SECYT SECRETARIA DE CIENCIA Y TECNOLOGIA | FACULTAD REGIONAL SAN FRANCISCO

Proyectos de investigación vigentes

Título de proyecto	Modelo de seguridad para controladores SDN en una red híbrida universitaria
Código UTN	SITCSF0008757
Director/a	Calloni, Juan Carlos
Dirección de correo	jcalloni@frsfco.utn.edu.ar / jcalloni@hotmail.com
Codirector/a	
Dirección de correo	
Palabras clave	Modelo; seguridad; redes definidas por software; controlador; red SDN híbrida.
Desde	01/04/2023
Hasta	31/03/2026
Resumen técnico del PID	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.

[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: 2602-8085j, 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.

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