AJEA- Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1145.2022

Modelo de seguridad para controlador SDN

Security model for SDN controller

Presentación: 26 y 27 de octubre de 2022

Juan Carlos Calloni
Universidad Tecnológica Nacional Facultad Regional San Francisco Argentina
jccalloni@gmail.com

Javier Daniel Saldarini
Universidad Tecnológica Nacional Facultad Regional San Francisco Argentina
saldarinijavier@gmail.com

Antonela Calloni
Universidad Tecnológica Nacional Facultad Regional San Francisco Argentina,
antocalloni@gmail.com

Mauricio Hilario Trossero
Universidad Tecnológica Nacional Facultad Regional San Francisco Argentina
maurytrossero@gmail.com

Gonzalo Luque
Universidad Tecnológica Nacional Facultad Regional San Francisco Argentina
gonzaloluque@hotmail.com.ar

Resumen

En respuesta al creciente tráfico y los requisitos de calidad, las redes han cambiado rápidamente. Este crecimiento ha llevado a empresas y a Universidades a cambiar su enfoque para operar la infraestructura de red. En este escenario de crecimiento exponencial y significativo se plantea este proyecto a través de las redes definidas por software (SDN). En estos escenarios la seguridad se está convirtiendo en una inquietud importante, ya que en las redes híbridas se hace muy complejo cubrir toda la superficie. Los ataques de DDoS hacia el controlador SDN pueden agotar sus recursos de procesamiento, lo cual afectaría a la disponibilidad de toda la red. Lo que se propone es un modelo abstracto que permita definir la gestión de tráfico a través de controladores SDN, para distribuir sus políticas de seguridad. Dado estos antecedentes y debido a que un campus universitario posee características únicas y basándonos en estas necesidades de asegurar una red híbrida SDN; el presente trabajo propone aplicar una revisión de antecedentes sobre un modelo de seguridad para controladores SDN en una red Universitaria.

Palabras clave: Redes definidas por Software, Modelo, Controladores, Seguridad, Redes Híbridas.

Abstract

In response to growing traffic and quality requirements, networks have changed rapidly. This growth has led companies and universities to change their approach to operating network infrastructure. In this scenario of exponential and significant growth, this project is proposed through software-defined networks (SDN). In these scenarios, security is becoming an important concern, since in hybrid networks it becomes very complex to cover the entire surface. DDoS attacks against the SDN controller can exhaust its processing resources, affecting the availability of the entire network. What is proposed is an abstract model that allows defining traffic management through SDN controllers, to distribute their security policies. Given this background and because a university campus has unique characteristics and based on these needs to ensure a hybrid SDN network; The present work proposes to apply a background review on a security model for SDN controllers in a University network

AJEA- Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1145.2022

Keywords: Software Defined Networks, Model, Controllers, Security, Hybrid Networks.

Introducción

En la última década, los requisitos de la red han cambiado rápidamente en respuesta al tamaño creciente del tráfico de la red y los requisitos de calidad. Las arquitecturas de red convencionales son estáticas y complejas para abordar las condiciones dinámicas de la red. Para permitir que las redes sean adaptativas, aparece un nuevo modelo de red emergente denominado SDN [1].

Las redes definidas por software SDN, básicamente se enfocan en la programación por software de las redes, a través de un controlador, en el cual el control se desvincula del hardware.

El plano de control es separado de la capa de red física y puede controlar flujos por separado, dependiendo de las necesidades de las políticas en capas superiores, buscando optimizar el funcionamiento de una red y mejorar drásticamente la eficiencia [2]. Un controlador SDN actúa como un cerebro virtual de la red, y ofrece a los administradores una vista de la red general. No sólo puede monitorizar el tráfico de una red con facilidad, sino que ordena a los sistemas por debajo, *switches*, *routers* y otros equipos de la red; cómo deben manejar el tráfico de red, haciendo una gestión inteligente del tráfico [3]. Entonces las SDN se definen como una arquitectura de red dinámica, gestionable, adaptable, de costo eficiente, lo cual la hace ideal para las altas demandas de ancho de banda y la naturaleza dinámica de las aplicaciones actuales [4].

