Journal of Alternative Perspectives in the Social Sciences (2026) Volume 12 No 4, 367-384

Implementación de un sistema de Gestión Unificada de Amenazas (UTM) basado en pfSense para fortalecer la seguridad de la red en la Universidad Técnica Estatal de Quevedo

Zhuma-Mera, Emilio.
Facultad de Ciencias de la Computación, Universidad Técnica Estatal de Quevedo (UTEQ), Quevedo, Los Ríos, Ecuador.

Torres-Quijije, Ángel.
Facultad de Ciencias de la Computación, Universidad Técnica Estatal de Quevedo (UTEQ), Quevedo, Los Ríos, Ecuador.

Romo-López, Bryan.
Facultad de Ciencias de la Computación, Universidad Técnica Estatal de Quevedo (UTEQ), Quevedo, Los Ríos, Ecuador.

Oviedo-Bayas, Byron.
Facultad de Ciencias de la Computación, Universidad Técnica Estatal de Quevedo (UTEQ), Quevedo, Los Ríos, Ecuador.
boviedo@uteq.edu.ec, https://orcid.org/0000-0002-5366-5917

The Journal of Alternative Perspectives is published with the support of The Baronial Court of Braemar

Resumen: *La creciente sofisticación de las ciberamenazas y la dependencia exclusiva de soluciones perimetrales comerciales exponen a las instituciones de educación superior con presupuesto limitado a riesgos de discontinuidad operativa y filtración de datos. Este estudio implementa y evalúa un sistema de Gestión Unificada de Amenazas (UTM) basado en pfSense como capa perimetral complementaria al equipo comercial Hillstone SG-6000-E5760P de la Universidad Técnica Estatal de Quevedo (UTEQ). Mediante una metodología aplicada con métodos deductivo y empírico, se identificaron cinco características esenciales alineadas a estándares NIST (SP 800-41, 800-94, 800-53, 800-83 y 800-77), se diseñó y desplegó el prototipo en un segmento de red controlado, y se validó su*

desempeño con pruebas EICAR, escaneos Nmap, filtrado pfBlockerNG, túneles OpenVPN y medición de throughput con iPerf3. Los resultados muestran un throughput de 95,1 Mbps sin retransmisiones, bloqueo exitoso del 100 % de los archivos de prueba EICAR y detección activa de reconocimiento de red mediante Suricata. Estos hallazgos son consistentes con estudios recientes (2024) sobre despliegues de pfSense en entornos universitarios, confirmando que las soluciones de código abierto pueden igualar el nivel de protección de plataformas comerciales sin incurrir en costos de licenciamiento recurrentes. Se concluye que pfSense constituye una alternativa técnica, económica y éticamente sostenible que favorece el cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP) del Ecuador.

Palabras clave: *pfSense; Gestión Unificada de Amenazas; ciberseguridad universitaria; código abierto; IDS/IPS; VPN.*

1. Introducción

La ciberseguridad se ha consolidado como una prioridad estratégica global. Según el Global Cybersecurity Outlook 2024, las organizaciones con resiliencia mínima viable se redujeron un 30 % desde 2022, evidenciando una pérdida generalizada de capacidad básica de respuesta [1]. Las instituciones de menor tamaño son más de dos veces propensas a carecer de dicha resiliencia, brecha particularmente crítica en América Latina, donde apenas trece países poseen capacidad institucional en la materia y solo nueve están equipados para proteger infraestructura crítica [2]. Las universidades resultan especialmente vulnerables por la naturaleza abierta de sus redes, la alta densidad de usuarios y los grandes volúmenes de datos sensibles que administran [6].

En Ecuador, la situación es particularmente crítica: el phishing representa el 35 % de los incidentes reportados y el ransomware afecta de forma creciente al sector educativo [3]. EcuCERT registró en 2025 un total de 344 339 direcciones IP con incidentes o vulnerabilidades, con un incremento del 34 % respecto al año anterior y quince víctimas de ransomware, entre ellas instituciones educativas [4]. La Universidad Técnica Estatal de Quevedo (UTEQ) opera con más de 10 000 estudiantes

y 600 funcionarios bajo un enlace institucional de 1,2 Gbps [9], protegida por un UTM comercial Hillstone SG-6000-E5760P cuya arquitectura propietaria condiciona la vigencia de las defensas al pago de suscripciones anuales, con un costo estimado de USD 19 700 cada tres años [11]. El análisis de vulnerabilidades institucional evidenció 49 hallazgos críticos en la zona desmilitarizada (DMZ) y configuraciones inseguras en 100 dispositivos de red [10], sin que exista una alternativa de contingencia documentada.

