Análisis comparativo de Gestión Unificada de Amenazas (UTM) de código abierto para fortalecer la seguridad de la información en las PYMES

Comparative analysis of an Open-Source Unified Threat Management (UTM) to strengthen information security in SMEs

Carlos Camacho, Daniel Núñez-Agurto
Departamento de Ciencias de la Computación, Universidad de las Fuerzas Armadas - ESPE, 230102, Santo Domingo de los Tsáchilas, Ecuador
cscamacho2@espe.edu.ec, adnunez1@espe.edu.ec

Resumen

En la actualidad, las PYMES se encuentran conectadas a Internet exponiendo su información y aplicaciones a diferentes tipos de ataques, que pueden ser ejecutados a través de malware, spyware, accesos no autorizados y diversas combinaciones de amenazas externas e internas. En la mayoría de los casos no implementan sistemas de seguridad por los altos costos en licenciamiento. Una alternativa para contrarrestar estas amenazas es la implementación de sistemas UTM Open-Source. Sin embargo, existen varias soluciones de UTMs Open-Source, y debido a la variedad y enfoque de los estudios comparativos disponibles, se dificulta determinar de manera objetiva la mejor opción que se ajuste a las necesidades de seguridad de las PYMES. Por lo tanto, la presente investigación busca realizar un análisis comparativo de un UTM Open-Source, para fortalecer la seguridad de la información en las PYMES. A partir de la revisión sistemática de literatura de la documentación y de proyectos desarrollados sobre la implementación de los UTM Open-Source, se determinaron los tres UTMs Open-Source con mejores prestaciones de seguridad. Se desarrolló un entorno de pruebas controlado para analizar el funcionamiento de los servicios bajo diferentes tipos de ataques, como la descarga de archivos maliciosos, escaneo de puertos y vulnerabilidades. Los resultados obtenidos determinaron que el UTM Open-Source Endian obtuvo los mejores resultados.

Palabras Claves: Antivirus; Firewall; Open-Source; Proxy; UTM.

Abstract

SMEs are currently connected to the Internet, exposing their information and applications to different types of attacks, which can be executed through malware, spyware, unauthorized access, and various combinations of external and internal threats. They do not implement security systems in most cases due to high licensing costs. An alternative to counteract these threats is the implementation of Open-Source UTM systems. However, there are several Open-Source UTM solutions. Due to the variety and focus of the available comparative studies, it is difficult to objectively determine the best option that fits the security needs of SMEs. Therefore, this research seeks to perform a comparative analysis of an Open-Source UTM to strengthen information security in SMEs. From the systematic literature review of the documentation and projects developed on the implementation of Open-Source UTMs, the three Open-Source UTMs with the best security performance were determined. A controlled test environment was developed to analyze the performance of the services under different types of attacks such as downloading malicious files, port scanning, and vulnerabilities. The results obtained determined that the Open-Source Endian UTM obtained the best results.

Keywords: Antivirus; Firewall; Open-Source; Proxy; UTM.

Fecha de Recepción: 31/10/2021 - Aceptado: 15/12/2021 – Publicado: 31/12/2021
ISSN: 2477-9253 – DOI: https://dx.doi.org/10.24133/RCSD.VOL06.N04.2021.05

I. Introducción

La seguridad de la información es uno de los aspectos más importantes en una organización, debido a que garantiza la disponibilidad, integridad y confidencialidad de la información. Esto se logra mediante la aplicación de un conjunto de controles, que son seleccionados a través del proceso de gestión de riesgos y gestionados mediante un sistema de gestión de la seguridad de la información (SGSI) (ISO/IEC 27000, 2018). La gestión de la seguridad tiene como objetivo garantizar la protección de la información en las redes y sus instalaciones de procesamiento. Para la gestión de la seguridad existen sistemas como los firewalls, los cuales tienen la capacidad de inspeccionar los paquetes entrantes o salientes de la red a nivel de la capa de aplicación, y realizar operaciones para comprobar, permitir o denegar el tráfico de la red (Senthilkumar & Muthukumar, 2018). Además, pueden aplicar controles de seguridad para garantizar la protección de los servicios conectados contra el acceso no autorizado (ISO/IEC 27002, 2013).

En la actualidad, el uso del Internet es indispensable para la operatividad de las PYMES, por ende, sus sistemas de información están expuestos a diferentes tipos de ataques. Estos ataques pueden ser ejecutados a través de malware, spyware, accesos no autorizados, robos de contraseñas y combinaciones de amenazas externas e internas.

