes en un entorno SDN. Los conmutadores SDN son capaces de almacenar reglas para la transmisión de paquetes administradas por un controlador SDN a través de una interfaz descendente como la RCI de la Figura 6-2. Se requiere, por lo tanto, que el conmutador SDN interactúe con la gestión de la capa de recursos (RLM) y la SDN-CL.

4) Administrador de seguridad (SM): una función de la ALM que transfiere las políticas de seguridad a una aplicación SDN. Por lo tanto, se requiere que el administrador de seguridad interactúe con las aplicaciones SDN mediante la AL-MSO. En la Figura 7-1 se observa la ubicación de los recursos de la red de la Figura 6-2. Se requiere que esos recursos de red cumplan los requisitos de la [UIT Y.3301].

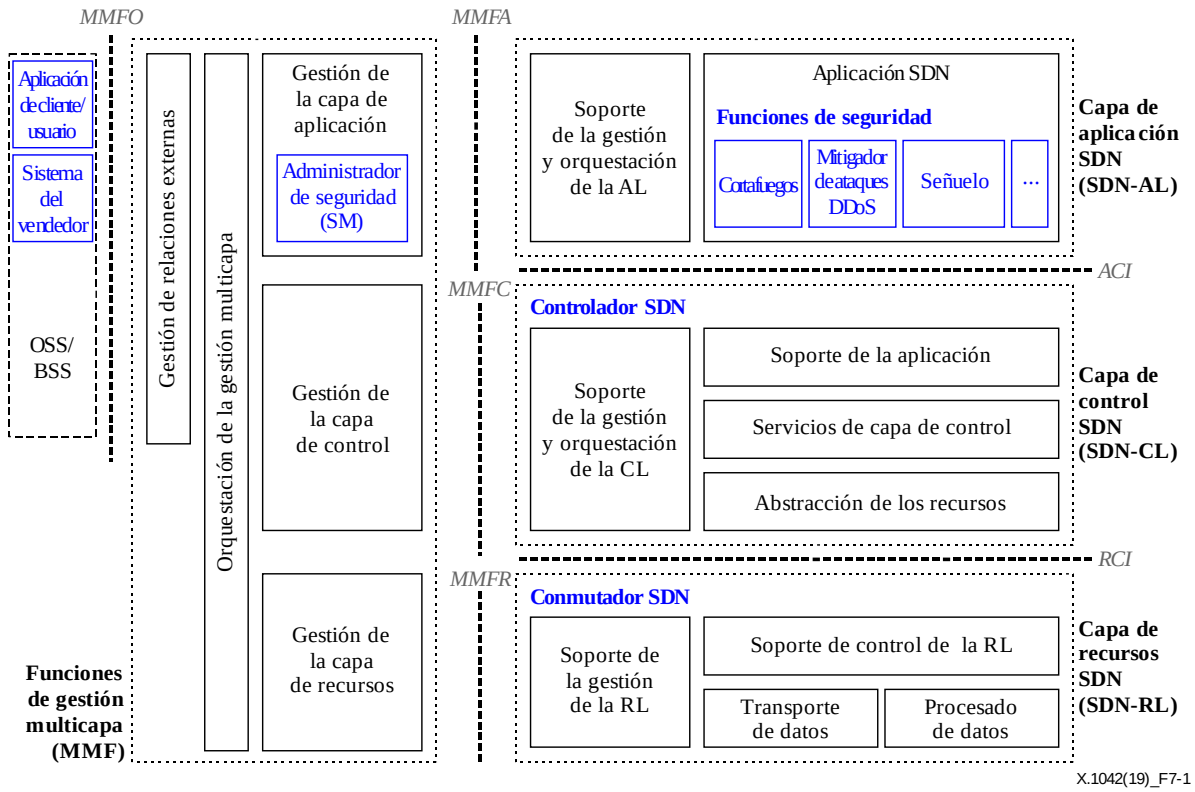


Figura 7-1 – Recursos de la red en los servicios de seguridad basados en las SDN

8 Servicios de seguridad basados en las SDN

En esta cláusula se presentan los servicios de seguridad que utilizan las SDN en dos tipos de redes: i) las redes intradominio, por ejemplo, los servicios de cortafuegos centralizados y los servicios de señuelo centralizados; y ii) las redes de red interdominios, por ejemplo, los servicios de mitigación de ataques DDoS centralizados y los servicios de gestión de dispositivos ilícitos centralizados. A efectos de la presente Recomendación, el dominio se refiere a un grupo de recursos de red que se administra sobre la base de reglas y procedimientos comunes.

8.1 Servicio de cortafuegos centralizado

8.1.1 Concepto básico del servicio de cortafuegos centralizado

En esta cláusula se describe el concepto básico del servicio de cortafuegos centralizado. Este servicio gestiona los recursos de red para permitir que las reglas de cortafuegos se cumplan de forma flexible. En la Figura 8-1 se observa que un cortafuegos centralizado gestiona los conmutadores SDN y que se pueden añadir o suprimir reglas de cortafuegos a esos conmutadores.

NOTA – Si bien es fácil trasladar una estrategia de filtrado de paquetes emitida por la aplicación cortafuegos a una tabla de flujos a través del controlador, el protocolo entre el controlador y los conmutadores (por ejemplo, los protocolos OpenFlow y NETCONF) de momento solo puede utilizarse con la capa del protocolo de control de transmisión (TCP), no existiendo un campo correspondiente para introducir la información de identificación del paquete de datos por encima de la capa TCP. Por consiguiente, no es posible implementar una estrategia cortafuegos para identificar la información por encima de la capa TCP sin una modificación del protocolo.

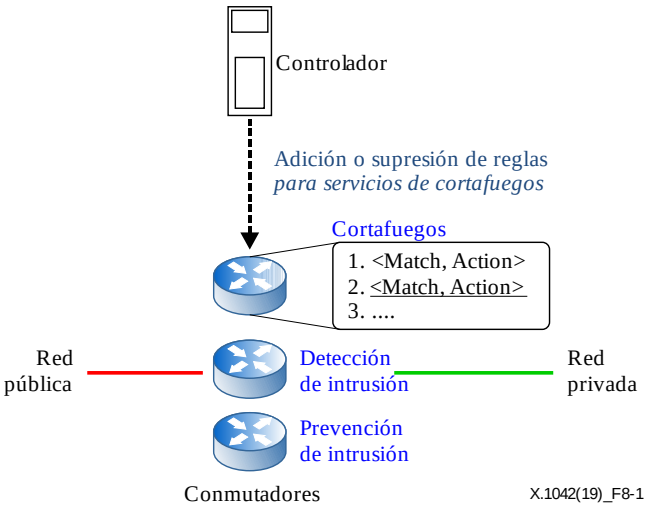


Figura 8-1 – Características de los servicios de cortafuegos centralizados

8.1.2 Escenario de funcionamiento del servicio de cortafuegos centralizado

En la Figura 8-2 se ilustra un ejemplo de escenario de servicio de cortafuegos centralizado destinado a bloquear la propagación de un gusano informático.

Como condición previa de este escenario, el administrador de seguridad (SM) deberá transmitir una nueva política a la aplicación cortafuegos en el momento en que recibe información de la presencia de un nuevo gusano. Para impedir la propagación de los paquetes que transportan el gusano, el usuario podría añadir la nueva política (por ejemplo, "suprimir los paquetes con archivo gusano") en la aplicación cortafuegos que opera por encima del controlador SDN. También puede gestionarse de forma centralizada, en cuyo caso, el SM podría determinar las políticas de seguridad de la aplicación cortafuegos a través de un punto único, es decir, un controlador SDN.

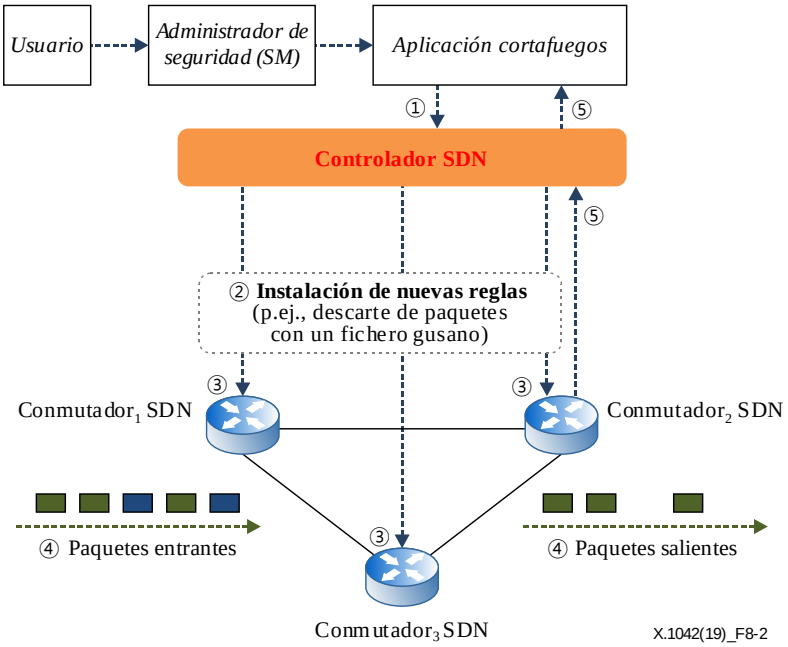


Figura 8-2 – Escenario intradominio de un servicio de cortafuegos centralizado

– Etapa 1: la aplicación cortafuegos instala nuevas reglas.

  La aplicación cortafuegos definirá una nueva regla cuando reciba la notificación de un nuevo gusano. La nueva regla (por ejemplo, "suprimir los paquetes con archivo gusano") se incorpora en el controlador SDN.

– Etapa 2: el controlador SDN distribuye una nueva entrada de flujo a todos los conmutadores SDN.

  Una vez instalada, el controlador SDN distribuye la nueva entrada de flujo a todos los conmutadores. Así pues, el controlador SDN transmite una operación de inserción de flujo que contiene la regla en cuestión (por ejemplo, "suprimir los paquetes con archivo gusano") a todos los conmutadores SDN.

  Ese nuevo gusano notificado en esta cláusula puede ser un gusano conocido o un gusano que se encuentra "en su día cero". En el caso de gusanos conocidos, en el servicio de cortafuegos se definen mecanismos como la "firma" y la "huella dactilar" con el fin de detectarlo y rechazarlo. Sin embargo, un gusano en su "día cero" debe someterse a un procedimiento de exploración y detección para poder aplicar posteriormente una contramedida defensiva. Los gusanos transportan una carga útil maliciosa que puede explotar algunas aplicaciones o servicios vulnerables. Esos gusanos pueden detectarse mediante la inspección de la carga útil del paquete. En el Apéndice II se ilustra un ejemplo de detección mediante la exploración de los datos de los paquetes.

