Ciencia y Educación
(L-ISSN: 2790-8402 E-ISSN: 2707-3378)
Vol. 7 No. 4.1
Edición Especial IV 2026

EVALUACIÓN DEL USO DE FIREWALLS DE NUEVA GENERACIÓN (NGFW) EN ENTORNOS EDUCATIVOS MEDIANTE SIMULACIÓN Y ANÁLISIS
EVALUATION OF THE USE OF NEXT-GENERATION FIREWALLS (NGFW) IN EDUCATIONAL ENVIRONMENTS THROUGH SIMULATION AND ANÁLISIS

Autores: [1]Jorge Eduardo Pinargote Quijije y [2]Wilmer Antonio Moreira Sánchez.
[1]ORCID ID: https://orcid.org/0009-0003-6861-6215
[2]ORCID ID: https://orcid.org/0000-0001-7772-6254
[1]E-mail de contacto: Jpinargote4909@utm.edu.ec
[2]E-mail de contacto: wilmer.moreira@utm.edu.ec
Afiliación: [1*2*]Universidad Técnica de Manabí, (Ecuador).
Artículo recibido: 19 de Abril del 2026
Artículo revisado: 21 de Abril del 2026
Artículo aprobado: 23 de Abril del 2026
[1]Estudiante de la Universidad Técnica de Manabí, (Ecuador).
[2]Ingeniero en Sistemas Informáticos, egresado de la Universidad Técnica de Manabí, (Ecuador). Magíster en Tecnologías de la Información mención en Seguridad de Redes y Comunicaciones, egresado de la Universidad Técnica de Manabí, (Ecuador). Actualmente, Docente de la Universidad Técnica de Manabí, (Ecuador).

Resumen

La creciente digitalización de los procesos académicos y administrativos en las instituciones educativas ha incrementado la exposición a amenazas cibernéticas, lo que justifica la necesidad de implementar mecanismos de seguridad avanzados que garanticen la protección de la información y la continuidad de los servicios. En este contexto, el presente estudio tuvo como objetivo evaluar la efectividad de un firewall de nueva generación (NGFW) en un entorno educativo virtualizado, analizando su impacto en la seguridad de la red, el rendimiento del sistema y el consumo de recursos. La metodología aplicada fue de tipo experimental con enfoque cuantitativo, basada en la simulación de tráfico mixto que integró tanto tráfico legítimo como ataques controlados. Se compararon métricas antes y después de la implementación del NGFW, considerando variables como tiempo de respuesta, latencia, pérdida de paquetes, uso de CPU, memoria, almacenamiento y tráfico de red. Los resultados evidenciaron altos niveles de detección y bloqueo de amenazas, sin afectar el tráfico legítimo. Asimismo, se observó un impacto mínimo en el rendimiento de la red, manteniéndose valores de latencia y respuesta dentro de rangos aceptables. El consumo de recursos del sistema se mantuvo estable, lo que confirma la eficiencia operativa del firewall en un entorno virtualizado. Se concluye que la implementación de un NGFW basado en software de código abierto constituye una solución viable, eficiente y adaptable para fortalecer la seguridad en instituciones educativas, permitiendo mejorar la protección de la red sin comprometer el rendimiento ni la disponibilidad de los servicios digitales.

Palabras clave: Firewall de nueva generación, Ciberseguridad, Redes educativas, Virtualización, Seguridad informática, NGFW.

Abstract

The increasing digitization of academic and administrative processes in educational institutions has increased exposure to cyber threats, justifying the need to implement advanced security mechanisms that guarantee information protection and service continuity. In this context, this study aimed to evaluate the effectiveness of a next-generation firewall (NGFW) in a virtualized educational environment, analyzing its impact on network security, system performance, and resource consumption. The methodology employed was experimental with a quantitative approach, based on the simulation of mixed traffic that integrated both legitimate traffic and controlled attacks. Metrics were compared before and after the NGFW implementation, considering variables such as response time, latency, packet loss, CPU usage, memory, storage, and network traffic. The results showed high levels of threat detection and blocking without affecting legitimate traffic.

Furthermore, a minimal impact on network performance was observed, with latency and response times remaining within acceptable ranges. System resource consumption remained stable, confirming the firewall's operational efficiency in a virtualized environment. It is concluded that implementing an open-source software-based NGFW is a viable, efficient, and adaptable solution for strengthening security in educational institutions, improving network protection without compromising the performance or availability of digital services.
Keywords: Next-generation firewall, Cybersecurity, Educational networks, Virtualization, Information security, NGFW.

Sumário

A crescente digitalização dos processos acadêmicos e administrativos em instituições de ensino aumentou a exposição a ameaças cibernéticas, justificando a necessidade de implementar mecanismos de segurança avançados que garantam a proteção da informação e a continuidade dos serviços. Nesse contexto, este estudo teve como objetivo avaliar a eficácia de um firewall de próxima geração (NGFW) em um ambiente educacional virtualizado, analisando seu impacto na segurança da rede, no desempenho do sistema e no consumo de recursos. A metodologia empregada foi experimental, com abordagem quantitativa, baseada na simulação de tráfego misto que integrava tanto tráfego legítimo quanto ataques controlados. As métricas foram comparadas antes e depois da implementação do NGFW, considerando variáveis como tempo de resposta, latência, perda de pacotes, uso da CPU, memória, armazenamento e tráfego de rede. Os resultados mostraram altos níveis de detecção e bloqueio de ameaças sem afetar o tráfego legítimo. Além disso, observou-se um impacto mínimo no desempenho da rede, com latência e tempos de resposta permanecendo dentro de faixas aceitáveis. O consumo de recursos do sistema permaneceu estável, confirmando a eficiência operacional do firewall em um ambiente virtualizado. Conclui-se que a implementação de um NGFW baseado em software de código aberto é uma solução viável, eficiente e adaptável para reforçar a segurança em instituições de ensino, melhorando a proteção da rede sem comprometer o desempenho ou a disponibilidade dos serviços digitais.
Palavras-chave: Firewall de próxima geração, Cibersegurança, Redes educacionais, Virtualização, Segurança da informação, NGFW.

