

ENTORNOS VIRTUALIZADOS PARA LA SEGURIDAD EN GNU/LINUX: CASO DE ENDIAN FIREWALL

Jisell Fernanda Gómez Rodríguez 1233894039
jfgomezrod@unavirtual.edu.co

RESUMEN: Este artículo presenta la implementación de seguridad en GNU/Linux mediante la distribución Endian Firewall en un entorno virtualizado con VirtualBox. Se configuraron las zonas: verde (LAN), roja (WAN) y naranja (DMZ), asignando roles específicos para garantizar la segmentación de la red y el control del tráfico. Se realizaron pruebas de conectividad, validación de servicios web en las zonas y verificación de reglas de firewall. Los resultados evidencian la correcta operación de los servicios, la disponibilidad de la red y la efectividad de las políticas de seguridad aplicadas. Este trabajo demuestra la importancia de la virtualización y de las buenas prácticas en la administración de sistemas operativos open source para entornos académicos y profesionales.

PALABRAS CLAVE: Endian, GNU/Linux, VirtualBox, Seguridad

ABSTRACT: This paper presents the implementation of security in GNU/Linux using Endian Firewall within a virtualized environment in VirtualBox. The system was configured with three network zones: green (LAN), red (WAN), and orange (DMZ), each assigned specific roles to ensure segmentation and traffic control. The methodology included the configuration of network adapters, firewall rules, and connectivity tests between zones, as well as the validation of web services in the demilitarized zone. Results demonstrate the correct segmentation of networks, the availability of services such as Apache, and the effectiveness of firewall policies in mitigating potential risks. This work highlights the relevance of virtualization as a safe and efficient tool for learning, experimentation, and the administration of open source operating systems in academic and professional contexts.

1 INTRODUCCIÓN

La seguridad en sistemas operativos GNU/Linux es un aspecto fundamental en la administración de infraestructuras tecnológicas. Endian Firewall, como distribución especializada, permite segmentar la red en zonas diferenciadas para garantizar control y protección del tráfico. El objetivo de este trabajo es implementar Endian en un entorno virtualizado con VirtualBox, configurando las zonas verde (LAN), roja (WAN) y naranja (DMZ), y validando su funcionamiento mediante pruebas de conectividad y servicios..

2 TEMATICA 1

2.1 CONFIGURACIÓN DE LA INSTANCIA EN VIRTUALBOX

La máquina virtual se configuró con tres adaptadores de red, cada uno asignado a una zona específica

Tabla 1.

Zona	Adaptador VirtualBox	Modo de conexión	IP/ Máscara	Rol
Naranja (LAN)	Adaptador 1	Red interna (red verde)	192.168.10.1/24	Gateway verde
Verde (DMZ)	Adaptador 2	Red interna (red naranja)	192.168.9.1/24	Gateway naranja
Roja (WAN)	Adaptador 3	NAT (o Puente)	DHCP	Salida a Internet

Fuente: Autoría Propia

Se asignaron las siguientes funciones:

- Zona verde: red interna (LAN).
- Zona naranja: servidores (DMZ).
- Zona roja: acceso a Internet (WAN).