– Etapa 3: todos los conmutadores SDN incorporan la nueva entrada de flujo en su tabla de flujos.

  Al recibir la operación de inserción de flujo relativo al archivo gusano, cada conmutador SDN añade una entrada de flujo a su tabla de flujos que le permitirá descartar futuros paquetes con archivos gusano. A partir de ese momento, el conmutador SDN descarta los paquetes que contengan el archivo gusano.

– Etapa 4: el conmutador SDN ejecuta la entrada de flujo para descartar los paquetes que contengan archivos gusano.

  Un conmutador SDN descartará todos los paquetes que reciba que contengan un archivo gusano. En aplicación de las reglas, no se retransmitirán los paquetes con archivo gusano.

– Etapa 5: un conmutador SDN notifica al controlador la recepción de cualquier paquete desconocido.

  Cuando un conmutador SDN recibe un tipo de paquete que nunca ha procesado previamente, lo borra y envía una notificación al controlador acerca de ese tipo de paquete. El controlador analiza si se trata de un ataque. Si es el caso, el controlador envía un mensaje a la aplicación cortafuegos y se pone en marcha la etapa 1. Si no es el caso, el controlador mantiene una entrada de flujo regular que comunica a los conmutadores cómo tratar ese caso en paquetes ulteriores.

8.1.3 Escenario de funcionamiento del servicio de cortafuegos colaborativo

En la Figura 8-3 se ilustra el escenario de funcionamiento colaborativo de la aplicación cortafuegos con una aplicación de inspección detallada de paquetes (IDP) con miras a asegurar una supervisión y gestión centralizadas de flujos del servicio de voz por el protocolo de Internet (VoIP) y de voz por el sistema de evolución a largo plazo (VoLTE). En este caso se puede observar que la aplicación IDP controla cada conmutador SDN para asegurar la gestión de flujos de llamada VoIP/VoLTE mediante reglas que pueden ser añadidas, suprimidas o modificadas dinámicamente. Esta aplicación puede colaborar con una aplicación cortafuegos para la protección del servicio VoIP/VoLTE. En concreto, un conmutador en el que se haya habilitado un cortafuegos realiza las verificaciones de seguridad básicas de los paquetes de flujos desconocidos. Si el conmutador detecta que se trata de un paquete

de un flujo de llamada VoIP desconocido que presenta patrones sospechosos, alerta al controlador SDN para que realice un análisis de seguridad especializado del paquete de llamada VoIP sospechoso.

Como condición previa de este escenario, el administrador de seguridad deberá definir una nueva política para la aplicación del cortafuegos y de la IDP al recibir una notificación de patrón sospechoso. Con el fin de evitar que los paquetes incorporen esos patrones, el usuario incorporará la nueva política (por ejemplo, "suprimir los paquetes con patrones sospechosos") a la aplicación cortafuegos y a la aplicación IDP que se ejecutan por encima del controlador SDN. También puede administrarse de forma centralizada, en cuyo caso, el administrador de seguridad podría establecer políticas de seguridad para las aplicaciones a través de un punto único, a saber, el controlador SDN.

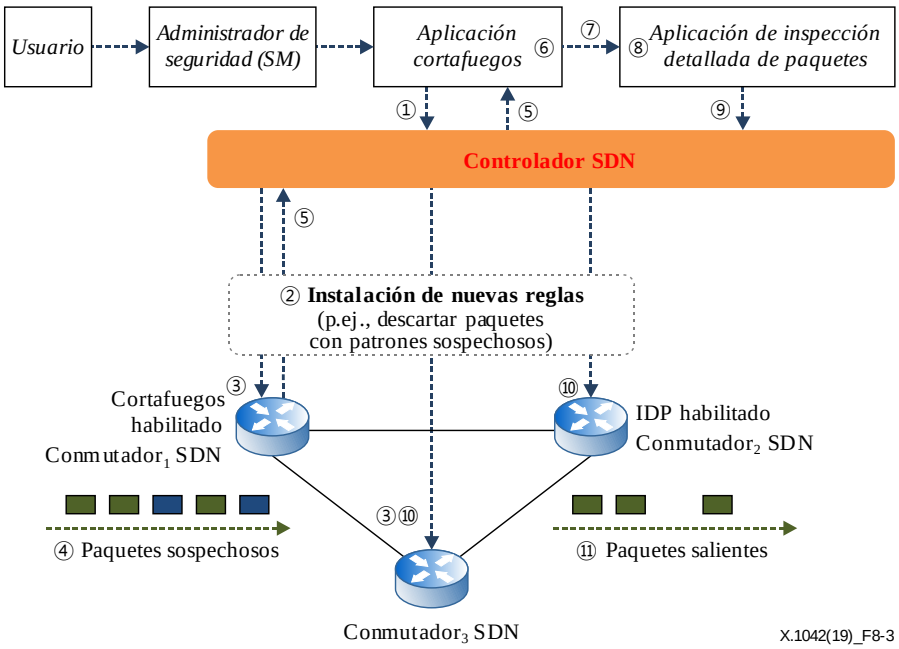


Figura 8-3 – Escenario intradominio del servicio de cortafuegos colaborativo

– Etapa 1: las aplicaciones cortafuegos e IDP instalan nuevas reglas para patrones conocidos.

  Las aplicaciones cortafuegos e IDP definirán una nueva regla cuando reciban una notificación sobre un nuevo patrón. La nueva regla (por ejemplo, "transmitir paquetes con el patrón al controlador SDN") se añade al controlador SDN.

– Etapa 2: el controlador SDN distribuye una nueva entrada de flujo a todos los conmutadores SDN.

  El controlador SDN transmite una nueva entrada de flujo a todos los conmutadores. Así, el controlador SDN envía una operación de inserción de flujo que contiene la regla en cuestión (por ejemplo, "transmitir al controlador SDN paquetes con el patrón especificado") a todos los conmutadores SDN. Si los conmutadores tienen funciones diferentes, el controlador SDN envía las diferentes entradas de flujo a cada uno. En otros términos, los conmutadores habilitados como cortafuegos no deben recibir las entradas de flujo relativas a la función de IDP.

– Etapa 3: todos los conmutadores SDN incorporan las nuevas entradas de flujo en su tabla de flujos.

  Al recibir la operación de inserción del flujo del controlador SDN, los conmutadores SDN incorporan en su tabla de flujos una entrada de flujo que afectará al tratamiento de futuros paquetes con el patrón sospechoso.

– Etapa 4: el conmutador SDN ejecuta las entradas de flujo para el tratamiento de paquetes con patrones sospechosos.

  El conmutador SDN que recibe paquetes con un patrón sospechoso los envía al controlador SDN. En aplicación de las reglas, todos los paquetes con patrones sospechosos deben retransmitirse al controlador SDN.

– Etapa 5: al recibir un paquete desconocido, el conmutador SDN y el controlador SDN lo envían a la aplicación cortafuegos.

  Cuando el controlador SDN recibe un tipo de paquete que nunca ha procesado antes, lo envía a la aplicación cortafuegos para que se proceda a una inspección de seguridad básica.

– Etapa 6: la aplicación cortafuegos analiza el paquete desconocido.

  La aplicación cortafuegos analiza los campos de la cabecera del paquete y determina si se trata de un paquete de un flujo de llamada VoIP desconocido, por ejemplo, un paquete del protocolo de iniciación de sesión (SIP) con patrón sospechoso.

– Etapa 7: la aplicación cortafuegos pone en marcha la aplicación IDP.

  La aplicación cortafuegos pone en marcha una aplicación apropiada, como es la IDP, para un análisis de seguridad detallado de los paquetes de señales sospechosos. Luego, envía los paquetes a la aplicación IDP.

– Etapa 8: la aplicación IDP analiza el paquete desconocido.

  La aplicación IDP analiza la cabecera y el contenido de los paquetes de la señal, como el número llamante y las cabeceras de descripción de sesión. Por ejemplo, la aplicación IDP descarta el paquete si determina que se trata de un paquete enmascarado enviado por piratas informáticos o de un paquete de exploración que busca dispositivos VoIP/VoLTE.

– Etapa 9: la aplicación IDP pide al controlador SDN que bloquee ese tipo de paquete.

  La aplicación IDP pide al controlador SDN que bloquee ese paquete y los paquetes subsiguientes que contengan el mismo identificador de llamada.

– Etapa 10: el controlador SDN instala nuevas reglas.

  El controlador SDN transmite una nueva entrada de flujo (por ejemplo, "descartar los paquetes") a todos los conmutadores SDN como en la etapa 2. A partir de ese momento, los conmutadores SDN descartarán todos los paquetes ilícitos.

8.2 Servicio de señuelo centralizado

8.2.1 Concepto básico del servicio de señuelo centralizado

En esta cláusula se describe el concepto básico del servicio de señuelo (o tarro de miel) centralizado. El señuelo puede gestionar dinámicamente varios emplazamientos de señuelos. Como se muestra en la Figura 8-4, un señuelo centralizado gestiona conmutadores y nuevos trayectos de encaminamiento para atraer a atacantes a un lugar empleado como trampa, es decir, un señuelo. El señuelo se configura para ser objetivo de ataques y comunica la información que recopila al servicio de señuelo centralizado.

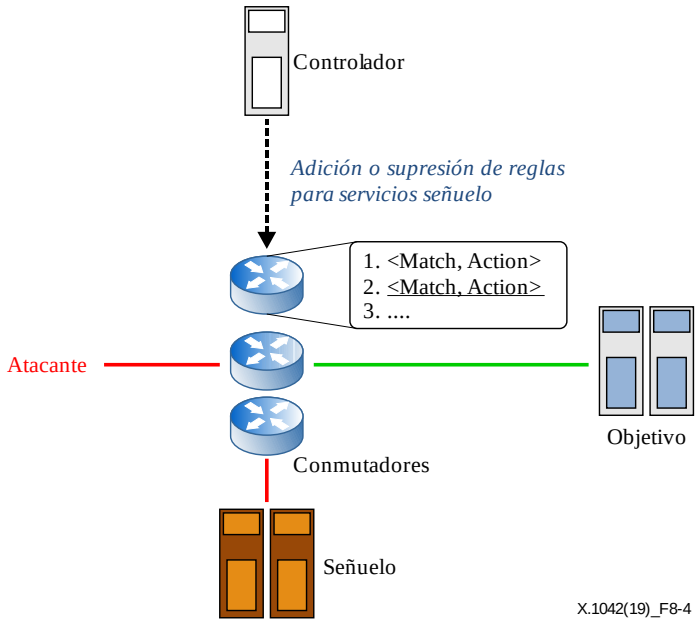


Figura 8-4 – Concepto de un servicio de señuelo centralizado

8.2.2 Escenario de servicio de señuelo centralizado

La Figura 8-5 muestra un ejemplo de escenario de servicio de señuelo centralizado en el que se añade un trayecto de encaminamiento hacia un señuelo que sustituye al objetivo real del ataque compuesto por conmutadores SDN.

