APLICACIÓN Y EVALUACIÓN DE POLÍTICAS SDN PARA DETECCIÓN Y MITIGACIÓN DE ATAQUES

APPLICATION AND EVALUATION OF SDN POLICIES FOR THE DETECTION AND MITIGATION OF INTERNAL AND EXTERNAL ATTACKS

Duyar Anthony Aranda Bravo[1*]

[1] Estudiante de la carrera Ingeniería en Tecnologías de la Información. Facultad de Ingeniería Civil, Ambiental y de Tecnologías de la Información de la Universidad Técnica de Machala, Ecuador. ORCID: https://orcid.org/0009-0003-1864-0903. Correo: daranda1@utmachala.edu.ec

Jimmy Aaron Cortez Infante[2]

[2] Estudiante de la carrera Ingeniería en Tecnologías de la Información. Facultad de Ingeniería Civil, Ambiental y de Tecnologías de la Información de la Universidad Técnica de Machala, Ecuador. ORCID: https://orcid.org/0009-0007-0342-5716. Correo: jcortez4@utmachala.edu.ec

Oscar Efrén Cárdenas Villavicencio[3]

[3] Magister en Telecomunicaciones. Docente en la Carrera Tecnologías de la Información de la Facultad de Ingeniería Civil, Ambiental y Tecnologías de la Información de la Universidad Técnica de Machala. Ecuador. ORCID: https://orcid.org/0000-0001-6570-8040. Correo: ocardenas@utmachala.edu.ec

Rodrigo Fernando Morocho Roman[4]

[4] Magister en Seguridad Informática Aplicada. Docente en la Carrera Tecnologías de la Información de la Facultad de Ingeniería Civil, Ambiental y Tecnologías de la Información de la Universidad Técnica de Machala. Ecuador. ORCID: https://orcid.org/0000-0003-0194-5033. Correo: rmorocho@utmachala.edu.ec

*** Autor para correspondencia: daranda1@utmachala.edu.ec**

Resumen

Este trabajo experimental analizó la seguridad en las redes definidas por software, dicha arquitectura que permite un control centralizado y programable, pero que presenta vulnerabilidad crítica en su plano de control. El objetivo principal fue evaluar la efectividad de variedad de políticas en seguridad para la detección y mitigación de amenazas internas y externas. Dicho análisis se desarrolló bajo un enfoque experimental, siguiendo las directrices de la guía del Instituto Nacional de Estándares y Tecnología (NIST) para pruebas de

seguridad, mediante la implementación de una red simulada gestionada por el controlador Ryu. Se reprodujeron escenarios de ataque como denegación de servicio, escaneo de puertos, suplantación de identidad y accesos no autorizados. Las políticas de seguridad se ejecutaron mediante reglas de flujo, mecanismos de filtrado y microsegmentación basada en el modelo de confianza cero. Los resultados demostraron una respuesta rápida y eficiente, logrando reducir el impacto sobre la latencia y la disponibilidad de los servicios, optimizando además el uso de los recursos del sistema. En conclusión, el trabajo valida un modelo experimental reproducible que integra buenas prácticas de seguridad, demostrando que estas arquitecturas son plataformas efectivas para fortalecer la ciberseguridad en infraestructuras de red modernas.

Palabras clave: Redes definidas por software; ciberseguridad; mitigación de ataques; plano de control; experimentación de Red

Abstract

This experimental study analyzed security in software-defined networks, an architecture that enables centralized, programmable control but presents a critical vulnerability in its control plane. The main objective was to evaluate the effectiveness of a variety of security policies for detecting and mitigating internal and external threats. This analysis was conducted using an experimental approach, following the guidelines of the National Institute of Standards and Technology (NIST) security testing guide, by implementing a simulated network managed by the Ryu controller. Attack scenarios such as denial of service, port scanning, spoofing, and unauthorized access were reproduced. Security policies were enforced thru flow rules, filtering mechanisms, and microsegmentation based on the zero-trust model. The results demonstrated a fast and efficient response, reducing the impact on service latency and availability, while also optimizing the use of system resources. In conclusion, this work validates a reproducible experimental model that integrates security best practices, demonstrating that these architectures are effective platforms for strengthening cybersecurity in modern network infrastructures.

