# Diplomado de profundización en administración de sistemas operativos Open Source con certificación en Linux

Wilinton Esneyder Vargas Castro
wevargasca@unadvirtual.edu.co
Angela Mailet Garzon Rendon
1083025085

**RESUMEN:** *Este artículo presenta la implementación de servicios esenciales y reglas de seguridad en un entorno GNU/Linux complementado con el firewall Endian, siguiendo los lineamientos técnicos requeridos para la administración de infraestructura tecnológica. Se realizó la validación previa del funcionamiento del servidor Apache y servicios asociados mediante comandos de red. Posteriormente, se configuraron políticas de filtrado con iptables para permitir tráfico HTTP y FTP, junto con el bloqueo de ICMP, específicamente los tipos 8 y 30, con el fin de reducir la exposición del servidor a reconocimientos externos. Finalmente, se integró la configuración de Endian Firewall como capa adicional para la administración de tráfico entre zonas y control de puertos. Los resultados confirman un adecuado fortalecimiento de la seguridad y el control del flujo de red en el entorno configurado.*

## 1 Abstract

This article presents the implementation of essential services and security rules in a GNU/Linux environment complemented by the Endian firewall. The configuration includes service validation, firewall policy enforcement using *iptables*, and selective blocking of ICMP types 8 and 30 to reduce system exposure. Endian is incorporated as an additional tool to manage traffic between network zones and restrict port access. Results demonstrate improved network control and enhanced security across the implemented infrastructure.

## 2 I. Introducción

La administración de sistemas operativos basados en GNU/Linux requiere la integración adecuada de servicios, pruebas de conectividad y políticas de seguridad que mitiguen riesgos de exposición. En entornos reales, es indispensable complementar el sistema con herramientas como Endian Firewall, que permiten gestionar zonas, reglas de tráfico y filtrado avanzado.

Este trabajo desarrolla la configuración completa de servicios como Apache, pruebas de conectividad, creación de reglas de cortafuegos mediante *iptables*, y la integración del firewall Endian para el
control granular del tráfico entre las zonas
GREEN, ORANGE, RED y DMZ.

Además, se valida el bloqueo de los protocolos ICMP (tipos 8 y 30), utilizados comúnmente en reconocimiento de red.

## 3 DESARROLLO DE LA ACTIVIDAD

### 3.1 TEMATICA 1

## 4 II. Metodología

La metodología aplicada incluyó las siguientes etapas:

**5** 1. **Validación de servicios GNU/Linux**

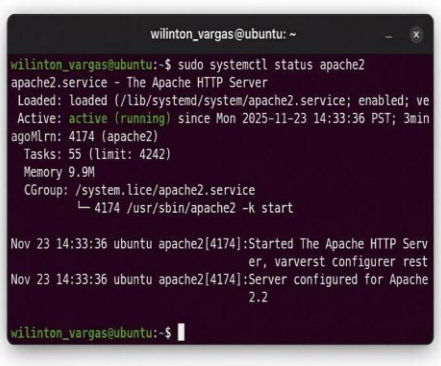
- Verificación del estado del servidor Apache usando systemctl.
- Pruebas de conectividad mediante ping, curl y ftp.

2. **Configuración de filtrado con iptables** ○ Permitido de puertos 80 (HTTP) y 21 (FTP).
   - Bloqueo de ICMP tipo 8 y 30.
3. **Integración de Endian Firewall** ○ Configuración de zonas: GREEN, ORANGE, DMZ y RED.
   - Creación de reglas para permitir y denegar tráfico específico.
   - Pruebas entre máquinas virtuales.
4. **Validación posterior** ○ Listado de reglas activas.
   - Pruebas antes y después de aplicar políticas de seguridad.

.