Para minimizar el riesgo a estas amenazas existe la Gestión Unificada de Amenazas (Unified Threat Management, UTM). Estos son dispositivos de seguridad con una combinación de hardware, software y tecnologías de red cuyo objetivo principal es realizar múltiples funciones de seguridad (Qi et al., 2007). Los sistemas UTM Open-Source ofrecen varios servicios de seguridad como antivirus, firewall, IDS, IPS, servidor proxy, servidor DHCP (Hamid et al., 2016). Además, pueden ser implementados para uso doméstico o entornos de trabajo como las PYMES.

En el estudio propuesto por (Pablo & Loor, 2017), se realizó la recopilación de información haciendo uso de herramientas, tales como encuestas, fichas de observación y entrevistas; y escogieron tres sistemas de firewall, los cuales fueron IpFire, pfSense y Untangle. Mediante un estudio comparativo determinaron que pfSense es el más adecuado para los requisitos de la universidad ESPAM MFL. Los autores (Fuertes et al., 2014), en su proyecto "Repowering an Open Source Firewall Based on a Quantitative Evaluation", realizaron un análisis de varios Firewalls Open-Source. Establecieron varios tipos de ataques para obtener resultados con respecto a la evaluación del desempeño, consumo de CPU y memoria de los sistemas de firewall. Ellos determinaron que ClearOS obtuvo los mejores resultados en optimización de memoria RAM y mejor desempeño ante actividades sospechosas de red. En el trabajo propuesto por (Arunwan et al., 2016), se realizó la comparación del rendimiento de detección de ataques entre dos firewalls Endian y pfSense. En los escenarios de ataque se incluyen el escaneo de puertos, ping de la muerte, inundación y ataque de contraseña en diferentes condiciones. Además, determinaron que Endian podría ser el adecuado para pequeñas empresas. En el trabajo de (Iriarte Solís et al., 2018), se evalúan firewalls Open-Source con las características que permitan integrarse en escenarios de pruebas, en la cual se estudiaron, evaluaron y analizaron diversos entornos de red y escenarios de ataque. Las distribuciones que revisaron fueron IPCop, Endian, ClearOS y Fedora. Los resultados revelaron a ClearOS con buena respuesta en la defensa de los ataques. En el trabajo de (León Casas, 2016) se analizó las capacidades de protección de las soluciones UTM de Open-Source Endian Firewall Community, Sophos UTM Home Edition y Untangle NG Firewall. Se desarrollaron diferentes escenarios para simular las amenazas básicas y avanzadas, y se determinó que Sophos obtuvo los mejores resultados en las pruebas realizadas.

Los UTMs Open-Source son una alternativa para fortalecer la seguridad de la información en una PYME. Sin embargo, al existir varias opciones y diferentes estudios comparativos entre algunos UTMs Open-

Source, se dificulta determinar el mejor UTM, para implementar en una PYME. Por esta razón, se debería realizar la selección de los UTMs Open-Source más utilizados, mediante una evaluación basada en sus características, documentación, estudios realizados y el soporte a sus distribuciones. De esta manera podrían ser puestos a prueba en diferentes escenarios de ataques, con el propósito de determinar qué UTM Open-Source presenta las mejores características en seguridad y desempeño.

Sobre la base de la revisión sistemática realizada, se determinó que pfSense, Endian y ClearOS obtuvieron los mejores resultados en las diferentes pruebas realizadas. Sin embargo, no se encontró ninguna investigación en la que se haya puesto a prueba los tres UTM Open-Source. Por esta razón se han seleccionado estos tres UTM Open-source para ser implementados y puestos a prueba en diferentes escenarios de ataques.

El presente artículo tiene como objetivo realizar un análisis comparativo de UTMs Open-Source, para fortalecer la seguridad de la información en las PYMES. Por lo tanto, se realizó la selección de tres UTM Open-Source más utilizados, mediante una evaluación basada en sus características, documentación, estudios realizados y el soporte a sus distribuciones. Los UTMs seleccionados serán puestos a prueba en diferentes escenarios de ataques, con el propósito de determinar cuál UTM Open-Source tiene los mejores resultados de seguridad y desempeño.

El resto de este documento se organiza como sigue. La sección II describe los materiales y métodos combinados. La sección III describe los resultados y discusión sobre las pruebas realizadas a los UTM open-source. La sección IV termina con las conclusiones y describe las líneas de trabajo futuro.

