IMPLEMENTANDO SEGURIDAD EN GNU/LINUX

Laura Guiney Perez Rojas
lgperezro@unadvirtual.edu.co

RESUMEN: *Este informe documenta la implementación de una solución de seguridad perimetral utilizando Endian Firewall Community (EFW) sobre una plataforma virtualizada en Oracle VirtualBox. Se estableció una arquitectura de red segmentada en zonas de confianza (RED, GREEN y ORANGE) mediante la configuración de adaptadores virtuales y direccionamiento IP diferenciado. La metodología incluyó el despliegue de la respectiva imagen ISO, la asignación lógica de interfaces y la administración de servicios del sistema mediante scripts SysV en la consola bash. Se validó la conectividad y el aislamiento de las zonas, además de implementar una estrategia de trazabilidad temporal basada en el reloj de hardware del sistema para auditar la gestión del servicio httpd. Los resultados confirman la eficacia de EFW como herramienta UTM para el control de tráfico y la defensa en profundidad. Esta práctica evidencia la viabilidad de soluciones de código abierto para la protección de activos de información en infraestructuras corporativas.*

PALABRAS CLAVE: Firewall, GNU/Linux, Seguridad, Virtualización.

1 INTRODUCCIÓN

La transformación digital y la interconexión masiva de sistemas corporativos han expandido significativamente la superficie de ataque organizacional, haciendo indispensable la adopción de estrategias de defensa en profundidad y controles perimetrales robustos, tal como lo señala la investigación de Z. Yue y L. Chen sobre tecnología de firewalls en redes corporativas. En este contexto, las soluciones de código abierto se han consolidado como alternativas técnica y económicamente viables, permitiendo una personalización avanzada de los mecanismos de protección, como lo documentan J. K. Gonzalez Pinto y colaboradores en su análisis de seguridad en sistemas GNU/Linux mediante Endian Firewall.

El presente informe documenta el desarrollo técnico de la implementación de Endian Firewall Community como appliance de Gestión Unificada de Amenazas, desplegado sobre una infraestructura virtualizada en Oracle VirtualBox y alineado con los lineamientos de virtualización y seguridad en entornos de red establecidos por la Universidad Nacional Abierta y a Distancia en su guía técnica institucional. El trabajo aborda la configuración integral de una arquitectura segmentada en zonas de confianza diferenciadas (RED/WAN, GREEN/LAN y ORANGE/DMZ), validando el aislamiento lógico de tráfico y la asignación de roles operativos a cada interfaz.

La metodología integra los fundamentos de administración de sistemas operativos alineados con los objetivos del examen LPIC-1 del Linux Professional Institute, combinados con prácticas de hardening y gestión de servicios. Se detalla el proceso de mapeo físico-lógico de interfaces, la configuración de direccionamiento IP estático y dinámico, y el control de demonios mediante scripts SysV en entorno de consola. Adicionalmente, se implementa una estrategia de auditoría forense basada en la lectura directa del reloj de hardware (RTC), técnica ampliamente recomendada por Jay LaCroix en su obra Mastering Ubuntu Server para garantizar trazabilidad temporal inmutable en servidores críticos. A lo largo del documento se exponen los procedimientos ejecutados, los desafíos técnicos resueltos y la evaluación de la segmentación como medida de mitigación de riesgos.

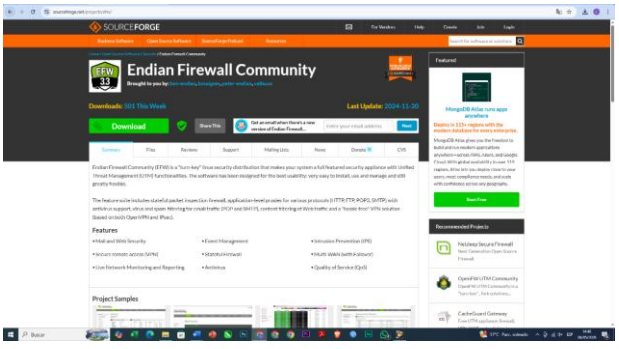
2 TEMÁTICA

2.1 Temática 1: configuración de la instancia para gnu/linux endian en virtualbox (tarjetas de red) e instalación efectiva del mismo.