Introducción

La seguridad de la información constituye un conjunto de prácticas, tecnologías y políticas orientadas a garantizar la confidencialidad, integridad y disponibilidad de los datos en entornos digitales. Dentro de estos mecanismos, los firewalls representan dispositivos de control perimetral que permiten gestionar el tráfico de red y prevenir accesos no autorizados (Neupane et al., 2018). En los últimos años, han evolucionado hacia los denominados firewalls de nueva generación (NGFW), que integran inspección profunda de paquetes, control de aplicaciones, sistemas de detección y prevención de intrusiones y análisis contextual del tráfico (Islam et al., 2023). A nivel global, la transformación digital ha incrementado la interconectividad y la dependencia de infraestructuras tecnológicas, generando un aumento significativo de ciber amenazas cada vez más sofisticadas, como ataques dirigidos, ransomware y explotación de vulnerabilidades en aplicaciones web (Bellamkonda, 2024; Heredia et al., 2025).

En América Latina, el crecimiento sostenido de incidentes de seguridad informática ha evidenciado la vulnerabilidad de sectores con alta exposición de datos, entre ellos el educativo, donde se gestionan grandes volúmenes de información sensible (Heino et al., 2022). En el ámbito institucional, las redes educativas presentan características particulares como alta

densidad de usuarios, dispositivos heterogéneos y acceso abierto a servicios digitales, lo que incrementa la superficie de ataque y la probabilidad de intrusiones (Maheswari et al., 2024). Muchas instituciones continúan utilizando firewalls tradicionales con capacidades limitadas de inspección y control, lo que dificulta la detección de amenazas avanzadas y el monitoreo del tráfico cifrado. En el contexto local, la falta de evaluación técnica de soluciones de seguridad, así como las limitaciones presupuestarias, han impedido la adopción de tecnologías NGFW en diversas instituciones educativas. Esta situación genera la necesidad de analizar el desempeño de estas herramientas mediante entornos controlados de simulación, con el propósito de determinar su efectividad, impacto en el rendimiento de la red y viabilidad operativa.

El entorno educativo contemporáneo se caracteriza por la incorporación de plataformas virtuales de aprendizaje, sistemas de gestión académica, repositorios digitales y servicios en la nube. Estas infraestructuras requieren conectividad permanente y generan flujos constantes de tráfico de red que deben ser gestionados de forma segura. En instituciones de educación superior, el acceso simultáneo de estudiantes, docentes y personal administrativo a recursos internos y externos incrementa la complejidad de la gestión de la red. A pesar de ello, muchas infraestructuras aún dependen de esquemas tradicionales de seguridad perimetral que no permiten identificar aplicaciones, usuarios o comportamientos anómalos dentro del tráfico (Lamdakkar et al., 2024). Además, la ausencia de entornos de laboratorio para la simulación de ataques limita la capacidad de evaluar el desempeño de los sistemas de seguridad antes de su implementación real. Esto dificulta la toma de decisiones informadas y aumenta el riesgo de interrupciones en los servicios institucionales y exposición de datos sensibles. La evaluación del uso de firewalls de nueva generación en entornos educativos resulta relevante desde una perspectiva tecnológica, académica y social.

En el ámbito tecnológico, los NGFW permiten integrar múltiples funciones de seguridad en una sola plataforma, mejorando la visibilidad del tráfico, el control de aplicaciones y la capacidad de respuesta ante amenazas avanzadas (Patel et al., 2024; Bellamkonda, 2020). Desde el punto de vista académico, el análisis mediante entornos de simulación aporta evidencia empírica sobre el comportamiento de estas tecnologías, permitiendo medir indicadores como eficiencia de detección, consumo de recursos y rendimiento de la red. Este tipo de estudios contribuye al desarrollo de investigaciones aplicadas en el campo de la ciberseguridad educativa. En el plano social, la protección de la información institucional garantiza la privacidad de estudiantes, docentes y personal administrativo, fortaleciendo la confianza en los sistemas digitales utilizados para la gestión del conocimiento.

Adicionalmente, la posibilidad de implementar NGFW mediante herramientas de código abierto representa una alternativa económicamente viable para instituciones con recursos limitados, permitiendo acceder a tecnologías de seguridad avanzadas sin incurrir en altos costos de licencias (Bellamkonda, 2024). Por tanto, el estudio se justifica en la necesidad de fortalecer la seguridad de las redes educativas mediante soluciones tecnológicas eficientes, evaluadas de forma rigurosa y adaptadas a las condiciones reales del entorno institucional. La evolución de la seguridad de redes ha estado determinada por el incremento de amenazas informáticas y la

creciente complejidad de los entornos digitales. Los firewalls tradicionales operan principalmente en las capas de red y transporte del modelo OSI, basando su funcionamiento en reglas estáticas de filtrado por direcciones IP, puertos y protocolos (Neupane et al., 2018). Este enfoque ha demostrado ser limitado frente a amenazas modernas que emplean técnicas de evasión, tráfico cifrado y explotación de vulnerabilidades en aplicaciones web (Islam et al., 2023).

Ante estas limitaciones, los firewalls de nueva generación (NGFW) se consolidan como una solución integral que combina inspección profunda de paquetes (DPI), control de aplicaciones, análisis de comportamiento y sistemas de detección y prevención de intrusiones (IDS/IPS) en una arquitectura unificada (Smit y Paneri, 2025). Estas capacidades permiten analizar el tráfico en capas superiores del modelo OSI, identificar aplicaciones independientemente del puerto utilizado y detectar patrones de ataque en tiempo real, lo que mejora significativamente la visibilidad de la red.

