Diseño y Despliegue de una Infraestructura de Red WAN/LAN/WLAN con Seguridad a través de FortiGate en GNS3

Design and Deployment of a WAN/LAN/WLAN Network Infrastructure with Security using FortiGate in GNS-3

Jonathan Chillagana, Jimmy Simbaña, Kevin Suntaxi
Departamento de Ciencias de la Computación, Universidad de las Fuerzas Armadas ESPE, 170126 Sangolquí, Ecuador.
{jpchillagana2, jasimbana14, kgsuntaxi1}@espe.edu.ec

Resumen

La seguridad en redes informáticas es de vital importancia para conservar la integridad de los datos, disponibilidad de servicios, protección de la privacidad y sobre todo la protección contra amenazas cibernéticas, por tanto, la incorporación de mecanismos de seguridad es esencial y obligatorio. El presente estudio presenta el diseño, configuración y evaluación de un entorno que simula una topología segura de red LAN/WAN/WLAN con servicios DHCP y DNS. Para lograrlo, se configuró un Firewall que actúa como una barrera protectora entre las redes internas y externas, utilizando el simulador y emulador GNS-3, al considerar aspectos de calidad y rendimiento. Los resultados muestran que el Firewall incrementó la seguridad en las diferentes redes asociadas, gracias a las configuraciones adicionales implementadas para el filtrado de contenido, segmentación de red, monitoreo y controles de acceso.

Palabras Claves: *DHCP; DNS; Firewall; Seguridad de redes; WLAN, GNS-3.*

Abstract

The security of computer networks is a paramount concern in today's interconnected world, where data integrity, service availability, and privacy are constantly under threat. The primary objective of this work has been to design, implement, and evaluate a comprehensive network topology incorporating WLAN, LAN, and WAN technologies within the GNS-3 simulation environment. The focus is squarely on addressing specific network security challenges with the aim of bolstering protective measures and analyzing the impact of this configuration on overall network security. Additionally, a Firewall has been seamlessly integrated to act as a robust defensive barrier, safeguarding the network against external threats. By examining the impact of Firewall integration, this study demonstrates how it enhances security across WLAN, LAN, and WAN domains. The results underscore the pivotal role of a well-configured firewall in strengthening network defenses and ensuring the confidentiality, availability, and integrity of data.

Keywords: *DHCP; DNS; Firewall; Network security; WLAN; GNS-3.*

Fecha de Recepción: 30/08/2023 - Aceptado: 15/09/2023 - Publicado: 22/12/2023
ISSN: 2477-9253 – DOI: http://dx.doi.org/10.24133/RCSD.VOL08.N03.2023.05

I. Introducción

En el dinámico mundo de la ingeniería de redes de computadoras, la optimización y gestión eficiente de las conexiones, se ha convertido en un pilar fundamental para el funcionamiento fluido de las organizaciones modernas (Jonathan López, 2020). La topología de red, en particular, desempeña un papel esencial en la configuración y administración de los recursos de conectividad, tanto en entornos WAN, LAN como WLAN. En este contexto, la utilización de emuladores de redes se ha transformado en un enfoque invaluable para diseñar, probar y optimizar las infraestructuras de red de manera virtual, antes de su implementación en el mundo real (Del & Tda, 2020).

En este contexto, surge la problemática de cómo diseñar una topología de red WAN/LAN/WLAN eficiente y segura utilizando GNS-3 como emulador. Esto implica abordar desafíos como la correcta asignación de recursos de hardware y software, la configuración precisa de políticas de seguridad de la información y la optimización de la operatividad de la red en su conjunto. Además, se plantea la cuestión de cómo capacitar a los ingenieros de redes para que sean capaces de resolver problemas complejos y aplicar conceptos fundamentales de redes de computadoras en un entorno de ingeniería práctico (Carrasco, 2020).

La literatura existente subraya la importancia de la simulación y emulación de redes como un paso esencial en el diseño y la gestión de topologías de red. Investigaciones previas han destacado cómo las herramientas tipo GNS-3 permiten a los ingenieros de redes probar configuraciones, simular escenarios diversos y prever posibles fallas antes de la implementación real. Además, se han abordado temas relacionados con la seguridad de la información en redes, subrayando la necesidad de establecer políticas sólidas que protejan los activos digitales de las organizaciones en un entorno cada vez más interconectado.