La seguridad y confiabilidad de las redes SDN se está convirtiendo en una preocupación seria para la industria ya que la superficie a cubrir se hace cada vez más amplia en redes híbridas. Las redes SDN, traen beneficios en términos de programabilidad de la red y centralización de la lógica de control pero introducen nuevas posibilidades de ataques [5]. Al hablar de una red híbrida se hace referencia a una red en la que operan juntos protocolos de redes tradicionales con los de una red SDN (protocolo OpenFlow).

En definitiva, una red híbrida permite a los administradores de red introducir nuevas tecnologías de SDN como OpenFlow a entornos heredados sin una completa visión de la arquitectura de la red. Un administrador de red puede configurar el controlador SDN para descubrir y controlar el flujo de tráfico o para administrar la seguridad de la red, mientras que la red tradicional continúa dirigiendo el resto del tráfico de la red [6].

Se identifica también la seguridad en la protección de datos, dispositivos y activos tecnológicos de las compañías que operan conectadas a los controladores SDN, evidenciando que estas se encuentren protegidas y blindadas de forma eficiente, con el fin de determinar posibles anomalías, amenazas, o vulnerabilidades que se hayan presentado y a partir de ahí obtener unos resultados que mejoren de manera eficiente la seguridad en las redes SDN logrando una trasformación de las arquitecturas de los controladores SDN [7].

La naturaleza centralizada del controlador lo convierte en un elemento vulnerable a ataques que pueden provocar la interrupción del servicio de toda la red. [8] Como ejemplo, uno de los desafíos críticos es el impacto de los ataques de Denegación de Servicio Distribuido (DDoS) en las redes SDN. Un ataque de DDoS dirigido hacia el controlador SDN podría agotar sus recursos de procesamiento, volviéndolo inaccesible para los paquetes legítimos, lo cual afectaría a la disponibilidad de servicio [9].

Dado estos antecedentes y debido a que un campus universitario posee características únicas y basándonos en estas necesidades de asegurar de manera eficiente una red híbrida SDN; el presente trabajo de investigación propone aplicar SDN en la infraestructura de telecomunicaciones de la red de nuestro campus universitario, para determinar y proponer un modelo de seguridad para controladores SDN. En nuestro proyecto se plantea usar los controladores NOX y POX, con el objetivo de generar un modelo de seguridad para los controladores SDN en una red híbrida universitaria. Para ello se parte de una descripción detallada de la red a estudiar, verificando si sus principales arquitecturas garantizan autenticidad, integridad, confidencialidad y disponibilidad de la información. Luego se realizará un modelo seguro propuesto para la implementación de cada controlador SDN en la red híbrida universitaria.

La hipótesis

En la actualidad no existe un modelo de seguridad para controladores SDN en una red universitaria híbrida. Esta característica hace que los controladores SDN no puedan operar de forma segura, lo que puede traer aparejada la imposibilidad de elaborar soluciones óptimas para diferentes tipos de problemas. Es posible resolver este problema a través de un vocabulario común para los diferentes controladores puedan dialogar en un modelo estándar de seguridad. Lograr definir un Modelo Ontológico de seguridad para un controlador SDN en una red híbrida Universitaria, para la comunicación de dominios de redes y generaría una comunicación segura clara sin importar el fabricante del controlador ni el lenguaje de programación en el que está construido.

AJEA- Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1145.2022

Conceptos

SDN está cambiando la forma en que se controlan, gestionan y configuran las infraestructuras de redes de TI [10]. La perspectiva SDN se basa en la separación del plano de control del plano de datos, en donde, uno toma las decisiones de reenvío de datos y el otro las ejecuta. En cuanto con la arquitectura SDN, el plano de control está bajo la responsabilidad de un controlador centralizado que toma todas las decisiones de reenvío de flujo en la red. La comunicación entre los dos planos se logra a través del protocolo OpenFlow especificado por la Open Networking Foundation (ONF) [10].