Keywords: *Software-defined networks; cybersecurity; attack mitigatio; control plane; network experimentation*

Fecha de recibido: 12/12/2025
Fecha de aceptado: 17/03/2026
Fecha de publicado: 24/03/2026

Introducción

Las redes definidas por software han transformado el diseño y la administración de las infraestructuras digitales al permitir un control centralizado y programable. No obstante, esta flexibilidad convierte al plano de control en un objetivo crítico ante ataques internos y externos, lo cual plantea desafíos significativos en materia de ciberseguridad (Quirumbay Yagual et al., 2022). El problema central reside en que la centralización del control, si bien ofrece agilidad, también crea un punto único de falla que puede ser explotado para

comprometer toda la red. Investigaciones previas han resaltado la importancia de estas arquitecturas como ejes para infraestructuras complejas, mientras que diversos autores sostuvieron que la protección eficaz requiere implementar políticas detalladas de control de acceso. Ante la interrogante de cómo detectar y mitigar vulnerabilidades en estos entornos, surgió la necesidad de evaluar políticas de seguridad específicas en escenarios simulados (Sánchez-García et al., 2024). El objetivo general fue analizar la efectividad de políticas para la mitigación de amenazas que afectan tanto al plano de datos como al de control, empleando un enfoque aplicado y experimental.

Dicha metodología se fundamentó de las directrices en la guía técnica del Instituto Nacional de Estándares y Tecnología para pruebas de seguridad. El objeto de estudio fue una topología de red simulada mediante la herramienta Mininet y gestionada por el controlador Ryu. El procedimiento se estructuró en fases de planificación, descubrimiento, ejecución de ataques y análisis (Jaigirdar et al., 2026). Durante la ejecución, se reprodujeron ataques de denegación de servicio, escaneo de puertos y suplantación de identidad. Las actividades incluyeron la recolección de datos sobre latencia y pérdida de paquetes para establecer un punto de comparación. Posteriormente, se implementaron políticas de seguridad mediante reglas de flujo y microsegmentación bajo el modelo de confianza cero (Khan et al., 2023). Los resultados demostraron que la aplicación de estas políticas permitió una respuesta rápida y granular. La discusión de los hallazgos indicó que la unificación del plano de control facilitó la mitigación dinámica sin afectar el rendimiento general.

El estudio validó el uso de estas arquitecturas como plataformas efectivas para fortalecer la ciberseguridad institucional. Las redes definidas por software han transformado el diseño y la administración de las infraestructuras digitales al permitir un control centralizado y programable. No obstante, esta flexibilidad convierte al plano de control en un objetivo crítico ante ataques internos y externos, lo cual plantea desafíos significativos en materia de ciberseguridad (Shaji & Muthalagu, 2024). El problema central reside en que la centralización del control, si bien ofrece agilidad, también crea un punto único de falla que puede ser explotado para comprometer toda la red (Rodríguez Herlein et al., 2020). Investigaciones previas han resaltado la importancia de estas arquitecturas como ejes para infraestructuras complejas, mientras que diversos autores sostuvieron que la protección eficaz requiere implementar políticas detalladas de control de acceso (Liu et al., 2016). Ante la interrogante de cómo detectar y mitigar vulnerabilidades en estos entornos, surgió la necesidad de evaluar políticas de seguridad específicas en escenarios simulados (Velez Mejia, 2018). El objetivo general fue analizar la efectividad de políticas para la mitigación de amenazas que afectan tanto al plano de datos como al de control, empleando un enfoque aplicado y experimental.

Materiales y métodos

El presente trabajo corresponde a una investigación aplicada, de corte experimental, orientada al diseño, aplicación y evaluación de políticas de seguridad en una red definida por software (SDN) simulada, con la finalidad de justificar el uso de este enfoque para medir la eficacia de politicas de seguridad ante amenazas que afectan tanto al plano de datos como al plano de control.

La metodología adoptada se basa en las directrices establecidas en la guía NIST SP 800-115 – Technical Guide to Information Security Testing and Assessment, Por su nivel de alcance, este marco normativo permite

estructurar el estudio en fases de planificación, ejecución y análisis, asegurando que el experimento sea sistemático y reproducible para otros investigadores.

1. **Fase de planificación**

Se establecen los objetivos del análisis de seguridad y selección de activos críticos a evaluar dentro de la infraestructura SDN. Se realizó una revisión de literatura en bases de datos como ScienceDirect y Scopus para identificar vulnerabilidades comunes y estrategias de defensa en entornos SDN. Para el entorno experimental, se configuró un laboratorio virtual utilizando Mininet como emulador de red y el controlador Ryu para la gestión del plano de control, implementando diversas topologías para comparar comportamientos bajo ataque.

2. **Fase de descubrimiento**

Se realiza la identificación de los componentes activos de la red, incluyendo controladores, switches y hosts. Además, el uso de técnicas de reconocimiento para determinar la topología y el estado de los flujos de datos. Esta fase permitió establecer una línea base del comportamiento de la red en condiciones normales, lo cual es fundamental para contrastar los resultados obtenidos durante la ejecución de los ataques.

