FORTALECIENDO LA SEGURIDAD EN GNU/LINUX: ESTRATEGIAS Y MEJORES PRÁCTICAS

Julian Antonio Gaviria Jiménez
e-mail: jagaviriaj@unadvirtual.edu.co

RESUMEN: *En Este trabajo documenta el proceso completo de implementación de seguridad perimetral utilizando la distribución Endian Firewall (EFW), una herramienta basada en GNU/Linux diseñada para funcionar como firewall y gateway de red. El propósito principal fue establecer reglas de traducción de direcciones de red (NAT) y configurar el reenvío de puertos (Port Forwarding) con el fin de garantizar una segmentación lógica efectiva y permitir una comunicación controlada entre las zonas LAN (interna), DMZ (zona desmilitarizada) y WAN (Internet simulada).*

El procedimiento inició con la descarga de la imagen ISO de Endian desde su sitio oficial, seguido por la creación y configuración de una máquina virtual en VirtualBox, donde se asignaron tres interfaces de red, representando las zonas mencionadas. La instalación del sistema se realizó de forma guiada, configurando parámetros básicos como contraseñas de administración y direcciones IP para cada zona de red.

Posteriormente, desde la interfaz web de EFW, se configuraron reglas NAT para permitir la navegación desde la LAN y la DMZ hacia la red externa (WAN), asegurando el aislamiento entre las zonas internas. Además, se implementó una regla de reenvío de puertos que permite el acceso desde la WAN a un servidor web ubicado en la DMZ, simulando así un entorno empresarial donde ciertos servicios deben estar disponibles públicamente, pero protegidos del resto de la red interna.

Durante la verificación, se utilizó un equipo cliente en la LAN y un servidor en la DMZ para ejecutar comandos como ping, curl y apt update, lo que permitió confirmar la correcta conectividad hacia el exterior y el funcionamiento del redireccionamiento de puertos. Las pruebas realizadas demostraron que Endian Firewall permite controlar eficientemente el tráfico entre zonas, fortaleciendo la seguridad de la red y permitiendo una administración intuitiva a través de su entorno gráfico.

Este proyecto evidencia la importancia de una arquitectura de red segmentada y de herramientas libres como EFW para la enseñanza y práctica de conceptos clave en la administración de redes seguras. La solución implementada puede escalarse o adaptarse a distintos contextos educativos o empresariales, y constituye un ejemplo aplicable a escenarios reales donde se requiere protección perimetral, aislamiento de servicios críticos y administración centralizada de políticas de red.

PALABRAS CLAVE: NAT, GNU/Linux, Endian Firewall, DMZ, seguridad de red

ABSTRACT: This article presents the implementation of network security measures using Endian Firewall, a GNU/Linux-based distribution designed for perimeter protection and secure network management. The objective was to configure Network Address Translation (NAT) and port forwarding rules to enable controlled access between the LAN, DMZ, and WAN (simulated Internet) zones. The project involved the installation of Endian Firewall in a virtualized environment using VirtualBox, configuring network interfaces for each security zone, and applying NAT rules to allow outbound traffic and publish internal services externally. The configuration process was performed through the Endian web interface, simplifying management and verification. Practical tests confirmed the successful implementation of the proposed security architecture. This experience demonstrates the effectiveness of free and open-source solutions for strengthening network infrastructure and provides a practical approach to teaching cybersecurity principles in academic or enterprise settings.

KEYWORDS: NAT, Endian Firewall, GNU/Linux, DMZ, network security.

1. INTRODUCCIÓN

En la actualidad, el crecimiento constante de las redes informáticas y la creciente dependencia de servicios en línea exigen niveles cada vez mayores de seguridad para proteger los activos digitales y garantizar la continuidad del servicio. La seguridad perimetral se ha convertido en una de las estrategias fundamentales para salvaguardar los sistemas de información ante accesos no autorizados, ataques externos y tráfico malicioso. En este contexto, la segmentación de red, la gestión adecuada del tráfico entre zonas de confianza diferenciadas (LAN, DMZ y WAN), y la aplicación de políticas de control mediante firewalls especializados juegan un papel esencial.

Este proyecto se enmarca dentro de ese enfoque de seguridad perimetral, haciendo uso de Endian Firewall Community (EFW), una distribución GNU/Linux orientada a proporcionar funciones de firewall, puerta de enlace (gateway), servidor proxy y sistema de prevención de amenazas. Su interfaz gráfica de fácil manejo y su arquitectura basada en zonas de red la convierten en una herramienta idónea tanto para entornos académicos como para pequeñas y medianas empresas que requieren una solución de seguridad robusta sin altos costos.