II. Materiales y Métodos

2.1. Entorno de pruebas

El proceso de virtualización permite hacer que un solo recurso físico, como un servidor, un dispositivo de almacenamiento o un sistema operativo, se utilice como múltiples recursos virtuales, y que varios recursos se utilicen como un único recurso virtual (Ma et al., 2012) (Santoso et al., 2014). Para la creación de los escenarios de ataque se utilizaron máquinas virtuales (MVs), mediante la plataforma Virtual Box. En total se desplegaron seis máquinas virtuales, donde cada una desempeña su rol dentro del entorno de pruebas. Basándose en los antecedentes investigativos se han seleccionado pfSense, Endian y ClearOS para ser implementados y puestos a prueba en diferentes escenarios de ataques.

2.1.1 pfSense

PfSense es una distribución de firewall gratuita, basada en el sistema operativo FreeBSD, con el soporte de paquetes gratuitos de terceros. Puede integrar funciones adicionales y ofrecer las mismas funcionalidades de los firewalls comerciales. El firewall pfSense incluye una interfaz web, que se utiliza en la configuración de todos los componentes. Por lo tanto, no es necesario tener conocimientos de UNIX, no se utiliza la línea de comandos y no es necesario editar manualmente ningún conjunto de reglas (pfSense, 2021).

2.1.2 Endian

Endian Firewall Community (EFW) es un producto de software de seguridad basado en Linux. Se trata de una solución de Gestión Unificada de Amenazas (UTM) con todas las funciones de seguridad. Cuenta con una interfaz web, que se utiliza en la configuración de todos los servicios. Endian Community está pensado para simplificar la estabilidad y contribuir en la defensa de las redes domésticas usando el poder del código abierto (Endian, 2021).

2.1.3 ClearOS

ClearOS 7 Community Edition es un sistema operativo de servidor Linux Open-Source. Esta edición está diseñada para expertos en Linux y aficionados que disfrutan del código de vanguardia. Todas las actualizaciones, correcciones de errores, parches y correcciones de seguridad se proporcionan de forma gratuita, aunque no probada, desde fuentes originales. Las características abarcan más de 75 funciones de TI desde control de dominio, control de red y ancho de banda, mensajería y más, para la configuración de los servicios cuenta con una interfaz web (ClearOS, 2021).

2.2. Topología de la red

En la Figura 1 se muestra la topología de red del entorno de pruebas. La topología está basada en la red básica de una PYME. Los UTMs Open-Source están configurados con una red WAN, LAN y DMZ. En la red LAN se encuentra una VM con el sistema operativo Ubuntu Desktop y en la red DMZ se implementó un servidor web sobre Ubuntu server. Todo el tráfico que venga desde la WAN hacia las redes internas será filtrado por el UTM. La VM con Kali Linux realiza el escaneo de puertos y vulnerabilidades hacia el UTM. La VM de la red LAN se utiliza para descargar de archivos maliciosos.

Así mismo, los UTM Open-Source se instalaron en diferentes máquinas virtuales, para realizar una comparación equitativa. Se asignaron iguales características de hardware a las tres máquinas virtuales con similares ajustes. Además, se configuraron los siguientes servicios en común en los tres UTMs: 1) Antivirus; 2) Servidor DHCP; 3) IDS/IPS; 4) Servidor Proxy.

Los parámetros del antivirus fueron configurados para pfSense, Endian y ClearOS respectivamente. Los antivirus que utilizan estos UTM están basados en un antivirus Open-Source llamado ClamAV. De igual manera, se configuraron los parámetros tanto para la instalación del IPS/IDS en pfSense, Endian y ClearOS, así como para la instalación del servidor Proxy en pfSense, Endian y ClearOS respectivamente.