Diversos estudios evidencian que los NGFW incrementan la eficacia en la detección de amenazas y reducen la incidencia de falsos positivos mediante el uso de técnicas de inteligencia artificial y aprendizaje automático (Mohile, 2023). Estas tecnologías permiten analizar grandes volúmenes de tráfico, identificar comportamientos anómalos y aplicar políticas de seguridad basadas en el contexto del usuario, el tipo de aplicación y el comportamiento del sistema. En el ámbito educativo, los entornos de simulación y virtualización se han convertido en herramientas fundamentales para evaluar el desempeño de soluciones de ciberseguridad sin comprometer la infraestructura institucional. Estas plataformas permiten recrear escenarios de ataque, analizar el comportamiento del tráfico y medir indicadores clave como latencia, consumo de recursos y eficiencia en la detección de amenazas (Lamdakkar et al., 2024).

Materiales y Métodos

La investigación se desarrolló bajo un enfoque experimental y descriptivo, orientado a evaluar el desempeño de un firewall de nueva generación (NGFW) en un entorno educativo simulado. El estudio se basó en la recreación de una infraestructura de red académica mediante virtualización, lo que permitió analizar de manera controlada el comportamiento del sistema ante tráfico legítimo y malicioso sin comprometer la red institucional real. El diseño metodológico contempló la configuración de un laboratorio virtual, la implementación de políticas de seguridad adaptadas al contexto educativo y la ejecución de escenarios de ataque simulados. Para el análisis de resultados se emplearon métricas de desempeño tales como tasa de detección de amenazas, porcentaje de bloqueo, latencia, consumo de recursos y eficiencia global del sistema. Los datos obtenidos fueron procesados mediante estadística descriptiva, utilizando medidas de frecuencia, porcentajes y comparaciones de rendimiento antes y después de la implementación del NGFW.

Para el desarrollo de la investigación se dispuso de un conjunto de recursos tecnológicos orientados a la simulación controlada de un entorno educativo y a la evaluación del desempeño de un firewall de nueva generación (NGFW). Estos materiales permitieron reproducir la arquitectura de una red académica real, incluyendo dispositivos de usuario, servidores y segmentos de red, así como generar

tráfico legítimo y malicioso para analizar la capacidad de detección, respuesta y rendimiento del sistema de seguridad implementado. La selección de herramientas se basó en su compatibilidad con entornos virtualizados, su disponibilidad en versiones de código abierto y su pertinencia para el análisis de ciberseguridad en contextos educativos.

Tabla 1. *Recursos tecnológicos utilizados en el estudio*

Categoría	Recurso / Herramienta	Especificaciones técnicas	Función dentro del estudio
Infraestructura de hardware	Equipos de cómputo	Procesador multinúcleo (Intel i5 o superior), 8–16 GB RAM, almacenamiento SSD ≥ 256 GB	Soporte para la ejecución del entorno virtualizado y simulación de red
Conectividad	Red local (LAN)	Conectividad Ethernet 1 Gbps	Interconexión de máquinas virtuales y simulación del tráfico de red
Plataforma de virtualización	VirtualBox / VMware	Hipervisor tipo 2 con soporte para múltiples máquinas virtuales	Creación del laboratorio virtual y segmentación de la red educativa
Firewall NGFW	pfSense / OPNsense	Sistema basado en FreeBSD con DPI, filtrado de aplicaciones, control por políticas y soporte SSL/TLS	Control del tráfico, protección perimetral y gestión de políticas de seguridad
Sistema IDS/IPS	Suricata / Snort	Motor de detección basado en firmas y análisis de comportamiento en tiempo real	Identificación y bloqueo de intrusiones y tráfico malicioso
Monitoreo de red	Wireshark, ntopng, Zabbix	Captura de paquetes, análisis de flujo y monitoreo de rendimiento	Evaluación del comportamiento del tráfico, latencia y consumo de recursos
Simulación de ataques	Kali Linux, Metasploit, hping3, LOIC	Herramientas de pruebas de penetración y generación de tráfico malicioso	Simulación de ataques controlados (DoS, intrusión, malware, accesos no autorizados)
Análisis de datos	Microsoft Excel / software estadístico	Herramientas de procesamiento de datos y generación de gráficos	Organización, análisis e interpretación de resultados experimentales

Fuente: Elaboración propia

La configuración del entorno experimental se realizó mediante la creación de un laboratorio virtual que reproduce la arquitectura de una red educativa institucional. Este entorno fue diseñado considerando la segmentación típica de una infraestructura académica, incluyendo áreas de usuarios (estudiantes y docentes), servicios académicos, administración y una zona de control de seguridad perimetral. El firewall de nueva generación (NGFW) se ubicó como punto central de control del tráfico, permitiendo la inspección, filtrado y gestión de las comunicaciones entre los distintos segmentos de la red.

El NGFW fue configurado con políticas de seguridad adaptadas al contexto educativo, incluyendo reglas de control de acceso por roles de usuario, filtrado de contenido web, bloqueo de aplicaciones no autorizadas y supervisión del tráfico cifrado mediante certificados SSL/TLS. Asimismo, se integró un sistema de detección y prevención de intrusiones (IDS/IPS), encargado de analizar en tiempo real los paquetes de datos, identificar patrones de ataque y bloquear actividades maliciosas. La configuración del entorno incluyó la definición de subredes virtuales, asignación de direcciones IP, establecimiento de rutas de comunicación y activación de mecanismos de registro de eventos (logs), lo que permitió realizar un seguimiento detallado del comportamiento del tráfico y del rendimiento del sistema de seguridad durante las pruebas.

El proceso experimental se diseñó con un enfoque metodológico cuantitativo–aplicado, orientado a evaluar el impacto de la implementación de un firewall de nueva generación (NGFW) en un entorno de red educativa simulada. Para ello, se estructuraron tres fases secuenciales que permitieron analizar

comparativamente el comportamiento de la red antes, durante y después de la aplicación de los mecanismos de seguridad.

Figura 1. *Fases del proceso experimental*

Fuente: Elaboración propia

Resultados y Discusión

El análisis de los resultados se desarrolló a partir de las pruebas experimentales ejecutadas en el entorno virtualizado, en el cual se simuló una red educativa con diferentes tipos de tráfico, tanto legítimo como malicioso. La evaluación se centró en tres dimensiones principales: detección de amenazas, rendimiento de la red y consumo de recursos del sistema, permitiendo observar el comportamiento del firewall de nueva generación bajo condiciones controladas. Con el objetivo de evaluar la capacidad del sistema para identificar y gestionar amenazas, se analizaron los eventos generados durante la simulación de tráfico malicioso y legítimo. Los resultados obtenidos permiten observar la relación entre eventos detectados, bloqueados y permitidos dentro del entorno de prueba.