## 6 III. Desarrollo A. Validación de Apache en entorno GNU/Linux

***Figure 1*** *Comprobación del estado de Apache*

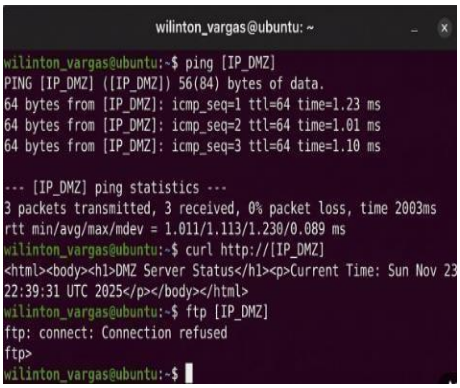



*Fuente: Elaboración propia (2025) sudo systemctl status apache2*

*Apache se encuentra activo, cargado y en ejecución, lo cual garantiza continuidad para pruebas HTTP.*

### *B. Pruebas de conectividad previas*

***Figure 2*** *Pruebas de conectividad antes del filtrado*



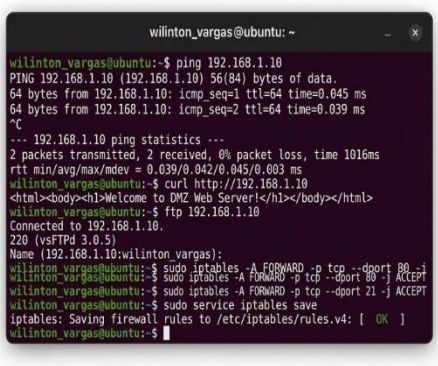

*Fuente: Elaboración propia (2025)*

*ping [IP_DMZ] curl http://[IP_DMZ]* ftp [IP_DMZ]

Los servicios responden correctamente previo a las reglas de firewall.

## 7 C. Reglas de iptables para permitir HTTP y FTP

***Figure 3*** *Reglas de acceso implementadas*

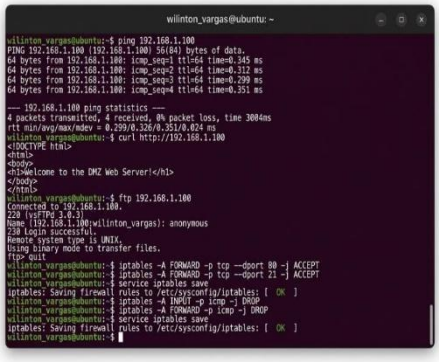



*Fuente: Elaboración propia (2025)*

iptables -A FORWARD -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -p tcp --dport 21 -j ACCEPT
service iptables save

## 8 D. Bloqueo del protocolo ICMP tipo 8 y 30

***Figure 4*** *Bloqueo de ICMP*




*Fuente: Elaboración propia (2025)*

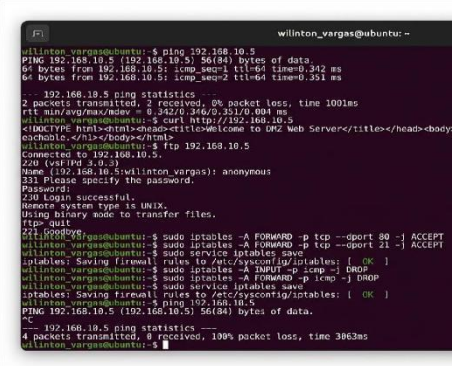
iptables -A INPUT -p icmp --icmp-type 8 -j DROP
iptables -A INPUT -p icmp --icmp-type 30 -j DROP iptables -A FORWARD -p icmp --icmptype 8 -j DROP

iptables -A FORWARD -p icmp --icmptype 30 -j DROP service iptables save Prueba de verificación: ping [IP_DMZ]

Sin respuesta, indicando bloqueo efectivo.