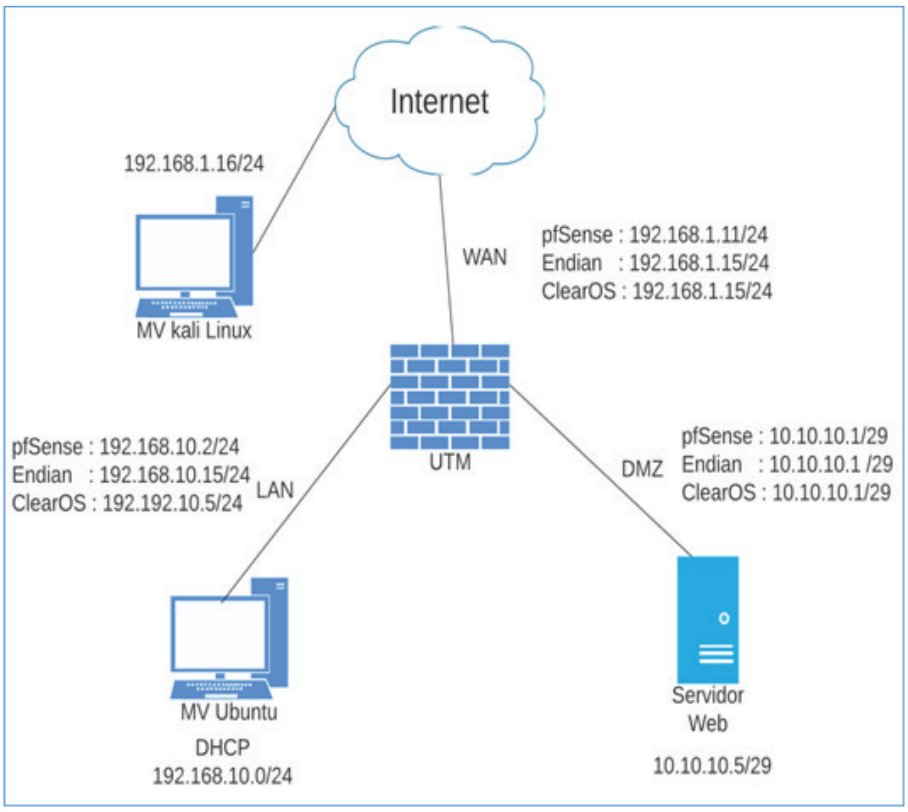

Figura 1: Topología de red para el entorno de pruebas

2.3. Configuración de las máquinas virtuales

En la Tabla 1 se muestran las características de configuración de las máquinas virtuales para la implementación del entorno de pruebas.

Se instaló el sistema operativo Kali Linux versión 2021.2 en la máquina con el rol de atacante. Para el escaneo de los puertos abiertos se utilizó la herramienta Nmap. Para el escaneo de vulnerabilidades al UTM Open-Source y el servidor web, se utilizó la herramienta Nessus.

En la MV del servidor web se instaló el sistema operativo Ubuntu Server versión 20.04.1 LTS, además, se instaló y configuró Apache web server versión 2.4.41 y se lo asignó en la red DMZ. En la máquina virtual asignada a la red LAN se instaló el sistema operativo Ubuntu Desktop versión 20.04.2; en esta MV se realizaron las pruebas sobre descarga de archivos maliciosos, con el uso de las herramientas web EICAR Test y HTTP Evader.

Tabla 1: Configuración de las MVs para los UTM Open-Source

Máquinas Virtuales	Configuración
pfSense Community Edition (version 2.5.2) Endian Firewall Community (version 3.3.2) ClearOS 7 Community Edition (versión 7.2.0)	3 GB de Memoria RAM. 2 procesadores. 3 particiones, cada una de 16 GB. 3 adaptadores de red, una en adaptador puente (WAN) y los otros en red interna (DMZ, LAN).
Kali Linux versión 2021.2	2 GB de Memoria RAM. 1 procesador. 1 partición de 16 GB. 1 adaptador puente (WAN).
Ubuntu Server versión 20.04.1 LTS	1 GB de Memoria RAM. 1 procesador. 1 partición de 10 GB. 1 adaptador de red en red interna (DMZ).
Ubuntu Desktop versión 20.04.2	1,5 GB de Memoria RAM. 1 procesador. 1 partición de 10 GB. 1 adaptador de red en red interna (LAN).

2.4. UTM Open-Source

La Tabla 2 presenta una comparación entre los servicios que ofrecen pfSense Community Edition, Endian Firewall Community y ClearOS 7 Community Edition.

Tabla 2: Matriz comparativa entre los UTM opens source

Servicios	pfSense Community Edition (versión 2.5.2)	Endian Firewall Community (versión 3.3.2)	ClearOS 7 Community Edition (versión 7.2.0)
Servidor DNS	X	X	X
Servidor DHCP	X	X	X
VPN (IPsec y OpenVPN)	X	X	X
Balanceo de carga NAT	X	X	X
Tabla de estado	X	X	X
Proxy	X	X	X
Enrutamiento	X	X	
IP virtuales	X		
Portal cautivo	X		
Filtrado web	X	X	X
IPS	X	X	X
IDS	X	X	X
AntiSpam	X	X	X
Antivirus	X	X	X
Antiphishing			X
Servidor PPPoE	X		
Control de usuarios	X		X
Servidor SNMP		X	
Spyware	X		X

2.5. Definición de ataques

Se realizó un escaneo de vulnerabilidades y de puertos, además, se utilizó la herramienta web de EICAR Test y HTTP Evader para descargar archivos maliciosos para probar la funcionalidad del antivirus de cada UTM.