Tabla 1. *Detección de amenazas*

Tipo de tráfico	Eventos detectados	Eventos bloqueados	Eventos permitidos	Eficiencia (%)
Malware	50	46	4	92 %
Intentos de intrusión	40	38	4	95 %
Accesos no autorizados	35	33	2	94 %
Tráfico normal	120	0	120	100 %

Fuente: Elaboración propia

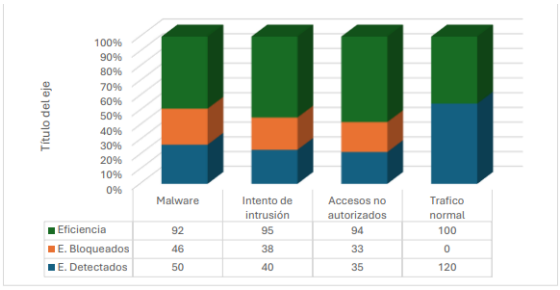

Figura 1. *Detección de amenazas*

Fuente: Elaboración propia

Los resultados evidencian que el sistema mantiene un control efectivo sobre el tráfico malicioso, logrando bloquear la mayoría de los eventos detectados. La diferencia entre eventos detectados y permitidos responde a políticas de clasificación que priorizan el análisis antes de ejecutar acciones definitivas. En el caso del tráfico legítimo, no se registraron bloqueos, lo que confirma la correcta diferenciación entre actividades normales y amenazas. Para profundizar en el comportamiento del sistema, se analizaron los tiempos de respuesta asociados a la detección y bloqueo de amenazas.

Tabla 2. *Tasa de respuesta del sistema por tipo de amenaza*

Tipo de amenaza	Tiempo de detección (ms)	Tiempo de bloqueo (ms)
Malware	18	25
Intrusión	15	22
Accesos no autorizados	12	20

Fuente: Elaboración propia

Los datos obtenidos evidencian que el sistema presenta tiempos de respuesta reducidos tanto en la fase de identificación como en la neutralización de amenazas, lo que refleja un procesamiento ágil y eficiente frente a eventos de seguridad. Esta capacidad de reacción oportuna permite contener de manera temprana la propagación de tráfico malicioso dentro de la red, evitando que las amenazas se expandan hacia otros nodos o servicios. En consecuencia, se reduce el impacto potencial sobre la infraestructura, se preserva la integridad de la información y se mantiene la continuidad operativa del entorno educativo, incluso ante escenarios de tráfico hostil o concurrente. Adicionalmente, se realizó una clasificación de los eventos en función de su nivel de riesgo, con el fin de analizar la forma en que el sistema prioriza y gestiona cada tipo de amenaza.

Tabla 3. *Clasificación de eventos por nivel de riesgo*

Nivel de riesgo	Número de eventos	Acción del sistema
Alto	78	Bloqueo inmediato
Medio	32	Monitoreo activo
Bajo	35	Registro

Fuente: Elaboración propia

La clasificación de los eventos evidencia que el sistema implementa un enfoque diferenciado en su gestión, en el cual se prioriza el bloqueo inmediato ante situaciones de alto riesgo, mientras que en escenarios de riesgo moderado se opta por estrategias de monitoreo y análisis continuo. Este comportamiento permite no solo responder de manera efectiva ante amenazas críticas, sino también evitar decisiones innecesarias que puedan afectar el tráfico legítimo. De esta forma, el firewall demuestra una gestión contextual del tráfico, en la que las acciones no se limitan a reglas estáticas, sino que consideran el nivel de riesgo, el tipo de evento y su posible impacto sobre la red, optimizando así el equilibrio entre seguridad y operatividad. Con el propósito de analizar el impacto del firewall en el desempeño de la red, se realizó una comparación de métricas antes y después de su implementación, considerando condiciones de tráfico similares en ambos escenarios. Como se detalla en la tabla 5:

Tabla 5. *Comparación detallada del rendimiento*

Métrica	*Sin NGFW*	*Con NGFW*	*Variación*
Tiempo de respuesta (ms)	120	135	+15
Latencia promedio (ms)	95	110	+15
Pérdida de paquetes	2.1	2.4	+0.3
Throughput (Mbps)	250	240	-10

Fuente: Elaboración propia

Los resultados evidencian que la implementación del firewall introduce un incremento moderado en los tiempos de respuesta y en la latencia, lo cual se asocia directamente al procesamiento adicional que implica la inspección y validación del tráfico en tiempo real. Este comportamiento es inherente a los mecanismos de seguridad avanzados, como el análisis profundo de paquetes y la aplicación de políticas de filtrado. No obstante, dichas variaciones se mantienen dentro de rangos operativos aceptables y no generan afectaciones significativas en el funcionamiento general de la red, permitiendo que los servicios académicos y administrativos se desarrollen con normalidad y sin interrupciones perceptibles para los usuarios.

Con el fin de analizar de manera más precisa el impacto del firewall en el entorno educativo, se evaluó su comportamiento en diferentes tipos de actividades representativas del uso cotidiano de la red por parte de los usuarios. Estas actividades incluyen navegación web, transferencia de

archivos y acceso a plataformas académicas, permitiendo identificar cómo las variaciones en el rendimiento influyen en cada servicio.

Tabla 4. *Rendimiento según tipo de actividad*

Actividad	Tiempo sin NGFW (ms)	Tiempo con NGFW (ms)
Navegación web	100	115
Transferencia de archivos	140	155
Acceso a plataforma LMS	110	125

Fuente: Elaboración propia

Se observa que el impacto del firewall se mantiene uniforme a lo largo de las distintas actividades evaluadas, evidenciando un comportamiento estable en los tiempos de respuesta independientemente del tipo de servicio utilizado. A pesar del procesamiento adicional asociado a los mecanismos de seguridad, no se registran interrupciones ni degradaciones perceptibles en la prestación de los servicios, lo que indica que el sistema logra integrarse adecuadamente en el entorno educativo sin afectar la experiencia del usuario ni la continuidad de las operaciones.