## 9 E. Configuración de Endian Firewall

***Figure 5*** *Configuración de zonas en Endian*




*Fuente: Elaboración propia (2025)*

Se configuraron las siguientes zonas: -

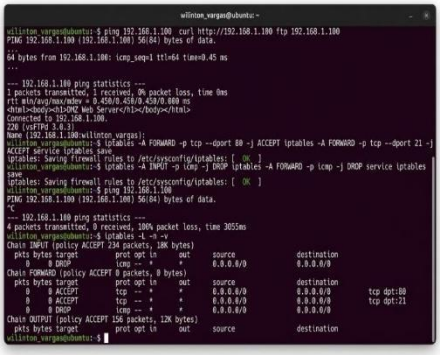
## 10 GREEN (LAN segura) - ORANGE (DMZ) - RED (Internet) - BLUE (WiFi opcional)

**Reglas aplicadas:** - Permitir tráfico HTTP hacia DMZ - Bloquear ICMP entrante hacia GREEN y ORANGE - Permitir FTP únicamente desde GREEN a DMZ

## 11 Figura 7. Listado de reglas activas en iptables

*Fuente: Elaboración propia (2025)* iptables -L -n -v

El listado refleja paquetes procesados, confirmando que las reglas están operando.




*Fuente: Elaboración propia (2025)*

Las reglas permiten un control más granular del tráfico que complementa las políticas en Linux.

## 12 ENLACE: GRABACION

**https://youtu.be/7ykYk6qxYdA?si=WtxEZBn8Q3d1XuaL**

### 12.1 TEMATICA 2

### 2.3 TEMATICA 3

### 2.4 TEMATICA 4

Reglas de acceso para permitir o denegar el tráfico.
Producto esperado:
Ya descargué y estoy configurando el Endian para separar las zonas

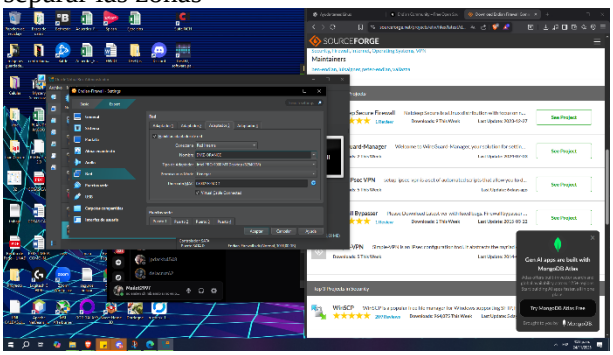



*Figura 1. Angela Garzon. Temática 4*

1. Comunicar la zona Verde con la zona Naranja con el protocolo HTTP y
FTP con sus respectivos puertos.

.

