Novasinergia
Revista digital de ciencia, ingeniería y tecnología

Unach
UNIVERSIDAD NACIONAL DE CHIMBORAZO

Artículo de Investigación

Evaluación del rendimiento de cortafuegos basados en software libre

Performance evaluation of free software based firewalls

Rudibel Perdigón Llanes
Universidad de Pinar del Río "Hermanos Saíz Montes de Oca", Pinar del Río, Cuba; 20100

*Correspondencia: rperdigon90@gmail.com

Citación: Perdigón, R., (2022). Evaluación del rendimiento de cortafuegos basados en software libre. *Novasinergia.* 5(1). 31-42. https://doi.org/10.37135/ns.01.09.03

Recibido: 10 noviembre 2021
Aceptado: 29 enero 2022
Publicado: 31 enero 2022

Novasinergia
ISSN: 2631-2654

Resumen: El objetivo de la presente investigación fue evaluar cuantitativamente los rendimientos y las funcionalidades de seguridad de los principales cortafuegos basados en software libre existentes en la actualidad. Para medir los rendimientos de red de los cortafuegos se emplearon métricas como el ancho de banda, el *jitter* y la tasa de pérdida de paquetes mediante la herramienta iPerf3. Se utilizó la herramienta htop para comprobar el consumo de CPU y memoria RAM de las soluciones. Se identificó que Endian, Zentyal, pfSense, OPNsense, VyOS, IPFire y ClearOS brindan un conjunto de funcionalidades que contribuyen a elevar la seguridad en las redes de datos. Los resultados obtenidos evidenciaron que ClearOS posee de forma general, los mejores índices de consumo de CPU y memoria RAM, lo cual confirma su elevada eficiencia para asegurar las redes de datos con ahorro y uso óptimo de los recursos de hardware. Los hallazgos identificados facilitan la toma de decisiones para el despliegue de herramientas de ciberseguridad en redes digitales de organizaciones con escasos recursos computacionales.

Palabras clave: Ciberseguridad, cortafuego, evaluación de rendimiento, PYMES, recursos computacionales.

Abstract: *The objective of this research is to quantitatively evaluate the performance and security functionalities of the main firewalls based on free software currently available. Metrics such as bandwidth, jitter and packet loss rate were used to measure the network performance of the firewalls using the iPerf3 tool. The htop tool was used to check the CPU and RAM consumption of the solutions. It was identified that Endian, Zentyal, pfSense, OPNsense, VyOS, IPFire and ClearOS provide a set of functionalities that contribute to increase the security in data networks. The results obtained showed that ClearOS has the best overall CPU and RAM consumption rates, which demonstrated its high efficiency in securing data networks with savings and optimal use of hardware resources. The identified findings facilitate decision making for the deployment of cyber-security tools in digital networks of organizations with scarce computational resources.*

Keywords: *Cyber-security, enterprises, firewall, performance evaluation, SME, computational resources.*

1. Introducción

En la economía digital son numerosas las empresas que adoptan las tecnologías de la información y las comunicaciones (TIC) para desarrollar sus negocios y satisfacer sus intereses comerciales. La aplicación de las TIC en los procesos de gestión empresarial aporta marcados beneficios para el crecimiento económico de estas organizaciones (Perdigón & Pérez, 2020). Sin embargo, la proliferación de estas tecnologías conlleva enormes desafíos de seguridad, relacionados con el aumento de programas maliciosos y ataques informáticos (Rafamantanantsoa & Rabetafika, 2018; Mora & Villero, 2020). Los ataques informáticos ocupan la octava posición de las amenazas con mayor impacto económico a nivel mundial (World Economic Forum, 2020). Datos de Eset Security para Latinoamérica reflejaron que durante 2020 las empresas de la región sufrieron ataques informáticos relacionados fundamentalmente con la infección por malware (34%), ataques de ingeniería social (20%), acceso indebido a aplicaciones e información (18%), y denegación de servicios (11%) (Eset Security, 2021). Las pérdidas económicas generadas por estas transgresiones impactan negativamente en las economías de las empresas, principalmente en las pequeñas y medianas empresas (PYMES) que son incapaces de sostener sus negocios luego de sufrir un ciberataque de envergadura (Bustamante, Valles & Levano, 2020).

Incrementar la seguridad de las redes digitales empresariales constituye una necesidad para garantizar la integridad y usabilidad de los datos y los recursos digitales de las empresas (Morales, Toapanta & Toasa, 2020). Según los autores Rafamantanantsoa & Rabetafika (2018); Mora & Villero (2020) y Togay, Kasif, Catal & Tekinerdogan (2021), los cortafuegos constituyen una de las principales herramientas empleadas para alcanzar este propósito.