El despliegue de la solución perimetral inició con la preparación del entorno virtualizado, configurando Oracle VirtualBox conforme a los estándares de gestión de hipervisores descritos en el Manual de usuario oficial de Oracle. Se estructuró una topología de red lógica aislada que permitiera aplicar el modelo de zonas de seguridad sin interferir con la infraestructura física anfitriona.

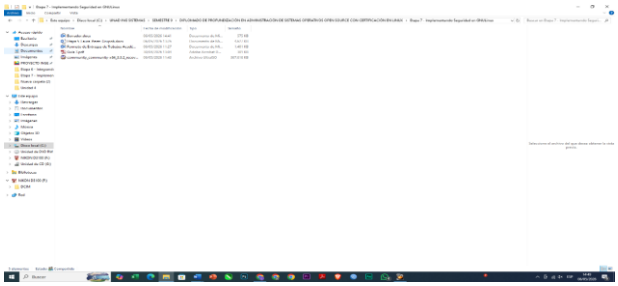
La adquisición del software base se realizó mediante el repositorio oficial en SourceForge, siguiendo las directrices de distribución publicadas por la comunidad Endian. Tras la descarga del archivo endian_community-x64_3.3.2..., se validó su integridad y disponibilidad en el sistema anfitrión (figuras 1 y 2). Posteriormente, se asignaron tres adaptadores de red virtuales, configurados según su función operativa dentro de la arquitectura perimetral.

Figura 1
Repositorio oficial de descarga de Endian Firewall Community.



Fuente: Autoría Propia

Figura 2
Verificación del archivo ISO descargado en el sistema anfitrión.

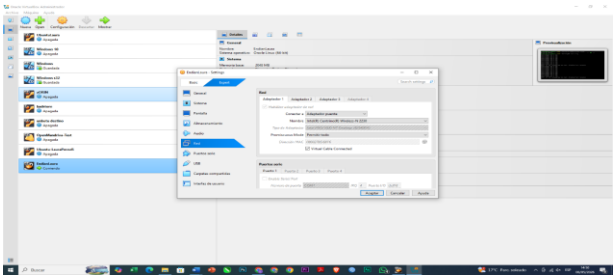


Fuente: Autoría Propia

El adaptador principal se estableció en modalidad Adaptador Puente (Bridged), vinculando directamente la interfaz virtual con la tarjeta inalámbrica del host. Esta configuración otorga visibilidad en la red física local, permitiendo la obtención de direccionamiento mediante DHCP del router perimetral y actuando como enlace de salida (uplink) hacia Internet. La interfaz cumple la función de zona RED/WAN, gestionando el tráfico proveniente de dominios no confiables (figura 3).

Nota técnica: tras pruebas de persistencia de configuración y en coordinación con el tutor Iván Guillermo Duarte Pacheco, se mantuvo esta modalidad debido al restablecimiento automático de parámetros por parte del hipervisor, garantizando así el cumplimiento de los objetivos de la temática 1.

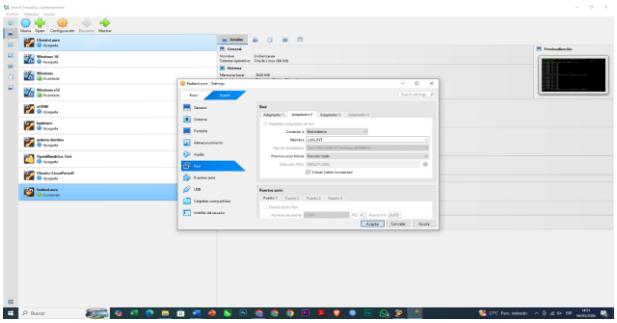
Figura 3
Configuración del Adaptador 1 en modo Puente (Zona RED/WAN).