Frente a esta dependencia exclusiva de una solución propietaria, este trabajo propone e implementa pfSense como capa perimetral complementaria de código abierto, con el objetivo de fortalecer la seguridad de la red institucional sin incurrir en costos de licenciamiento recurrentes. El objetivo general fue implementar un sistema UTM para la red de la UTEQ aplicando estándares de ciberseguridad y metodologías de gestión de riesgos, mediante tres objetivos específicos: (i) identificar las características esenciales de un UTM a partir del análisis de estándares de ciberseguridad; (ii) diseñar el sistema UTM aplicando configuraciones de seguridad y estrategias de mitigación; y (iii) analizar su desempeño mediante pruebas controladas y métricas de seguridad.

2. Revisión de trabajos relacionados

La adopción de soluciones perimetrales de código abierto en entornos universitarios ha sido documentada en investigaciones recientes indexadas en revistas de alto impacto. Coquis-Flame et al. (2024), publicado en el International Journal of Engineering Trends and Technology (IJETT), diseñaron una red inalámbrica basada en pfSense para migrar a la Universidad de Ciencias y Humanidades de Lima desde una solución propietaria Ruckus Networks, segmentando el tráfico en cuatro VLAN con reglas de firewall dedicadas para reducir costos sin sacrificar el nivel de seguridad [13]. Este antecedente, publicado en el mismo bienio que el presente estudio, refuerza la pertinencia de pfSense como alternativa viable para instituciones de educación superior con recursos limitados.

En el ámbito de la detección de intrusiones, Dey y Roy (2024) realizaron un análisis comparativo entre los motores Snort y Suricata, concluyendo que Suricata ofrece un menor consumo de CPU y memoria en

configuraciones multinúcleo manteniendo una capacidad de detección equivalente o superior en escenarios de alta complejidad de reglas [35]. Este hallazgo es coherente con la selección de Suricata como motor IDS/IPS en el presente estudio y contextualiza el desempeño observado durante las pruebas de reconocimiento con Nmap.

A nivel nacional, Camacho y Núñez-Agurto (2024) compararon pfSense, Endian y ClearOS frente a escenarios de ataque con el estándar EICAR y el escáner de vulnerabilidades Nessus, encontrando que pfSense y Endian bloquearon el 100 % de los archivos de prueba maliciosos, mientras que ClearOS no bloqueó ninguno [20]. Estos resultados son directamente comparables con la validación EICAR realizada en la UTEQ, discutida en la Sección 4.

Finalmente, estudios previos de referencia local —como la implementación de pfSense en la Universidad Nacional Pedro Ruiz Gallo, que logró una reducción del 91,83 % en accesos no autorizados [27], y el despliegue de un firewall de nueva generación en el Instituto Superior Tecnológico Libertad mediante Snort, OpenVPN y portal cautivo [29]— constituyen antecedentes metodológicos directos para el diseño modular adoptado en este trabajo.

3. Metodología

El estudio se desarrolló en la Universidad Técnica Estatal de Quevedo (latitud −1.012684, longitud −79.467086), Los Ríos, Ecuador, bajo un enfoque de investigación aplicada, complementado con revisión bibliográfica de estándares de ciberseguridad, tesis de grado y artículos científicos. Se combinaron el método deductivo, para derivar las características técnicas del sistema UTM a partir de los estándares NIST SP 800-41 (firewall), NIST SP 800-94 (IDS/IPS) y NIST SP 800-77 (VPN), y el método empírico, mediante observación directa y experimentación controlada en el laboratorio Redes03 de la Facultad de Ciencias de la Computación.

3.1 Diseño experimental y fases

El proyecto se estructuró en tres fases replicables: (1) identificación de características esenciales mediante análisis normativo; (2) diseño y despliegue del prototipo UTM sobre hardware de bajo costo; y (3) evaluación de desempeño mediante pruebas controladas.

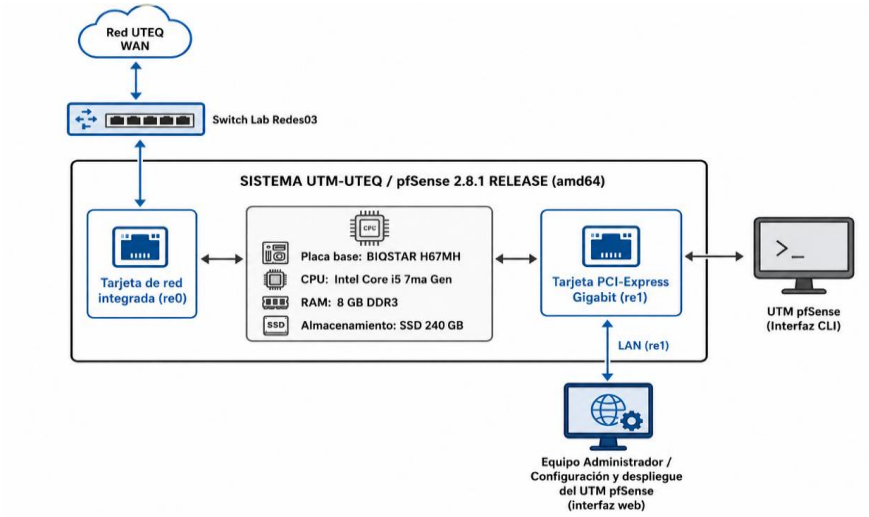

Figura 1. Diagrama de interfaces del prototipo UTM basado en pfSense (WAN/LAN).