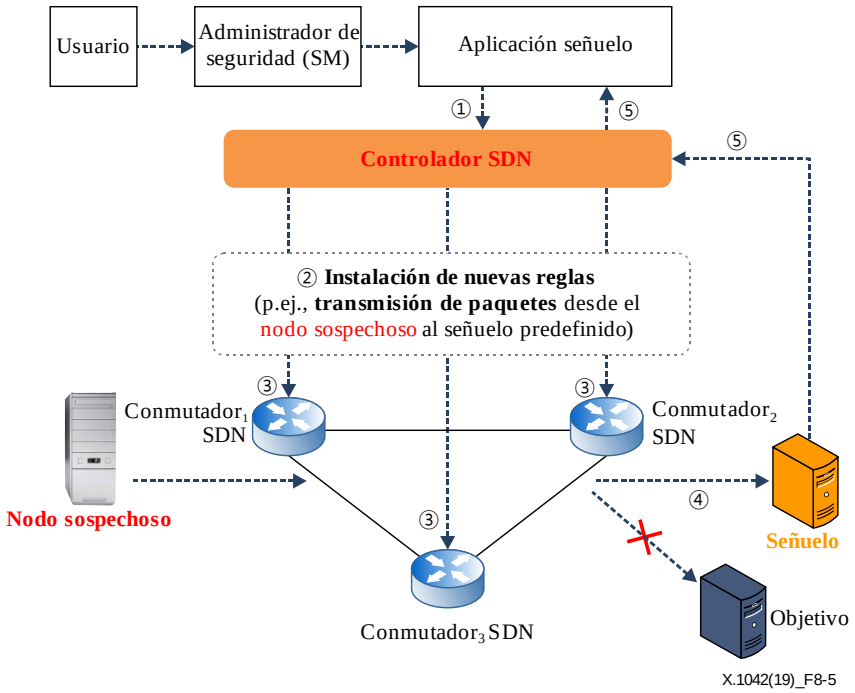


Figura 8-5 – Escenario intradominio de un servicio de señuelo centralizado

– Paso 1: la aplicación señuelo instala nuevas reglas en el controlador SDN.

  La aplicación señuelo especifica una nueva regla cuando se notifica la presencia de algunos nodos sospechosos. Para supervisar el tráfico procedente del nodo sospechoso, la aplicación de señuelo que se ejecuta por encima del controlador SDN añade la nueva regla al controlador SDN (por ejemplo, "transmitir los paquetes del nodo sospechoso a un señuelo").

– Paso 2: el controlador SDN distribuye nuevas reglas a los conmutadores SDN apropiados.

  Una vez instalada la nueva regla, el controlador SDN la distribuye a todos los conmutadores. Así pues, el controlador SDN transmite una operación de inserción de flujo que contiene la regla en cuestión (por ejemplo, "trasmitir los paquetes del nodo sospechoso al señuelo") a todos los conmutadores SDN. La gestión también puede ser centralizada, de manera que un administrador de seguridad (SM) pueda establecer las políticas de seguridad para sus servicios a través de un único punto, a saber, un controlador SDN.

– Paso 3: todos los conmutadores SDN incorporan las nuevas reglas en sus tablas de flujos.

  Al recibir la operación de inserción de flujo relativa a un nodo sospechoso, los conmutadores SDN, añaden una entrada de flujo en sus tablas de flujos en virtud de la cual futuros paquetes procedentes de un nodo sospechoso se retransmitirán a un señuelo. A partir de ese momento, el conmutador SDN puede retransmitir los paquetes del nodo sospechoso a un señuelo.

– Paso 4: el conmutador SDN ejecuta las nuevas reglas del servicio de señuelo.

  Cuando un conmutador SDN recibe paquetes de un nodo sospechoso, los transmite a un señuelo. Las nuevas reglas no permiten retransmitir paquetes de un nodo sospechoso a un nodo objetivo. Los paquetes retransmitidos se recopilan en el señuelo.

– Paso 5: el servicio de señuelo notifica al controlador sobre paquetes sospechosos.

  Cuando el servicio de señuelo recibe los paquetes de nodos sospechosos, los procesa y envía al controlador un informe acerca de estos paquetes a fin de apoyar el análisis de paquetes que realiza el controlador.

8.3 Servicio de mitigación de ataques DDoS centralizado

8.3.1 Concepto básico del servicio de mitigación de ataques DDoS centralizado

En la Figura 8-6 se muestra un servicio de mitigación de ataques DDoS centralizado. Este servicio permite añadir, eliminar o modificar reglas en cada conmutador SDN. A diferencia del "servicio de cortafuegos centralizado" propio de un escenario intradominio, este servicio se desarrolla en un ámbito interdominios.

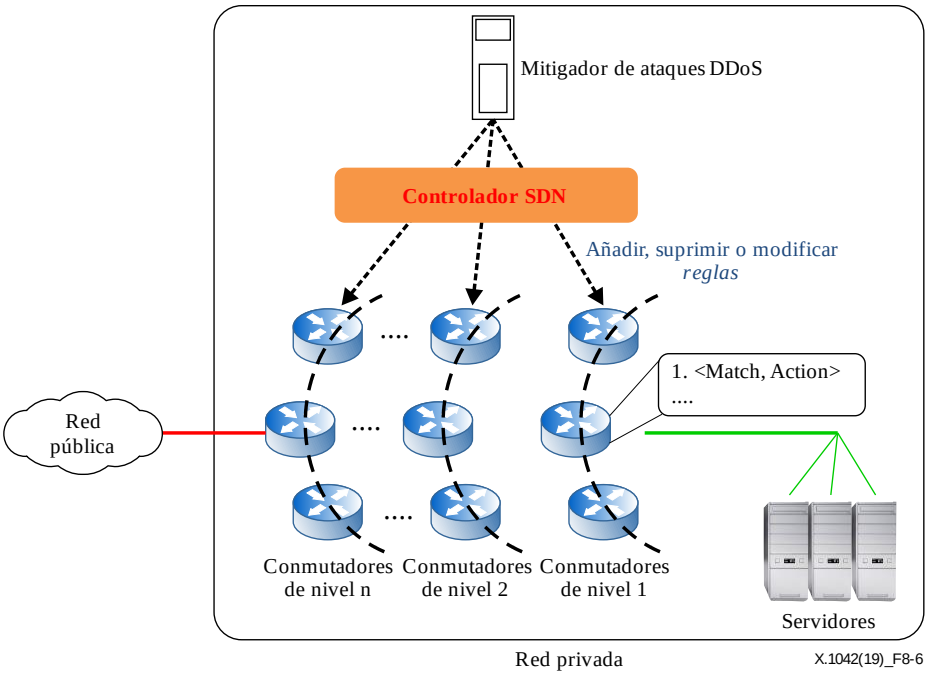


Figura 8-6 – Concepto del servicio de mitigación de ataques DDoS centralizado

8.3.2 Servicio de mitigación de ataques DDoS centralizado para servidores no basados en estados

La Figura 8-7 muestra un ejemplo de escenario de un servicio de mitigación de ataques DDoS centralizado para servidores de sistema de nombre de dominio (DNS) no basados en estados.

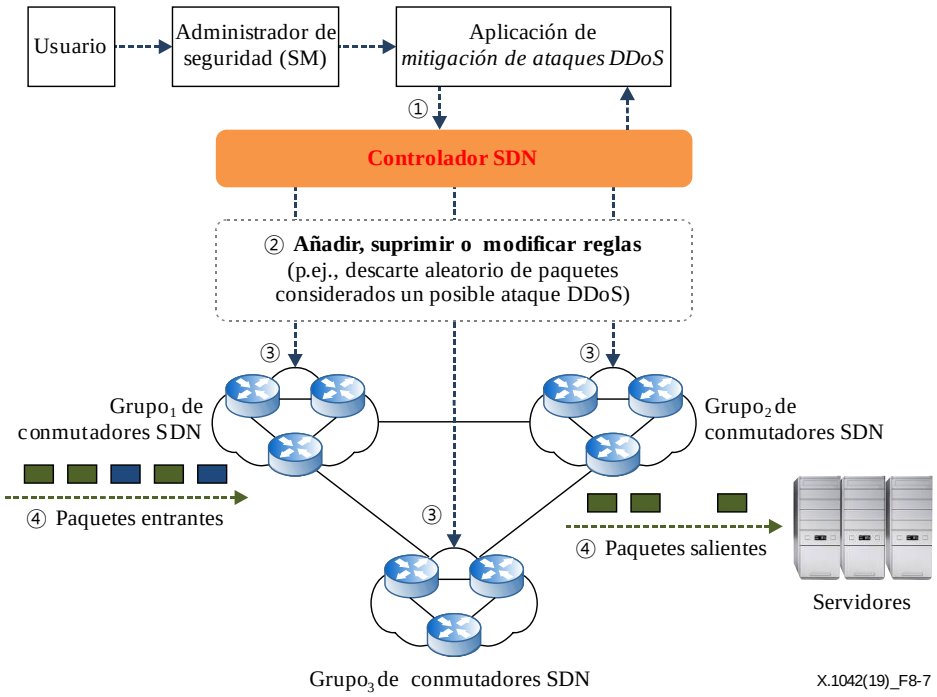


Figura 8-7 – Escenario interdominios del servicio de mitigación de ataques DDoS centralizado para servidores no basados en los estados

– Paso 1: la aplicación de mitigación instala nuevas reglas en el controlador SDN.