Algunos trabajos relacionados son los siguientes: En el estudio propuesto por López, J. (2020), se presenta un proyecto de emulación de SD-WAN Híbrida utilizando tecnología FORTINET en GNS-3, que proporcionó a los estudiantes una valiosa experiencia práctica y conocimientos en áreas clave de redes y telecomunicaciones, desde la virtualización de servidores hasta la seguridad de las redes definidas por software. Sus autores destacan la relevancia de la SD-WAN en el entorno actual de transformación digital. Según Tamayo Domínguez, M. F. (2013), explica que los resultados proporcionan una visión general de cómo se planificaron y llevaron a cabo las prácticas de emulación de redes con GNS-3, así como los beneficios que los estudiantes obtuvieron de esta experiencia. Además, GNS-3 funciona en conjunto con otros programas, mencionando específicamente Dynamips y QEMU como servidores de emulación de enrutadores y firewalls Pix. En este mismo contexto, en el estudio realizado por Carrasco, F. (2020) se diseñó y configuró una red de acceso utilizando el software GNS-3 y equipos Fortigate. Esta red se desarrolló teniendo en cuenta las necesidades y requerimientos específicos de una empresa como CONSTELEC en Ecuador. Los resultados demuestran la viabilidad y los beneficios de la tecnología SD-WAN en la configuración de redes de acceso para empresas como CONSTELEC en Ecuador, así como la capacidad de utilizar el software GNS-3 como herramienta de emulación y evaluación de rendimiento en proyectos de este tipo.

El propósito de este artículo es explorar en profundidad la metodología para diseñar una topología de red WAN/LAN/WLAN utilizando GNS-3 como emulador de redes. Se busca proporcionar a los lectores una guía práctica que les permita comprender los aspectos clave de la configuración de redes virtuales, la asignación eficiente de recursos, la implementación de políticas de seguridad y la resolución de problemas en un entorno simulado. Además, se pretende resaltar la importancia de adquirir habilidades prácticas en ingeniería de redes que sean directamente aplicables en entornos profesionales, donde la capacidad de gestionar y optimizar las redes es crucial para garantizar la continuidad de las operaciones y la integridad de los datos.

La contribución principal de este estudio radica en proporcionar a los profesionales de la ingeniería de redes y a los estudiantes una guía detallada y práctica sobre cómo diseñar una topología de red WAN/LAN/WLAN eficiente y segura utilizando GNS-3 como emulador. Se abordan desafíos críticos, desde la asignación precisa de recursos de hardware y software hasta la configuración de políticas de seguridad de la información. Además, este artículo destaca la relevancia de capacitar a los ingenieros de redes para resolver problemas complejos y aplicar conceptos esenciales de redes de computadoras en un entorno de ingeniería práctica.

El resto del artículo está organizado en tres secciones principales: materiales y métodos, conclusiones y futuras direcciones de investigación. Cada sección cumple un papel fundamental en la presentación lógica y coherente del estudio, desde la contextualización inicial hasta las perspectivas futuras.

II. Materiales y Métodos

Esta sección se centra en el núcleo del método empleado para abordar el desafío de diseñar una topología de red WAN/LAN/WLAN con integración de redes inalámbricas y servicios cruciales como DHCP y DNS, además de un Firewall como salvaguarda entre las redes internas y externas. El objetivo primordial es suministrar un relato exhaustivo de la metodología de diseño, tanto en el plano experimental como no experimental. Esta descripción minuciosa es esencial, ya que la base del método científico radica en la capacidad de reproducir resultados; así, se proveen los detalles necesarios para que otros investigadores repliquen los experimentos con precisión. En los siguientes párrafos de este artículo se explorarán cada una de estas etapas de manera exhaustiva, proporcionando ejemplos específicos y consideraciones clave en el contexto del diseño de una topología de red WAN/LAN/WLAN con servicios DHCP, DNS y un Firewall, utilizando GNS-3 y otros recursos esenciales.