Los cortafuegos (*firewalls*) son sistemas de seguridad que controlan el tráfico de red mediante reglas prestablecidas (Neupane, Haddad & Chen, 2018). Estas herramientas se ubican fundamentalmente de cara a internet y son capaces de prevenir el acceso no autorizado desde y hacia las redes internas de una organización (Lee, Kim, Park & Woo, 2015; Rafamantanantsoa & Rabetafika, 2018). Sampaio & Bernardino (2017) y Zare, Olsen, Zare, & Azadi (2018) determinaron que los cortafuegos pueden implementarse mediante herramientas basadas en software o dispositivos de hardware especializados. Los *firewalls* basados en software son implementados en un sistema operativo estándar y utilizan los recursos computacionales del ordenador donde este opera, por su parte, los *firewalls* basados en hardware constituyen dispositivos físicos fabricados exclusivamente para esta función que poseen su propia CPU, memoria RAM, almacenamiento interno y sistema operativo (Konikiewicz & Markowski, 2017). Agbenyegah & Asante (2017) y Konikiewicz & Markowski (2017) reportaron que los *firewalls* inciden de forma negativa en el rendimiento de las redes donde son implementados. El rendimiento de las redes de datos influye significativamente en la disponibilidad de los recursos digitales de las organizaciones (Shahsavari, Shahhoseini, Zhang, & Elbiaze, 2019).

Evaluar las capacidades defensivas de los *firewalls* y su impacto en las comunicaciones de las redes que monitorean constituyen aspectos esenciales para determinar su efectividad como herramientas de seguridad, y para facilitar su selección en correspondencia con las necesidades de las organizaciones (Lee *et al*., 2015; Konikiewicz & Markowski, 2017; Mora

& Villero 2020). Cotret, Gogniat & Sepúlveda (2016) concluyeron que los *firewalls* basados en hardware poseen elevadas funcionalidades de seguridad y mantienen índices de desempeño de red eficientes. Sin embargo, los costos de estos dispositivos dificultan su adquisición por parte de las PYMES de países en vías de desarrollo. Las PYMES poseen características organizativas y económicas que las sitúan en una posición desventajosa respecto a las grandes corporaciones. Estas organizaciones carecen de capacidades tecnológicas para implementar infraestructuras de red potentes y de altos estándares como las grandes empresas (Logroño, 2017). Por esta razón, es importante adoptar alternativas tecnológicas confiables en las PYMES para minimizar fallas, garantizar la gestión de sus recursos digitales de forma eficiente y con ahorro de costos, en aras de incrementar su productividad (Perdigón & Ramírez, 2020). Las herramientas basadas en software libre representan una solución viable para las PYMES porque reducen costos, facilitan el despliegue de servicios digitales con un aprovechamiento óptimo de los recursos de hardware, son capaces de reemplazar dispositivos de interconexión de redes de altas prestaciones y contribuyen a impulsar la soberanía tecnológica de naciones en desarrollo (Dagnesses, 2019; Perdigón & Ramírez, 2020).

En la literatura se identificaron diversas investigaciones donde se analizó el desempeño de *firewalls* basados en software libre en diferentes entornos simulados. Los autores Shahsavari *et al*. (2019) plantean que el uso de las simulaciones como metodología experimental para modelar y analizar el desempeño de *firewalls* de red permite alcanzar una comprensión más profunda de su dinámica y comportamiento; además, posibilita identificar parámetros óptimos para la asignación de recursos en aras de mejorar el rendimiento general de la red. Los autores Arunwan, Laong & Atthayuwat (2016) compararon la capacidad de Endian y pfSense para detectar ataques de fuerza bruta, escaneo de puertos, ping de la muerte e inundación de tráfico de red. En su estudio Konikiewicz & Markowski (2017), analizaron el rendimiento de red de los *firewalls* Cisco ASA 5505, Juniper Netscreen 50, IPTables y VyOS y su capacidad para resistir ataques de denegación de servicio (DoS, por sus siglas en inglés). Sampaio & Bernardino (2017), analizaron las funcionalidades de seguridad de IPCop, pfSense y Zentyal. Iriarte *et al*. (2018), evaluaron el desempeño de IPCop, Endian, ClearOS y Fedora 21 frente ataques DoS. Sin embargo, los autores anteriormente mencionados limitaron su análisis a unas pocas soluciones y no evaluaron sus desempeños en ordenadores de bajas prestaciones, que son ampliamente utilizados en PYMES de países en desarrollo. Así, el objetivo de este trabajo es evaluar cuantitativamente los rendimientos y las funcionalidades de seguridad de los principales *firewalls* basados en software libre existentes en la actualidad.