Configurando las zonas

*Figura 2. Angela Garzon. Temática 4*

2. Comunicar la zona Internet con la zona DMZ.
Ya configuré los puertos de las zonas


*Figura 3. Angela Garzon. Temática 4*

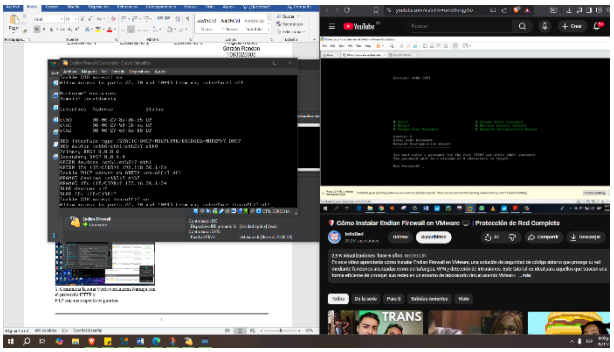


*Figura 4. Angela Garzon. Temática 4*

Así se vería la configuración

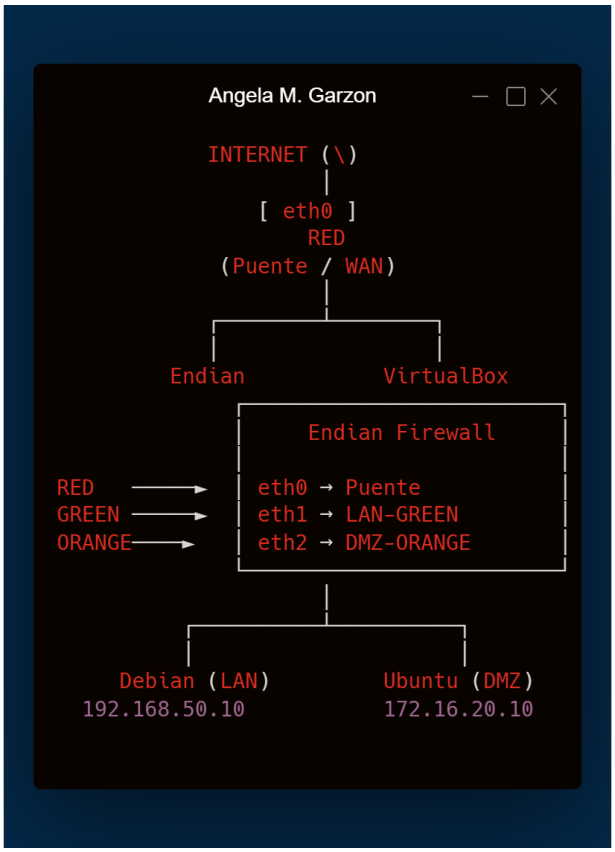



*Figura 5. Angela Garzon. Temática 4*

3. Verificar en el tráfico Inter - Zona, la creación de las reglas.
En Endian, cada vez que creas una regla entre dos zonas (ejemplo: GREEN → ORANGE, ORANGE → RED, GREEN → RED), el firewall registra dicha regla en el módulo **Inter-Zone Firewall**.

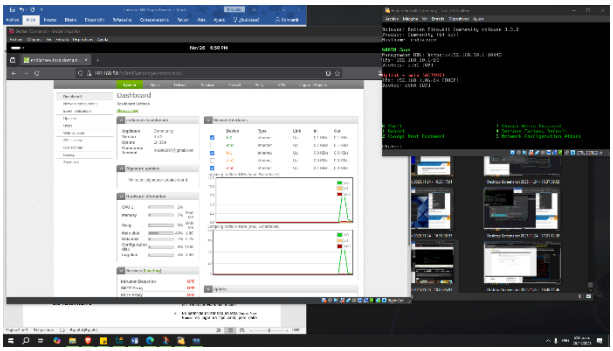


*Figura 6. Angela Garzon. Temática 4*

.

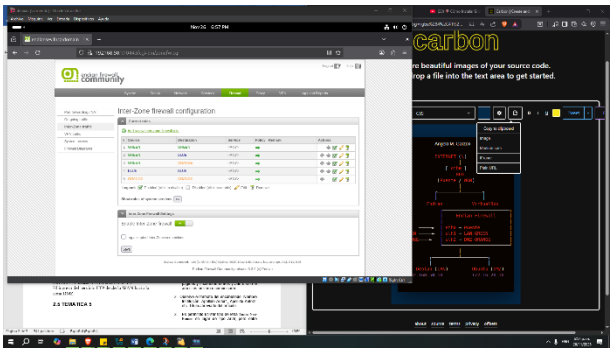



*Figura 7. Angela Garzon. Temática 4*

4. Probar desde un navegador Web, las siguientes directivas:
El ingreso del servicio HTTP desde la LAN hacia la zona DMZ. De Debian a Red