Con el propósito de evaluar la estabilidad de la red frente a distintos niveles de exigencia, se analizó el comportamiento del sistema bajo escenarios de tráfico progresivamente más intensos, incluyendo condiciones normales, mixtas y situaciones de alta carga. Este enfoque permitió observar la capacidad del firewall para adaptarse a variaciones en el volumen y tipo de tráfico, así como su desempeño ante incrementos sostenidos en la demanda, proporcionando una visión más completa de su funcionamiento.

Tabla 5. *Estabilidad de la red bajo carga*

Escenario	Estado de la red	Observación
Tráfico normal	Estable	Sin retrasos
Tráfico mixto	Estable	Ligera latencia
Ataque simulado (DoS)	Estable	Sin caída del sistema

Fuente: Elaboración propia

Los resultados indican que la red mantiene un comportamiento estable incluso en condiciones de alta demanda, lo que evidencia la capacidad del sistema para gestionar volúmenes elevados de tráfico sin generar interrupciones ni degradaciones críticas en el servicio. Este desempeño refleja que el firewall es capaz de procesar de manera eficiente múltiples flujos de datos simultáneos, manteniendo la continuidad operativa y garantizando la disponibilidad de los servicios, aun en escenarios donde la carga de la red se incrementa significativamente.

El análisis del consumo de recursos permite evaluar de manera integral la eficiencia operativa del firewall durante su funcionamiento en distintos escenarios de carga. A través de la medición del uso de CPU, memoria, almacenamiento y ancho de banda, es posible identificar cómo el sistema responde ante variaciones en la demanda, así como su capacidad para mantener un desempeño estable sin generar sobrecargas. Este enfoque facilita la comprensión del equilibrio entre el nivel de seguridad implementado y la utilización de recursos, lo cual resulta fundamental para determinar la viabilidad del sistema dentro de entornos educativos con limitaciones tecnológicas.

Tabla 6. *Consumo de CPU por tipo de tráfico*

Tipo de tráfico	Uso promedio CPU	Uso máximo CPU
Tráfico normal	30	40
Tráfico mixto	41	58
Ataque simulado	50	58

Fuente: Elaboración propia

El uso de CPU se incrementa de manera proporcional al nivel de carga y a la complejidad del tráfico procesado, especialmente durante la inspección simultánea de múltiples flujos y la activación de reglas de seguridad avanzadas. No obstante, este comportamiento se mantiene dentro de rangos controlados, evidenciando que

el sistema es capaz de gestionar de forma eficiente el procesamiento requerido sin alcanzar niveles críticos de saturación, incluso en escenarios de alta exigencia operativa. Para complementar el análisis del desempeño del sistema, se evaluó el comportamiento de la memoria bajo distintas condiciones operativas, considerando escenarios de carga normal, tráfico mixto y situaciones de mayor exigencia. Este enfoque permitió identificar cómo el firewall gestiona los recursos de memoria durante la ejecución de procesos de inspección, análisis y registro de eventos, así como su capacidad para mantener estabilidad sin generar sobrecargas que puedan afectar el rendimiento general del sistema.

***Tabla 7**. Uso de memoria según actividad*

Escenario	Uso promedio RAM	Pico máximo RAM
Operación normal	3.2 GB	3.8 GB
Tráfico mixto	3.9 GB	4.6 GB
Ataque activo	4.2 GB	4.6 GB

Fuente: Elaboración propia

Los datos reflejan una utilización estable de la memoria a lo largo de los distintos escenarios evaluados, sin presentar fluctuaciones abruptas ni incrementos inesperados que puedan comprometer el rendimiento del sistema. Este comportamiento evidencia una adecuada gestión de los recursos, permitiendo que las tareas de inspección, análisis y registro de eventos se ejecuten de manera continua y eficiente, sin generar saturación ni afectar la estabilidad operativa del entorno.

Se analizó el comportamiento del tráfico de red con el propósito de evaluar la capacidad del sistema para gestionar el ancho de banda durante la ejecución de las pruebas, considerando distintos niveles de carga y concurrencia. Este análisis permitió observar cómo el firewall administra los flujos de datos en tiempo real, identificando su desempeño frente a incrementos en la demanda y su capacidad para mantener la eficiencia en la transmisión sin generar congestión ni afectar la calidad del servicio.

***Tabla 8**. Uso de red por escenario*

Escenario	Tráfico promedio (Mbps)	Pico (Mbps)
Tráfico normal	120	150
Tráfico mixto	180	240
Ataque simulado	200	240

Fuente: Elaboración propia

El sistema demuestra una adecuada capacidad para gestionar incrementos en el volumen de tráfico, manteniendo un flujo de datos continuo y ordenado incluso en escenarios de alta concurrencia. No se evidencian signos de congestión ni interrupciones en la comunicación, lo que indica una gestión eficiente del ancho de banda y una correcta priorización de los flujos de red. Este comportamiento garantiza la estabilidad en la transmisión de datos y contribuye a la continuidad de los servicios dentro del entorno evaluado. Con el propósito de validar la consistencia de los resultados obtenidos, se aplicó un análisis estadístico descriptivo a las principales métricas del sistema, considerando valores promedio y su variabilidad a partir de múltiples ejecuciones del entorno de simulación.

***Tabla 9**. Medidas de tendencia central*

Métrica	Media
Latencia (ms)	110
Tiempo de respuesta (ms)	135
Uso de CPU	41
Uso de RAM (GB)	3.9

Fuente: Elaboración propia

Los valores promedio reflejan el comportamiento representativo del sistema bajo condiciones de operación normal y escenarios de carga mixta, permitiendo identificar una tendencia consistente en el desempeño del

firewall. Estos resultados evidencian que el sistema mantiene estabilidad en su funcionamiento, respondiendo de manera uniforme ante variaciones en el tráfico sin presentar fluctuaciones significativas que puedan afectar su operatividad.