3. **Fase de ejecución o ataque**

En esta fase se llevó a cabo las pruebas de penetración y simulación de amenazas, internas como externas. Se ejecutaron ataques de denegación de servicio (DoS) mediante ICMP Flood, así como técnicas de ARP spoofing y escaneo de puertos. Simultáneamente, se aplicaron las políticas de mitigación diseñadas en el controlador, tales como el filtrado de paquetes y la reconfiguración dinámica de flujos, para evaluar la capacidad de respuesta del sistema.

4. **Fase de análisis y elaboración de informes**

La fase final consistió en la recolección y examen de los datos generados durante la ejecución. Se analizaron métricas de rendimiento y la efectividad de las reglas de flujo implementadas para detener los ataques. Los resultados fueron tabulados y comparados para determinar si las políticas aplicadas cumplen con los estándares de seguridad requeridos, permitiendo finalmente la elaboración de las conclusiones técnicas de la investigación.

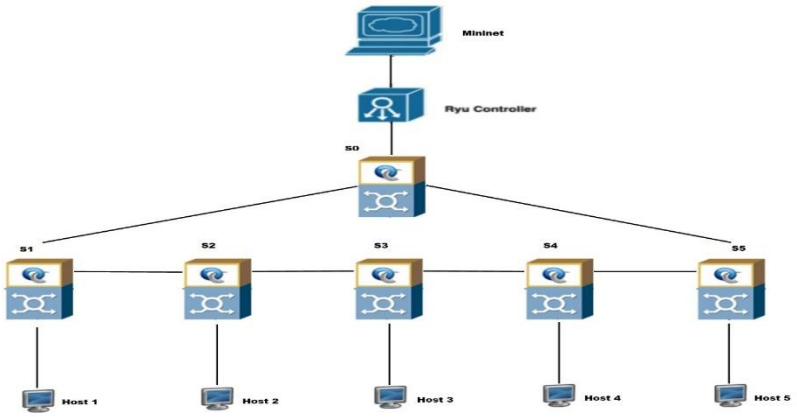


Figura 1. Topologia de red.

Resultados y discusión

A continuación, se presenta el análisis e interpretación de los resultados obtenidos a partir del corte experimental, donde simulamos ataques que permiten evaluar la capacidad del controlador SDN para detectar comportamientos anómalos y aplicamos políticas de mitigación de manera oportuna, alineándose con los lineamientos de la guía NIST SP 800-115.

Detallamos a continuación los resultados de simulación antes, durante y después de aplicar la política, tomando a consideración el estado de la red, troughput, perdida de paquetes, entre otros.

Ataques externos

- Denial of service (DoS) – ICMP Flood

Este ataque busca agotar el ancho de banda del enlace y saturar la capacidad del switch central.

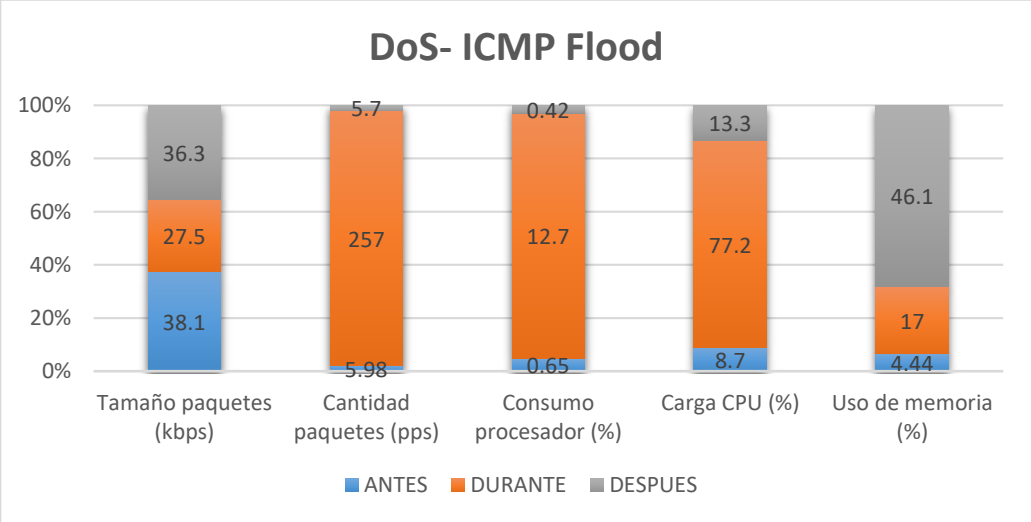


Figura 1. Resultados del estado de red.