2. Metodología

En este trabajo se realizó un análisis cuantitativo de las funcionalidades de seguridad, los rendimientos de red y el consumo de recursos de hardware de los principales *firewalls* basados en software libre existentes hasta el momento. La evaluación de los *firewalls* se realizó mediante el método experimental en un entorno con tráfico de red simulado y se utilizaron métricas como el ancho de banda, el *jitter* y la tasa de pérdida de paquetes de red. La metodología y los indicadores mencionados son ampliamente utilizados en la literatura

científica para evaluar el desempeño de los cortafuegos (Iriarte *et al*., 2018; Cheminod, Durante, Seno & Valenzano, 2018; Shahsavari *et al*., 2019). Estos indicadores fueron analizados mediante la herramienta iPerf3. Se utilizó la herramienta htop para evaluar el consumo de CPU y memoria RAM de cada solución.

El ancho de banda, expresado en Mbit/s, puede definirse como una medida de transferencia de datos por unidad de tiempo entre un emisor y un receptor (Putra, Vita & Saputra, 2018). Buñay, Pastor, Paguay & Moreno (2019) definieron el *jitter* como la variación de tiempo en milisegundos (ms), de los paquetes de red que viajan entre el emisor y el receptor, según estos autores la tasa de pérdida se determina como el cociente entre los paquetes de red recibidos por el receptor y la totalidad de paquetes enviados por el emisor.

2.1. Cortafuegos seleccionados

Para seleccionar los cortafuegos a evaluar se realizó un análisis de la literatura científica disponible en internet y se identificaron las soluciones basadas en software libre con licencias de uso gratuitas más estudiadas por los diferentes autores consultados. La tabla 1 muestra los *firewalls* identificados, los sistemas operativos base donde operan y los requerimientos mínimos de hardware para su funcionamiento, estos datos fueron extraídos de los sitios oficiales de cada solución.

Tabla 1: Cortafuegos cuyo desempeño se ha evaluado y reportado en la literatura.

Autor (es)	Nombre del cortafuego/ Proveedor	Última versión disponible	Sistema Operativo	Requerimientos de hardware			Disponibilidad de soporte técnico por su fabricante
				CPU	RAM (MB)	HDD	
Arunwan *et al*. (2016); Sampaio & Bernardino (2017	pfSense / Netgate	2.5.2	FreeBSD	64-bit amd64 (x86-64)	1024	80 GB	Sí
Arunwan *et al*. (2016); Iriarte *et al*. (2018)	Endian / Endian SRL	3.3.2	Red Hat	Dual core (x86-64) 1 GHz	2048	8 GB	Sí
Konikiewicz & Markowski (2017); Dagnesses (2019)	VyOS / The VyOS Project	1.2.8	Debian	64-bit amd64 (x86-64) Dual core 1 Ghz	512	2 GB	Sí
Sampaio & Bernardino (2017); Iriarte *et al*. (2018)	IPCop / Dafos Training	2.1.9	LFS	cpu i486	64	512 MB	No
Sampaio & Bernardino (2017)	Zentyal / Gesforeda, S.L.	7.0	Ubuntu	64-bit amd64 (x86-64) Dual core 2 GHz	1024	80 GB	Sí
Iriarte *et al*. (2018)	ClearOS / ClearFoundation	7.9.1	CentOS	cpu 64-bit	1024	10 GB	Sí

Continuación Tabla 2: Cortafuegos cuyo desempeño se ha evaluado y reportado en la literatura.

O'Leary (2019)	IPFire / Lightning Wire Labs GmbH	2.27	LFS	cpu (x86-64) 1 GHz	1024	4 GB	Sí
Berbecaru, Lioy & Cameroni (2020)	Zeroshell / Fulvio Ricciardi	3.9.5	LFS Live CD	Pentium (x86-64) 233 MHz	96	32MB	No
Stubbig (2019)	OPNsense / Deciso B.V.	21.7.1	FreeBSD	64-bit amd64 (x86-64) Dual core 1 Ghz	2048	2 GB	Sí

Los cortafuegos IPCop y Zeroshell aunque requieren de escasos recursos computacionales para su funcionamiento, fueron excluidos del análisis porque actualmente carecen de soporte técnico por parte de sus fabricantes, sus últimas actualizaciones fueron liberadas en 2019 y 2021 respectivamente, situación que puede vulnerar su desempeño ante ataques informáticos y comprometer la seguridad de las redes de datos.

2.2. *Ambiente de pruebas*

Para las pruebas realizadas se utilizaron 3 ordenadores físicos. Los *firewalls* fueron instalados en un computador de propósito general con las siguientes características; CPU: Celeron E1400, RAM: 2Gb DDR2, HDD: 500 Gb y 2 NIC (TP-LINK TG-3269): 1000 Mbit/s (WAN y LAN). Se emplearon 2 ordenadores con sistema operativo Ubuntu 20.04 para simular las conexiones establecidas entre un equipo cliente (A) y otro servidor (B), ambos con similares características de hardware: CPU: Core-i5 7500, RAM: 4Gb DDR4, HDD 250 Gb y NIC: 1000 Mbit/s. Las conexiones de red entre los ordenadores y los *firewalls* se realizaron mediante cables de cobre trenzado UTP categoría 5e. La figura 1 describe las características del entorno donde se desarrollaron las pruebas de rendimiento.