2.5.1 Escaneo de vulnerabilidades

En el escaneo de vulnerabilidades se utilizó Nessus Essentials (Nessus Essentials, 2019). Esta herramienta permite escanear hasta 16 direcciones IP por escáner, con la misma velocidad, evaluaciones y comodidad de escaneo que las versiones de pago. Cuando termina un escaneo, la herramienta separa las vulnerabilidades en los siguientes tipos: crítico, alto, medio, bajo e informativo, y muestra los detalles de cada vulnerabilidad. En la VM Kali Linux se instaló Nessus Essentials versión 8.15, para realizar un escaneo avanzado y un escaneo web hacia los UTMs.

2.5.2 Escaneo de puertos

Para el escaneo de puertos se utilizó nmap, esta herramienta permite hacer un escáner y obtener información sobre los puertos de un destino en específico (KALI, 2021). Desde la VM Kali Linux, se realizó el escaneo de puertos hacia los UTMs.

El comando utilizado para el escaneo de puertos fue el siguiente:

nmap -sS-SV-PN-P 1-65535-r-w ipDestino

En donde:

- SS: Es un escaneo de tipo SYN, que envía un paquete SYN como si fuese a abrir una conexión real, marca el puerto como abierto si recibe un SYN/ACK, como cerrado si recibe un RST, o como filtrado si después de varios intentos no recibe respuesta alguna o recibe un ICMP unreachable error.
- SV: Es un escaneo de servicio, para intentar adivinar el servicio detrás de cada puerto abierto.
- PN: Forzar escaneo, para no comprobar si el host responde a ping o no.
- p 1-65536: Se comprueba todos los puertos del sistema.
- r: Se comprueba los puertos de forma consecutiva.
- w. Aumenta el nivel de información mostrada por pantalla.

2.5.3 Descarga de archivos maliciosos

EICAR Test es una herramienta web que permite probar la funcionalidad del antivirus. En la página web de EICAR hay cuatro archivos que se pueden descargar, con las extensiones .com, .com.txt, .zip (EICAR, 2006). HTTP Evader es una herramienta web que permite probar vulnerabilidades de los UTMs (HTTP Evader, 2015). En la página web oficial de HTTP Evader se puede realizar la descarga automática de malware. Al terminar este proceso, la misma página devuelve los resultados sobre el funcionamiento del UTM.

Las herramientas EICAR Test y HTTP Evader, se utilizaron para la descarga de archivos maliciosos. Con la VM de Ubuntu conectada a la red LAN se ingresa a la página web de EICAR y se intenta descargar los archivos en los cuatro formatos para realizar las pruebas con HTTP Evader, se debe ingresar a la página oficial y realizar la prueba de vulnerabilidad del UTM.

III. Evaluación de Resultados y Discusión

El objetivo de las pruebas ha sido comparar el rendimiento de las capacidades de protección de los tres UTMs frente a las amenazas, empleando los escenarios propuestos en la sección anterior.

Una de las ventajas de los UTMs es la existencia de un punto central de gestión de todas las funciones de seguridad, que están integradas en una única plataforma. Por este motivo, y ya que son soluciones de seguridad para PYMES, se ha valorado la facilidad de uso y configuración de dichas funcionalidades. Por lo tanto, a través de la interfaz web se configuró las comunicaciones para permitir los flujos de información y la activación de los mecanismos de seguridad utilizando la política más restrictiva. A continuación, se detallan los resultados obtenidos para cada uno de los ataques propuestos en la sección previa.

3.1. Uso de la herramienta Nessus

Es importante realizar un escaneo avanzado de vulnerabilidades hacia los hosts de los UTM. Los resultados obtenidos tras el escaneo avanzado de vulnerabilidades con la herramienta Nessus se muestran en la Tabla 3. En los resultados de los UTMs pfSense y Endian se detectaron 13 vulnerabilidades de tipo informativo, en el UTM ClearOS se detectaron 18 vulnerabilidades de tipo informativo y una vulnerabilidad de tipo media.

De igual manera, se realizó un escaneo web hacia los hosts de los UTMs. Los resultados obtenidos tras el escaneo web se pueden observar en la Tabla 4. Los resultados obtenidos sobre los UTMs pfSense y Endian, detectaron 17 vulnerabilidades de tipo informativo, en el UTM ClearOS se detectaron 17 vulnerabilidades de tipo informativo y 2 vulnerabilidades de tipo media.

Tabla 3: Escaneo avanzado de vulnerabilidades hacia los hosts de los UTM

UTM	Vulnerabilidades
pfSense Community Edition (versión 2.5.2)	13 del tipo informativo.
Endian Firewall Community (versión 3.3.2)	13 del tipo informativo.
ClearOS 7 Community Edition (versión 7.2.0)	18 del tipo informativo. 1 del tipo media.