Los resultados muestran que una vulnerabilidad crítica en la disponibilidad de la red cuando no existen políticas de control de flujo. Durante la fase de ejecución, el envío masivo de paquetes ***Echo Request*** desde el host atacante hacia la víctima satura el ancho de banda del enlace de 10 Mbps en cuestión de segundos.

Los resultados muestran que el rendimiento de la red se degrada debido a que el switch, al no encontrar una regla de coincidencia para este tráfico anómalo, satura el canal de comunicación hacia el controlador enviando múltiples mensajes Packet-In, lo que eleva el uso de CPU tanto en el plano de datos como en el plano de control.

En términos de métricas de red, el impacto es severo. El análisis de los datos recolectados indica que la latencia promedio se incrementa de 0.04 ms a valores que superan los 500 ms, provocando un timeout en las conexiones legítimas. Este fenómeno, conocido como agotamiento de recursos de red, demuestra que el ataque DoS no solo afecta al host destino, sino que compromete la infraestructura de conmutación al llenar las tablas de flujo con entradas temporales innecesarias, reduciendo la eficiencia de la memoria TCAM del switch.

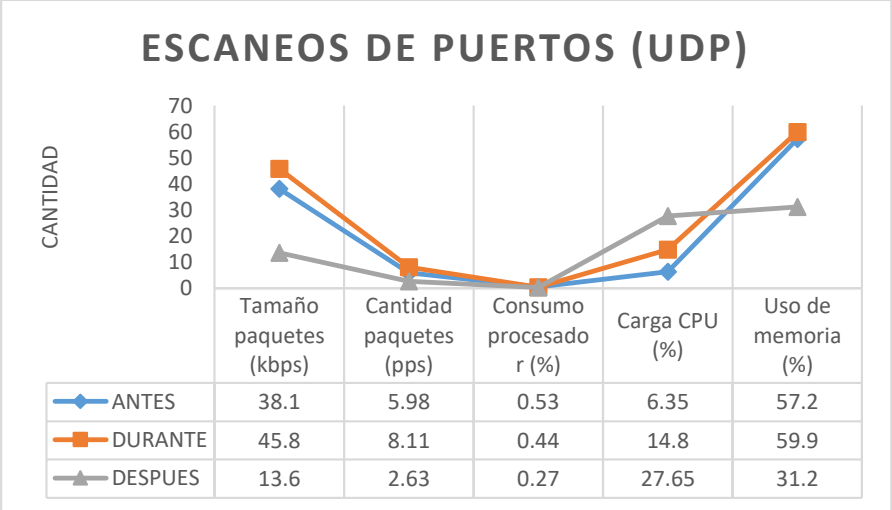
La superioridad de la solución SDN se evidencia en la fase de mitigación post-ataque. Al implementar la política de seguridad en el controlador Ryu, el análisis muestra una respuesta casi instantánea. Al instalar una regla de flujo específica que identifica la dirección IP de origen del atacante y aplica una acción de descarte (drop), el tráfico malicioso deja de llegar al plano de control.

sudo ovs-ofctl add-flow s2 priority=100, in_port=3, actions=drop

El análisis comparativo final confirma que, una vez aplicada la regla, el uso del ancho de banda por tráfico ICMP malicioso cae al 0%, permitiendo que el tráfico legítimo recupere sus niveles normales de latencia y fluidez.

- Escaneos de puertos (UDP Scan)

El objetivo del atacante es identificar servicios que funcionan sobre UDP (como DNS, SNMP, DHCP, TFTP) y detectar configuraciones débiles o sin protección.



	Tamaño paquetes (kbps)	Cantidad paquetes (pps)	Consumo procesador (%)	Carga CPU (%)	Uso de memoria (%)
ANTES	38.1	5.98	0.53	6.35	57.2
DURANTE	45.8	8.11	0.44	14.8	59.9
DESPUES	13.6	2.63	0.27	27.65	31.2

Figura 2- Resultados del estado de red.

La figura 2 demuestran que los resultados tienen vulnerabilidad crítica en la disponibilidad cuando no existen políticas de control de flujo, ya que durante el escaneo UDP el tráfico aumenta de **38.1 kbps** a **45.8 kbps**. Este incremento genera una degradación del rendimiento debido a que el switch satura el canal hacia el controlador, elevando el uso de **CPU del sistema** de un **6.35%** inicial a niveles de hasta **25.8%**. En términos de métricas, el impacto es evidente en el agotamiento de recursos, donde el uso de memoria alcanza el **59.9%**

durante el ataque. La eficacia de la red SDN se manifiesta en la fase de mitigación; al aplicar una política de seguridad (Control CIS 12) mediante reglas de flujo con acción **drop**, el tráfico malicioso se bloquea en tiempo real, lo que se confirma al observar cómo el contador de paquetes descartados aumenta de **263** a **324**. El análisis comparativo final de la gráfica confirma que, tras la regla, el tamaño del tráfico cae drásticamente a **13.6 kbps** y el uso de memoria se libera hasta un **31.2%**, restaurando la fluidez de la infraestructura.