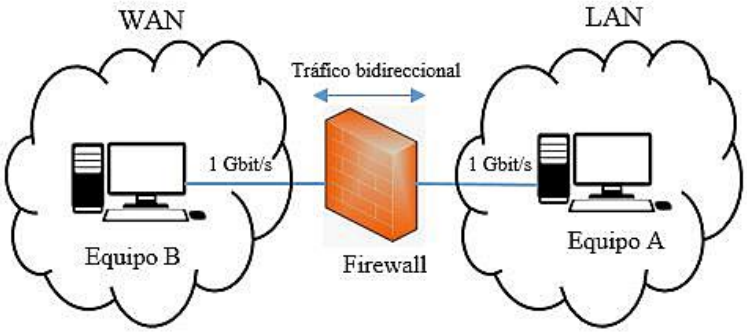

Figura 1: Entorno de pruebas.

Los autores Karim, Vien, Anh Le, & Mapp (2017) plantean que el tráfico de una red con grandes flujos de datos puede simularse combinando la cantidad de paquetes enviados, sus dimensiones e intervalos de tiempo entre cada envío. En correspondencia con los criterios de Karim *et al*. (2017), en esta investigación se realizó el envío de 10000 paquetes de red de 512 bytes cada 1 segundo mediante el protocolo TCP para simular el tráfico de una red empresarial con grandes flujos de datos y generar la mayor carga de trabajo y estrés en los cortafuegos analizados. Se estableció un tamaño de 512 bytes para los paquetes de red porque esta es la dimensión de la trama *Ethernet* (Rafamantanantsoa & Rabetafika, 2018).

Mediante la herramienta iPerf3 se generó el tráfico de red en sentido bidireccional entre los equipos A y B ubicados en 2 subredes distintas simulando una red LAN y WAN respectivamente, ambas divididas por los *firewalls* a evaluar. iPerf3 se ejecutó durante 45 minutos en los ordenadores A y B, permitiendo medir el rendimiento de red de los *firewalls*; simultáneamente al proceso anterior, se monitoreó a través de la herramienta htop su consumo de recursos de hardware.

Rafamantanantsoa & Rabetafika (2018) determinaron que la cantidad de reglas de filtrado implementadas en los cortafuegos incide desfavorablemente en sus índices de desempeño, por tal motivo, y en aras de obtener resultados precisos, fueron implementadas similares reglas de filtrado en cada solución, garantizando la comunicación entre los ordenadores A y B.

3. Resultados

Los autores Mora & Villero (2020) plantean que los *firewalls* además de sus funcionalidades básicas deben ser complementados con un conjunto de herramientas y protocolos de seguridad para incrementar sus capacidades de monitorear y resguardar las redes de datos. Se realizó un análisis de los módulos de filtrado y las diferentes prestaciones de seguridad que brindan los *firewalls* seleccionados, la tabla 2 resume las características de cada solución, la información fue extraída de los sitios oficiales de cada herramienta.

Tabla 3: Funcionalidades de seguridad.

Cortafuego	Módulos para el filtrado de paquetes	Filtrado URL	Antivirus	IDS/IPS	VPN	Filtro de correo	Calidad de Servicio	Administración
Endian	iptables	Sí	Sí	Sí	Sí	Sí	Sí	Web
Zentyal	iptables, libxtables, libnfnetlink	Sí	Sí	Sí	Sí	Sí	Sí	GUI y Web
pfSense	pf	Sí	Sí	Sí	Sí	No	Sí	Web
OPNsense	pf	Sí	Sí	Sí	Sí	Sí	Sí	Web
VyOS	iptables, ipset	Sí	No	No	Sí	No	Sí	Consola
IPFire	iptables, ipset	Sí	Sí	Sí	Sí	Sí	Sí	Web
ClearOS	iptables	Sí	Sí	Sí	Sí	Sí	Sí	Web

Se identificó que los módulos para el filtrado de paquetes de red utilizados en las soluciones analizadas se basan fundamentalmente en pf y Netfilter, en correspondencia con la versión del núcleo y la distribución Linux sobre la que opera cada solución. Se evidenció que Endian, Zentyal, OPNsense, ClearOS e iPFire ofrecen un amplio conjunto de funcionalidades para fortalecer la seguridad de las redes de datos. Aunque en su instalación por defecto VyOS carece de diferentes funciones de seguridad respecto al resto de las soluciones analizadas, estas características pueden ser añadidas desde los repositorios oficiales de Debian; sin embargo, la ausencia de una interfaz gráfica en VyOS puede dificultar la implementación de estas funcionalidades. Se determinó que la mayoría de los

cortafuegos estudiados permiten su administración y configuración mediante una interfaz web, elemento que facilita el trabajo con estas herramientas.