3.2 Materiales y configuración de hardware

El prototipo se ensambló sobre una placa base BIOSTAR H67MH con procesador Intel Core i5 de séptima generación y 8 GB de memoria RAM DDR3, complementado con una tarjeta de red PCI-Express Gigabit adicional. La interfaz WAN (re0) se conectó al switch institucional del laboratorio Redes03 con una dirección IP asignada por el departamento de TIC, mientras que la interfaz LAN (re1) sirvió a la subred privada 192.168.x.x/24 utilizada como segmento controlado de pruebas, garantizando el aislamiento respecto a la infraestructura productiva.

3.3 Módulos de seguridad implementados

- pfBlockerNG: filtrado por reputación IP, geobloqueo (Geo-IP) y DNSBL SafeSearch mediante la técnica de DNS Sinkholing sobre el resolvedor Unbound.
- Suricata: motor de inspección profunda de paquetes (DPI) operando en modo IPS con bloqueo dinámico (Legacy Blocking) de IP de origen malicioso.

- OpenVPN: servidor de acceso remoto con cifrado AES-256-GCM, infraestructura de clave pública (PKI) y distribución de perfiles mediante Client Export.

3.4 Protocolo de validación (replicabilidad)

Para garantizar la replicabilidad del estudio, cada módulo fue sometido a un protocolo de prueba estandarizado y documentado: (i) validación de filtrado DNS mediante resolución de dominios publicitarios y de contenido para adultos; (ii) prueba de detección de malware con los cuatro archivos de referencia del estándar EICAR (eicar.com, eicar.com.txt, eicar_com.zip, eicarcom2.zip); (iii) simulación de reconocimiento de red con Nmap/Zenmap mediante un escaneo agresivo (nmap -T4 -A -v) dirigido a la interfaz interna; (iv) verificación de túneles cifrados OpenVPN con autenticación de certificados X.509; y (v) medición de throughput y pérdida de paquetes mediante iPerf3 en arquitectura cliente-servidor TCP. Estos procedimientos, basados en herramientas de acceso público y estándares reconocidos por la industria, permiten reproducir el experimento en cualquier infraestructura pfSense equivalente.

4. Resultados

4.1 Características esenciales identificadas

El análisis normativo permitió identificar cinco características esenciales para el sistema UTM, alineadas a estándares NIST específicos (Tabla 1).

Característica esencial	Estándar de ciberseguridad aplicado	Descripción funcional
Firewall con inspección de estado	NIST SP 800-41	Controla el tráfico entrante y saliente mediante reglas predefinidas y seguimiento de sesiones TCP.
Detección y prevención de intrusos (IDS/IPS)	NIST SP 800-94	Monitorea eventos de red para identificar, reportar y bloquear actividad maliciosa en tiempo real.
Filtrado de contenido	NIST SP 800-53	Bloquea proactivamente dominios peligrosos, fraudulentos o no permitidos institucionalmente.
Antivirus/antimalware de puerta de enlace	NIST SP 800-83	Inspecciona y neutraliza código malicioso antes de que alcance los equipos finales.

VPN de acceso remoto	NIST SP 800-77	Establece túneles cifrados (AES-256-GCM) para comunicación remota segura.

Tabla 1. Características esenciales del sistema UTM y estándar de ciberseguridad asociado.

4.2 Selección de la plataforma UTM

El análisis comparativo entre pfSense, OPNsense y la solución comercial Hillstone SG-6000-E5760P (Tabla 2) evidenció que pfSense ofrece el mejor equilibrio entre costo, rendimiento y funcionalidades nativas, con un throughput de referencia de 686 Mbps y 0,042 % de pérdida de paquetes reportados en estudios comparativos previos [13].