Tabla 4: Escaneo web de vulnerabilidades hacia los hosts de los UTM

UTM	Vulnerabilidades
pfSense Community Edition (versión 2.5.2)	17 del tipo informativo.
Endian Firewall Community (versión 3.3.2)	17 del tipo informativo.
ClearOS 7 Community Edition (versión 7.2.0)	17 del tipo informativo. 2 de tipo media.

3.2. Escaneo de puertos con nmap

El escaneo de puertos hacia los hosts y los UTMs, se lo realizó con la herramienta nmap. Los resultados obtenidos con nmap, se muestran en la Tabla 5. En los resultados se observa que los UTMs pfSense y Endian, tienen el puerto 80 abierto con el servicio HTTP en la versión Apache HTTPD 2.4.41 (Ubuntu). En el UTM ClearOS se detectaron dos puertos abiertos, el puerto 80 con servicio HTTP en la versión Apache HTTPD 2.4.41 (Ubuntu), y el puerto 81 con servicio SSL/HTTP con la versión Apache HTTPD 2.4.6 (ClearOS) Open SSL/1.

Tabla 5: Escaneo de puertos con nmap

UTM	Puerto	Estado	Servicio	Versión
pfSense Community Edition (versión 2.5.2)	80	Abierto.	http	Apache httpd 2.4.41 ((Ubuntu)).
Endian Firewall Community (versión 3.3.2)	80	Abierto.	http	Apache httpd 2.4.41 ((Ubuntu)).
ClearOS 7 Community Edition (versión 7.2.0)	80	Abierto.	http	Apache httpd 2.4.41 ((Ubuntu)).
	81	Abierto.	ssl/http	Apache httpd 2.4.6 ((ClearOS) Open SSL/1.

3.3. Evaluación de las pruebas de escaneo puertos y vulnerabilidades

En resumen, la Tabla 6 presenta los resultados obtenidos en las pruebas de escaneo anteriormente mostradas. Se determinó que pfSense y Endian obtuvieron resultados similares. Además se demuestra que son los menos vulnerables en comparación con ClearOS, el cual obtuvo resultados menos favorables en las tres pruebas.

Tabla 6: Resultados de las pruebas de escaneo

Prueba	pfSense Community Edition (versión 2.5.2)	Endian Firewall Community (versión 3.3.2)	ClearOS 7 Community Edition (versión 7.2.0)
Escaneo avanzado	Menos vulnerable	Menos vulnerable	Mas vulnerable
Escaneo web	Menos vulnerable	Menos vulnerable	Mas vulnerable
Escaneo de puertos	Menos vulnerable	Menos vulnerable	Mas vulnerable

3.4. Descarga de archivos maliciosos con EICAR Test

La descarga de archivos maliciosos se la realizó con la herramienta EICAR Test, para poner a prueba el funcionamiento del Antivirus en cada UTM; los resultados obtenidos de la descarga de archivos maliciosos se muestran en la Tabla 7. Los UTMs pfSense y Endian bloquearon la descarga de todos los archivos maliciosos. Sin embargo, el UTM ClearOS no bloqueó las descargas de los archivos maliciosos.

Tabla 7: Descarga de archivos con EICAR test

Archivos de prueba	pfSense Community Edition (versión 2.5.2)	Endian Firewall Community (versión 3.3.2)	ClearOS 7 Community Edition (versión 7.2.0)
eicar.com	Bloqueado.	Bloqueado.	No bloqueado.
eicar.com.txt	Bloqueado.	Bloqueado.	No bloqueado.
eicar_com.zip	Bloqueado.	Bloqueado.	No bloqueado.
eicarcom2.zip	Bloqueado.	Bloqueado.	No bloqueado.

3.5. Pruebas de evasión de firewall con HTTP Evader

Las pruebas de evasión fueron realizadas con el uso del sitio web HTTP Evader, para detectar evasiones de archivos maliciosos. Los resultados obtenidos con HTTP Evader se muestran en la Figura 2. El UTM pfSense obtuvo 55 evasiones con el protocolo HTTP y HTTPS, el UTM Endian obtuvo 21 evasiones con el protocolo HTTP y HTTPS, el UTM ClearOS obtuvo 23 evasiones con HTTP. No obstante, con el protocolo HTTPS no se obtuvo resultados porque el UTM ClearOS bloquea el sitio web donde se realiza la prueba de evasiones.