Para complementar el análisis, se evaluó la dispersión de los datos con el fin de determinar el nivel de estabilidad del sistema durante la ejecución de las pruebas. Este enfoque permitió identificar el grado de variabilidad de las métricas analizadas y verificar si los valores obtenidos se mantienen cercanos a la media, lo cual resulta fundamental para validar la consistencia del comportamiento del firewall bajo distintas condiciones de operación.

Tabla 10. *Medidas de dispersión*

Métrica	Desviación estándar
Latencia (ms)	3
Tiempo de respuesta (ms)	4
Uso de CPU	5
Uso de RAM (GB)	0.4

Fuente: Elaboración propia

La baja variabilidad observada indica que los valores se mantienen cercanos a la media, lo que evidencia un comportamiento consistente y predecible del sistema a lo largo de las pruebas. Esta estabilidad en los datos permite afirmar que el firewall opera de manera uniforme frente a distintas condiciones de carga, sin presentar fluctuaciones significativas que puedan comprometer su rendimiento o confiabilidad. Finalmente, se evaluó la confiabilidad de los resultados mediante la repetición de pruebas bajo condiciones similares, con el fin de verificar la consistencia del comportamiento del sistema en diferentes ejecuciones. Este procedimiento permitió confirmar que los datos obtenidos no corresponden a eventos aislados, sino a un desempeño estable y reproducible del firewall dentro del entorno analizado.

Tabla 13. *Confiabilidad de resultados*

Parámetro evaluado	Resultado
Repetición de pruebas	5 ejecuciones
Variación entre pruebas	Baja
Consistencia general	Alta

Fuente: Elaboración propia

Estos resultados confirman que el sistema mantiene un comportamiento estable a lo largo de las distintas ejecuciones realizadas, evidenciando una respuesta consistente ante condiciones operativas similares. Esta uniformidad en el desempeño respalda la validez de los datos obtenidos y fortalece la confiabilidad del análisis, al demostrar que los resultados son reproducibles y representativos del funcionamiento real del firewall en el entorno evaluado. Los resultados obtenidos evidencian que la implementación de firewalls de nueva generación (NGFW) en entornos educativos virtualizados constituye una estrategia eficaz para fortalecer la seguridad de la red sin comprometer la operatividad del sistema.

Este comportamiento coincide con lo planteado por diversos estudios que destacan que los NGFW combinan inspección profunda de paquetes, control de aplicaciones y análisis contextual del tráfico, permitiendo una defensa más precisa frente a amenazas avanzadas (Stallings, 2017). En relación con la detección y bloqueo de amenazas, los niveles de correspondencia entre eventos detectados y bloqueados confirman la eficacia de los mecanismos de correlación de eventos y análisis de comportamiento. Estos hallazgos coinciden con lo señalado por investigaciones recientes, donde se establece que los sistemas de seguridad basados en firmas combinados con análisis heurístico incrementan significativamente la tasa de detección de malware y ataques de intrusión (Kaufman et al., 2022). Asimismo, la capacidad de discriminar correctamente el tráfico legítimo del malicioso respalda lo propuesto en estudios

que destacan la importancia del control de acceso basado en identidad y contexto, especialmente en redes académicas con alta diversidad de dispositivos (Silva, 2020). El comportamiento observado en el tráfico normal, el cual no fue bloqueado, demuestra una adecuada calibración de las políticas de seguridad, evitando falsos positivos. Este resultado es coherente con lo planteado en investigaciones sobre gestión de políticas en NGFW, donde se enfatiza que la correcta definición de reglas permite mantener la disponibilidad de servicios sin afectar la experiencia del usuario (Madhloom et al., 2023).

En este sentido, el equilibrio entre seguridad y accesibilidad constituye un elemento clave en entornos educativos, como lo indican diversos autores en el ámbito de la ciberseguridad institucional (Savoine et al., 2018). Desde la perspectiva del rendimiento de la red, las variaciones en latencia y tiempo de respuesta se mantienen dentro de parámetros aceptables, lo cual concuerda con estudios que sostienen que los NGFW introducen una sobrecarga computacional moderada debido a la inspección profunda de paquetes, pero que esta no afecta de manera significativa la calidad del servicio cuando la infraestructura está correctamente dimensionada (Mohile, 2023).

Este comportamiento también ha sido documentado en entornos virtualizados, donde se destaca que la virtualización permite optimizar el uso de recursos y mantener la estabilidad operativa de los sistemas de seguridad (Montalvo et al., 2025). En cuanto al consumo de recursos, los resultados reflejan una gestión eficiente de CPU, memoria y almacenamiento, lo cual coincide con investigaciones que señalan que los NGFW incorporan mecanismos de optimización como el análisis selectivo de paquetes y la priorización de tráfico (Herman et al., 2020). Este aspecto es especialmente relevante en instituciones educativas con recursos limitados, donde la eficiencia del sistema resulta determinante para su viabilidad operativa (Tanenbaum et al., 2021).

Otro aspecto importante es la aplicabilidad en entornos educativos, donde la literatura destaca que las redes académicas presentan características particulares, como acceso abierto, alta rotación de usuarios y diversidad de dispositivos, lo que incrementa la superficie de ataque (Khan, 2016). En este contexto, la implementación de soluciones integrales de seguridad, como los NGFW, se alinea con las recomendaciones actuales en ciberseguridad educativa, orientadas a proteger la información institucional y garantizar la continuidad de los servicios (Gajjar y Taherdoost, 2024). Además, el uso de entornos virtualizados y laboratorios de simulación para la evaluación de mecanismos de defensa ha sido ampliamente recomendado en la literatura, ya que permite analizar el comportamiento de las amenazas sin comprometer la infraestructura real (Cui et al., 2019; Mohammed y Shaik, 2025). Este enfoque no solo fortalece la seguridad, sino que también contribuye a la formación académica en ciberseguridad, generando entornos de aprendizaje prácticos y controlados (Storm et al., 2023).