La aplicación de iPerf3 permitió identificar que los cortafuegos analizados mantienen en su mayoría, similares índices de rendimiento de red con una tasa de pérdida de paquetes prácticamente nula en el ambiente de pruebas utilizado, la tabla 3 muestra el rendimiento de red de las soluciones estudiadas.

Tabla 4: Resultados de las pruebas de rendimiento de red.

	Ancho de banda (Mbit/s)			
Cortafuego	Velocidad de envío	Velocidad de recepción	*Jitter* (ms)	Pérdida de paquetes de red (%)
Endian	658	656	0.051	0
Zentyal	728	728	0.021	0
pfSense	686	686	0.045	0.042
OPNsense	336	334	0.097	0.076
VyOS	787	785	0.359	0
IPFire	661	661	0.070	0
ClearOS	658	658	0.059	0

Los resultados anteriores demostraron que VyOS y Zentyal brindan un ancho de banda superior al resto de los cortafuegos estudiados, mientras OPNsense obtuvo los resultados más desfavorables. Se evidenció que pfSense y OPNsense mostraron una ligera pérdida de paquetes de red durante las pruebas realizadas. Xuan, Yang, Dong, & Zhang (2016) determinaron que el consumo de recursos de los dispositivos de seguridad incide significativamente en su correcto funcionamiento. Las figuras 2 y 3 muestran el consumo de CPU y de memoria RAM de los cortafuegos durante las pruebas de rendimiento.

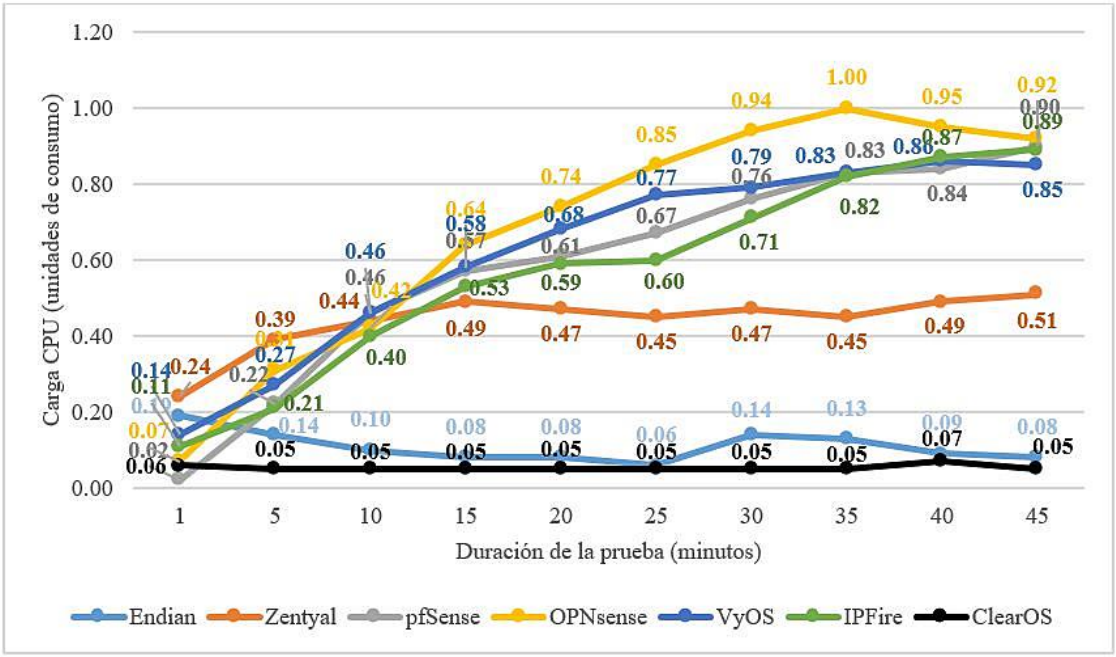

Figura 2: Consumo CPU.