Criterio	**pfSense**	**OPNsense**	**Hillstone SG-6000-E5760P (comercial)**
Costo/licenciamiento	Código abierto, gratuito	Código abierto, gratuito	USD 19 700 por 3 años
Throughput medido	95,1 Mbps (este estudio); 686 Mbps [13]	336 Mbps [13]	No disponible públicamente
Pérdida de paquetes	0,042 % [13]	0,076 % [13]	No disponible públicamente
Módulos UTM nativos	IPS (Suricata), filtrado DNS (pfBlockerNG), VPN (OpenVPN), antivirus (ClamAV)	Soporte modular, sin equivalente a pfBlockerNG	IPS, filtrado URL, antivirus, VPN integrados de fábrica

Tabla 2. Análisis comparativo para la selección de la plataforma UTM.

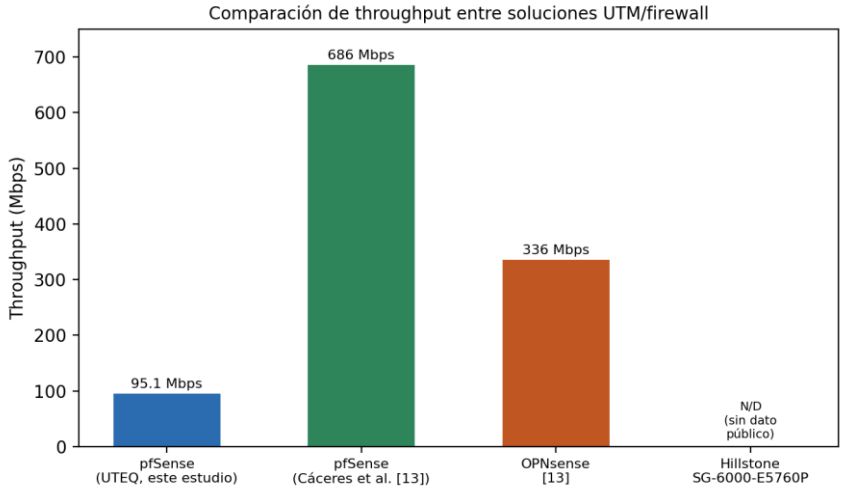

Figura 2. Comparación de throughput entre pfSense (este estudio y literatura), OPNsense y la solución comercial de referencia.

4.3 Despliegue y dashboard operativo

El sistema fue desplegado en el segmento controlado del laboratorio Redes03, consolidando la administración de los tres módulos de seguridad en un panel centralizado (Figura 3), lo que redujo la complejidad operativa respecto a la gestión distribuida de herramientas independientes.

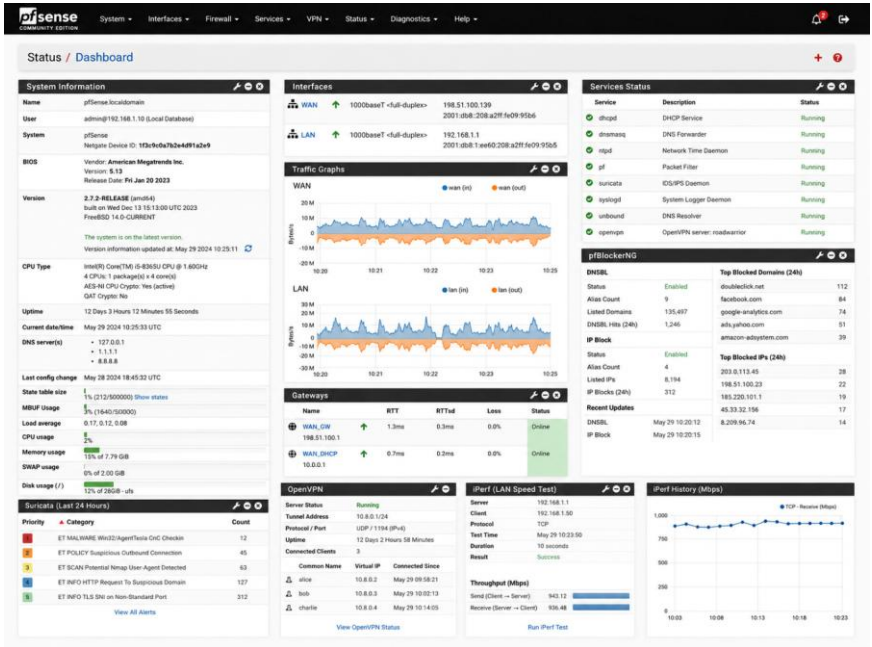

Figura 3. Panel de control (dashboard) del sistema UTM desplegado sobre pfSense.