Fuente: Autoría Propia

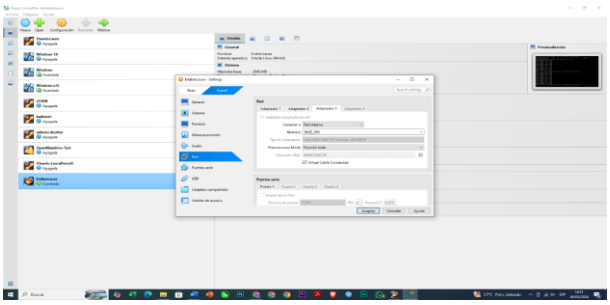
Los adaptadores secundarios se configuraron en modalidad Red Interna (Internal Network), creando segmentos aislados a nivel de hipervisor. El segundo adaptador se asoció a la red LAN_PKT, destinada a la zona GREEN/LAN para estaciones de trabajo confiables (figura 4). El tercero se vinculó a DMZ_SFY, implementando la zona ORANGE/DMZ para servidores de aplicaciones expuestos de manera controlada (figura 5). Esta segmentación, alineada con los principios de aislamiento perimetral descritos por Granados Navarro y colaboradores en su investigación sobre seguridad basada en zonas en GNU/Linux, permite exponer servicios críticos sin comprometer la integridad de la red interna corporativa.

Figura 4
Configuración del Adaptador 2 en Red Interna (Zona GREEN/LAN).



Fuente: Autoría Propia

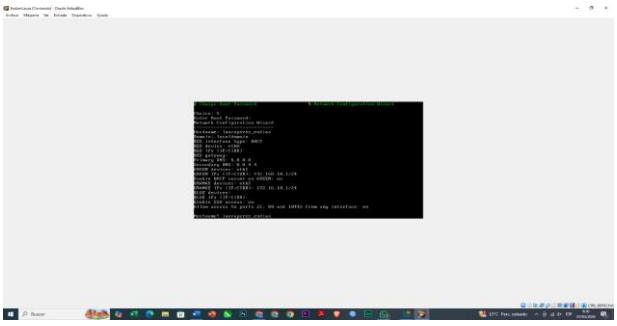
Figura 5
Configuración del Adaptador 3 en Red Interna (Zona ORANGE/DMZ).



Fuente: Autoría Propia

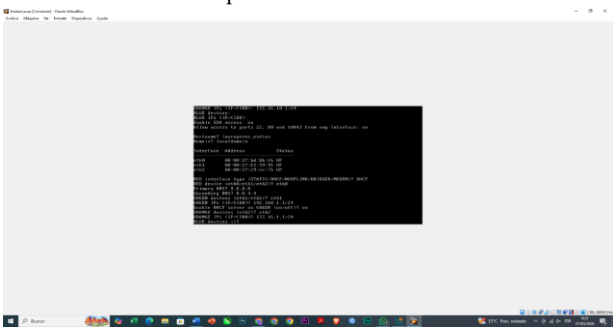
Durante el asistente de instalación de EFW release 3.3.2, se ejecutó el mapeo lógico-físico de las interfaces detectadas por el kernel (figura 6). El hostname se estableció como lauraperez_endian, garantizando la identificación unívoca del appliance en la red. La interfaz eth0 se asignó a la zona RED (configuración DHCP), mientras que eth1 y eth2 se vincularon a GREEN y ORANGE, respectivamente, con direccionamiento estático. Se definieron los servidores DNS 8.8.8.8 (primario) y 8.8.4.4 (secundario), se habilitó el servicio DHCP en la zona GREEN y se autorizaron accesos SSH a los puertos 22, 80 y 10443, validando finalmente los parámetros de despliegue (figura 7).

Figura 6
Asistente de configuración de red y asignación de interfaces.



Fuente: Autoría Propia

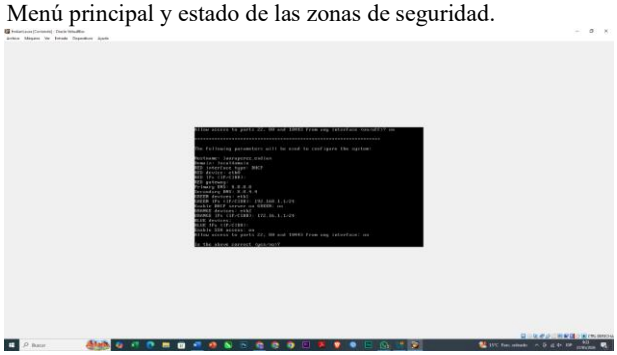
Figura 7
Validación final de los parámetros del sistema.