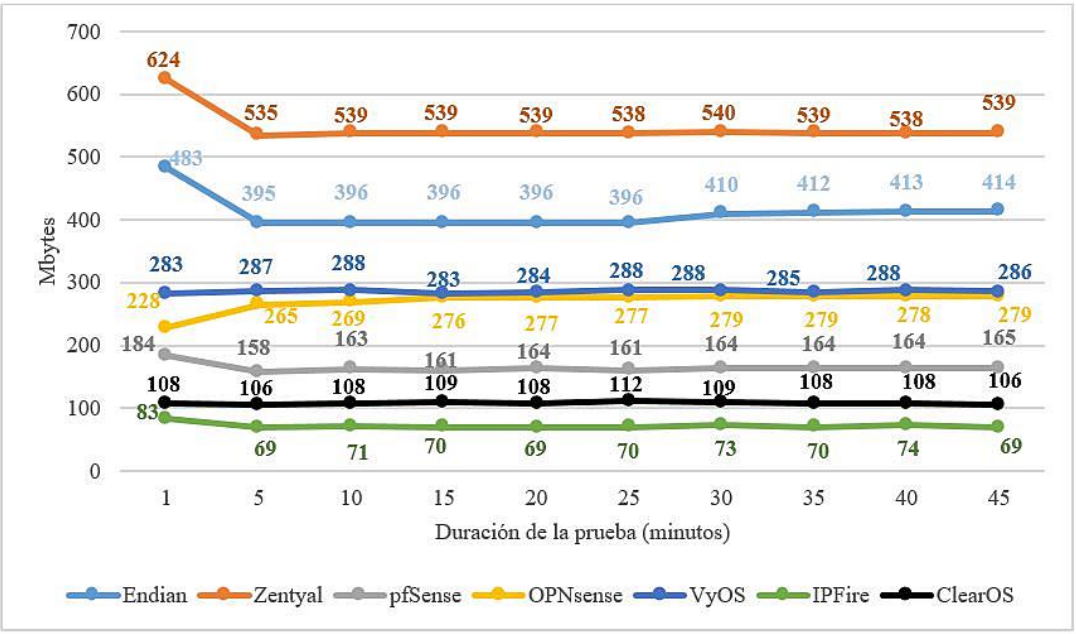

Figura 3: Consumo memoria RAM.

Los resultados derivados de la aplicación de la herramienta htop evidenciaron que las soluciones analizadas mantuvieron un consumo eficiente de recursos de hardware, principalmente de memoria RAM. Respecto a este indicador se identificó que su consumo no sobrepasó el 31% de la memoria RAM disponible en el ordenador donde se implementaron los cortafuegos. ClearOS y Endian mostraron los menores índices de consumo de CPU, mientras IPFire y ClearOS se destacaron por su consumo mínimo de memoria RAM, de manera general, ClearOS demostró los mejores rendimientos de hardware.

4. Discusión

Rafamantanantsoa, Aubert & Haja (2021) determinaron que FreeBSD ofrece mejores indicadores de desempeño para la gestión de redes respecto a otras distribuciones Linux. Sin embargo, los hallazgos obtenidos en la presente investigación evidenciaron que los índices de rendimiento de red y de consumo de CPU y RAM de los cortafuegos pfSense y OPNsense, ambos basados en FreeBSD, fueron superados por ClearOS, solución basada en CentOS. Konikiewicz & Markowski (2017) demostraron que los *firewalls* basados en software son resistentes a diferentes ataques informáticos y poseen similares rendimientos de red respecto a los cortafuegos basados en hardware. Los autores Sampaio & Bernardino (2017) determinaron que pfSense posee mayores funcionalidades de seguridad que IPCop y Zentyal. Por su parte, Iriarte *et al.* (2018) identificaron que ClearOS brinda mejores rendimientos de red que las soluciones IPCop, Endian y Fedora 21 frente ataques DoS.

En este trabajo se evaluaron las funcionalidades de seguridad y los rendimientos de varios cortafuegos basados en software libre. En el análisis realizado no se comprobó el comportamiento de las soluciones abordadas ante ataques informáticos, ni su desempeño respecto a soluciones privativas, estas carencias constituyen limitaciones de la presente investigación.

Sin embargo, los resultados obtenidos evidenciaron que la totalidad de los cortafuegos analizados poseen numerosas funcionalidades orientadas a incrementar la seguridad de las redes de datos, no obstante, pfSense carece de un filtro para asegurar la mensajería electrónica y VyOS requiere de herramientas ajenas a su núcleo de instalación para implementar filtros de correo, antivirus y detección/prevención de intrusiones. En contraposición a los resultados obtenidos por Sampaio & Bernardino (2017), en este trabajo se evidenció que Zentyal supera a pfSense en relación a las funcionalidades de seguridad que poseen ambas soluciones en su núcleo básico de instalación, hallazgo que demuestra el desarrollo y nivel de madurez alcanzado por este cortafuego. En concordancia con los resultados de Iriarte *et al*. (2018), se identificó que ClearOS constituye una solución integral para garantizar la seguridad de las redes de datos, además, este cortafuegos evidenció un rendimiento de red satisfactorio y un consumo de recursos de hardware inferior al resto de las herramientas estudiadas.

Los resultados y las limitaciones de este estudio constituyen una base para investigaciones futuras relacionadas con el despliegue y la efectividad de cortafuegos basados en software libre. Como líneas de trabajo futuro se propone comparar el desempeño de las herramientas abordados en esta investigación respecto a soluciones propietarias y *firewalls* basados en hardware, así como analizar sus comportamientos ante diferentes ataques informáticos.