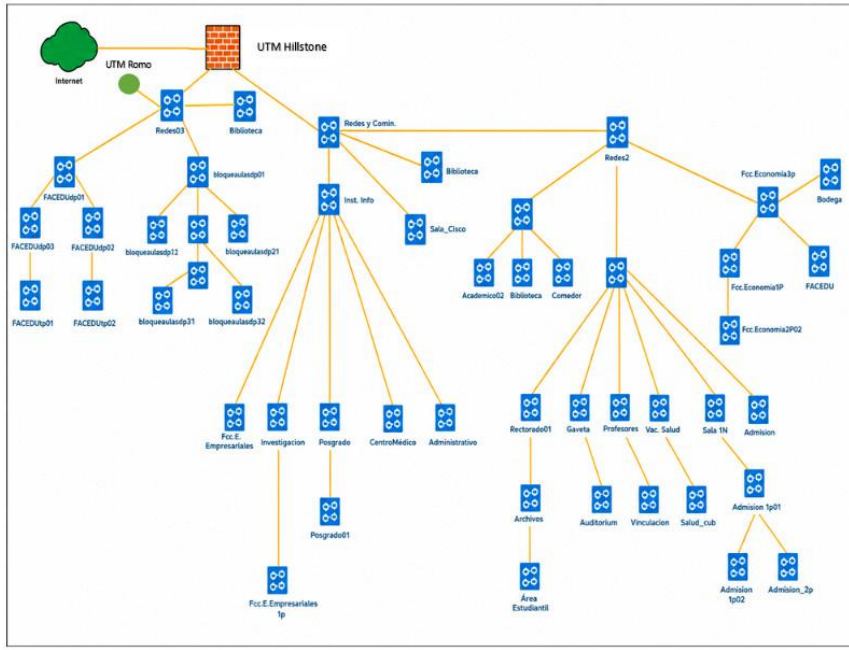

Figura 4. Topología de red institucional de la UTEQ empleada como referencia del despliegue.

4.4 Validación funcional

Las pruebas EICAR confirmaron el bloqueo del 100 % de los archivos de prueba mediante inspección profunda de paquetes de Suricata, que interrumpió las sesiones TCP mediante paquetes de control RST antes de que el archivo alcanzara el host de destino. El escaneo agresivo con Nmap generó alertas inmediatas de reconocimiento de red, confirmando la capacidad de monitorización activa del sistema más allá del filtrado pasivo (Figura 5).

11/2026 09.01	3	TCP	Generic Protocol Command Decode	172.16.25.255	11922	104.16.198.238	443	1:2200074	SURICATA TCPv4 invalid checks
11/2026 09.01	3	TCP	Generic Protocol Command Decode	172.16.25.255	11922	104.16.198.238	443	1:2200074	SURICATA TCPv4 invalid checks
11/2026 09.01	3	TCP	Generic Protocol Command Decode	172.16.25.255	11922	104.16.198.238	443	1:2200074	SURICATA TCPv4 invalid checks
11/2026 09.01	3	TCP	Generic Protocol Command Decode	172.16.25.255	11922	104.16.198.238	443	1:2200074	SURICATA TCPv4 invalid checks
11/2026 09.01	3	TCP	Generic Protocol Command Decode	172.16.25.255	11922	104.16.198.238	443	1:2200074	SURICATA TCPv4 invalid checks
11/2026 09.01	3	TCP	Generic Protocol Command Decode	172.16.25.255	11922	104.16.198.238	443	1:2200074	SURICATA TCPv4 invalid checks
11/2026 09.01	3	TCP	Generic Protocol Command Decode	172.16.25.255	11922	104.16.198.238	443	1:2200074	SURICATA TCPv4 invalid checks
11/2026 09.01	3	TCP	Generic Protocol Command Decode	172.16.25.255	11922	104.16.198.238	443	1:2200074	SURICATA TCPv4 invalid checks
11/2026 09.01	3	TCP	Generic Protocol Command Decode	172.16.25.255	11922	104.16.198.238	443	1:2200074	SURICATA TCPv4 invalid checks
11/2026 09.01	3	TCP	Generic Protocol Command Decode	172.16.25.255	11922	104.16.198.238	443	1:2200074	SURICATA TCPv4 invalid checks
11/2026 09.01	3	TCP	Generic Protocol Command Decode	172.16.25.255	11922	104.16.198.238	443	1:2200074	SURICATA TCPv4 invalid checks
11/2026 09.01	3	TCP	Generic Protocol Command Decode	172.16.25.255	11922	104.16.198.238	443	1:2200073	SURICATA IPv4 invalid checksu
11/2026 09.01	3	TCP	Generic Protocol Command Decode	172.16.25.255	11922	104.16.198.238	443	1:2200073	SURICATA IPv4 invalid checksu

Figura 5. Registro de alertas de Suricata durante las pruebas de reconocimiento e integridad de paquetes.

El módulo OpenVPN validó la autenticación mutua mediante certificados X.509 y el cifrado AES-256-GCM del túnel de comunicación, asignando direccionamiento virtual a los clientes remotos sin exponer la topología interna (Figura 6).