2. TEMATICA.

2.1 TEMÁTICA 2: Configuración NAT en ENDIAN FIREWALL.

2.1.1 Descripción de la implementación.

Endian Firewall Community (EFW) es una distribución de seguridad de red basada en GNU/Linux que transforma una computadora común en un firewall y gateway completo de nivel empresarial. Es ampliamente utilizada en entornos académicos y empresariales gracias a su facilidad de uso, interfaz web intuitiva y potentes funcionalidades de seguridad.

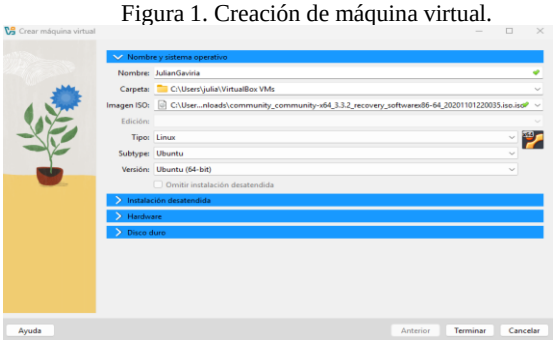
La implementación del sistema operativo de seguridad Endian Firewall Community (EFW) se llevó a cabo en un entorno de virtualización utilizando Oracle VirtualBox, con el propósito de simular una arquitectura de red empresarial que incluya segmentación por zonas y políticas de acceso controlado.

Se descargó la imagen ISO de instalación de la versión **Endian Firewall Community 3.3.2**, compatible con arquitecturas de 64 bits, en VirtualBox se creó una nueva máquina virtual con las siguientes especificaciones:

Nombre: JulianGaviria
Tipo: Linux
Versión: Ubuntu (64-bit)
Memoria RAM: 9120 MB
Procesador: 4 núcleo
Disco duro virtual: 25 GB VDI (almacenamiento dinámico)
Controlador de almacenamiento: ISO de Endian

2.1.2 instalación de Endian Firewall.

Figura 1. Creación de máquina virtual.



Fuente: Autoría propia

Figura 2. Configuración del sistema

Fuente: Autoría propia

2.1.3 Configuración NAT en Endian Firewall.

Para simular la arquitectura de red segmentada (LAN, DMZ, WAN), se habilitaron tres interfaces de red en VirtualBox, asignadas así.

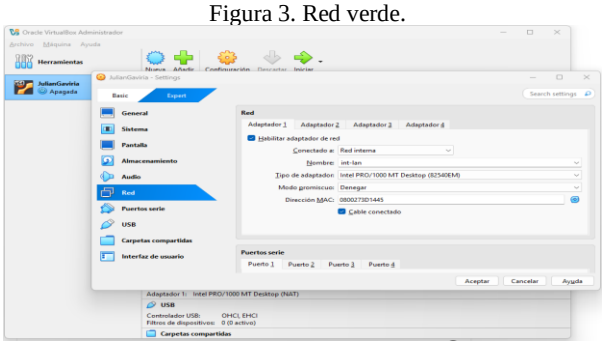
Tabla 1. Interfaces de Red

Zona	VirtualBox	Tipo de Red	IP
Verde(LAN)	Adaptador 1	Red Interna	192.168.0.15
Naranja (DMZ)	Adaptador 2	Red Interna	192.168.10.1
Roja (WAN)	Adaptador 3	NAT	10.0.4.15

Fuente: Autoría propia

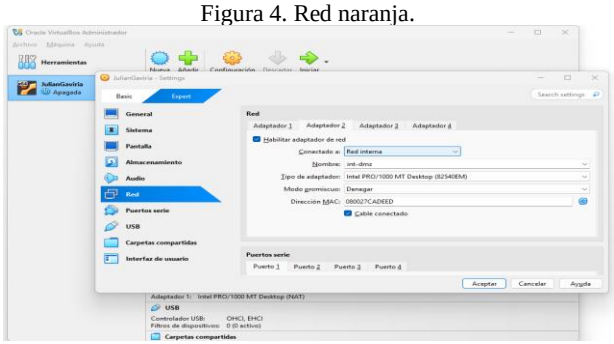
La instalación se llevó a cabo siguiendo el asistente gráfico de Endian Firewall, configurando la zona GREEN como puerta de enlace con la IP 192.168.0.15.

Figura 3. Red verde.



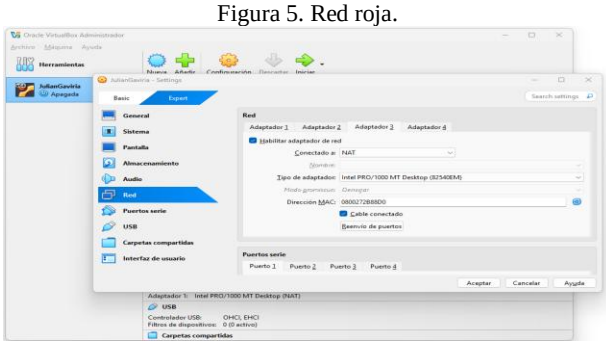
Fuente: Autoría propia

Figura 4. Red naranja.