5. Conclusiones

En la presente investigación se realizó un análisis comparativo de los cortafuegos Endian, Zentyal, pfSense, OPNsense, VyOS, IPFire y ClearOS. Estas herramientas poseen como característica común que son *firewalls* basados en software libre y operan mediante los módulos de filtrado pf y Netfilter, respectivamente. El estudio realizado permitió identificar que las soluciones analizadas brindan un conjunto de funcionalidades que permiten elevar la seguridad de las redes de datos, asimismo se evidenció que Endian, Zentyal, pfSense, VyOS, IPFire y ClearOS poseen rendimientos de red superiores a OPNsense. ClearOS demostró de forma general, los mejores índices de consumo de CPU y memoria RAM, lo cual corroboró su elevada eficiencia para asegurar las redes de datos con ahorro y uso óptimo de recursos de hardware. Los resultados obtenidos en este trabajo facilitan la toma de decisiones para el despliegue de herramientas de ciberseguridad en redes digitales de organizaciones con escasos recursos computacionales.

Conflicto de Interés

El autor declara que no existen conflictos de interés de naturaleza alguna.

Referencias

Agbenyegah, F. K., & Asante, M. (2017). Impact of Firewall on Network Performance. *International Journal of Scientific & Technology Research*, *6*(3), 32-38. Retrieved from: https://www.ijstr.org/final-print/mar2017/Impact-Of-Firewall-On-Network-Performance.pdf

Arunwan, M., Laong, T., & Atthayuwat, K. (2016). Defensive Performance Comparison of Firewall Systems. En *Management and Innovation Technology International Conference (MITicon)*, Bang-San, Thailand, p. 221- 224. https://doi.org/10.1109/MITICON.2016.8025212

Berbecaru, D., Lioy, A., & Cameroni, C. (2020). Supporting Authorize-then-Authenticate for Wi-Fi access based on an electronic identity infrastructure. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *11*(2), 34-54. https://dx.doi.org/10.22667/JOWUA.2020.06.30.034

Buñay, P., Pastor, D., Paguay, P., & Moreno, S. (2019). Análisis de la Arquitectura DIFFSERV sobre redes MPLS para la provisión de QoS en aplicaciones en tiempo real (VoIP). *NOVASINERGIA*, *2*(1), 33-40. https://doi.org/10.37135/unach.ns.001.03.04

Bustamante, S., Valles, M. A., & Levano, D. (2020). Factores que contribuyen en la pérdida de información en las organizaciones. *Revista Cubana de Ciencias Informáticas*, *14*(3), 148-164. Retrieved from: http://scielo.sld.cu/pdf/rcci/v14n3/2227-1899-rcci-14-03-148.pdf

Cheminod, M., Durante, L., Seno, L., & Valenzano, A. (2018). Performance evaluation and modeling of an industrial application-layer firewall. *IEEE Transactions on Industrial Informatics*, 14(5), 2159-2170. https://doi.org/10.1109/TII.2018.2802903

Cotret, P., Gogniat, G., & Sepúlveda, M. J. (2016). Protection of heterogeneous architectures on FPGAs: An approach based on hardware firewalls. *Microprocessors and Microsystems*, 42, 124-141. https://doi.org/10.1016/j.micpro.2016.01.013

Dagnesses, D. (2019). Experiencia en la utilización de la Distribución GNU/Linux VyOS como software para PC-routers en una institución de Salud. *Revista Cubana de Informática Médica*, *11*(2), 36-47. Retrieved from: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1684-18592019000200036

Eset Security (2021). *Eset Security Report Latinoamérica 2021*. Retrieved from https://www.welivesecurity.com/wp-content/uploads/2021/06/ESET-security-report-LATAM2021.pdf

World Economic Forum (2020). *The Global Risks Report 2020 15th Edition*. Retrieved from: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

Iriarte, A., Velarde, P., Aguirre, A., Mena, L. J., Martínez, R., & Ochoa, A. M. (2018). Evaluación de firewalls basados en software libre. *Pistas Educativas*, *40*(130), 625-637. Retrieved from: http://www.itc.mx/ojs/index.php/pistas/article/view/1738

Karim, I.; Vien, Q. T.; Anh Le, T.; Mapp, G. (2017). A Comparative Experimental Design and Performance Analysis of Snort-Based Intrusion Detection System in Practical Computer networks. *Computers, 6*(1), 1-15. https://doi.org/10.3390/computers6010006

Konikiewicz, W., & Markowski, M. (2017). Analysis of performance and efficiency of hardware and software firewalls. *Journal of Applied Computer Science Methods*, *9*(1), 49-63. https://doi.org/10.1515/jacsm-2017-0003