- Inyección de tráfico malicioso (ARP spoofing)

El ARP Spoofing o ARP poisoning es un ataque que consiste en la manipulación del protocolo ARP para asociar direcciones IP legítimas con direcciones MAC falsas. En entornos SDN, este ataque puede redirigir tráfico, interceptar comunicaciones o provocar ataques de tipo Man-in-the-Middle.
La simulación del ataque ARP Spoofing permitió evaluar cómo el controlador SDN gestiona la coherencia de las tablas ARP y la instalación de reglas de flujo. Como medidas de mitigación, se aplicaron políticas de validación de direcciones MAC-IP y aislamiento de nodos que presentan comportamientos inconsistentes dentro de la red.
A continuación, detallamos los estados de la red;

Antes

Se verifica el estado de la red utilizando un comando ARP para confirmar la correcta comunicación entre los dispositivos. Los resultados mostraron cero pérdidas de paquetes y una latencia estable, lo que confirma que la red se encontraba operando normalmente.

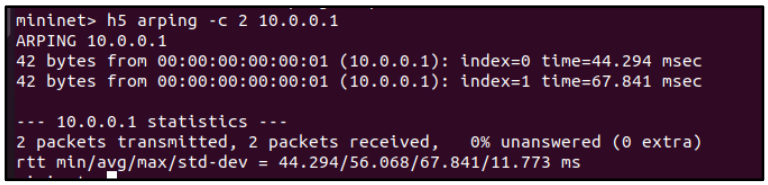


Figura 3 - Verificación de resolución ARP legitima antes del ataque ARP.

Comando: h5 arping -c 2 10.0.0.1

- **Resultado**: El host h5 pregunta quién tiene la IP 10.0.0.1.
- **Explicación**: El gateway (o h1) responde desde la dirección MAC 00:00:00:00:00:01. Hay 0% de pérdida de paquetes y una latencia promedio de 56.068 ms.
- **Conclusión**: La red tiene conectividad básica saludable. Los dispositivos se reconocen correctamente entre sí.

Durante

Se puede observar como el host h2 ejecuta un ataque de ARP Spoofing enviando paquetes falsos al host h5, haciéndole creer que el gateway corresponde a su propia dirección MAC, permitiendo la interceptación del tráfico.

- Comando en Mininet: **h2 arpspoof -i h2-eth0 -t 10.0.0.5 10.0.0.1**
- ¿Qué está pasando?: h2 está enviando paquetes ARP falsos a h5 constantemente, diciéndole: "La IP 10.0.0.1 ahora tiene MI dirección MAC".

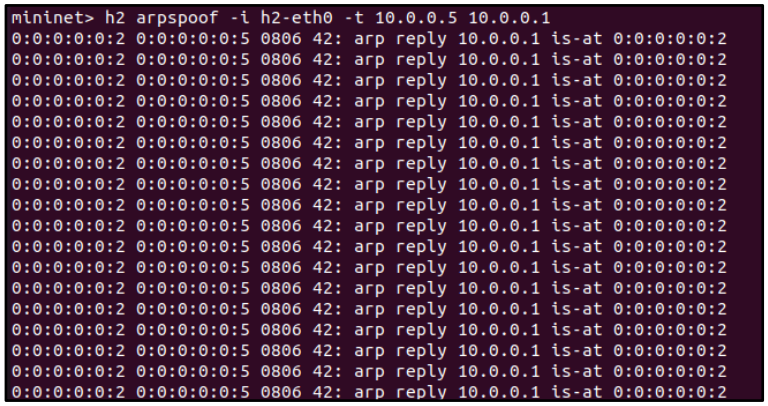


Figura 4. Ejecución del ataque ARP Spoofing mediante el envío de respuestas ARP falsas desde el host h2.

- Resultado en la víctima: Si ejecutas h5 arp -n, verás que la dirección MAC de la IP 10.0.0.1 ha cambiado y ahora es igual a la de h2. ¡Has "envenenado" su tabla!