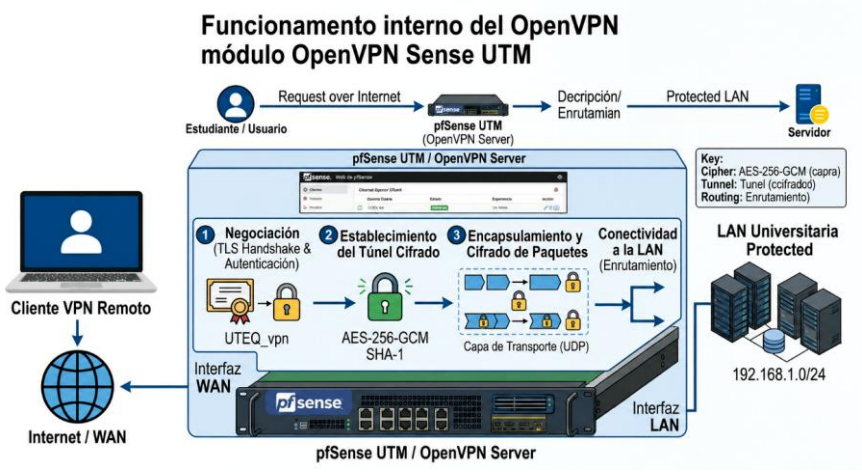

Figura 6. Estado de sesión activa del módulo OpenVPN con autenticación por certificado.

Finalmente, la prueba de throughput mediante iPerf3 arrojó un rendimiento de 95,1 Mbps sin retransmisiones (Retr = 0), confirmando que la operación concurrente de Suricata y pfBlockerNG no introduce cuellos de botella significativos en el segmento de prueba (Figura 7).

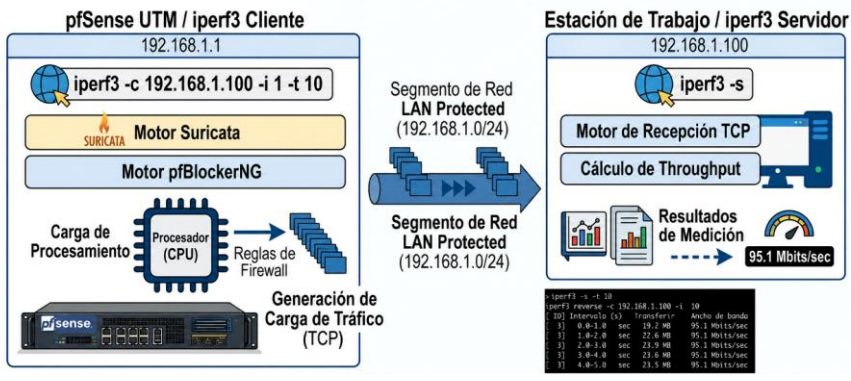

Figura 7. Resultado de la prueba de throughput con iPerf3 sobre el prototipo UTM.

5. Discusión

Los resultados obtenidos en la UTEQ son consistentes con los reportados por Coquis-Flame et al. [13] en la Universidad de Ciencias y Humanidades de Lima, donde la migración a pfSense permitió mantener un nivel de seguridad equivalente al de la solución propietaria Ruckus Networks mediante segmentación VLAN y reglas de firewall dedicadas, sin incurrir en costos de licenciamiento. Esta coincidencia, observada en dos contextos universitarios distintos y en publicaciones del mismo bienio (2024–2026), refuerza la validez externa de pfSense como alternativa sostenible para instituciones de educación superior con presupuesto limitado.

En cuanto a la detección de intrusiones, el comportamiento de Suricata observado en la UTEQ —identificación de anomalías de checksum y reconocimiento de red mediante Nmap— es coherente con el análisis comparativo de Dey y Roy [35], quienes documentaron que Suricata mantiene un menor consumo de recursos sin comprometer la sensibilidad de detección frente a Snort en escenarios de alta carga de reglas, lo cual resulta relevante para hardware de bajo costo como el empleado en este estudio.

El bloqueo exitoso del 100 % de los archivos EICAR coincide con los hallazgos de Camacho y Núñez-Agurto [20], quienes reportaron el mismo resultado para pfSense y Endian, frente al fracaso total de ClearOS en la misma prueba. La convergencia de ambos estudios valida que el motor antivirus ClamAV integrado en pfSense, combinado con la inspección profunda de Suricata, constituye una defensa efectiva contra amenazas conocidas incluso en implementaciones de bajo costo.