  La aplicación de mitigación de ataques DDoS especifica una nueva regla cuando el administrador de seguridad (SM) informa de un ataque DDoS. Para evitar que los paquetes lleguen a servidores y desperdicien los recursos de estos, se incorpora en el controlador SDN una nueva regla (por ejemplo, "descartar paquetes de un ataque DDoS aleatoriamente con una cierta probabilidad"). La aplicación mitigación de ataques DDoS que se ejecuta por encima del controlador SDN realiza la adición de esta regla.

– Paso 2: el controlador SDN distribuye nuevas reglas a los conmutadores apropiados.

  Una vez instalada la nueva regla, el controlador SDN la distribuye a todos los conmutadores. Así pues, el controlador SDN transmite a todos los conmutadores SDN una operación de inserción de flujo que contiene la regla en cuestión (por ejemplo, "descartar paquetes considerados un ataque DDoS aleatoriamente con una determinada probabilidad"). La gestión también puede ser centralizada, de manera que un administrador de seguridad (SM) establezca las políticas de seguridad para sus servicios a través de un único punto, a saber, un controlador SDN.

– Paso 3: todos los conmutadores SDN incorporan las nuevas reglas en sus tablas de flujos.

  Al recibir la operación de inserción de flujo relativa a la mitigación de ataques DDoS, todos los conmutadores SDN añaden a sus tablas de flujos una entrada de flujo en virtud de la cual descartarán futuros paquetes que se consideren parte de un ataque DDoS. A partir de ese momento, un conmutador SDN podrá descartar paquetes de un ataque DDoS con una probabilidad proporcional a la gravedad del ataque DDoS.

– Paso 4: un conmutador SDN ejecuta las nuevas reglas para mitigar el ataque DDoS.

Al recibir paquetes que forman parte de un ataque DDoS, un conmutador SDN descarta paquetes selectivamente. Los paquetes del ataque DDoS se descartan de forma aleatoria en los conmutadores SDN de cada domino con arreglo a las capacidades de procesamiento y las características de los dominios. A partir de ese momento, se debe informar del resultado de los descartes al controlador SDN.

8.3.3 Servicio de mitigación de ataques DDoS centralizado para servidores basados en estados

La Figura 8-8 muestra un ejemplo de escenario de mitigación de ataques DDoS centralizado para servicios web basados en estados.

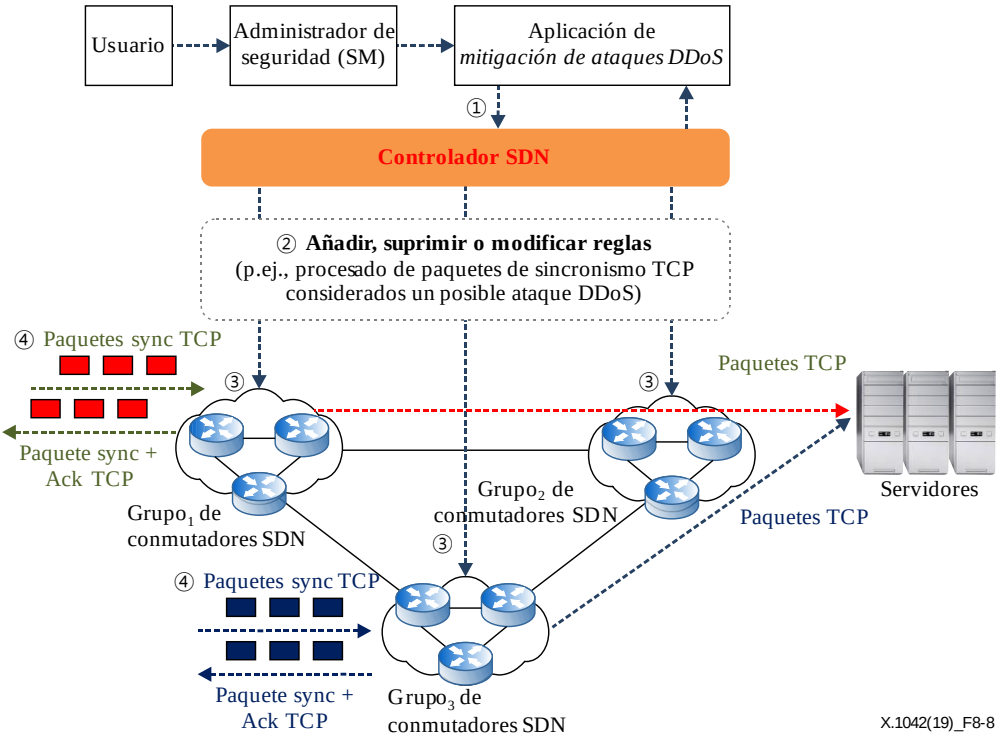


Figura 8-8 – Escenario interdominios de mitigación de ataques DDoS centralizado para servidores basados en estados

– Paso 1: una aplicación de mitigación instala nuevas reglas para el controlador SDN.

La aplicación de mitigación de ataques DDoS debe seleccionar qué conmutador realiza la función de representante ("proxy") para el servicio TCP. La aplicación de mitigación de ataques DDoS que se ejecuta sobre el controlador SDN realiza la adición de la nueva regla.

– Paso 2: el controlador SDN distribuye nuevas reglas a los conmutadores apropiados.

Una vez instalada la nueva regla, el controlador SDN la distribuye a los conmutadores apropiados para la mitigación de ataques DDoS. Por lo tanto, el controlador SDN envía una operación de inserción de flujo que contiene la regla en cuestión (por ejemplo, "generar sincronismo y acuse de recibo (Sync+Ack) para paquetes que se consideran que son un ataque DDoS"). Así pues, la nueva regla se instala en el conmutador seleccionado de forma que éste pueda generar paquetes Sync-Ack TCP para las peticiones de Sync TCP recibidas. Si las peticiones llegan a un ritmo mucho más alto que el esperado, el controlador SDN selecciona otro conmutador que pasará a comportarse como servidor. Para un Sync TCP normal, el conmutador transfiere la sesión TCP al correspondiente servidor en la red privada. La gestión también puede ser centralizada de forma que un administrador de seguridad (SM) determine

las políticas de seguridad para sus servicios a través un único punto, a saber, el controlador SDN.

– Paso 3: todos los conmutadores SDN incorporan las nuevas reglas en sus tablas de flujos.

  Al recibir la operación de inserción de flujo relativa a ataques DDoS, todos los conmutadores SDN añaden en sus tablas de flujos una entrada de flujo en virtud de la cual descartarán futuros paquetes que se consideren parte de un ataque DDoS. A partir de ese momento, el conmutador SDN puede descartar paquetes Sync-Ack TCP con una probabilidad proporcional a la gravedad del ataque DDoS.

– Paso 4: el conmutador SDN aplica las nuevas reglas para mitigar el ataque DDoS.

  Al recibir paquetes que forman parte de un ataque DDoS, un conmutador SDN responde a los paquetes Sync TCP de un nodo adversario de forma aleatoria. Las peticiones asociadas a ataques DDoS dirigidos a servidores basados en estados son gestionadas por conmutadores en lugar de por los servidores reales. A partir de ese momento, se debe transmitir al controlador SDN el resultado de la ejecución del conmutador SDN para la mitigación del ataque DDoS.

8.4 Servicio de gestión de dispositivos ilícitos centralizado

8.4.1 Concepto básico del servicio de gestión de dispositivos ilícitos centralizado

En esta cláusula se describe el concepto básico del servicio de gestión de dispositivos ilícitos centralizado. Como se muestra en la Figura 8-9, el servicio de gestión de dispositivos ilícitos centralizado gestiona una lista negra de dispositivos ilícitos para bloquear el tráfico de esos dispositivos. La lista de dispositivos ilícitos se almacena en una base de datos de lista negra y puede ser actualizada de forma manual o automática por aplicaciones independientes. El administrador de dispositivos ilícitos centralizado carga periódicamente la lista de dispositivos ilícitos de la base de datos de lista negra e informa de esos eventos a la aplicación de dispositivos ilícitos lo cual genera nuevas reglas de seguridad para bloquear el tráfico en la red desde y hacia dispositivos ilícitos.

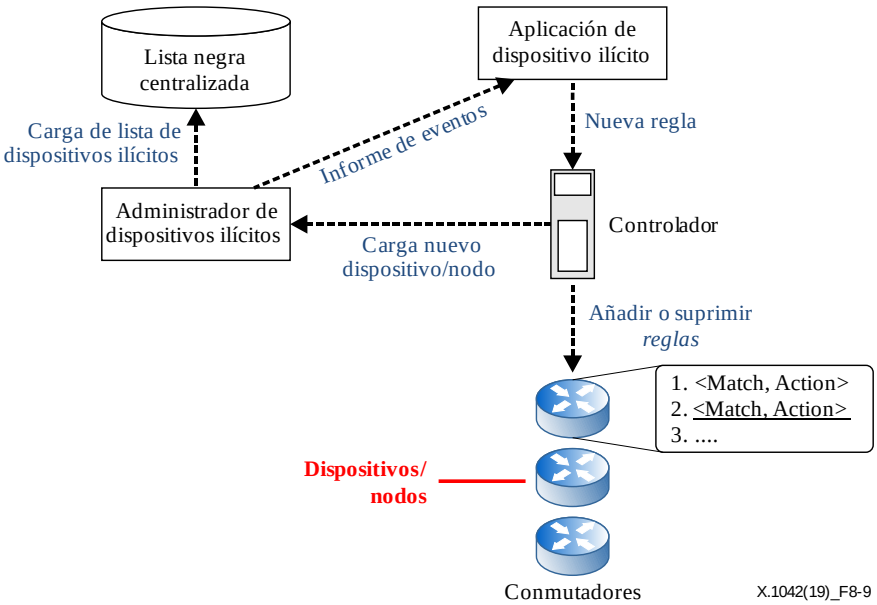


Figura 8-9 – Concepto de servicio de gestión de dispositivos ilícitos centralizado

8.4.2 Escenario de servicio del servicio de gestión de dispositivos ilícitos centralizado

La Figura 8-10 muestra un escenario del servicio de gestión de dispositivos ilícitos centralizado para bloquear el tráfico desde un dispositivo móvil robado.