Fuente: Autoría Propia

Una vez completado el proceso de instalación y reiniciado el sistema, se accedió al menú principal de Endian Firewall. En la (figura 8) se verifica visualmente el estado operativo de las zonas configuradas. Se confirma que la Zona GREEN aparece marcada como [DHCP SERVER ENABLED] y la sección Uplink - main (Zona RED) se muestra como [ACTIVE], indicando conectividad funcional hacia el exterior.

Figura 8
Menú principal y estado de las zonas de seguridad.

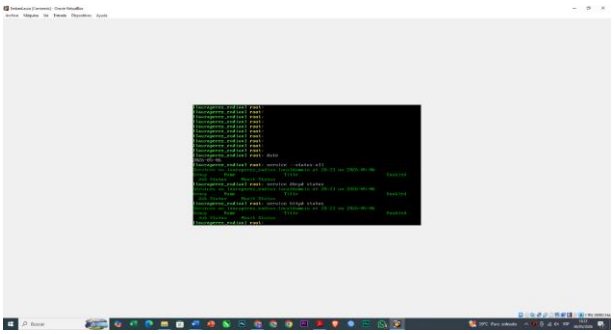


Fuente: Autoría Propia

Para la gestión avanzada, se accedió a la consola bash con privilegios de root mediante la opción 0 Shell. Inicialmente se intentó enumerar demonios con service --status-all, verificando posteriormente el estado de dhcpd y httpd (figura 9). Sin embargo, se identificó que esta distribución gestiona los servicios mediante scripts SysV ubicados en /etc/init.d/, práctica respaldada por la documentación oficial de Ubuntu de Canonical y los estándares de inicialización de sistemas GNU/Linux definidos por el Linux Professional Institute.

El enfoque se centró en el servicio httpd (Apache HTTP Server), componente crítico para la interfaz web de administración. Dado que el comando date depende del reloj del sistema y es susceptible a modificaciones o desincronizaciones NTP, se implementó una estrategia de trazabilidad forense consultando directamente el reloj de hardware mediante /proc/driver/rtc. Esta metodología, documentada por Jay LaCroix en su obra Mastering Ubuntu Server, garantiza registros temporales inmutables y auditables, independientemente del estado del sistema operativo.

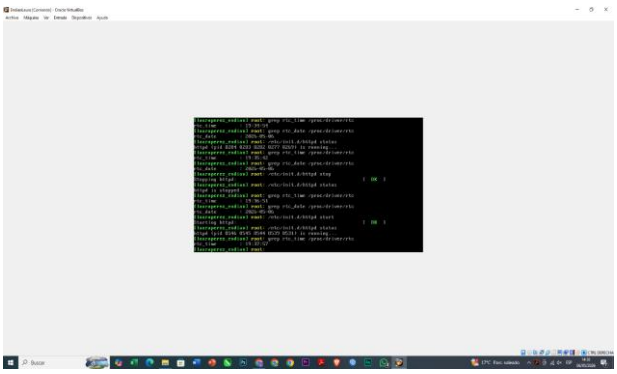
Figura 9
Acceso a la consola y verificación inicial de servicios.



Fuente: Autoría Propia

Se procedió a realizar la manipulación controlada del servicio httpd (Apache HTTP Server), componente fundamental para la interfaz web de administración. Dado que el comando estándar date retornaba únicamente la fecha sin la precisión horaria requerida para la auditoría, se implementó una estrategia de trazabilidad consultando el reloj de hardware (RTC) mediante el archivo /proc/driver/rtc. En la figura 10 se documenta la ejecución de los comandos grep rtc_time /proc/driver/rtc intercalados con las operaciones de detención (stop) e inicio (start) del servicio httpd, creando un registro forense preciso de las intervenciones.

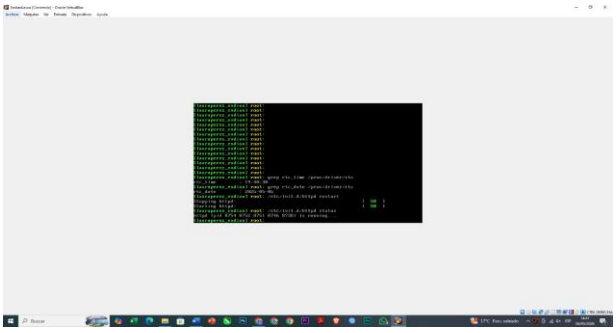
Figura 10
Auditoría de tiempo y gestión del servicio httpd (Stop/Start).