Figura 1. Configuración de adaptadores en VirtualBox

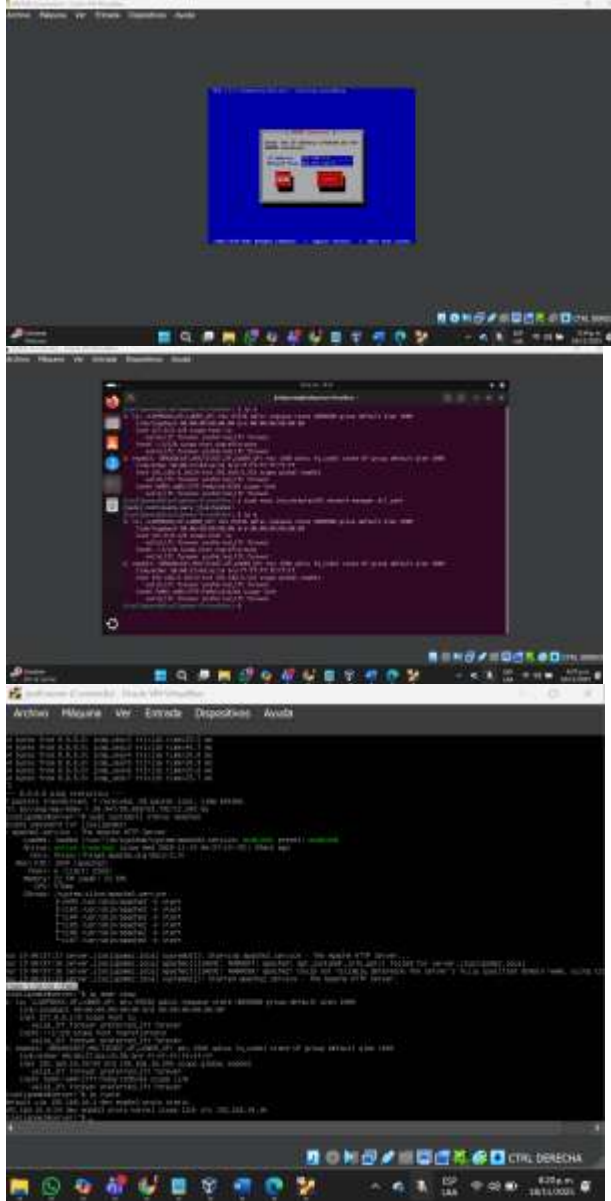


Fuente: Autoría Propia

3 CONFIGURACIÓN DE LA RED VERDE Y NARANJA

Se verificó la asignación de direcciones IP mediante los comandos ip a e ip route.

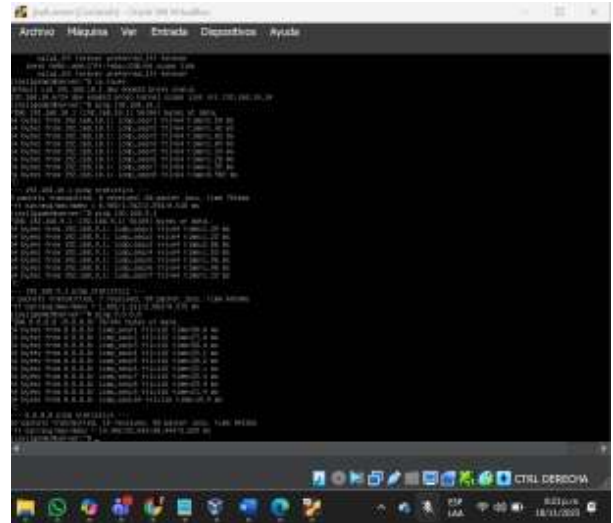
Figura 2. Interfaces de red configuradas en Endian



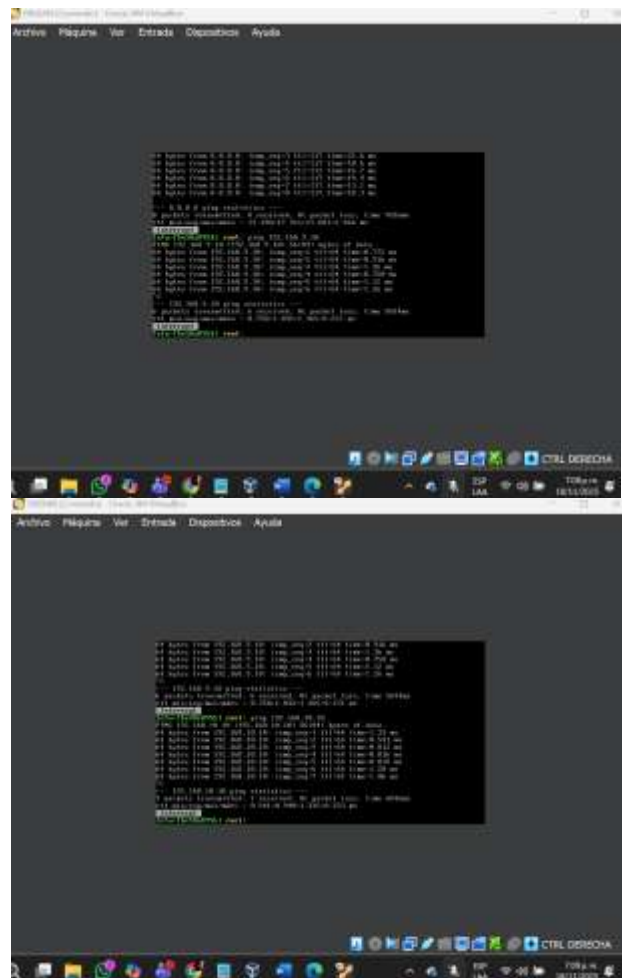
. Fuente: Autoría Propia

Las pruebas de conectividad confirmaron la comunicación entre estaciones de la red verde y naranja.

Figura 3. Prueba de ping entre zonas internas



. Fuente: Autoría Propia

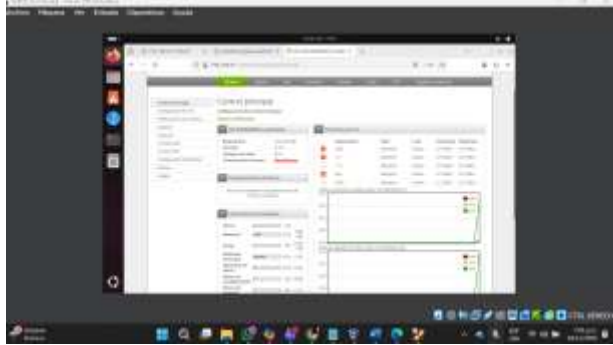


. Fuente: Autoría Propia

4 CONFIGURACIÓN DEL FIREWALL

Se implementaron reglas de firewall para controlar el tráfico entre zonas.