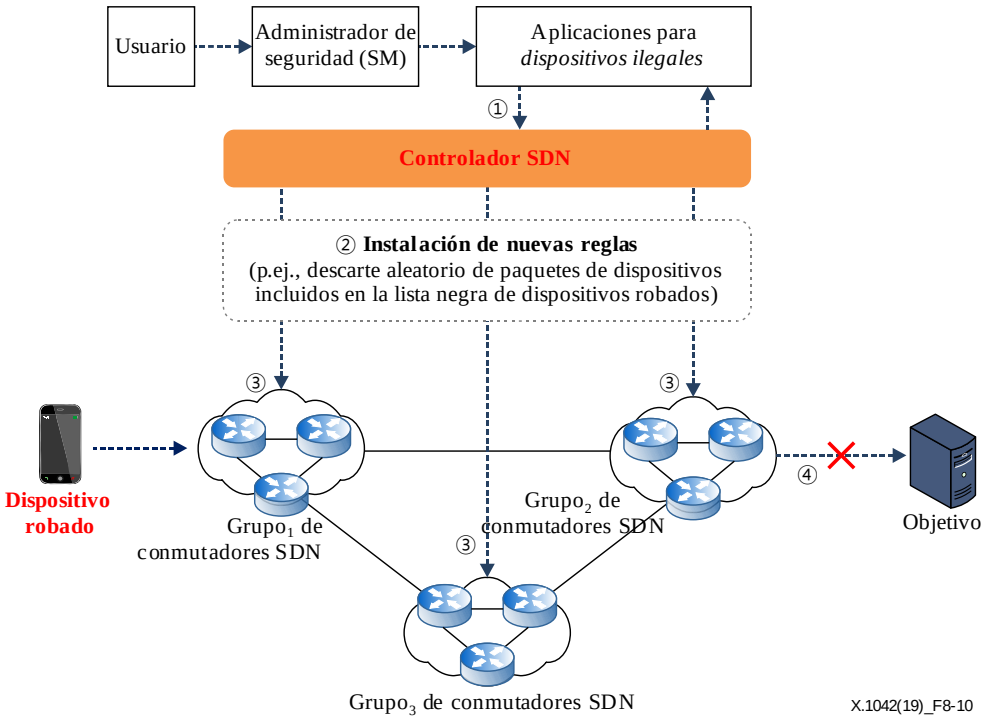


Figura 8-10 – Escenario interdominios para el servicio de gestión de dispositivos ilícitos centralizado

– Paso 1: la aplicación de gestión de dispositivos ilícitos instala nuevas reglas.

  Una aplicación de dispositivos ilícitos especificará una nueva regla cuando el administrador de dispositivos ilícitos centralizado informe de nuevos dispositivos robados. Como condición previa de este escenario, la aplicación de dispositivos ilícitos o el SM añade la nueva regla (por ejemplo, "descartar paquetes procedentes de los dispositivos almacenados en una lista negra de dispositivos robados") al controlador SDN.

– Paso 2: el controlador SDN distribuye nuevas reglas.

  Una vez instalada la nueva regla, el controlador SDN la distribuye a todos los conmutadores. Por lo tanto, el controlador SDN envía una operación de inserción de flujo que contiene la regla en cuestión (por ejemplo, "descartar paquetes procedentes de nuevos dispositivos robados") a todos los conmutadores SDN. También puede ser gestionado de forma centralizada de manera que un administrador centralizado de dispositivos ilícitos o SM pueda determinar políticas de seguridad para sus servicios a través de un único punto, a saber, un controlador SDN.

– Paso 3: todos los conmutadores SDN incluyen las nuevas reglas en sus tablas de flujos.

  Al recibir la operación insertar flujo relativa a dispositivos robados, todos los conmutadores SDN añaden una entrada de flujo en sus tablas de flujos para descartar futuros paquetes procedentes de esos dispositivos.

– Paso 4: el conmutador SDN aplica las nuevas reglas.

  El conmutador SDN descarta todos los paquetes que recibe de esos dispositivos. Según las reglas aplicables, no se retransmitirá ningún paquete procedente de esos dispositivos. A partir de ese momento, deberá transmitirse el resultado de la aplicación al controlador SDN.

NOTA – Es importante identificar los dispositivos ilícitos. Se utiliza una identidad única asignada por el administrador de dispositivos ilícitos centralizado para identificar cualquier dispositivo ilícito. Si el controlador SDN sólo identifica la dirección de red, como la dirección de Protocolo Internet (IP) del dispositivo o la dirección de control de acceso a los medios (MAC) que pueden ser modificadas de forma dinámica, se

aplica una nueva regla y luego se suprime la anterior en el controlador SDN cada vez que cambia la dirección de red de un dispositivo ilícito.

8.5 Servicio de gestión del control de acceso

8.5.1 Concepto básico del servicio de gestión del control de acceso

En esta cláusula se describe el concepto básico del servicio de gestión del control de acceso (ACM). El módulo ACM con controlador SDN puede gestionar de forma jerárquica las políticas de derecho de acceso. Como se muestra en la Figura 8-11, un módulo ACM gestiona los derechos de acceso a fin de impedir accesos ilícitos a los recursos.

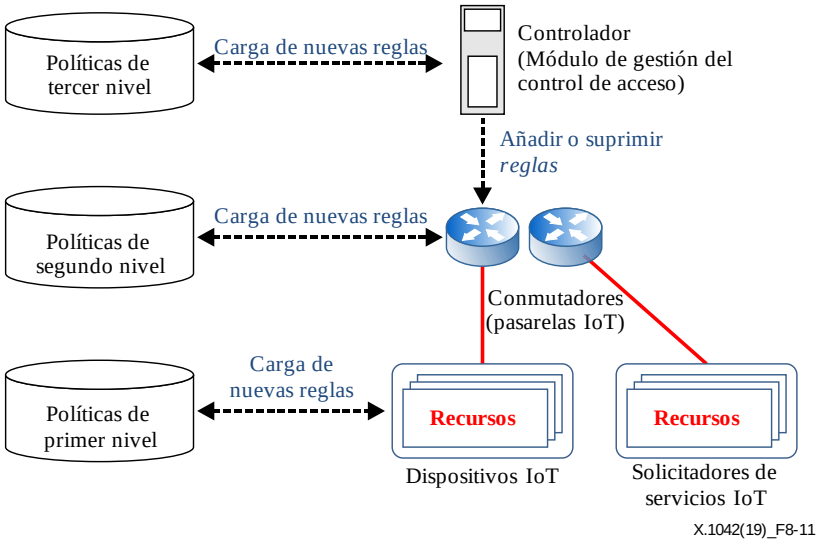


Figura 8-11 – Concepto de un servicio de gestión del control de acceso

8.5.2 Escenario de servicio del servicio de gestión del control de acceso

La Figura 8-12 muestra un ejemplo de escenario de servicio ACM gestionado por un controlador de seguridad. En este escenario participan el controlador SDN y los conmutadores.

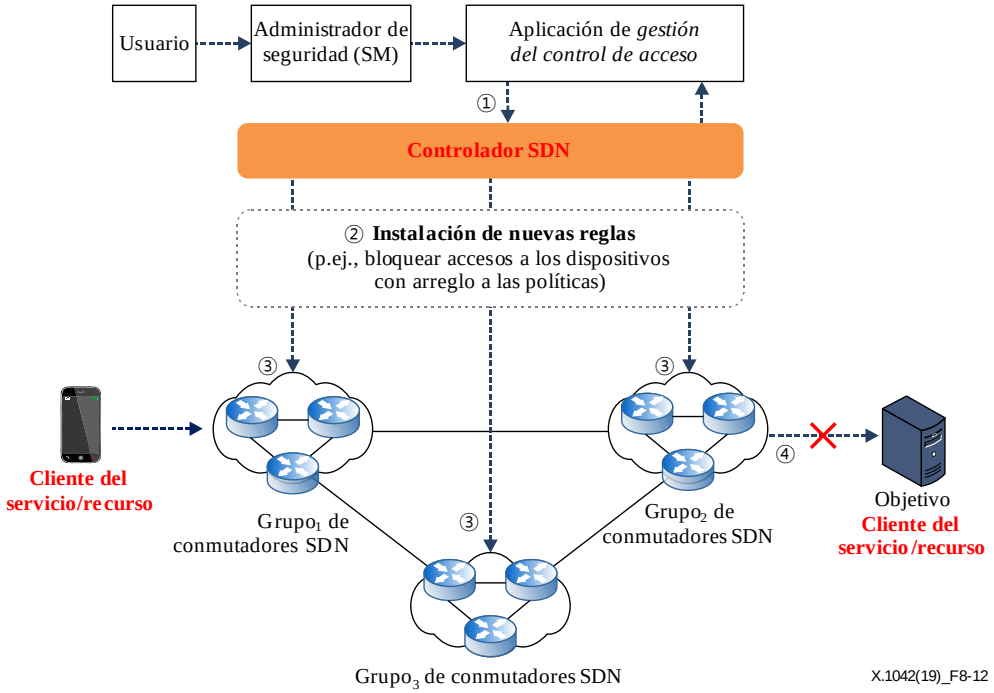


Figura 8-12 – Escenario interdominios del servicio de gestión del control de acceso

– Paso 1: una aplicación de ACM instala nuevas políticas del SM.

  Una aplicación de ACM debe especificar nuevas políticas para el acceso a los recursos en dispositivos distribuidos del servicio/recurso (por ejemplo, dispositivos de IoT). Como condición previa a este escenario, el SM ya ha añadido nuevas políticas a esta aplicación de ACM.

– Paso 2: el controlador SDN distribuye nuevas reglas.

  Deben almacenarse una o varias nuevas reglas. El controlador SDN las puede distribuir a todos los conmutadores. El controlador SDN puede transmitir una petición de acceso para explotar los recursos en un dispositivo del servicio/recurso. En ese caso, el controlador SDN no recibe ninguna petición de los conmutadores SDN para la distribución de la regla. Los conmutadores SDN pueden pedir al controlador SDN que les facilite reglas de acceso a recursos en dispositivos de servicio/recurso antes de enviar al controlador SDN peticiones de distribución de la regla.

– Paso 3: todos los conmutadores SDN añaden las nuevas reglas a sus bases de datos locales.

  Todos los conmutadores SDN añaden nuevas reglas a sus bases de datos locales para procesar las solicitudes de autorización de acceso dirigidas a dispositivos del servicio/recurso.

– Paso 4: el conmutador SDN aplica las nuevas reglas.

  De conformidad con las reglas de acceso, el conmutador SDN puede descartar todos los paquetes que reciba de un cliente del servicio/recurso. En este caso, cada dominio de conmutación SDN debe poder tener reglas de acceso diferentes con arreglo a las capacidades de cada dominio. De conformidad con las reglas aplicables, el conmutador SDN no retransmitirá los paquetes procedentes de dichos clientes. Debe informarse al controlador SDN de cualquier paquete que carezca de reglas de acceso para que la aplicación de ACM pueda gestionarlo.