La tecnología SDN se está adoptando ampliamente en los dominios de redes comerciales, gubernamentales y, especialmente, en el sector universitario. Ahora bien, los modelos de redes tradicionales, sobre los cuales se han desarrollado todos los servicios que estas ofrecen y, además donde se basan los nuevos servicios digitales, considera a la red como un conjunto de elementos independientes, relacionados entre sí y que transfieren datos entre ellos. La dificultad se genera al tratar de establecer la red como un todo, y hay que entender que son elementos individuales, con conexiones y diferentes características. Es aquí donde entra en juego la arquitectura SDN, la cual ofrece posibilidades de interactuar directamente con la red como si fuera un todo, teniendo entonces las siguientes características: 1) flexibilidad: ya que el flujo de datos se ajusta dinámicamente a los cambios de la red. 2) programable: porque se permite establecer reglas de flujo mediante la programación, 3) administrable: ya que se tiene el control de la red centralizado, y 4) rentable: puesto a que no se necesita estar atado a un software propietario [11].

Por lo tanto, las redes requieren una reconfiguración frecuente en enrutamiento, QoS, firewall, etc. La velocidad y la escala de estos cambios llevan a la inestabilidad de la red. Por esta razón, se necesita una red programable para aumentar la flexibilidad de la red y mantener al mínimo los efectos secundarios causados por los cambios [12].

OpenFlow es un protocolo estándar que administra los comportamientos de reenvío de conmutadores SDN de varios proveedores. Facilita la gestión del controlador SDN y la supervisión de los conmutadores SDN. El protocolo controla de forma programática y dinámica los comportamientos de reenvío de los conmutadores SDN y, a través del protocolo OpenFlow, envía mensajes a los conmutadores para controlar el comportamiento de reenvío de una red. Un conmutador OpenFlow puede tener más de una tabla de flujo, lo que se denomina cadena. Cuando un paquete ingresa a un conmutador OpenFlow, el paquete se verifica con tablas de flujo, respectivamente. Las reglas en las tablas de flujo tienen tres secciones, incluida la prioridad, el campo de coincidencia y la acción. El campo de prioridad define qué regla debe seleccionarse si el paquete coincide con campos de coincidencia de varias reglas. La regla elegida aplica la acción al paquete de acuerdo con las opciones correspondientes: reenviar el paquete a un puerto específico, descartar o modificar el encabezado del paquete [13].

Usos y Aplicaciones

***Data Centers*:** Un gran problema de los data centers, es el gran consumo energético que producen. Las redes SDN pueden permitir mejorar la eficiencia energética a través de métodos para usar solo una parte de la red, intentando que esto no repercuta en la eficiencia de la red. Más adelante nosotros también abordaremos este problema. [14]

Redes ópticas: Manejar el tráfico de datos mediante flujos, permite a las SDN y a OpenFlow en particular, soportar e integrar múltiples tipos de tecnologías de red. De acuerdo con el Optical Transport Working Group (OTWG) creado en 2013 por la Open Network Foundation (ONF), los beneficios de aplicar SDN y el estándar OpenFlow en particular a las redes de transporte ópticas incluyen: mejora el control de red del transporte óptico y la flexibilidad en la administración, permitiendo la implementación de administración de terceros y control de sistemas, e implementando nuevos servicios de virtualización.

Infraestructuras basadas en redes de acceso inalámbricas: Recientemente se está viendo un creciente interés académico y de la industria en para aplicar SDN a las redes móviles. La principal motivación detrás de esto es que SDN puede ayudar a los operadores móviles a simplificar la administración de sus redes y permitir nuevos servicios que soporten el crecimiento exponencial del tráfico previsto para las redes 5G [15].