2.1. Materiales

En el proceso de diseñar una topología de red WAN/LAN/WLAN con servicios esenciales de redes como DHCP, DNS y un Firewall como dispositivo de seguridad de la información, se requerirán una serie de herramientas de software clave para llevar a cabo una simulación efectiva. Entre los principales se incluyen:

GNS-3 (Graphical Network Simulator-3): Este software de simulación y emulación de redes sigue siendo el pilar fundamental de la infraestructura virtual. GNS-3 permite la creación de topologías complejas y la interconexión de dispositivos virtuales para replicar un entorno de red real.

VMware Workstation: Además de GNS-3, VMware Workstation se utilizará para crear máquinas virtuales que emulan dispositivos específicos en la red, especialmente relevantes para simular sistemas operativos y servicios como DHCP y DNS.

Switches Cisco 7200 Series (c7200): Las imágenes de estos switches permiten emular dispositivos con arquitecturas específicas en GNS-3. Tiene seis ranuras para adaptadores de puerto (PA). El chasis VXR, NPE-400 y C7200-IO-FE son los ajustes predeterminados en GNS-3.

Switches IOU (IOS on UNIX): Son dispositivos virtuales que permiten emular switches de capa 2 en una red. Estos switches utilizan imágenes de sistemas operativos Cisco (IOS) para proporcionar funcionalidades de switching en un entorno de laboratorio virtual. Con switches IOU, se puede diseñar, configurar y probar topologías de red complejas que incluyan dispositivos de capa de enlace de datos del modelo OSI/ISO, como switches, en el entorno de simulación de GNS-3.

Instancia Cloud: Herramienta propia de GNS-3 que proporciona una interfaz virtualizada para la conexión de la topología de red simulada con recursos externos, como la infraestructura de la nube o servicios en línea. Esta instancia posibilitará la simulación de la interacción entre la red local y entornos remotos, ofreciendo la capacidad de evaluar y optimizar configuraciones de red.

Imágenes de Firewall: Se requerirán imágenes virtuales del IOS de los firewalls para simular la barrera de seguridad entre las redes internas y externas. Esto permitirá implementar políticas de seguridad y evaluar el tráfico que fluye a través del firewall.

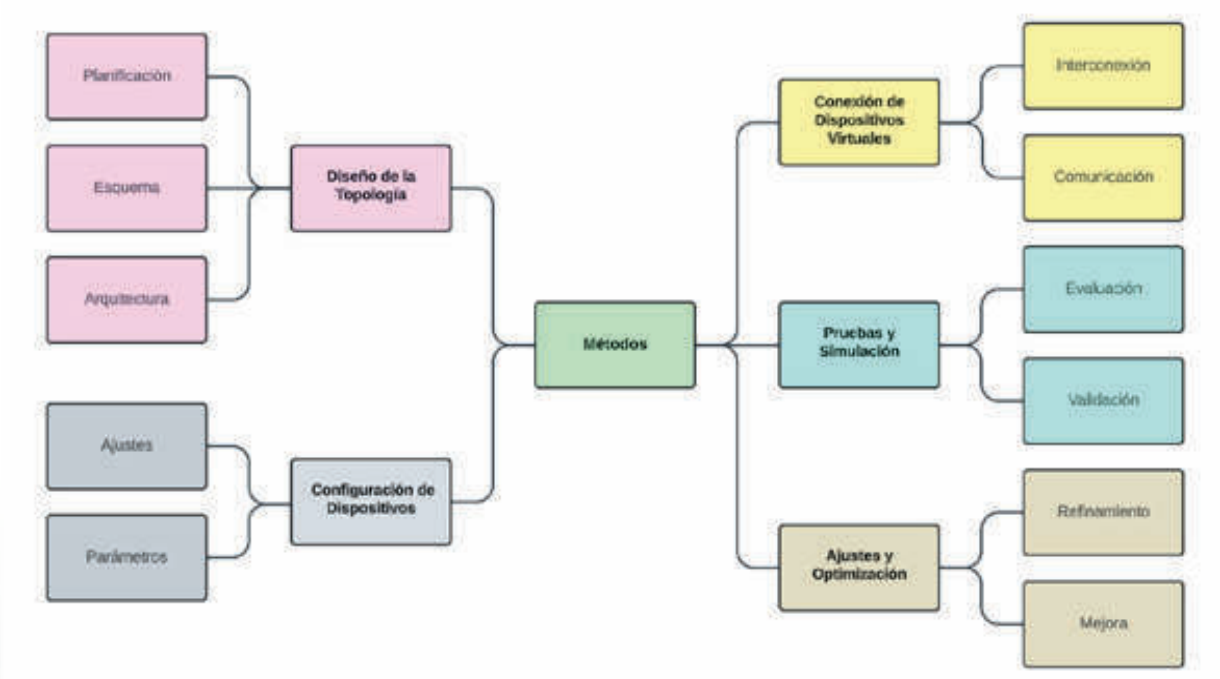
Wireshark: Una herramienta de análisis de tráfico de red que permite inspeccionar paquetes y entender el comportamiento de la red en tiempo real.