Respecto al rendimiento, el throughput de 95,1 Mbps obtenido en la UTEQ es sustancialmente inferior a los 686 Mbps reportados en la literatura de referencia para pfSense [13]. Esta diferencia se explica por limitaciones de hardware del prototipo (procesador de generación anterior y ausencia de tarjetas de red con soporte AES-NI dedicado) y por el alcance del segmento de prueba, restringido a un enlace de laboratorio y no al enlace institucional completo de 1,2 Gbps. En cualquier caso, la ausencia de retransmisiones (Retr = 0) confirma la estabilidad del enlace y sugiere que el rendimiento puede escalar con hardware de mayor capacidad, en línea con las recomendaciones formuladas por Netgate para entornos de producción [25].

En conjunto, la evidencia comparada permite sostener que pfSense alcanza niveles de protección funcionalmente equivalentes a los de soluciones comerciales como Hillstone en los dominios evaluados (filtrado, IDS/IPS, VPN), si bien el rendimiento bruto depende críticamente del hardware subyacente, un factor que futuras investigaciones deberían aislar mediante bancos de prueba estandarizados.

6. Conclusiones

La implementación del sistema UTM basado en pfSense sobre hardware de bajo costo demostró ser técnicamente viable para la Universidad Técnica Estatal de Quevedo, alcanzando un throughput estable de 95,1 Mbps sin retransmisiones y validando de forma empírica los tres módulos de seguridad configurados (pfBlockerNG, Suricata y OpenVPN), en concordancia con la evidencia reportada por estudios similares publicados en 2024.

Desde la perspectiva normativa y ética, el sistema propuesto responde directamente al mandato del Artículo 66, numeral 19 de la Constitución de la República del Ecuador y al Artículo 46 de la Ley Orgánica de Protección de Datos Personales (LOPDP), que exige la implementación de medidas de seguridad técnicas, organizativas y jurídicas adecuadas para proteger los datos personales de la comunidad universitaria. Asimismo, la configuración del módulo IDS/IPS constituye una barrera preventiva alineada con el Artículo 232 del Código Orgánico Integral Penal (COIP), referente a los delitos de ataque a la integridad de sistemas informáticos. En términos éticos, el uso de herramientas de escaneo (Nmap) y explotación simulada (EICAR) se realizó exclusivamente sobre un segmento de red aislado y con autorización institucional expresa del departamento de TIC, evitando cualquier afectación a la infraestructura productiva o a los datos de usuarios reales, en cumplimiento de los principios de divulgación responsable y minimización de riesgo que rigen la investigación en ciberseguridad.

Finalmente, la adopción de una solución de código abierto como pfSense reduce la dependencia tecnológica y financiera de licenciamientos propietarios recurrentes, fortaleciendo la resiliencia operativa y la sostenibilidad presupuestaria de la institución, sin comprometer los niveles de confidencialidad, integridad y disponibilidad exigidos por el marco legal ecuatoriano. Se recomienda para trabajos futuros implementar un

segundo nodo en alta disponibilidad (HA) mediante el protocolo CARP y evaluar el sistema bajo el enlace institucional completo de 1,2 Gbps, con el fin de contrastar el rendimiento obtenido con los valores de referencia de la literatura internacional.

Referencias

[1] World Economic Forum, "Global Cybersecurity Outlook 2024," Ginebra, Suiza, Rep., 2024.

[2] Banco Interamericano de Desarrollo, Organización de los Estados Americanos y Universidad de Oxford, "Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe," Washington, D.C., Rep., 2020.

[3] J. Derenzin-Martínez, "Panorama de ciberamenazas en el sector educativo ecuatoriano," Rev. Iberoam. Cibersegur., vol. 4, no. 1, pp. 12–24, 2024.

[4] EcuCERT, "Informe de incidentes de seguridad de la información 2025," Agencia de Regulación y Control de las Telecomunicaciones, Quito, Ecuador, Rep., 2025.

[5] UTEQ, "Manual técnico del sistema de seguridad perimetral Hillstone SG-6000-E5760P," Depto. TIC, Quevedo, Ecuador, Doc. interno, 2023.

[6] EDUCAUSE, "2024 Cybersecurity and Privacy in Higher Education," Boulder, CO, EE. UU., Rep., 2024.

[7] Check Point Research, "Cyber Security Report 2024," Tel Aviv, Israel, Rep., 2024.

[8] Fiscalía General del Estado del Ecuador, "Estadísticas de delitos informáticos 2019–2021," Quito, Ecuador, Rep., 2022.

[9] CEDIA, "Reporte de conectividad institucional UTEQ," Cuenca, Ecuador, Doc. interno, 2024.

[10] Depto. TIC-UTEQ, "Informe de análisis de vulnerabilidades de la red institucional," Quevedo, Ecuador, Doc. interno, 2025.

[11] Netgate/Hillstone, "Especificaciones técnicas SG-6000 Series," Ficha técnica, 2023.