Seguridad utilizando el paradigma de SDN: La arquitectura SDN puede permitir, facilitar o mejorar las aplicaciones de seguridad relacionados con la red debido a la visión central del controlador de la red y su capacidad para reprogramar el plano de datos en cualquier momento. Mientras que la seguridad de la arquitectura SDN en sí sigue siendo una pregunta abierta. Varios trabajos de investigación sobre SDN ya han investigado las aplicaciones de seguridad integradas en el controlador SDN, con diferentes objetivos en mente. Denegación de Servicio Distribuida (DDoS) detección y mitigación, así como *botnet* y la propagación de gusanos [16].

Análisis de Proyectos Similares

AJEA- Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1145.2022

En el proyecto **"Seguridad y rendimiento en redes híbridas SDN"** se hace un análisis de la seguridad pero con escenarios de menos carga de transmisión de datos como pueden ser los escenarios de extremo a extremo como las Video Conferencia para escenarios mixtos en campus Universitarios.
En el siguiente trabajo **"Implementación de Comunicaciones Unificadas en Computación en la Nube y Redes Híbridas"**, se focaliza la red híbrida pensando en múltiples servicios pero en la nube y en la nube privada concluyendo "Redes como Servicio (NaaS) con Neutrón en Openstack es una solución para la convergencia entre redes tradicionales y redes definidas por software para servicios en la nube (UCaaS)". Se realizaron pruebas de los diferentes servicios ofrecidos como telefonía IP, mensajería instantánea, video conferencia, etc. En donde el origen inicia dentro de una red tradicional y su destino era una red SDN, teniendo resultados positivos y alentadores en cuanto a calidad y consumo de ancho banda de los servicios antes mencionados, pero en ningún caso hace mención de la seguridad problema que hoy afecta a este tipo de redes híbridas y de múltiples servicios.

En el siguiente trabajo **"Metodología de detección y mitigación de ataques DDoS en entornos SDN basado en la norma ISO/IEC 27001 para mejorar la seguridad en el plano de control"** se menciona "El presente trabajo se realizó con el objetivo de desarrollar una Metodología para la implementación de una solución de seguridad relacionada a la detección y mitigación de ataques DDoS en el plano de control de SDN, capaz de ser utilizada como guía para los profesionales de la rama y demás interesados en la seguridad de la información. La metodología se desarrolló en base a la norma ISO 27001 y su alineación con el ciclo PDCA, de donde se tomaron las directrices generales para la realización de cada uno de los subprocesos de la metodología planteada: Identificación de riesgos, Planificación, Selección del mecanismo, Pruebas, Implementación, Monitoreo y Mejora" [17].
Una parte importante de este trabajo servirá de aporte a nuestro proyecto, la parte de simulación de ataques de DoS y la metodología planteada pero no resuelve el problema que nos planteamos en tener un modelo de seguridad para un controlador SDN en una red híbrida universitaria.

Conclusión

Podemos mencionar que la hipótesis planteada con sus objetivos fueron cumplidos. A pesar de sus especiales características, las redes SDN híbridas poseen diferentes debilidades desde el punto de vista de la seguridad. A lo largo del presente trabajo se pone de manifiesto la relevancia y preocupación actual en este aspecto. Por otro queremos destacar que los temas relacionados a la seguridad y a las redes SDN, que aparecen en la revisión de trabajos similares, son: Denegación de Servicios Distribuida (DDoS), los Controladores SDN, IOT relaciona con SDN, como los nuevos temas motores de trabajos en los últimos años. Motivados por lo anterior, podemos enfatizar la importancia de la propuesta de una ontología y un modelo, que ayudará a la clasificación de soluciones en esta línea y de soluciones de seguridad en redes híbridas SDN por parte de trabajos propuestos.

Trabajos futuros

Se plantea en proyectos futuros, desarrollar el modelo y refinarlo con pruebas en el mismo escenario y con ese modelo construir un algoritmo para realizar una API en distintos lenguajes para diferentes controladores, para luego generalizarlas y que sirva como intermediario para diferentes escenarios de proyectos de redes SDN híbridas mediante controladores SDN.