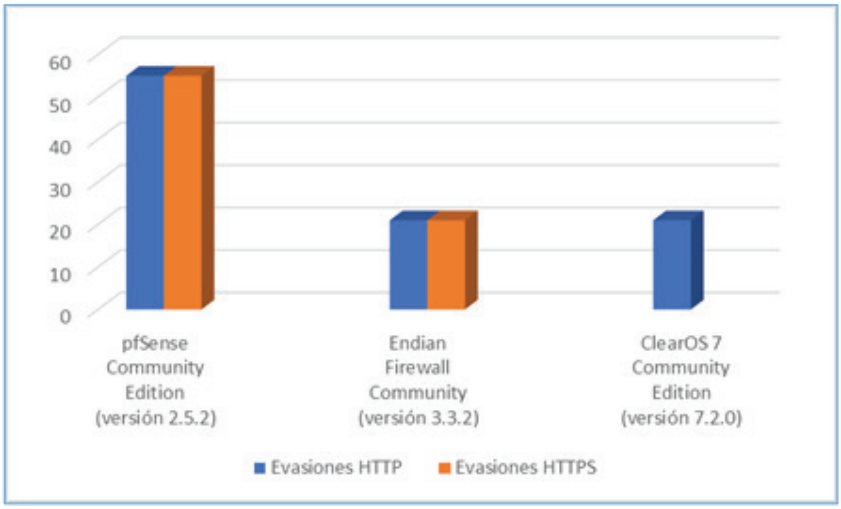

Figura 2: Evasiones con HTTP Evader

3.6. Evaluación de las pruebas con EICAR Test y HTTP Evader

En resumen, la Tabla 8 presenta los resultados obtenidos en las pruebas anteriormente expuestos. Endian y pfSense obtuvieron resultados iguales y favorables en la prueba con EICAR Test. Sin embargo, con la prueba de HTTP Evader, se determina que Endian tiene mejor rendimiento en la protección contra amenazas en comparación con ClearOS y pfSense.

Tabla 8: Resultados de las pruebas con EICAR Test y HTTP Evader

Prueba	pfSense Community Edition (versión 2.5.2)	Endian Firewall Community (versión 3.3.2)	ClearOS 7 Community Edition (versión 7.2.0)
EICAR Test	Mejor rendimiento	Mejor rendimiento	Menor rendimiento
HTTP Evader	Menor rendimiento	Mejor rendimiento	-

3.7. Discusión

Los resultados obtenidos de la presente investigación muestran que los UTMs Open-source pfSense y Endian obtuvieron los mismos resultados en las pruebas de escaneo de vulnerabilidades de tipo web y avanzado. Lo mismo sucede con el escaneo de puertos y con el uso EICAR Test. En los resultados obtenidos con la herramienta HTTP Evader, Endian es el UTM Open-Source que obtiene los mejores resultados en comparación con pfSense y ClearOS. De las cinco pruebas realizadas, en cuatro de ellas Endian y pfSense tienen los mejores resultados. Sin embargo, Endian demuestra mejores resultados en la prueba de HTTP Evader. Con los resultados obtenidos en este proyecto, se llegó a una conclusión similar al trabajo de (Arunwan et al., 2016) donde concluyen que Endian podría ser utilizado en pequeñas empresas. En los trabajos de (Iriarte Solís et al., 2018) y (Fuertes

et al., 2014), los resultados difieren porque determinaron que ClearOS es el UTM Open-Source que mejores resultados obtuvo en diferentes pruebas.

IV. Conclusiones y Trabajo Futuro

Con la revisión sistemática de literatura de la documentación y de proyectos desarrollados sobre la implementación de los UTM Open-Source, se determinaron las tres mejores soluciones.

Se realizó el análisis comparativo de tres UTM Open-Source, donde se determinó que el UTM Open-Source con los mejores resultados en estas pruebas fue Endian. Durante la fase de pruebas, los resultados demostraron que pfSense y Endian son los más efectivos para la protección de una red. Sin embargo, Endian sobresalió en una prueba, la cual consistió en la descarga de archivos maliciosos.

Se implementaron tres UTM Open-Source y se configuraron los mismos servicios e interfaces de red. No se presentaron problemas en el desarrollo de las pruebas realizadas hacia la red de pfSense y Endian. Sin embargo, en la prueba con HTTP Evader, ClearOS bloqueó las direcciones web que se utilizan para realizar esta prueba. No obstante, el sitio web de HTTP Evader proporcionó una dirección web adicional con el protocolo HTTP. Debido a este inconveniente no se obtuvieron resultados de este ataque con el protocolo https en ClearOS. Además, se demostró la potencialidad de implementar un sistema UTM Open-Source y sus beneficios.

Como trabajo futuro de la presente investigación, se planea realizar la implementación en un entorno de pruebas real, con el propósito de validar los resultados obtenidos en este entorno de pruebas.