Nmap: Una utilidad de código abierto para la exploración de redes y auditoría de seguridad. Nmap descubre dispositivos en una red y determina los servicios que están ejecutándose en ellos.

2.2. Métodos

Esta metodología combina el uso de GNS-3 para la simulación de redes y VMware para la creación de máquinas virtuales, lo que permite a los ingenieros de redes diseñar, configurar, probar y optimizar topologías de red de manera controlada y segura, preparándose para abordar desafíos en entornos de red del mundo real. La Figura 1 muestra el procedimiento utilizado para la experimentación de una red en GNS-3. A continuación, se describen brevemente los pasos respectivos:

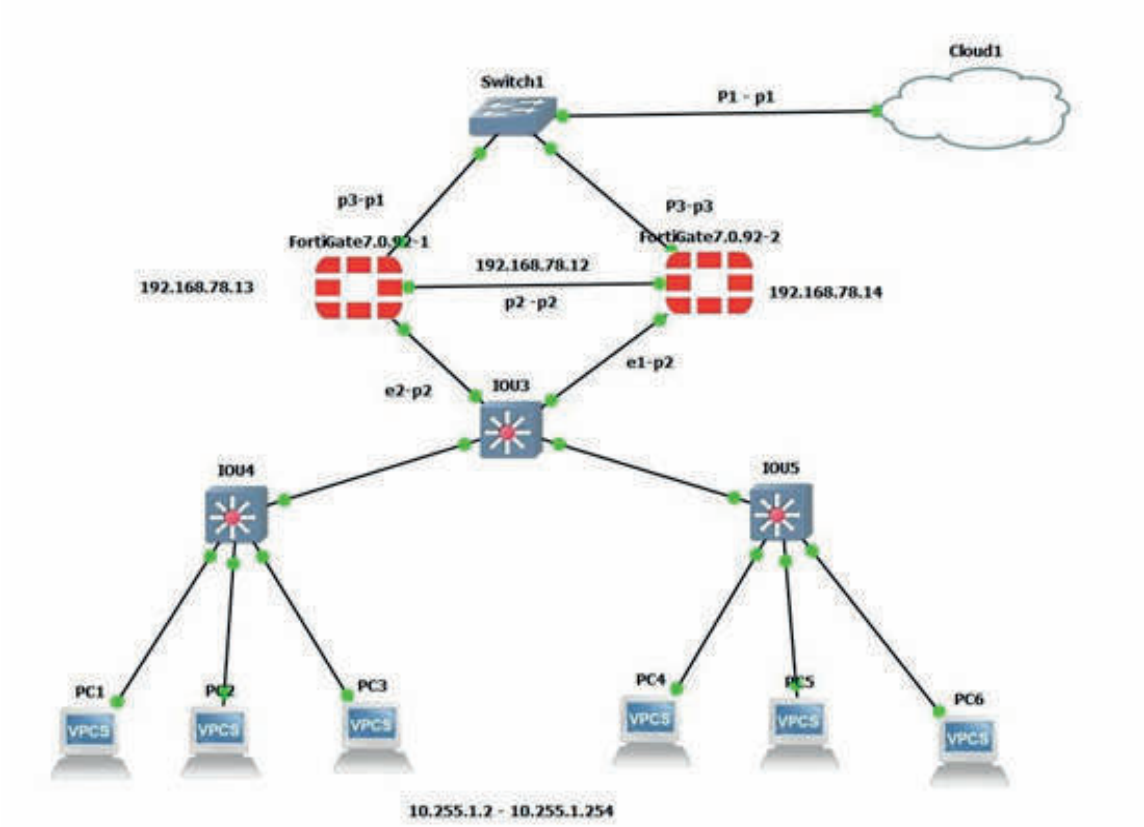
Figura 1: *Procedimiento para la experimentación de una red en GNS-3*