Referencias

[1] J. D. R. V. S. M. S. C. L. A. N. F. Miguel Fabricio Bone Andrade. 1, «Aplicaciones de SDN en infraestructura de redes educativas,» *Ciencia Digital (ISSN: 2602-8085¡,* vol. 5, nº 1, pp. 219-231, 2021.

[2] M. Rouse, «Searchsdn Techtarget,» Agosto 2015. [En línea]. Available: http://searchsdn.techtarget.com/definition/software-defined-networking-SDN.

[3] CCNA, «ccna-certification,» 25 10 2015. [En línea]. Available: http://www.ccna-certification.info/que-es-el-software-defined-networking-sdn.

[4] D. I. P. F. Á. &. F. A. R. De la Torre, «Combinación de mecanismos MPLS en una arquitectura SDN.,» *Telemática,* vol. 18, nº 1, pp. 1-10, 2019.

[5] S. S. Galiano, «ANÁLISIS DE DELTA COMO HERRAMIENTA DE SEGURIDAD EN SDN,» Universidad de Los Andes, Facultad de Ingeniería Departamento de Ingeniería de Sistemas y Computación, Bogotá, 2017.

AJEA- Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1145.2022

[6] Y. D. Herrera, «PROPUESTA DE ARQUITECTURA PARA LA GESTIÓN DE REDES DEFINIDAS POR SOFTWARES HÍBRIDAS,» Universidad de las Ciencias Informaticas, La Habana, 2016.

[7] C. L. V. MEJIA, «ANÁLISIS DE SEGURIDAD EN REDES SDN,» UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “, MEDELLIN, ANTIOQUIA, 2018.

[8] V. S. K. M. &. D. P. Deepa, «Detection of DDoS Attack on SDN Control plane using Hybrid Machine Learning Techniques.,» de *Conference on Smart Systems and Inventive Technology*, https://doi.org/10.1109/ICSSIT.2018.8748836, 2018.

[9] R. M. &. J. D. Thomas, «DDOS Detection a nd Denial u sing Third Party Application in SDN,» de *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, 3892–3897, 2017.

[10] B. H. &. A. N. Lawal, «Real-Time Detection and Mitigation of Distributed Denial of Service (DDoS) Attacks in Software Defined Networking (SDN),» de *26 Signal Processing and Communications Applications Conference (SIU)*, 1–4, 2018.

[11] J. Silva1, «Tecnología de red definida por software para el aprendizaje en grupos de investigación y educación,» de *Revista Innova Educación*, ISSN: 2664-1496 ISSN-L: 2664-1488, 2021.

[12] B. A. N. M. MM Tajiki, «Reconfiguración óptima de red compatible con QOS en centros de datos en la nube definidos por software,,» de *Comput. Neto*, Pag 71-86, 2017.

[13] b. c. ,. B. O. K. P. E. E. ramtin ario Anis Yazidi d, «SDN Spotlight: un marco de resolución de problemas de OpenFlow en tiempo real,» *Elseiver,* vol. 133, nº 133, pp. 364-377, 2022.

[14] R. J. a. S. Paul, «Network virtualization and software defined networking for cloud computing,» *Communications Magazine, IEEE,* vol. 51, nº 11, pp. 24-31, 2013.

[15] Z. F. a. R. H. Woon Hau Chin, «Emerging technologies and research challenges for 5g wireless networks,» *Wireless Communications, IEEE,* vol. 51, nº 11, pp. 106-112, 2014.

[16] R. &. W. B. Jin, «Malware detection for mobile devices using software-defined networking,» *Research and Educational Experiment Workshop,* vol. 2, pp. 81-88, 2013.

[17] J. E. B. Cheza, «“Metodología de detección y mitigación de ataques ddos en entornos sdn basado en la norma iso/iec 27001 para mejorar la seguridad en el plano de control”,» de *UNIVERSIDAD TÉCNICA DEL NORTE MAESTRÍA EN TELECOMUNICACIONES*, Ibarra, Ecuador, 2021.