Apéndice I

Criterios para los servicios de seguridad basados en la SDN

(Este apéndice no forma parte integrante de la presente Recomendación.)

Este Apéndice proporciona criterios para diversos servicios de seguridad.

I.1 Criterios para servicios de seguridad en redes intradominio

I.1.1 Servicio de cortafuegos centralizado

Los cortafuegos tradicionales presentan diversos problemas, como sus elevados costos, la calidad de funcionamiento, la gestión del control de acceso y el establecimiento de políticas y mecanismos de acceso en modo paquete. Para solucionar estos problemas, en esta Recomendación se presenta el marco de un servicio de cortafuegos centralizado basado en la SDN. Las reglas aplicables por los cortafuegos pueden ser gestionadas de manera flexible por un servidor centralizado. Es posible utilizar los protocolos SDN existentes a través de las interfaces entre las aplicaciones cortafuegos y los conmutadores.

– Costo

  El costo de añadir cortafuegos a los recursos de red, como encaminadores, pasarelas y conmutadores, es importante ya que es necesario incluir cortafuegos en todos los recursos de red. Para solventar este problema, es posible gestionar todos los recursos de red de forma centralizada de modo que un servidor centralizado manipule un único cortafuegos.

– Calidad de funcionamiento

  A menudo la velocidad de funcionamiento de los cortafuegos es inferior a las de los enlaces presentes en sus interfaces con la red. Todo recurso de red necesita verificar las reglas de los cortafuegos con independencia de las condiciones de la red. Los cortafuegos pueden desplegarse de forma adaptable en función de las condiciones de la red en este marco.

– Gestión del control de acceso

  Dado que en una red administrada pueden existir cientos de recursos de red, la gestión dinámica del control de acceso para los servicios de seguridad, como los cortafuegos, presenta problemas. Ello se debe a la necesidad de añadir dinámicamente reglas de cortafuegos para hacer frente a nuevos ataques a la red.

– Establecimiento de políticas

  Es necesario establecer la política de cada recurso de red. No obstante, es difícil describir cuáles son los flujos permitidos y los rechazados en una red gestionada con una determinada organización. Por lo tanto, una visión centralizada puede ser útil a fin de determinar las políticas de seguridad para dicha red.

– Mecanismo de acceso en modo paquete

  En la práctica, no es suficiente un mecanismo de acceso en modo paquete ya que normalmente la unidad básica de control de acceso está compuesta por usuarios o aplicaciones. Por lo tanto, es necesario que un administrador defina las reglas a nivel de aplicación y las añada al servicio de cortafuegos.

I.1.2 Servicio de señuelo centralizado

Los señuelos tradicionales presentan diversos problemas, como sus elevados costos, la calidad de funcionamiento, la gestión del control de acceso, el establecimiento de políticas y los mecanismos de acceso en modo paquete. Para solucionar estos problemas, en esta Recomendación se presenta el marco de un servicio de señuelo centralizado basado en la SDN. Los señuelos pueden ser

administrados de manera flexible por un servidor centralizado. Es posible utilizar los protocolos SDN existentes a través de las interfaces entre las aplicaciones de señuelo y los conmutadores.

– Costos

  El costo de implantar señuelos adicionales en una red es importante dada la necesidad de utilizar recursos adicionales, como los nodos anfitriones para los señuelos. Para solventar este problema, los señuelos pueden ser administrados de manera flexible por un servidor centralizado.

– Calidad de funcionamiento

  La calidad de funcionamiento de los señuelos es función de la capacidad de los nodos anfitriones. Los señuelos siempre se ejecutan de la misma manera con independencia de la red y/o condiciones del ataque. Los señuelos pueden implantarse de acuerdo con las condiciones de la red y/o del ataque en este marco.

– Gestión del control de acceso

  Dado que pueden existir cientos de recursos de red en una red administrada, la configuración dinámica de un señuelo presenta problemas. Ello se debe a la necesidad de realizar dinámicamente cambios contra nuevos ataques.

– Establecimiento de políticas

  Es necesario establecer la política correspondiente a cada recurso de red. No obstante, es difícil determinar la ubicación de señuelos contra ataques sospechosos en función de la red y las condiciones del ataque. Por lo tanto, una visión centralizada puede ser de utilidad para ajustar dinámicamente las políticas de seguridad a lo largo del tiempo.

– Mecanismo de despliegue de señuelos

  La ubicación apropiada de los señuelos debe elegirse en función de la red y las condiciones de los ataques. Un servicio de señuelo centralizado basado en la SDN determina el emplazamiento óptimo para supervisar y responder en tiempo real a los ataques. El señuelo se configura de forma centralizada como el objetivo del ataque pretendido mediante un servidor centralizado.

I.2 Criterios para los servicios de seguridad en redes interdominios

I.2.1 Servicio de mitigación de ataques DDoS centralizado

Un servicio de mitigación de ataques DDoS centralizado protege a los servidores de ataques DDoS realizados desde el exterior de las redes privadas, es decir, desde redes públicas. Los servidores se clasifican en servidores no basados en el estado (por ejemplo, los servidores DNS) y servidores basados en el estado (por ejemplo, servidores web). La Figura 8-6 muestra la configuración del servicio de mitigación de ataques DDoS en una red privada. Los conmutadores de la red privada se configuran en niveles de dominio jerárquicos, es decir, conmutadores de nivel 1, conmutadores de nivel 2, etc. Los servidores de nivel *n* corresponden a líneas de defensa dinámica contra diversos tipos de ataques DDoS.

Los servicios de mitigación de ataques DDoS centralizados se enfrentan a diversos problemas, como sus elevados costos, la calidad de funcionamiento, la gestión del control de acceso, el establecimiento de políticas y de mecanismos de acceso en modo paquete. Para solucionar estos problemas, en esta Recomendación se presenta el marco de un servicio de mitigación de ataques DDoS centralizado basado en la SDN. Las reglas de mitigación pueden ser gestionadas de manera flexible por un servidor centralizado. Los protocolos SDN existentes pueden utilizarse a través de interfaces normalizadas entre las aplicaciones de mitigación de ataques DDoS y los conmutadores.

– Costos

Todo recurso de red puede ser gestionado de manera centralizada y flexible a un costo mínimo, mediante un servidor centralizado que configure y manipule los conmutadores a varios niveles. Conforme mayor sea la gravedad del ataque DDoS para el servidor, los conmutadores multinivel realizan descartes selectivos de paquetes para reducir los efectos de los ataques DDoS. En otras palabras, los paquetes sospechosos de formar parte de un ataque DDoS serán descartados en una fase temprana, al inicio del trayecto de encaminamiento hacia el nodo víctima.

– Calidad de funcionamiento

A menudo la mitigación del ataque DDoS se produce a un ritmo más lento que la velocidad de los enlaces de sus interfaces con la red. En el servicio tradicional, todo recurso de red necesita verificar las reglas de mitigación de ataques DDoS con independencia de las condiciones de la red. No obstante, las aplicaciones de mitigación de ataques DDoS pueden desplegarse de forma adaptable en función de las condiciones de la red en este marco.

– Gestión del control de acceso

Dado que una red administrada puede tener cientos de recursos de red, la gestión dinámica del control de acceso de los servicios de seguridad, como la mitigación de ataques DDoS, presenta problemas. Ello se debe a la necesidad de añadir dinámicamente reglas de mitigación de ataques DDoS para hacer frente a nuevos ataques DDoS.

– Establecimiento de políticas

Es necesario establecer la política de todos los recursos de red. No obstante, es difícil determinar las políticas específicas de descarte de paquetes contra ataques DDoS en función de las condiciones de la red. Por lo tanto, una visión centralizada puede ser de utilidad para ajustar dinámicamente las políticas de seguridad a lo largo del tiempo.

– Mecanismos de detección de ataques DDoS

La detección de los ataques DDoS se realiza verificando si se reciben solicitudes de servicios de un cliente en los intervalos previstos. El mecanismo de detección de ataques DDoS determina la probabilidad de que las peticiones de un cliente sean en realidad ataques DDoS y realiza descartes selectivos de peticiones de manera proporcional a esa probabilidad.

I.2.2 Servicio de gestión de dispositivos ilícitos centralizado

Los servicios tradicionales de gestión de dispositivos ilícitos se enfrentan a diversos problemas, como sus elevados costos, la calidad de funcionamiento, la gestión del control de acceso y el establecimiento de políticas y de mecanismos de acceso en modo paquete. Para solucionar estos problemas, en esta Recomendación se presenta un servicio de gestión de dispositivos ilícitos centralizado basado en la SDN. Las reglas para incluir dispositivos en la lista negra pueden administrarse globalmente. Es posible utilizar protocolos SDN existentes a través de interfaces normalizadas entre las aplicaciones de dispositivos ilícitos y los conmutadores.

– Costos

El costo de actualizar listas negras para los recursos de red, como encaminadores, pasarelas y conmutadores, es elevado dada la necesidad de actualizar las listas negras individualmente para cada recurso de red. Para solventar este problema, las reglas de seguridad relativas a las listas negras de para cada recurso de red pueden gestionarse de manera centralizada de forma que sea un servidor central quien manipule un único servicio de gestión de dispositivos ilícitos.

– Calidad de funcionamiento

Dado que, a diferencia del servicio de gestión tradicional, los paquetes procedentes de dispositivos incluidos en la lista negra se descartan al comienzo del trayecto de encaminamiento, es posible mejorar en la práctica la calidad de funcionamiento del servicio de gestión de dispositivos ilícitos centralizado.

– Gestión del control de acceso

En caso de gestión local de listas negras, no es fácil sincronizar las distintas listas distribuidas localmente ya que pueden existir cientos de recursos de red en varios países. Es necesario añadir dinámicamente reglas de seguridad para nuevos dispositivos ilícitos.

– Establecimiento de políticas

Es necesario establecer la política de cada uno de los recursos de red. No obstante, es difícil identificar los dispositivos no permitidos en la red de una organización específica gestionada. Por lo tanto, una visión centralizada puede ser útil para determinar las políticas de seguridad para la red en cuestión.

– Mecanismo de actualización de listas negras

Es importante mantener una lista actualizada de dispositivos ilícitos. Por lo tanto, los servicios tradicionales deben actualizar regularmente la base de datos de la lista negra para tener acceso a la información más reciente de todos dispositivos ilícitos. En el servicio de gestión de dispositivos ilícitos centralizado, el servidor centralizado gestiona la lista negra de manera centralizada como una base de datos única.