Lee, J. K., Kim, S. J., Park, C. Y., & Woo, J. (2015). Performance Evaluation and Analysis of Network Firewalls in High Speed Networks. *Indian Journal of Science and Technology*, *8*(25). https://dx.doi.org/10.17485/ijst/2015/v8i25/80825

Logroño, E. (2017). *Análisis de los servicios Cloud Computing para una gestión empresarial eficaz*, (Tesis de Maestría en Redes de Comunicación), Pontificia Universidad Católica de Ecuador. Retrieved from: http://repositorio.puce.edu.ec/handle/22000/14419

Mora, E. F., & Villero, S. L. (2020). Importancia de la implementación de firewall en redes empresariales como mecanismo para la protección de información. *Ciencia e Ingeniería*, *7*(1), 28-35. Retrieved from: http://revistas.uniguajira.edu.co/rev/index.php/cei/article/view/202

Morales, F., Toapanta, S., & Toasa, R. M. (2020). Implementación de un sistema de seguridad perimetral como estrategia de seguridad de la información. *Revista Ibérica de Sistemas e Tecnologias de Informação*, (E27), 553-565. Retrieved from: https://www.proquest.com/openview/35d3af032ceee8d79daf8a813e2c7967/1?pq-origsite=gscholar&cbl=1006393

Neupane, K., Haddad, R., & Chen, L. (2018). Next Generation Firewall for Network Security: A Survey. En *SoutheastCon 2018*, St. Petersburg, FL, EE.UU. https://doi.org/10.1109/SECON.2018.8478973

O'Leary M. (2019) Firewalls. En *Cyber Operations*. Apress, Berkeley, CA, p. 857-896. https://doi.org/10.1007/978-1-4842-4294-0_17

Perdigón, R., & Pérez, M. T. (2020). Análisis holístico del impacto social de los negocios electrónicos en América Latina, de 2014 a 2019. *Paakat: Revista de Tecnología y Sociedad*, *10*(18). http://dx.doi.org/10.32870/Pk.a10n18.459

Perdigón, R., & Ramírez, R. (2020). Plataformas de software libre para la virtualización de servidores en pequeñas y medianas empresas cubanas. *Revista Cubana de Ciencias Informáticas*, *14*(1), 40-57. Retrieved from: http://scielo.sld.cu/pdf/rcci/v14n1/2227-1899-rcci-14-01-40.pdf

Putra, C. A., Vita, Y., & Saputra, W. S. J. (2018). Point to Point Protocol Tunneling VPN Simulation and Analysis on Sniffing. En *International Conference on Science and Technology (ICST 2018)*, 1094-1097. https://doi.org/10.2991/icst-18.2018.220

Rafamantanantsoa, F., Aubert, R.C., & Haja, R. L. (2021) Analysis and Evaluation of MPLS Network Performance. *Communications and Network*, *13*(1), 25-35. https://doi.org/10.4236/cn.2021.131003

Rafamantanantsoa, F., & Rabetafika, H. L. (2018). Performance Comparison and Simulink Model of Firewall Free BSD and Linux. *Communications and Network*, *10*(4), 180-195. https://doi.org/10.4236/cn.2018.104015

Sampaio, D., & Bernardino, J. (2017). Evaluation of Firewall Open Source Software. En: *Proceedings of the 13th International Conference on Web Information Systems and Technologies – WEBIST*, p. 356-362, Porto, Portugal. https://doi.org/10.5220/0006361203560362

Shahsavari, Y., Shahhoseini, H., Zhang, K., & Elbiaze, H. (2019). A Theoretical Model for Analysis of Firewalls Under Bursty Traffic Flows. *IEEE Access*, 7, 183311-183321. https://doi.org/10.1109/ACCESS.2019.2926925

Stubbig, M. (2019). *Practical OPNsense. Building Enterprise Firewall with Open Source*. Norderstedt, Alemania: BoD. Retrieved from: https://www.bod.de/buchshop/practical-opnsense-markus-stubbig-9783754302569

Togay, C., Kasif, A., Catal, C., & Tekinerdogan, B. (2021). A Firewall Policy Anomaly Detection Framework for Reliable Network Security. *IEEE Transactions on Reliability*, 1-9. https://doi.org/10.1109/TR.2021.3089511

Xuan, S., Yang, W., Dong, H., & Zhang, J. (2016) Performance Evaluation Model for Application Layer Firewalls. *PLoS ONE*, *11*(11): e0167280. https://doi.org/10.1371/journal.pone.0167280

Zare, H., Olsen, P., Zare, M.J., & Azadi, M. (2018). Operating System Security Management and Ease of Implementation (Passwords, Firewalls and Antivirus). En: Latifi S. (eds) *15th International Conference on Information Technology: New Generations, ITNG 2018. Advances in Intelligent Systems and Computing*, vol 738. Springer, Cham. https://doi.org/10.1007/978-3-319-77028-4_98