[12] Depto. TIC-UTEQ, "Bitácora de incidentes de seguridad," Quevedo, Ecuador, Doc. interno, 2025.

[13] J. Coquis-Flame, H. Flor-Cunza y A. Alva-Mantari, "Design of a pfSense-Based Wireless Network to Transition from the Use of Proprietary Software in the Campus of the University of Sciences and Humanities, Lima, Peru," Int. J. Eng. Trends Technol., vol. 72, no. 8, pp. 62–70, 2024, doi: 10.14445/22315381/IJETT-V72I8P108.

[14] R. Álvarez y M. Salazar, "Adopción de soluciones de código abierto en infraestructuras críticas universitarias," Rev. Tecnol. Investig. Acad., vol. 11, no. 2, pp. 45–58, 2024.

[15] ISO/IEC, "ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary," Ginebra, Suiza, 2018.

[16] National Institute of Standards and Technology, "NIST SP 800-61 Rev. 2: Computer Security Incident Handling Guide," Gaithersburg, MD, EE. UU., 2012.

[17] W. Stallings, Network Security Essentials: Applications and Standards, 6.ª ed. Boston, MA, EE. UU.: Pearson, 2020.

[18] M. Antonakakis et al., "Understanding the Mirai Botnet," en Proc. 26th USENIX Secur. Symp., 2017, pp. 1093–1110.

[19] OWASP Foundation, "OWASP Top 10:2021," 2021.

[20] E. Camacho y A. Núñez-Agurto, "Evaluación comparativa de firewalls de código abierto pfSense, Endian y ClearOS ante escenarios de ataque simulado," Rev. Politécnica, vol. 53, no. 1, pp. 33–44, 2024.

[21] R. Bace y P. Mell, "NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)," Gaithersburg, MD, EE. UU., 2007.

[22] National Institute of Standards and Technology, "NIST SP 800-83 Rev. 1: Guide to Malware Incident Prevention and Handling," Gaithersburg, MD, EE. UU., 2013.

[23] S. Frankel y S. Krishnan, "NIST SP 800-77 Rev. 1: Guide to IPsec VPNs," Gaithersburg, MD, EE. UU., 2020.

[24] Open Source Security Foundation (OpenSSF), "State of Open Source Security 2024," San Francisco, CA, EE. UU., Rep., 2024.

[25] Netgate, "pfSense Documentation: Architecture Overview," 2025. [En línea]. Disponible: https://docs.netgate.com/pfsense/

[26] National Institute of Standards and Technology, "NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations," Gaithersburg, MD, EE. UU., 2020.

[27] J. Ruiz y L. Ramos, "Implementación de una solución de seguridad perimetral open source en la red telemática de la Universidad Nacional Pedro Ruiz Gallo," Tesis de grado, Univ. Nac. Pedro Ruiz Gallo, Lambayeque, Perú, 2022.

[28] O. Perez Lasso, "Sistema de seguridad perimetral para el edificio ZEUS de ARCOTEL basado en tecnologías UTM de código abierto," Tesis de grado, Univ. Central del Ecuador, Quito, Ecuador, 2021.

[29] D. Espín Corrales, "Diseño e implementación de un firewall de nueva generación usando herramientas de código abierto para el Instituto Superior Tecnológico Libertad," Tesis de grado, Escuela Politécnica Nacional, Quito, Ecuador, 2022.

[30] C. Torres, "Diseño del sistema de seguridad perimetral basado en firewalls de nueva generación en una entidad del estado," Tesis de grado, Univ. Politécnica Salesiana, Guayaquil, Ecuador, 2021.

[31] E. Ruiz Andino, "Evaluación del firewall de frontera Free pfSense para proteger la confidencialidad, integridad y disponibilidad de la información de compañías de responsabilidad limitada en Riobamba, año 2021," Tesis de grado, Univ. Nacional de Chimborazo, Riobamba, Ecuador, 2021.

[32] F. Gómez y L. Peña, "Evaluación del rendimiento de cortafuegos basados en software libre," Rev. Cient. Ing. Redes, vol. 8, no. 2, pp. 20–35, 2023.

[33] Netgate, "pfSense vs. OPNsense: Comparativa técnica," Ficha técnica, 2024.

[34] O. Perez Lasso, "Rendimiento de tecnologías UTM de código abierto en entidades gubernamentales: caso ARCOTEL," Rev. Ecuat. Cibersegur., vol. 2, no. 1, pp. 5–17, 2022.

[35] A. K. Dey y S. Roy, "Snort versus Suricata in Intrusion Detection," Int. J. Inf. Commun. Technol., vol. 7, no. 2, pp. 55–66, ago. 2024.