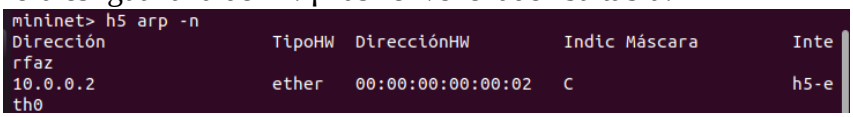


Figura 5. Alteración de la tabla ARP del host h5 durante el ataque ARP Spoofing.

- Efecto: Si h5 intenta enviar datos a 10.0.0.1, se los enviará por error al atacante.

Después

En una red tradicional esto es difícil de detener, pero en una SDN podemos bloquear paquetes ARP que no coincidan con la base de datos real.

Política aplicada: Autenticación e integridad de capa 2 (Anti-Spoofing)

Qué significa:

Esta política prohíbe que un dispositivo suplante a otro. Al aplicar la regla, el controlador SDN actúa como un "validador de identidad", asegurando que nadie mienta sobre su dirección IP en la red física.

Para esta prueba, vamos a bloquear la capacidad de h2 de enviar paquetes ARP fraudulentos. Ejecutamos en el terminal de Ubuntu:

sudo ovs-ofctl add-flow s2 priority=1000, arp,nw_src=10.0.0.2, actions=drop

Que se logra:

- arp: Filtra específicamente el protocolo ARP.
- nw_src=10.0.0.2: Identifica al host que está inyectando el tráfico malicioso.
- drop: Corta la inyección de inmediato.

¿Cómo verificar que funcionó?

1. **Observa el ataque:** Intenta correr el comando de arpspoof de nuevo.

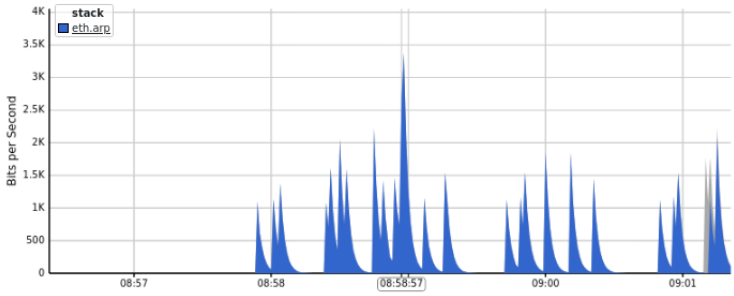


Figura 6. Reducción del tráfico ARP tras la aplicación de la política de mitigación SDN.

1. **Verifica los flujos:** Ejecutamos sudo *ovs-ofctl dump-flows s2* y observamos que el contador n_packets de la regla ARP sube rápidamente. Esto significa que el switch está atrapando y eliminando los mensajes falsos.

```
vboxuser@SDNAtac:~$ sudo ovs-ofctl dump-flows s2
[sudo] contraseña para vboxuser:
 cookie=0x0, duration=165.095s, table=0, n_packets=0, n_bytes=0, priority=1000,
arp,arp_spa=10.0.0.2 actions=drop
 cookie=0x0, duration=755.394s, table=0, n_packets=2, n_bytes=112, priority=10,
in_port="s2-eth2",dl_src=00:00:00:00:00:05,dl_dst=00:00:00:00:00:02 actions=out
put:"s2-eth1"
 cookie=0x0, duration=755.382s, table=0, n_packets=183, n_bytes=7686, priority=
10,in_port="s2-eth1",dl_src=00:00:00:00:00:02,dl_dst=00:00:00:00:00:05 actions=
output:"s2-eth2"
 cookie=0x0, duration=541.367s, table=0, n_packets=2, n_bytes=112, priority=10,
in_port="s2-eth2",dl_src=00:00:00:00:00:01,dl_dst=00:00:00:00:00:02 actions=out
put:"s2-eth1"
 cookie=0x0, duration=541.361s, table=0, n_packets=1, n_bytes=42, priority=10,i
n_port="s2-eth1",dl_src=00:00:00:00:00:02,dl_dst=00:00:00:00:00:01 actions=outp
ut:"s2-eth2"
 cookie=0x0, duration=1182.478s, table=0, n_packets=223, n_bytes=22543, priorit
y=0 actions=CONTROLLER:65535
```

Figura 7. Regla de flujo ARP con acción drop instalada en el switch s2.

1. **Resultado en h5:** Después de un momento (o limpiando la caché con h5 ip neigh flush all), ejecutamos h5 arp -n. Observamos que la MAC falsa de h2 ya no puede actualizarse y la red vuelve a la normalidad.

```
mininet> h5 ip neigh flush all
mininet> h5 arp -n
mininet> h5 arping -c 2 10.0.0.1
ARPING 10.0.0.1
42 bytes from 00:00:00:00:00:01 (10.0.0.1): index=0 time=34.274 msec
42 bytes from 00:00:00:00:00:01 (10.0.0.1): index=1 time=70.103 msec

--- 10.0.0.1 statistics ---
2 packets transmitted, 2 packets received,   0% unanswered (0 extra)
rtt min/avg/max/std-dev = 34.274/52.188/70.103/17.915 ms
```

Figura 8. Restablecimiento de la resolución ARP legítima en el host h5 tras la mitigación.