Paso 1: Diseño de la Topología

En esta fase, se diseña la topología de red WAN/LAN/WLAN, incluyendo la ubicación de dispositivos como routers, switches, puntos de acceso inalámbrico y firewalls. Se decide cómo se conectarán estos dispositivos y qué roles desempeñan en la red. La Figura 2 ilustra la topología experimental la cual consta de tres switch-routers, dos firewall FortiGate y varios usuarios finales. Además se debe crear un enlace entre el mundo virtual de GNS-3 y el mundo real del PC. El elemento que hizo de puente es el objeto Cloud de GNS-3, que se conectará mediante un switch Ethernet virtual a la WAN.

Figura 2: *Topología experimental implementada en GNS-3*



Paso 2: Configuración de Dispositivos

Se procede a cargar las imágenes de sistemas operativos y dispositivos virtuales en GNS-3. Luego, se configuran los dispositivos para reflejar su funcionalidad en la red real. Esto implicó asignar direcciones IP, configurar enrutamiento, habilitar servicios DHCP y DNS, y definir políticas de seguridad en el firewall.

Paso 3: Conexión de Dispositivos Virtuales

Los dispositivos virtuales se interconectan en GNS-3 mediante enlaces virtuales, emulando la conectividad física en una red real. Esto permite simular el flujo de datos y tráfico a través de los diferentes dispositivos y segmentos de red.

Paso 4: Pruebas, simulación y emulación

Se llevaron a cabo pruebas exhaustivas y simulaciones para evaluar el comportamiento de la topología de red. Esto incluyó pruebas de conectividad, pruebas de rendimiento inalámbrico, evaluación de la asignación de direcciones DHCP y el funcionamiento del sistema DNS, así como pruebas de tráfico a través del firewall.

Paso 5: Ajustes y Optimización

Basándose en los resultados de las pruebas, se realizan ajustes en la configuración de los dispositivos y servicios para mejorar el rendimiento y la seguridad de la red. Esto podría implicar ajustes en la asignación de ancho de banda, configuración de reglas de firewall y optimización de servicios como DHCP y DNS.

III. Evaluación de Resultados y Discusión

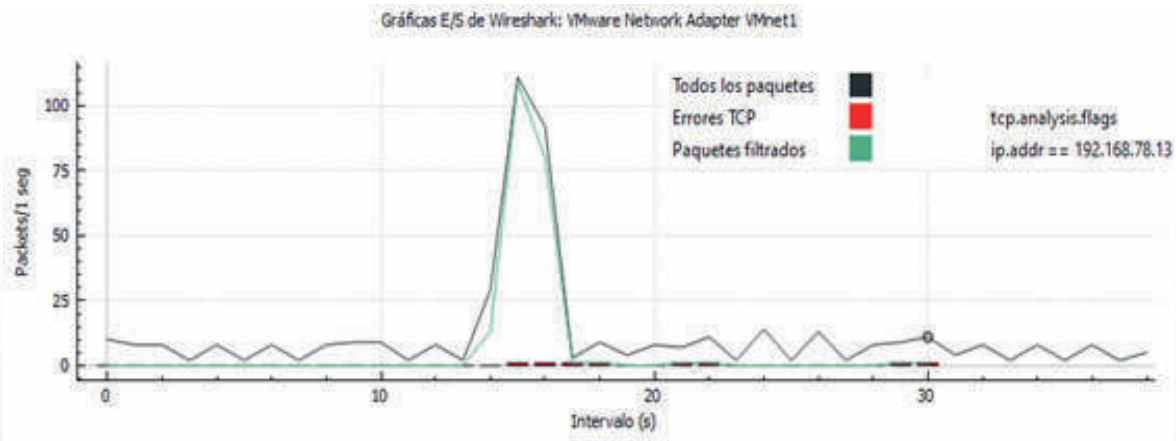
3.1. Evaluación de resultados

En una primera observación se incluye el análisis de tráfico generado, el tiempo de respuesta de los dispositivos de conectividad, la eficacia de los servicios DHCP y DNS, y otros aspectos relacionados con el rendimiento y la interacción de la red virtualizada. Estos datos proporcionan información valiosa sobre el diseño, implementación y configuración de la topología de experimentación, así como también sobre la eficacia de la solución de ciberseguridad implementada.