I.2.3 Servicio de gestión del control de acceso

Los servicios ACM se enfrentan a diversos problemas, como sus elevados costos, la calidad de funcionamiento, la gestión del control de acceso y el establecimiento de políticas y de mecanismos de acceso en modo paquete. Para solucionar estos problemas, en esta Recomendación se presenta un servicio ACM basado en la SDN. Las reglas para incluir dispositivos en la lista blanca pueden administrarse globalmente en los servicios de red distribuidos (por ejemplo, controlador SDN, conmutador). Es posible utilizar protocolos SDN existentes a través de interfaces normalizadas entre las aplicaciones ACM y los conmutadores por medio de un controlador SDN.

– Costos

El costo de actualizar listas blancas para los recursos de red, como encaminadores, pasarelas y conmutadores, es elevado dada la necesidad de actualizar las listas blancas para muchos recursos de red. Para solventar este problema, las reglas de seguridad relativas a las listas blancas de cada recurso de red pueden gestionarse de manera centralizada de forma que sea un servidor central quien manipule el servicio ACM.

– Calidad de funcionamiento

Dado que, a diferencia del servicio de gestión tradicional, los paquetes procedentes de dispositivos sin derecho de acceso se descartan al comienzo del trayecto de encaminamiento, es posible mejorar en la práctica la calidad de funcionamiento del servicio ACM. Además, la información relativa a los derechos de acceso se dividirá y almacenará en recursos de red en función de su nivel de seguridad.

– Gestión del control de acceso

En caso de gestión local de listas blancas, no es fácil sincronizarlas ya que pueden existir cientos de recursos de red en varios países. Es necesario difundir dinámicamente reglas de seguridad para transmitir nuevos derechos de acceso a los recursos de red.

– Establecimiento de políticas

  Es necesario establecer la política de cada uno de los recursos de red con arreglo a su nivel de seguridad. Por consiguiente, es difícil describir qué dispositivos de IoT no están permitidos en la red de una organización específica con arreglo a la ACM. Por lo tanto, una visión centralizada puede ser útil para determinar las políticas de seguridad para la red en cuestión.

– Mecanismo de actualización de listas blancas

  Es importante mantener actualizada una lista blanca de derecho de acceso para dispositivos de IoT. Por lo tanto, los servicios tradicionales deben actualizar regularmente la base de datos de listas blancas para tener acceso a la información más reciente de cualesquiera derechos de acceso para dispositivos de IoT. En el servicio ACM, el servidor centralizado gestiona la lista blanca de manera centralizada como una base de datos única. Además, algunas partes de las políticas pueden distribuirse en los recursos de red.

Apéndice II

Ejemplo de detección por exploración de datos en modo paquete

(Este apéndice no forma parte integrante de la presente Recomendación.)

La detección por exploración de datos en modo paquete requiere apoyo para detectar y mitigar algunos ataques, como los realizados mediante gusanos. El administrador configura las políticas a fin de detectar de forma aleatoria sólo algunos, no todos los paquetes del flujo, en aras de una mejor calidad de funcionamiento. Un posible esquema de detección mediante la exploración de datos en modo paquete [b-ICIN SDNSec] implica seleccionar los primeros *m* paquetes consecutivos de cada flujo para la citada detección. Este esquema puede establecerse para todos los flujos o sólo para aquellos que cumplan ciertas condiciones como, por ejemplo, los paquetes de una determinada fuente IP o dirigidos a un destino concreto.

El protocolo OpenFlow [b-ONF TS-012], una de las implementaciones presentes en la interfaz descendente de la SDN, puede ampliarse para permitir la detección mediante exploración de los paquetes de datos. Es posible añadir dos características adicionales en el formato de un flujo entrante. Estas actualizaciones deben reflejarse en el controlador y los conmutadores. Una de dichas características es el esquema que comprende los flujos de datos que cumplen las condiciones que configura el administrador o las aplicaciones. La otra característica es la condición que describen los flujos que cumplen las condiciones configuradas por el administrador o las aplicaciones. En consecuencia, debería añadirse a la cláusula "5.12 Actions" de [b-ONF TS-012] la actuación opcional (OFPAT_DETECTION) siguiente (en cursiva): *Optional Action: the Detection action forwards a packet to a specified OpenFlow port then to security appliances (e.g., FW, IDP, DPI, etc.) for further data scan detection* ("Actuación adicional: La acción 'Detección' transmite un paquete a un puerto OpenFlow especificado dirigido a alguno de los esquemas de seguridad (por ejemplo, FW, IDP, DPI, etc.) para una detección adicional mediante exploración de los datos"). Esta nueva acción es similar a la acción OFPAT_OUTPUT del protocolo Openflow. Finalmente, deberían actualizarse las estructuras de acción de la cláusula "7.2.4 Action Structures" de [b-ONF OpenFlow] tal como se muestra más abajo mediante texto en cursiva:

```
enum ofp_action_type {
OFPAT_OUTPUT = 0,                              /* Output to switch port. */
OFPAT_DETECTION = XX (a given number),      /*Output to switch port */
OFPAT_COPY_TTL_OUT = 11,      /* Copy TTL "outwards" – from
                                 next-to-outermost to outermost */
OFPAT_COPY_TTL_IN = 12,       /* Copy TTL "inwards" – from
                                outermost to next-to-outermost */
OFPAT_SET_MPLS_TTL = 15,      /* MPLS TTL */
OFPAT_DEC_MPLS_TTL = 16,      /* Decrement MPLS TTL */
OFPAT_PUSH_VLAN = 17,         /* Push a new VLAN tag */
OFPAT_POP_VLAN = 18,          /* Pop the outer VLAN tag */
OFPAT_PUSH_MPLS = 19,         /* Push a new MPLS tag */
OFPAT_POP_MPLS = 20,          /* Pop the outer MPLS tag */
OFPAT_SET_QUEUE = 21,          /* Set queue id when outputting to a port */
OFPAT_GROUP = 22,              /* Apply group. */
OFPAT_SET_NW_TTL = 23,         /* IP TTL. */
OFPAT_DEC_NW_TTL = 24,          /* Decrement IP TTL. */
OFPAT_SET_FIELD = 25,          /*Set a header field using OXM TLV format*/
OFPAT_PUSH_PBB = 26,            /* Push a new PBB service tag (I-TAG) */
OFPAT_POP_PBB = 27,            /* Pop the outer PBB service tag (I-TAG) */
OFPAT_EXPERIMENTER = 0xffff
};
A Detection action uses the following structure and fields:
/*Action structure for OFPAT_DETECTION which sends packets out 'port'.*/
struct ofp_action_detection {
uint16_t type;                  /* OFPAT_DETECTION. */
uint16_t len;                   /* Length is 16. */
uint32_t port;                  /* Output port. */
```

```
    uint16_t schema;                /* One possible schema is: to select the first m
                                     consecutive packets from each flow. */
    uint32_t condition;             /* One possible condition: packets
                                    of the flow to a certain destination . */
    };
OFP_ASSERT(sizeof(struct ofp_action_output) == 10);
```

Apéndice III

Arquitectura para la implementación de servicios de seguridad basados en la SDN

(Este apéndice no forma parte integrante de la presente Recomendación.)

III.1 Interfaz del IETF entre el marco de la función de seguridad de la red y la SDN

III.1.1 Visión general

Esta cláusula proporciona una interfaz elaborada por el IETF entre la interfaz con la función de seguridad de red (I2NSF) y la SDN para servicios de seguridad basados en la nube, como cortafuegos, IDP y funciones para la mitigación de ataques DDoS. La SDN permite hacer obligatorias determinadas reglas de filtrado de paquetes en los conmutadores de la red mediante el control de sus reglas de transmisión de paquetes. Aprovechando esta capacidad de la SDN, es posible optimizar el proceso de observancia de servicios de seguridad en el marco I2NSF.

La Figura III.1 muestra un marco I2NSF [b-IETF RFC 8329] con redes SDN para soportar servicios de seguridad basados en la red. En este marco, la observancia de reglas de política de seguridad se divide entre los conmutadores SDN y las funciones de seguridad de red (NSF). En este caso, se utilizan el protocolo NETCONF y el lenguaje de modelización YANG.

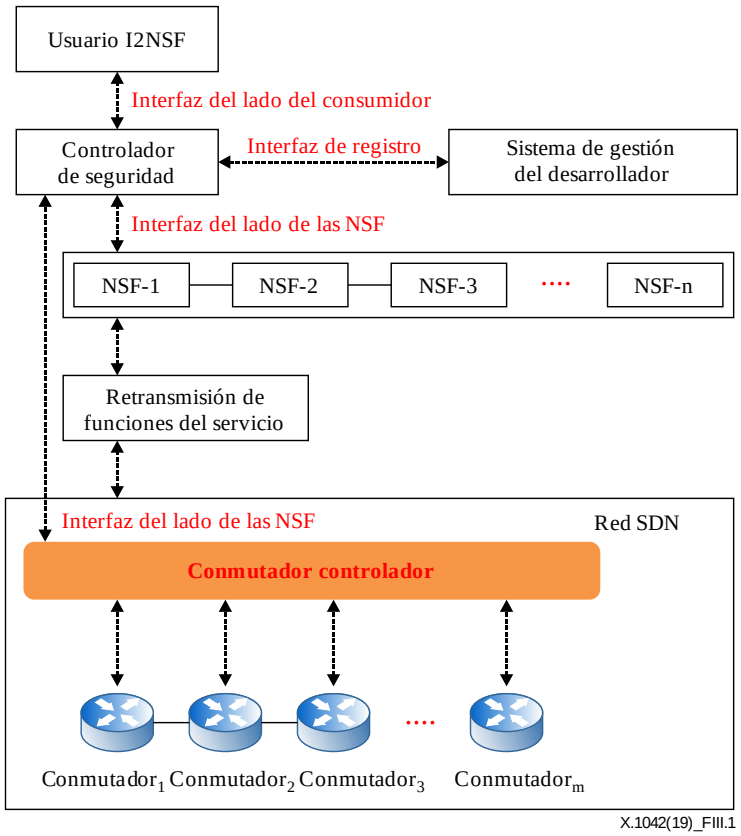


Figura III-1 – Interfaz del IETF con el marco de función de seguridad de la red

III.1.2 Comparación entre las arquitecturas del IETF y del UIT-T

En la Figura III.2 se ilustra la comparación entre el marco I2NSF utilizando la SDN y la arquitectura del UIT-T. En color azul se muestran los componentes del modelo del UIT-T.