Fuente: Autoría propia

Figura 5. Red roja.

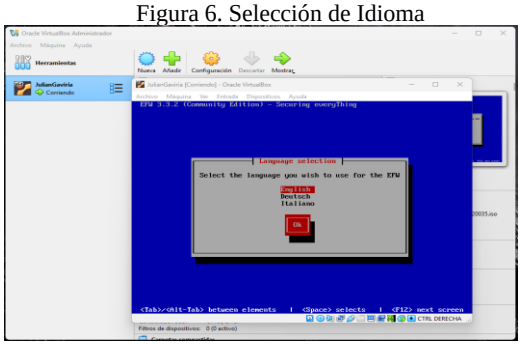


Fuente: Autoría propia

2.1.4 Inicio Endian Firewall

Desde la maquina virtual iniciamos la virtualización, seleccionamos el idioma, la solicitud de reiniciar las características y asignamos la dirección IP y la Network Mask.

Figura 6. Selección de Idioma



Fuente: Autoría propia

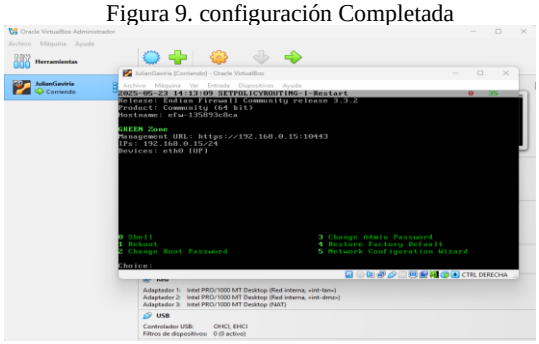
Figura 7. Aceptar condiciones

Fuente: Autoría propia

Figura 8. Asignación IP

Fuente: Autoría propia

Figura 9. configuración Completada



Fuente: Autoría propia

2.1.5 Configuración de NAT: DMZ hacia WAN

Posteriormente, se accedió a la interfaz web desde una máquina cliente ubicada en la red LAN para completar la configuración inicial, establecer las reglas NAT y habilitar el reenvío de puertos.

Este entorno permitió simular de forma efectiva un escenario empresarial con acceso a Internet, una red interna protegida, y una zona desmilitarizada para servicios públicos como servidores web

Iniciamos en el servidor y vamos al navegador para ir a la dirección que nos proporciono Endian para configurar la interfaz y las direcciones IP.