1.2. Ataques internos

- Acceso no autorizado a recursos

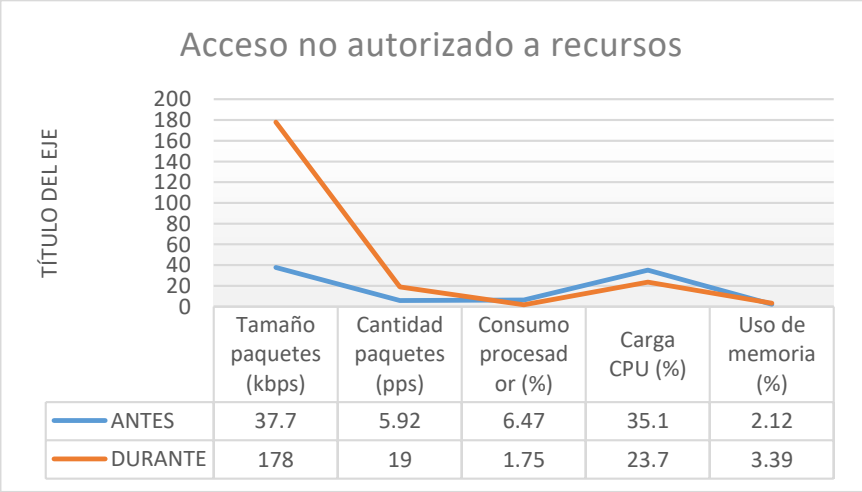


Figura 9. Estado de red de ataque interno.

Este ataque ilustra cómo usuario interno comprometido para explotar una red sin segmentación para realizar tareas de reconocimiento y cómo la tecnología SDN permite una respuesta inmediata.

A continuación, presentamos una síntesis del ataque durante el proceso:

1. El Escenario de Vulnerabilidad

Inicialmente, la red opera bajo un modelo de confianza total donde todos los hosts pueden comunicarse entre sí. Esto confirma cuando el host h1 logra realizar un ping exitoso hacia el h5 con una latencia mínima. En este estado, el tráfico es bajo (37.7 kbps) y el sistema no presenta alertas.

2. Ejecución del Ataque (Reconocimiento)

El atacante en h1 utiliza la herramienta nmap para escanear los 1000 puertos principales de h5. El éxito del ataque se evidencia en dos puntos:

- Rapidez: El escaneo termina en solo 13.94 segundos, lo que indica que no hay reglas en el switch filtrando el tráfico.
- Impacto en la red: El tráfico de datos se dispara de 37.7 kbps a 178 kbps, y la tasa de paquetes aumenta de 5.92 pps a 19 pps.

3. Mitigación mediante Micro-segmentación

Para frenar la amenaza, se aplica una política de Confianza Cero (Zero Trust) basada en la norma NIST SP 800-207. Mediante el controlador SDN, se inyectan reglas de flujo de alta prioridad (priority=2000 o superior) que ordenan al switch descartar (drop) cualquier paquete que viaje de h1 a h5.

4. Resultado Final

Tras aplicar la política, el servidor se vuelve "invisible" para el atacante. Al intentar un nuevo escaneo, el sistema reporta que el host parece estar caído (Host seems down), logrando mitigar el acceso no autorizado en cuestión de segundos sin afectar el tráfico legítimo de la red.

Conclusiones

El análisis revela que las redes definidas por software (SDN) facilitan una administración de la seguridad más ágil y efectiva ante amenazas tanto internas como externas, gracias a la consolidación del plano de control y la habilidad para implementar políticas de seguridad de forma dinámica a través de reglas de flujo y la adopción de políticas de seguridad que se centran en el filtrado del tráfico, la identificación de comportamientos inusuales y la microsegmentación ha sido fundamental para mitigar eficazmente ataques tales como el inundación de ICMP, exploraciones de puertos UDP, suplantación de ARP y accesos no autorizados desde dentro, disminuyendo su efecto en la latencia, el rendimiento y la disponibilidad de los servicios.