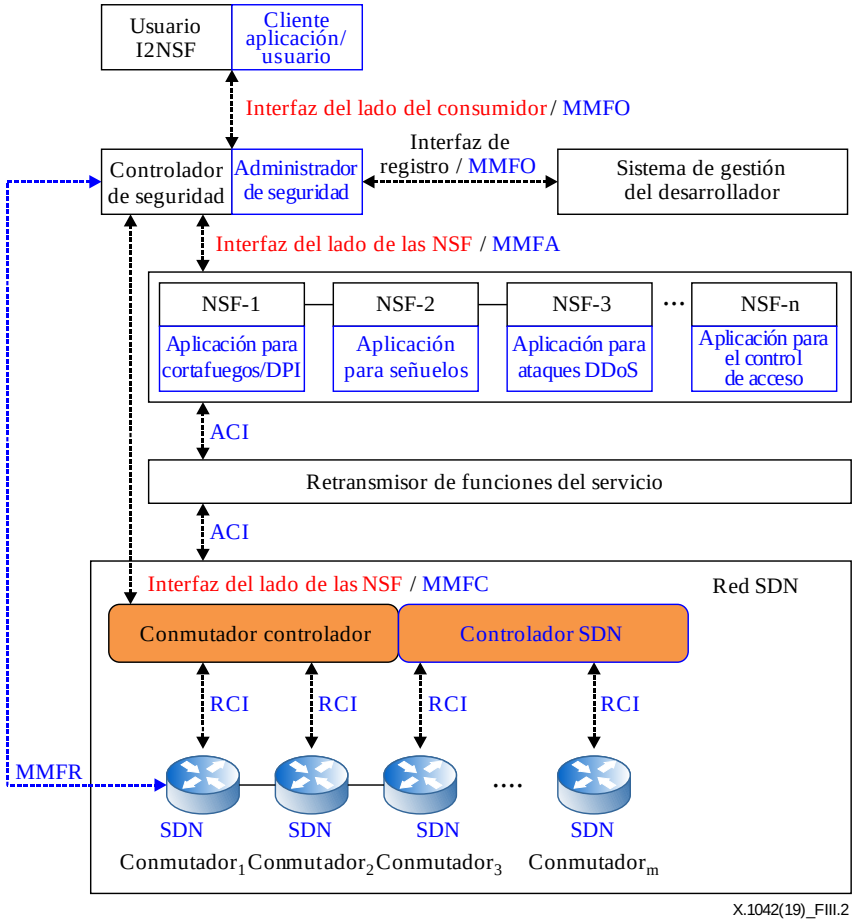


Figura III-2 – Comparación entre las arquitecturas del IETF y del UIT-T

III.2 Arquitectura SDN de la ONF

III.2.1 Visión general

En esta cláusula se proporciona la arquitectura SDN de la ONF. La Figura III.3 muestra la arquitectura SDN de [b-ONF TR-521]. En la Figura III.3 la SDN se modeliza como un conjunto de relaciones cliente-servidor entre los controladores SDN y otras entidades que también pueden ser controladores SDN. En su papel como servidor, un controlador SDN puede ofrecer servicios a cualquier número de clientes, mientras que un controlador SDN que actúe como cliente puede invocar los servicios de cualquier número de servidores. En la medida en que el comportamiento de estos sea adecuado, los detalles internos de entidades que no sean controladores SDN quedan fuera del alcance de la arquitectura. En este caso de utiliza el protocolo OpenFlow.

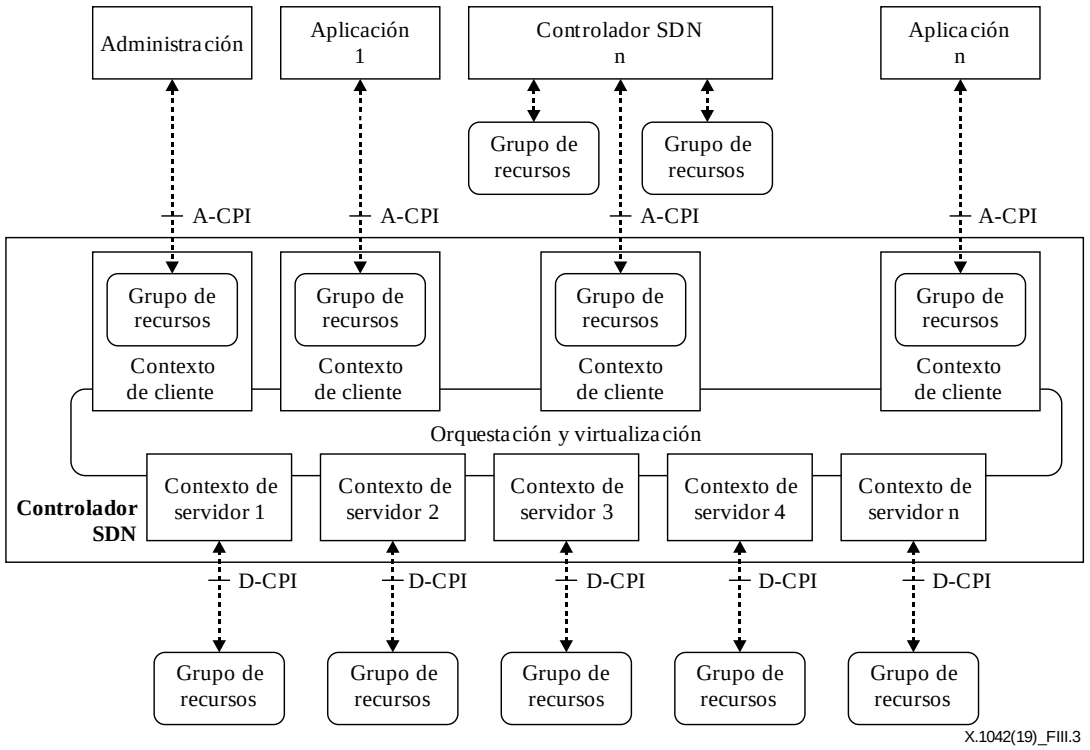


Figura III-3 – Arquitectura SDN de la ONF

III.2.2 Comparación entre las arquitecturas de la ONF y del UIT-T

La Figura III.4 ilustra la comparación entre las arquitecturas de la ONF y del UIT-T. Los componentes del UIT-T se representan en color azul.

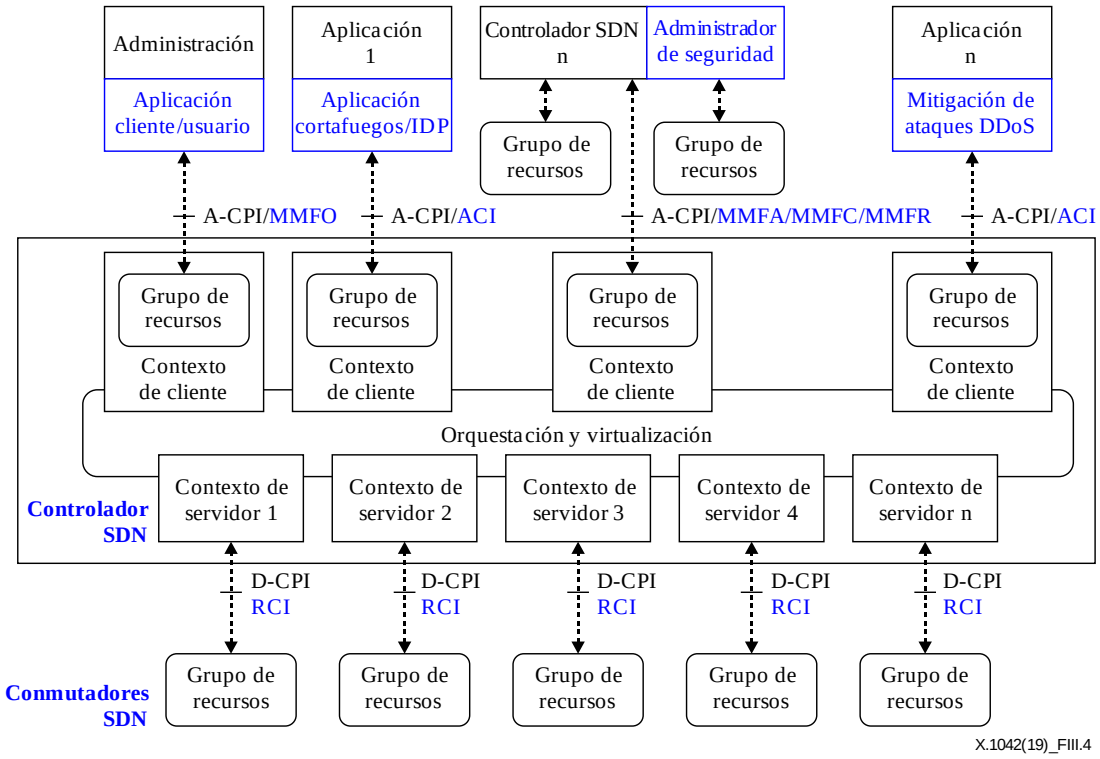


Figura III-4 – Comparación entre las arquitecturas de la ONF y el UIT-T

Bibliografía

[b-UIT-T X.812] Recomendación UIT-T X.812 (1995) | ISO/CEI 10181-3 (1996), *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Marco de control de acceso*.

[b-UIT-T X.1252] Recomendación UIT-T X.1252 (2010), *Términos y definiciones sobre gestión de identidad de referencia*.

[b-ICIN SDNSec] Z. Hu, M. Wang, X. Yan, Y. Yin y Z. Luo, "A comprehensive security architecture for SDN", en *18th International Conference on Intelligence in Next Generation Networks*, pp 30-37 – Nueva York, NY: IEEE. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7073803

[b-IETF RFC 8329] IETF RFC 8329 (2018), *Framework for interface to network security functions*. https://tools.ietf.org/html/rfc8329

[b-ONF TR-521] Open Networking Foundation TR-521 (2016), *SDN architecture*. https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/TR-521_SDN_Architecture_issue_1.1.pdf

[b-ONF TS-012] Open Networking Foundation TS-012 (2013), *OpenFlow switch specification V.1.4.0*. https://www.opennetworking.org/wp-content/uploads/2014/10/openflow-spec-v1.4.0.pdf

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios telegráficos
Serie T	Terminales para servicios telemáticos
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para los sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2019