Durante la fase de evaluación de la topología de red en GNS-3, se realizó un estudio detallado del tráfico mediante la combinación de las herramientas Wireshark y Nmap. Wireshark fue empleada para la captura y análisis exhaustivo de cada paquete de datos intercambiado entre los nodos de la red simulada, proporcionando una visión de las interacciones y patrones de tráfico.

Adicionalmente, se utilizó Nmap para realizar exploraciones a puertos específicos, enviando una cantidad definida de paquetes a través de la red simulada. Los resultados de estas exploraciones fueron capturados por Wireshark, permitiendo así una evaluación de la respuesta de la red ante ciertos estímulos y la identificación de posibles áreas de mejora en términos de rendimiento y seguridad.

Figura 3: *Análisis del tráfico de red*



La Figura 3 muestra el comportamiento del tráfico que pasa por el firewall durante el período de observación. Este tráfico filtrado es menor que el tráfico total, sin embargo, varía más a lo largo del tiempo. El tráfico de error TCP es relativamente bajo.

Por otro lado, en relación a la evaluación del rendimiento y la seguridad de la red simulada, la Tabla 1 resume diversas comprobaciones clave relacionadas con el funcionamiento de la topología. Estos datos permiten una evaluación del comportamiento de la red y son esenciales para la optimización y ajustes cara a mejorar el rendimiento y nivel de seguridad antes de ponerla en producción.

Tabla 2: *Métricas de rendimiento de la LAN/WAN/WLAN*

Categoría	Estadísticas	Valor Actual	Valor Promedio	Valor Máximo	Valor Mínimo
Rendimiento WAN	Ancho de banda	1000	950	1050	900
	Uso del ancho de banda	65%	70%	75%	60%
	Latencia promedio	20	18	25	15
	Pérdida de paquetes (%)	0.2%	0.1%	0.5%	0.1%
Tráfico LAN	Uso del ancho de banda	40%	45%	50%	35%
	Número de dispositivos conectados	15	12	20	10
	Uso de CPU en Fortigate (%)	35%	30%	40%	25%
	Uso de memoria en Fortigate (%)	70%	65%	75%	60%
Tráfico WLAN	Uso del ancho de banda (%)	25%	30%	35%	20%
	Número de dispositivos inalámbricos	20	18	25	15
Seguridad	Número de intentos de intrusos	10	8	15	5

3.2. Discusión

A través de este proyecto en GNS-3, se ha logrado construir un laboratorio completo sobre interconexión de Redes LAN/WAN/WLAN, sin costos de inversión de hardware, software experimentación e investigación. Los estudiantes se han empoderado de importantes conocimientos de la configuración de direccionamiento IP, servicios de redes y políticas de seguridad. Además, han requerido instalar diversos tipos de programas para analizar tráfico, escaneo de puertos, instalación de imágenes de los sistemas operativos de los dispositivos de conectividad, lo cual sin duda incrementa su formación especialmente, tuvieron la oportunidad de llevar a cabo sus prácticas y pruebas inclusive de manera remota.

En un segundo análisis, se evaluaron las políticas de acceso a Internet implementadas. Se establecieron dentro del entorno de simulación de GNS-3 configuraciones y políticas de seguridad, direccionamiento IP, enrutamiento, segmentación de redes y otros aspectos clave de la administración y seguridad de redes. Por tanto, se cumplió el propósito principal de este estudio, el cual consistió en comprobar los niveles de seguridad de la información utilizando una red virtual simulada y emulada, cual si fuera real. Otro beneficio implícito, fue la comprensión del funcionamiento de diversos dispositivos de red, tales como routers, switches, firewall entre otros. Finalmente, los estudiantes ahora disponen de la capacidad de realizar análisis de tráfico, y detectar tráfico malicioso configurando políticas de seguridad tanto en un firewall Fortigate de GNS-3 como en entornos de red reales.