Figura 4. Configuración del firewall en Endian



. Fuente: Autoría Propia

Se detectaron advertencias de seguridad que evidencian la importancia de aplicar políticas preventivas.

5 VALIDACIÓN DE SERVICIOS EN LA ZONA NARANJA

Se instaló y verificó el servicio Apache en la zona naranja.

Figura 5. Validación del servidor web Apache en la DMZ

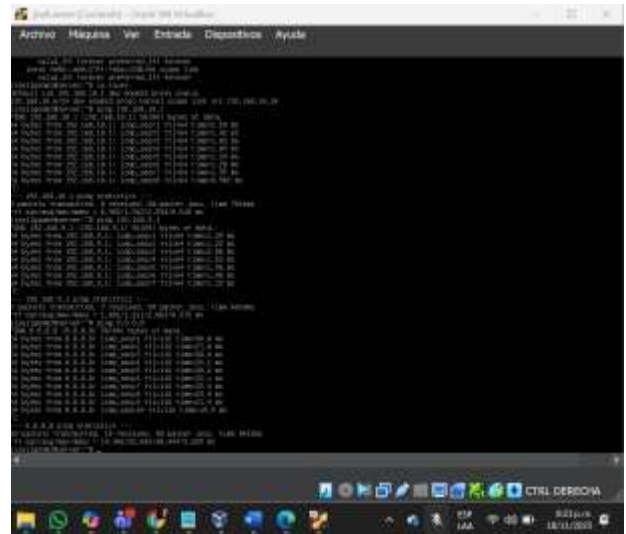


. Fuente: Autoría Propia

6 PRUEBAS DE CONECTIVIDAD ENTRE ZONAS

Se realizaron pruebas de ping hacia Internet (ping 8.8.8.8) y entre las zonas internas.

Figura 6. Prueba de conectividad hacia Internet desde Endian

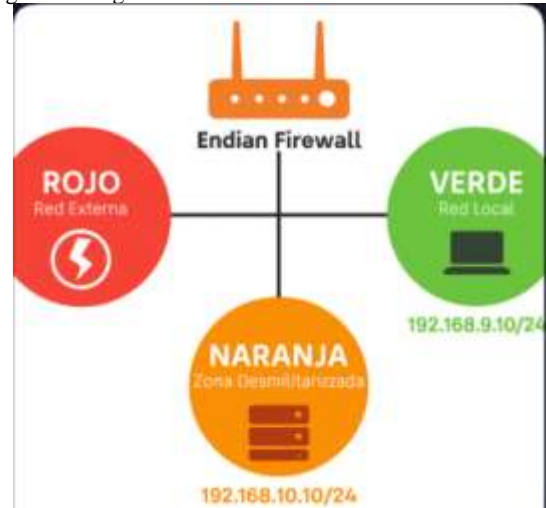


. Fuente: Autoría Propia

7 DIAGRAMA DE CONEXIÓN DE ZONAS

El diagrama resume la arquitectura implementada:

Figura 7. Diagrama de conexión de zonas en Endian Firewall



8 CONCLUSIONES

La configuración de Endian Firewall en VirtualBox permitió comprobar la segmentación de redes en tres zonas diferenciadas, asegurando un control eficiente del tráfico.

Las pruebas de conectividad y validación de servicios confirmaron la disponibilidad de la red y la correcta operación de Apache en la zona naranja.

La implementación de reglas de firewall evidenció la importancia de aplicar medidas preventivas para mitigar riesgos potenciales de seguridad.

El uso de entornos virtualizados facilita la experimentación y el aprendizaje en administración de sistemas GNU/Linux, ofreciendo un espacio seguro para

validar configuraciones antes de aplicarlas en entornos productivos.

9 REFERENCIAS

- [1] LPI Linux Essentials.(2022). Tema 4: El sistema operativo Linux . <https://learning.lpi.org/es/learning-materials/010-160/4/>
- [2] LPI Linux Essentials.(2022). Tema 5: Seguridad y sistema de permisos de archivos . <https://learning.lpi.org/es/learning-materials/010-160/5/>
- [3] Canonical (2023). Guía del Ubuntu desktop 20.04 LTS . Help Ubuntu. <https://help.ubuntu.com/20.04/ubuntu-help/index.html>
- [4] Debian (2023). El manual del administrador de Debian 12.5.0 . Debian <https://www.debian.org/releases/stable/amd64/index.es.html>
- [5] Oracle (2020). Manual de usuario VirtualBox . VirtualBox. <https://www.virtualbox.org/manual/>.