Fuente: Autoría Propia

Finalmente, se realizó la operación de reinicio del servicio mediante /etc/init.d/httpd restart, la cual ejecuta secuencialmente las operaciones de detención e inicio. Como se observa en la figura 11, esta transacción se completó exitosamente la verificación final corroboró la disponibilidad continua de la interfaz de gestión, cumpliendo con las buenas prácticas de operación y administración de sistemas descritas por Rodríguez Martínez en su investigación sobre gestión de servicios en entornos Linux (figura 11).

Figura 11
Reinicio del servicio httpd y verificación de estado.



Fuente: Autoría Propia

3 CONCLUSIONES

La implementación de Endian Firewall Community en un entorno virtualizado validó que las soluciones de código abierto constituyen alternativas técnicamente competitivas y económicamente eficientes para el despliegue de appliances UTM, en consonancia con los hallazgos de la comunidad Endian y los estudios de caso de Gonzalez Pinto y colaboradores. La segmentación mediante zonas RED, GREEN y ORANGE, junto con el aislamiento de la DMZ a nivel de hipervisor, confirmó la aplicabilidad del principio de defensa en profundidad propuesto por Granados Navarro y otros, respaldado además por los lineamientos institucionales de la UNAD. Esta arquitectura permitió simular topologías corporativas complejas, validar políticas de filtrado y garantizar el aislamiento de activos críticos sin exponer infraestructura productiva.

El control operativo mediante scripts SysV en /etc/init.d/, alineado con los estándares de Canonical y el Linux Professional Institute, sumado a la auditoría temporal basada en /proc/driver/rtc recomendada por LaCroix, aseguró la resiliencia del servicio de administración y la trazabilidad forense exigida en entornos regulados. Esta metodología, consistente con las prácticas de administración detalladas por Rodríguez Martínez, no solo garantiza la disponibilidad ante fallos o reconfiguraciones, sino que también eleva el cumplimiento de estándares de auditoría, consolidando la infraestructura como un entorno seguro, reproducible y alineado con las mejores prácticas de ingeniería en ciberseguridad.

4 REFERENCIAS

[1] Canonical (2023). Help Ubuntu . Help Ubuntu. https://help.ubuntu.com/

[2] Endian Firewall Community. (2024). Endian Firewall Community (Versión 3.3.2) [Software]. SourceForge. https://sourceforge.net/projects/efw/

[3] Gonzalez Pinto, J. K., Forero Rangel, W. O., Pinzón Sandoval, A. V., Molina Monroy, J. A., & Hernández Bonilla, J. E. (2025). *Seguridad en sistemas GNU/Linux a través de la implementación de un firewall Endian* [Trabajo de diplomado]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/76956

[4] Granados Navarro, B. M., Silva Maldonado, C. F., Garavito Feliciano, D. A., Rodríguez Martín, J. A., & Reyes Hernández, J. S. (2025). *Diseño e implementación de seguridad perimetral basada en zonas mediante Endian Firewall en entornos GNU/Linux* [Trabajo de diplomado]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/77418

[5] 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

[6] Linux Professional Institute. (n.d.). LPIC-1 Exam 101 objectives version 5.0. LPI Learning. https://learning.lpi.org/es/learning-materials/101-500/

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

[8] Rodríguez Martínez, L. F. (2025). Implementación y administración de sistemas GNU/Linux: Desde la seguridad perimetral hasta la gestión de servicios y la operación básica [Trabajo de diplomado]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/69017

[9] Universidad Nacional Abierta y a Distancia. (2023). *Guía técnica: Virtualización y seguridad en entornos de red*. Escuela de Ciencias Básicas, Tecnología e Ingeniería. https://hemeroteca.unad.edu.co/index.php/recursos-academicos

[10] Yue, Z., & Chen, L. (2010). The research of firewall technology in computer network security. *2010 International Conference on Computer Application and System Modeling (ICCASM 2010)*, V13-234–V13-237. https://doi.org/10.1109/ICCASM.2010.5622345