IV. Conclusiones y trabajo futuro

En este estudio se diseñó la topología experimental LAN/WAN/WLAN en la que se destaca la importancia de la configuración de políticas de seguridad en un firewall FortiGate en GNS-3. Esta configuración actuó como una barrera efectiva contra amenazas tanto internas como externas que podrían afectar a la red. La topología se construyó sin costos de inversión de hardware, software experimentación e investigación. Los estudiantes instalaron y configuraron diversos tipos de software para analizar tráfico, escaneo de puertos, instalación de imágenes de los sistemas operativos de los dispositivos de conectividad. Además evaluaron las políticas de seguridad, enrutamiento, segmentación de redes y otros aspectos clave de la administración y seguridad de redes. Los estudiantes ahora disponen de la capacidad de realizar análisis de tráfico, y detectar tráfico malicioso configurando políticas de seguridad tanto en un firewall FortiGate de GNS-3 como en entornos de red reales.

Como trabajo futuro se planea la continuación de investigaciones que profundicen aún más en la optimización de políticas de seguridad y en la adaptación de FortiGate en topologías de red más complejas.

Referencias

Aguilar Ruiz, L. E. (2020). Propuesta de diseño de una red privada de telecomunicaciones para accesos a aplicaciones de una entidad bancaria a través de internet. Universidad Tecnológica del Perú. https://renati.sunedu.gob.pe/handle/sunedu/3034284

Balsa, C. (2016). *Emulación de Redes Cisco con GNS-3.* 166. http://www.adminso.es/recursos/Proyectos/PFM/2013_14/PFM_Aprende_GNS/Proyecto_Aprende_a_emular_redes_cisco_con_GNS-3.pdf

Calvache, E & Tamayo, M. (2013). *Estudio, Diseño y Simulación en GNS3 de guías de laboratorio para Redes de Datos II y Networking de la Facultad de Electrónica de la Universidad Israel,* 66(1997), 168. https://repositorio.uisrael.edu.ec/handle/47000/326

Carrasco, F. (2020). *Diseño y Simulación de una Red de Accesos en GNS-3 utilizando la tecnología SD-WAN para medianas empresas en el Ecuador*. 77.

Fuertes, W. (2022). *Redes de computadoras un enfoque práctico.* ISBN: 978-9942-765-72-7. http://repositorio.espe.edu.ec/handle/21000/30282

Fuertes, W. & Macas, M. (2023). *Ciberseguridad: del cibercrimen a los ataques ciber-físicos*. ISBN: 978-9942-765-88-8, https://repositorio.espe.edu.ec/handle/21000/36481

Gobantes Martínez, F. (2023). Laboratorio Docente Virtual basado en el simulador GNS3 para la Gestión y Operación de Redes mediante el protocolo SNMP.

López Arévalo, J. J. (2020). Emulación de una red SD-WAN (Software-Defined Wide Area Network) utilizando tecnología Fortinet y el software GNS3 (Bachelor's thesis, Quito, 2020.).

Pérez Rosero, F. M. (2020). Detección y Evaluación de Vulnerabilidades en la Web con la Técnica Banner Grabbing en la Cooperativa de Ahorro y Crédito "Riobamba" Ltda (Bachelor's thesis, Universidad Nacional de Chimborazo, 2019).

Tamayo Domínguez, M. F. (2013). Estudio, diseño y simulación en gns3 de guías de laboratorio para redes de datos ii y networking de la facultad de electrónica de la Universidad Israel. Quito (Bachelor's thesis, Quito: Universidad Israel, 2013).

Tapia J., Reyes J. (2022). *Diseño de una red empresarial de telecomunicaciones para mantener la operación y comunicación de las tecnologías de voz y datos en la empresa TABACARCEN*. Repositorio de la Universidad Nacional del Chimborazo.

Tortosa, M. T., Álvarez, J. D., & Pellín, N. (2015). *Virtualización de Redes de Computadores con GNS-3: Evaluación de soluciones para el aprendizaje a distancia.*