Por otra parte, diversos estudios han destacado que la adopción de soluciones basadas en software libre o de bajo costo facilita la implementación de tecnologías avanzadas de protección en instituciones con restricciones presupuestarias (Oppliger, 2023). Este aspecto resulta coherente con la necesidad de promover infraestructuras tecnológicas sostenibles y escalables en el sector educativo (Greenberg, 2021). Los resultados obtenidos se alinean con la

tendencia global que señala un incremento constante de amenazas cibernéticas y la necesidad de adoptar enfoques de seguridad multicapa. En este sentido, los NGFW representan una solución integral que combina prevención, detección y respuesta ante incidentes, tal como lo indican diversas investigaciones recientes en el campo de la seguridad de redes (Bellamkonda, 2024).

La evidencia experimental obtenida en este estudio refuerza la validez de estas propuestas y confirma la pertinencia de su implementación en contextos educativos (Alqudhaibi et al., 2026). La discusión permite concluir que los resultados obtenidos no solo son consistentes con la literatura actual, sino que también aportan evidencia empírica sobre la efectividad de los NGFW en entornos virtualizados educativos, contribuyendo al fortalecimiento de la ciberseguridad institucional y al desarrollo de infraestructuras tecnológicas resilientes (Bonderud, 2024).

Conclusiones

A partir del análisis integral de los resultados obtenidos, se concluye que la implementación de un firewall de nueva generación (NGFW) en un entorno educativo virtualizado constituye una solución eficaz, viable y pertinente para el fortalecimiento de la seguridad de la red institucional. Los resultados evidencian una alta correspondencia entre los eventos detectados y los eventos bloqueados, lo que demuestra la capacidad del sistema para identificar y neutralizar amenazas como malware, intentos de intrusión y accesos no autorizados de manera oportuna, reduciendo el riesgo de comprometer la integridad de la red. De igual forma, el hecho de que el tráfico legítimo haya sido procesado sin bloqueos confirma la adecuada configuración de las políticas de seguridad, permitiendo mantener la continuidad de los servicios académicos y administrativos. Este comportamiento refleja un equilibrio funcional entre protección y disponibilidad, aspecto clave en entornos educativos donde el acceso a plataformas digitales es constante.

En relación con el rendimiento de la red, se identificaron incrementos moderados en el tiempo de respuesta y la latencia, asociados al procesamiento adicional del firewall. No obstante, estas variaciones se mantuvieron dentro de rangos operativos aceptables, sin generar interrupciones ni afectar el funcionamiento de los servicios evaluados. Esto evidencia que la incorporación de mecanismos como la inspección profunda de paquetes y los sistemas de detección y prevención de intrusiones no compromete la operatividad del entorno. Por otra parte, el análisis del consumo de recursos mostró un comportamiento estable del sistema, con valores controlados en el uso de CPU, memoria y ancho de banda, incluso en escenarios de tráfico mixto y alta demanda.

Este desempeño confirma la eficiencia operativa del firewall y su capacidad para adaptarse a diferentes condiciones sin presentar saturación ni degradación del servicio. Los resultados permiten validar que el NGFW logra una integración equilibrada entre seguridad, rendimiento y uso de recursos, garantizando la protección de la red sin afectar su estabilidad. En consecuencia, se concluye que la adopción de esta tecnología representa una estrategia adecuada para fortalecer la ciberseguridad en entornos educativos virtualizados, contribuyendo a la protección de la información y al funcionamiento continuo de los servicios digitales.

Referencias Bibliográficas

Alqudhaibi, A. (2026). Proactive cybersecurity in industry 4.0: A survey of cybersecurity threat prediction approaches. *International Journal of Information Security, 25*(1). https://doi.org/10.1007/s10207-025-01188-9

Bellamkonda, S. (2020). Network segmentation and microsegmentation: Reducing attack surfaces in modern enterprise security. *International Journal of Innovative Research in Computer and Communication Engineering, 8*(6). https://doi.org/10.15680/ijircce.2020.0806067

Bellamkonda, S. (2024). Next-gen firewalls and network security: Enhancing defense through advanced threat mitigation techniques. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 10*(6), 692–702. https://doi.org/10.32628/cseit241061110

Bonderud, D. (2024). Costo de una filtración de datos en 2024: Industria financiera. IBM. https://www.ibm.com/think/insights/cost-of-a-data-breach-2024-financial-industry

Cui, J., Wang, M., Luo, Y., & Zhong, H. (2019). DDoS detection and defense mechanism based on cognitive-inspired computing in SDN. *Future Generation Computer Systems, 97*, 275–283. https://doi.org/10.1016/j.future.2019.02.037

Gajjar, V., & Taherdoost, H. (2024). Cybercrime on a global scale: Trends, policies, and cybersecurity strategies. *Proceedings of ICMCSI 2024*, 668–676. https://doi.org/10.1109/ICMCSI61536.2024.00105

Greenberg, A. (2021). Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers. Anchor Books.

Heino, J., Hakkala, A., & Virtanen, S. (2022). Study of methods for endpoint aware inspection in a next generation firewall. *Cybersecurity, 5*(1). https://doi.org/10.1186/s42400-022-00127-8

Heredia-Quito, K., Barriga-Andrade, J., & Cuenca-Tapia, J. (2025). Seguridad informática con firewalls de nueva generación para detección de intrusos y protección contra DDoS. *MQRInvestigar, 9*(3), e1048. https://doi.org/10.56048/mqr20225.9.3.2025.e1048

Herman, M. (2020). NIST cloud computing forensic science challenges. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8006

Islam, M., Uddin, M., Hossain, M., Ahmed, M., & Moazzam, M. (2023). Analysis and evaluation of network and application security based on next generation firewall. *International Journal of Computing and Digital Systems, 13*(1), 193–202. https://doi.org/10.12785/ijcds/130116

Kaufman, C. (2022). Network security: Private communication in a public world. NIST. https://www.nist.gov/publications/network-security-private-communication-public-world-3rd-edition