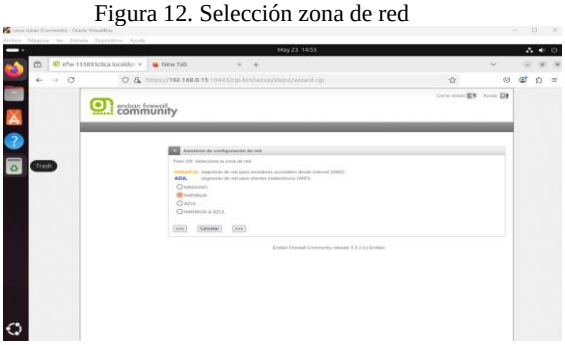
Figura 10. Inicio interfaz Endian

Fuente: Autoría propia

Figura 11. Modo de Red y enlace

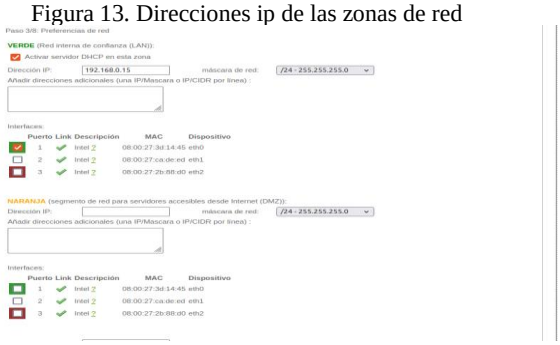
Fuente: Autoría propia

Figura 12. Selección zona de red



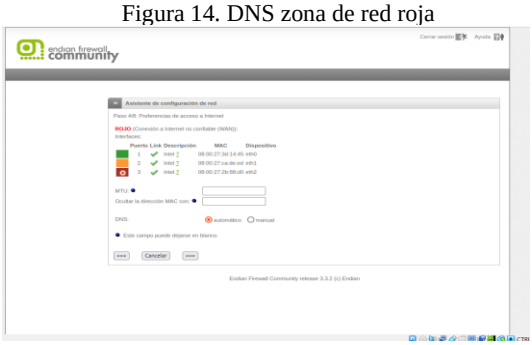
Fuente: Autoría propia

Figura 13. Direcciones ip de las zonas de red



Fuente: Autoría propia

Figura 14. DNS zona de red roja



Fuente: Autoría propia

2.1.6 Evaluación de la red de su correcta instalación

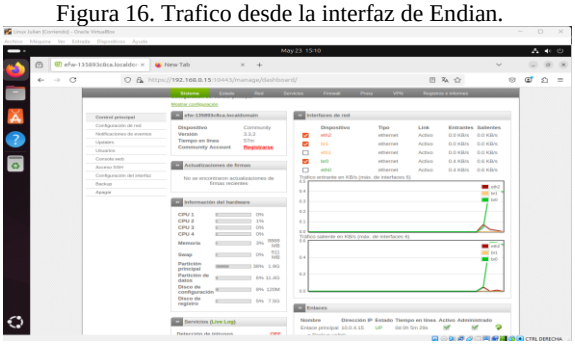
Una vez configuradas las interfaces y el direccionamiento IP de las máquinas virtuales (Endian y clientes en las zonas GREEN y ORANGE), es fundamental comprobar que exista comunicación entre ellas y con Internet. Esto se hace con el comando ping, que permite enviar paquetes ICMP a una dirección IP y recibir respuesta si hay conectividad.

Figura 15. Ping desde Linux Ubuntu.

Fuente: Autoría propia

Respuestas como las anteriores, significa que hay conexión entre el cliente y el firewall.

Figura 16. Trafico desde la interfaz de Endian.



Fuente: Autoría propia

3. CONCLUCIONES

La implementación de Endian Firewall como solución de seguridad perimetral permitió establecer un control efectivo del tráfico entre las zonas LAN, DMZ y WAN, garantizando segmentación, aislamiento lógico y reducción de riesgos asociados a accesos no autorizados.

La configuración de reglas NAT y de reenvío de puertos demostró ser funcional y sencilla de gestionar mediante la interfaz web de EFW, lo que facilita su adopción tanto en entornos académicos como empresariales, sin requerir conocimientos avanzados de línea de comandos.

El uso de una infraestructura virtualizada con VirtualBox permitió simular escenarios reales de red y validar el comportamiento del firewall frente a diferentes tipos de tráfico, destacando la importancia de las pruebas controladas para afianzar conocimientos teóricos y prácticos en redes y seguridad informática.

Endian Firewall se consolida como una herramienta versátil, gratuita y potente para proteger redes pequeñas y medianas, con capacidades que abarcan desde NAT y port forwarding hasta servicios adicionales como VPN, proxy y filtrado de contenido, promoviendo el uso de tecnologías de software libre para la defensa digital.

4. REFERENCIAS

[1] LPI LPIC-1 Exam 101. (2022). Tema 102: Comandos GNU y Unix . https://learning.lpi.org/es/learning-materials/101-500/102/.

[2] Canonical (2023). Guía del Ubuntu desktop 20.04 LTS . Help Ubuntu. https://help.ubuntu.com/20.04/ubuntu-help/index.html.

[3] Endian (2016), Endian UTM 3.2 Manual referencia . Endian. http://docs.endian.com/3.2/utm/index.html.

[4] Endian, “Endian Firewall Community Documentation,” Endian.com. [Online]. Available: https://docs.endian.com/ (Accessed: May 15, 2025).

[5] G. Obregón-Pulido, B. Castillo-Toledo, and A. Loukianov, “A globally convergent estimator for n frequencies,” IEEE Trans. Automat. Control, vol. 47, no. 5, pp. 857–863, May 2002

[6] Debian (2023). El manual del administrador de Debian 12.5.0 . Debian https://www.debian.org/releases/stable/amd64/index.es.html

[7] Oracle (2020). Manual de usuario VirtualBox . VirtualBox. https://www.virtualbox.org/manual/

[8] Jay LaCroix. (2020). Mastering Ubuntu Server : Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting Ubuntu Server . Packt Publishing.https://research-ebsco-com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b41952

[9] Cervelión, Á. J. (2023). Instalación de Nagios Core 4.4 en Ubuntu 22.04 . [Objeto_virtual_de_información_OVI]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/54230

[10] Villalba-Condori, K. O., Poma-Torres, M. L., & Huamán-Espinoza, M. (2022). Implementación de un sistema de firewall con software libre para mejorar la seguridad de la red en instituciones educativas. Revista de Investigación en Tecnologías de la Información, 10(1), 56–64.https://doi.org/10.32719/26310452.2022.10.1.6