Las situaciones de ataque interno pusieron de manifiesto que la confianza automática entre los nodos representa un peligro considerable en redes que no tienen segmentación. La implementación del modelo de confianza cero ha demostrado ser una táctica efectiva para limitar accesos no permitidos y reducir el movimiento lateral dentro de la red SDN. Por el cual, los hallazgos corroboran que la adopción de políticas de seguridad en el controlador SDN no afecta negativamente el rendimiento general de la red, siempre que las reglas de flujo se diseñen de manera adecuada, logrando un balance entre la seguridad y la eficiencia operativa.

Por último, el entorno experimental creado sirve como un modelo replicable y alineado con buenas prácticas y estándares de seguridad, como NIST SP 800-115, que puede funcionar como referencia en contextos académicos y como base para investigaciones futuras orientadas a situaciones reales y a la automatización de la detección de amenazas.

Agradecimientos

El presente trabajo de experimentación está dedicado, en primera instancia, al Mgs. Oscar Cárdenas Villavicencio y al Mgs. Rodrigo Morocho Roman, profesionales de amplia trayectoria y conocedores del área de seguridad de redes. Su guía técnica y rigurosidad académica han sido los pilares fundamentales para el desarrollo de este análisis y experimentación. Sus enseñanzas no solo han permitido alcanzar los objetivos planteados, sino que han fomentado un compromiso con la excelencia y la protección de las infraestructuras digitales.

A nuestros padres, quienes, con su apoyo incondicional, sacrificio y valores han sido el motor de este esfuerzo académico. Su confianza constante nos ha permitido superar los desafíos presentados a lo largo de la formación universitaria, convirtiéndose en la base moral sobre la cual se construye este logro profesional. También, este trabajo se dedica al estudio de las redes de datos, reconociendo su importancia crítica como el sistema circulatorio de la información en el mundo actual. El proceso de investigación representó un reto significativo al enfrentarnos a herramientas de vanguardia, tales como Mininet para la emulación de redes SDN y sFlow-RT para el análisis de telemetría. Aunque estas tecnologías eran completamente nuevas para nosotros, su dominio nos ha permitido comprender que la seguridad moderna exige una adaptación constante y una visión innovadora frente a las amenazas emergente.

Referencias

Jaigirdar, F. T., Jayatilaka, A., & Babar, M. A. (2026). Software vulnerability management in IoT systems: a systematic mapping study. *Cybersecurity*, *9*(1), 96. https://link.springer.com/content/pdf/10.1186/s42400-025-00543-6.pdf

Khan, N., Bin Salleh, R., Koubaa, A., Khan, Z., Khan, M. K., & Ali, I. (2023). Data plane failure and its recovery techniques in SDN: A systematic literature review. *Journal of King Saud University-Computer and Information Sciences*, *35*(3), 176-201. https://www.sciencedirect.com/science/article/pii/S1319157823000307

Liu, J., Li, Y., Wang, H., Jin, D., Su, L., Zeng, L., & Vasilakos, T. (2016). Leveraging software-defined networking for security policy enforcement. *Information Sciences*, *327*, 288-299. http://fi.ee.tsinghua.edu.cn/~wanghuandong/papers/infs16.pdf

Quirumbay Yagual, D. I., Castillo Yagual, C. A., & Coronel Suárez, I. A. (2022). Una revisión del aprendizaje profundo aplicado a la ciberseguridad. *Revista Científica y Tecnológica UPSE (RCTU)*, *9*(1), 57-65. http://scielo.senescyt.gob.ec/scielo.php?pid=S1390-76972022000200057&script=sci_arttext

Rodríguez Herlein, D. R., Talay, C. A., González, C. N., & Marrone, L. A. (2020). Explorando las redes definidas por software (SDN). XXII Workshop de Investigadores en Ciencias de la Computación (WICC 2020, El Calafate, Santa Cruz).

Sánchez-García, I. D., Rea-Guaman, A., Feliu, T. S., & Calvo-Manzano, J. A. (2024). Auditoría de riesgos de ciberseguridad: Revisión de Literatura, propuesta y aplicación. *RISTI-Revista Ibérica de Sistemas e Tecnologias de Informação*(53), 69-87. https://scielo.pt/scielo.php?pid=S1646-98952024000100069&script=sci_arttext&tlng=es

Shaji, N. S., & Muthalagu, R. (2024). Survey on security aspects of distributed software-defined networking controllers in an enterprise SD-WLAN. *Digital Communications and Networks*, *10*(6), 1716-1731. https://www.sciencedirect.com/science/article/pii/S2352864823001517

Velez Mejia, C. L. (2018). Análisis de Seguridad en Redes SDN (Redes definidas por software). https://repository.unad.edu.co/bitstream/handle/10596/27165/%20clvelezm.pdf?sequence=1