Khan, M. (2016). A survey of security issues for cloud computing. *Journal of Network and Computer Applications, 71*, 11–29. https://doi.org/10.1016/j.jnca.2016.05.010

Lamdakkar, O., Ameur, I., Eleyatt, M., Carlier, F., & Ibourek, L. (2024). Toward a modern secure network based on next-generation firewalls: Recommendations and best practices. *Procedia Computer Science, 238*, 1029–1035. https://doi.org/10.1016/j.procs.2024.06.130

Madhloom, J., Noori, Z., Ebis, S., Hassen, O., & Darwish, S. (2023). An information security engineering framework for modeling packet filtering firewall using neutrosophic Petri nets. *Computers, 12*(10), 202. https://doi.org/10.3390/computers12100202

Maheswari, S., Keerthi, T., Kumari, S., & Vennela, L. (2024). Semantics-preserving simplification of real-world firewall rule sets. *Lecture Notes in Computer Science, 9109*, 195–212. https://doi.org/10.1007/978-3-319-19249-9_13

Mohammed, K., & Shaik, N. (2025). Next-generation firewalls: Beyond traditional perimeter defense. *IJFMR, 7*(4). https://doi.org/10.36948/ijfmr.2025.v07i04.51775

Mohile, A. (2023). Next-generation firewalls: A performance-driven approach to contextual threat prevention. *International Journal of Computer Technology and Electronics Communication, 6*(1), 6339–6346. https://doi.org/10.15680/ijctece.2023.0601003

Montalvo, J. (2025). Computación en la nube y transformación digital empresarial. *Polo del Conocimiento, 10*(9), 2436–2449. https://doi.org/10.23857/pc.v10i9.10454

Neupane, K., Haddad, R., & Chen, L. (2018). Next generation firewall for network security: A survey. *Conference Proceedings - IEEE SOUTHEASTCON*. https://doi.org/10.1109/SECON.2018.8478973

Oppliger, R. (2023). SSL and TLS: Theory and practice. Artech House.

Patel, M., Amritha, P., Sudheer, V., & Sethumadhavan, M. (2024). DDoS attack detection model using machine learning algorithm in next generation firewall. *Procedia Computer Science, 233*, 175–183. https://doi.org/10.1016/j.procs.2024.03.207

Savoine, M., Menezes, M., & Andrade, D. (2018). Propuesta de una metodología para la evaluación de los niveles de seguridad de las redes de sensores inalámbricos IoT. *World Journal of Nuclear Science and Technology, 8*(2).

Silva, D. (2020). Evaluación de tecnologías UTM y NGFW para detección de vulnerabilidades en la red. https://dspace.espoch.edu.ec/handle/123456789/14080

Smit, K., & Paneri, D. (2025). Next-generation firewall technologies and their application in enterprise security. *International Journal of Sciences and Innovation Engineering, 2*(10), 106–115. https://doi.org/10.70849/ijsci

Stallings, W. (2017). Network security essentials: Applications and standards. Pearson.

Storm, J. (2023). Testing commercial intrusion detection systems for industrial control systems. *Electronics, 13*(1), 60. https://doi.org/10.3390/electronics13010060

Tanenbaum, A. (2021). Computer networks. Pearson.

Declaraciones éticas y editoriales del artículo

Contribución de los autores (Taxonomía CRediT)

Jorge Eduardo Pinargote Quijije: Conceptualización de la investigación, diseño metodológico, desarrollo del proceso investigativo, análisis formal de los datos, redacción del borrador original del manuscrito, revisión crítica del contenido científico y supervisión general del estudio.

Wilmer Antonio Moreira Sánchez: Curación y organización de los datos, participación en la recolección de información, validación de los resultados obtenidos y elaboración de representaciones gráficas y visualización de los datos.

Declaración de conflicto de intereses

Los autores declaran que no existe conflicto de intereses en relación con la investigación presentada, la autoría del manuscrito ni la publicación del presente artículo.

Declaración de financiamiento

La presente investigación no recibió financiamiento específico de agencias públicas, comerciales o de organizaciones sin fines de lucro. En caso de existir financiamiento institucional o externo, este deberá ser declarado explícitamente por los autores en esta sección.

Declaración del editor

El editor responsable certifica que el proceso editorial del presente artículo se desarrolló conforme a los principios de integridad científica, transparencia y buenas prácticas editoriales. El manuscrito fue sometido a un proceso de evaluación mediante revisión por pares doble ciego, garantizando la confidencialidad de la identidad de los autores y revisores durante todo el proceso de dictamen académico. Asimismo, el editor declara que el artículo cumple con los criterios científicos, metodológicos y éticos establecidos por la revista.

Declaración de los revisores

Los revisores externos que participaron en la evaluación del presente manuscrito declaran haber realizado el proceso de revisión de manera objetiva, independiente y confidencial. Asimismo, manifiestan que no mantienen conflictos de interés con los autores ni con la investigación evaluada, y que sus observaciones y recomendaciones se fundamentan exclusivamente en criterios científicos, metodológicos y académicos.

Declaración ética de la investigación

Los autores declaran que la investigación se desarrolló respetando los principios éticos de la investigación científica, garantizando la confidencialidad de los datos y el respeto a los participantes del estudio. En los casos en que la investigación involucre seres humanos, los procedimientos deben ajustarse a los principios éticos establecidos en la Declaración de Helsinki y a las normativas institucionales correspondientes.

Declaración sobre el uso de inteligencia artificial

Los autores declaran que el uso de herramientas de inteligencia artificial, en caso de haberse utilizado durante el proceso de investigación o redacción del manuscrito, se realizó únicamente como apoyo técnico para mejorar la claridad del lenguaje o el análisis de información, manteniendo siempre la responsabilidad intelectual sobre el contenido del artículo. Las herramientas de inteligencia artificial no fueron utilizadas como autoras del manuscrito ni sustituyen la responsabilidad académica de los investigadores.

Disponibilidad de datos

Los datos que respaldan los resultados de esta investigación estarán disponibles previa solicitud razonable al autor de correspondencia, respetando las normas éticas y de confidencialidad establecidas por la investigación.