Referencias Bibliográficas

Arunwan, M., Laong, T., & Atthayuwat, K. (2016). Defensive performance comparison of firewall systems. 2016 Management and Innovation Technology International Conference, MITiCON 2016, MIT221–MIT224. https://doi.org/10.1109/MITICON.2016.8025212

EICAR. (2006). ANTI MALWARE TESTFILE. eicar.org. https://www.eicar.org/?page_id=3950

Hamid, A., Abdullah, N. L., & Idrus, R. (2016). Framework for successful Open-Source Software implementation in the Malaysian Public Sector. 4th IGNITE Conference and 2016 International Conference on Advanced Informatics: Concepts, Theory and Application, ICAICTA 2016. https://doi.org/10.1109/ICAICTA.2016.7803143

HTTP Evader - Automate Firewall Evasion Tests. (2015). noxxi.de. https://noxxi.de/research/http-evader.html

Iriarte Solís, A., Velarde Alvarado, P., Aguirre Villaseñor, A., Mena Camaré, L. J., Martínez Peláez, R., & Ochoa Brust, A. M. (2018). Evaluación de Firewalls Basados en Software Libre. 40(130), 625–637.

ISO/IEC 27000. (2018). International Standard ISO / IEC Information technology — Security techniques — Information security management systems — Overview and vocabulary. ACM Workshop on Formal Methods in Security Engineering. Washington, DC, USA, 34(19), 45–55. http://www.worldcat.org/title/service-operation/oclc/254028066&referer=brief_results%0Ahttps://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf%0Ahttps://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf%0Ahttp://k504.kh

ISO/IEC 27002. (2013). ISO/IEC 27002:2013. Iec, 2013, 90. www.iso.org

KALI. (2021). nmap. kali.org. https://www.kali.org/tools/nmap/

León Casas, D. (2016). Estudio de soluciones Unified Threat Management (UTM) de libre acceso. Universidad Internacional de La Rioja, 1–105. https://reunir.unir.net/bitstream/handle/123456789/3621/LEON CASAS%2C DIEGO.pdf?sequence=1&isAllowed=y

León Casas, D. (2016). Estudio de soluciones Unified Threat Management (UTM) de libre acceso. Universidad Internacional de La Rioja, 1–105. https://reunir.unir.net/bitstream/handle/123456789/3621/LEON CASAS%2C DIEGO.pdf?sequence=1&isAllowed=y

Ma, L., Chen, Y., Sun, Y., & Wu, Q. (2012). Virtualization maturity reference model for green software. Proceedings - 2012 International Conference on Control Engineering and Communication Technology, ICCECT 2012, 573–576. https://doi.org/10.1109/ICCECT.2012.230

Ma, L., Chen, Y., Sun, Y., & Wu, Q. (2012). Virtualization maturity reference model for green software. Proceedings - 2012 International Conference on Control Engineering and Communication Technology, ICCECT 2012, 573–576. https://doi.org/10.1109/ICCECT.2012.230

Nessus Essentials. (2019). Tenable.Com. https://es-la.tenable.com/products/nessus/nessus-essentials.

pfSense. (2021). Introducción al software pfSense. Www.Pfsense.Org. https://www.pfsense.org/getting-started/

Pablo, D., & Loor, L. (2017). Sistema Perimetral Firewall Y Fortalecimiento De La Seguridad En El Data Center De La Espam MFL. 18–27.

Qi, Y., Yang, B., Xu, B., & Li, J. (2007). Towards system-level optimization for high performance unified threat management. 3rd International Conference on Networking and Services, ICNS 2007, 2–7. https://doi.org/10.1109/ICNS.2007.126

Santoso, G. Z., Jung, Y. W., & Kim, H. Y. (2014). Analysis of Virtual Machine Monitor as Trusted Dependable Systems. Proceedings - 2014 IEEE International Conference on Ubiquitous Intelligence and Computing, 2014 IEEE International Conference on Autonomic and Trusted Computing, 2014 IEEE International Conference on Scalable Computing and Communications and Associated Sy, 603–608. https://doi.org/10.1109/UIC-ATC-ScalCom.2014.32

Senthilkumar, P., & Muthukumar, M. (2018). A study on firewall system, scheduling and routing using pfsense scheme. Proceedings of IEEE International Conference on Intelligent Computing and Communication for Smart World, I2C2SW 2018, 14–17. https://doi.org/10.1109/I2C2SW45816.2018.8997167

Fuertes, W., Zambrano, P., Sánchez, M., Santillán, M., Villacís, C., Toulkeridis, T., & Torres, E. (2014). Repowering an open source firewall based on a quantitative evaluation. International Journal of Computer Science and Network Security (IJCSNS), International Journal of Computer Science and Network Security, 14(11), 118.