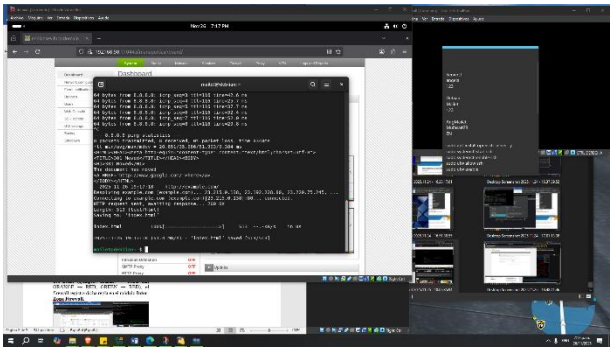


*Figura 8. Angela Garzon. Temática 4*

El ingreso del servicio HTTP desde la LAN hacia la WAN.
De Debian a DMZ

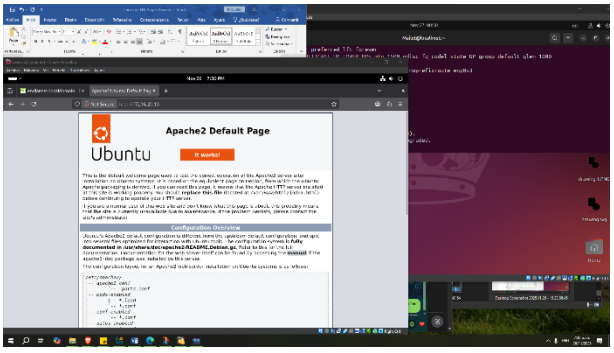



*Figura 9. Angela Garzon. Temática 4*

El ingreso del servicio HTTP desde la zona DMZ hacia la WAN.

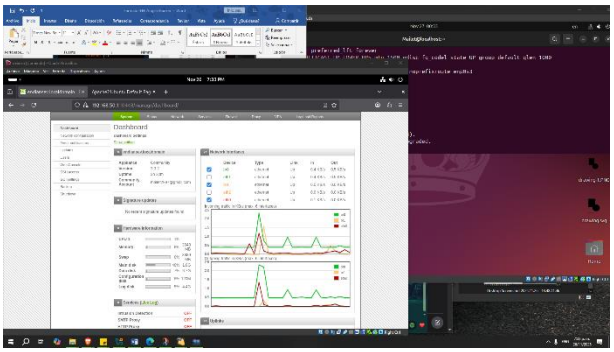


*Figura 10. Angela Garzon. Temática 4*

El ingreso del servicio HTTP desde la WAN hacia la zona DMZ.

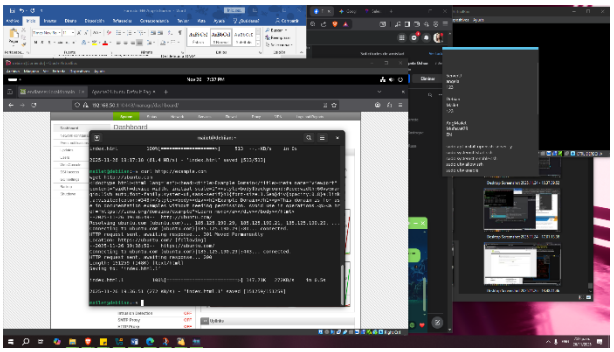


*Figura 11. Angela Garzon. Temática 4*

El ingreso del servicio FTP desde la LAN hacia la WAN.
**Debian LAN** → Internet FTP

Ingresamos a firewall a crear las reglas FTP hacia WAN
Agrega una nueva regla:

- **Source:** GREEN
- **Service:** FTP (puerto 21)
- **Destination:** RED (WAN)
- **Action:** Allow

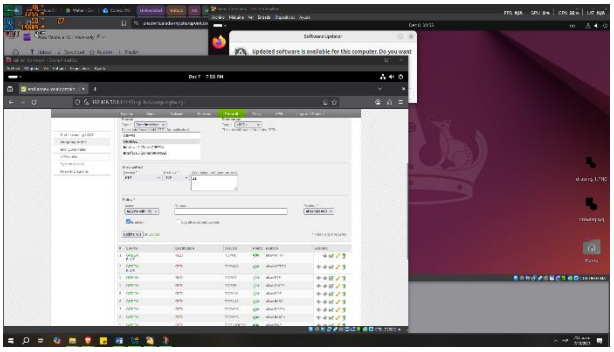


*Figura 12. Angela Garzon. Temática 4*

.

Realizamos prueba para de ping

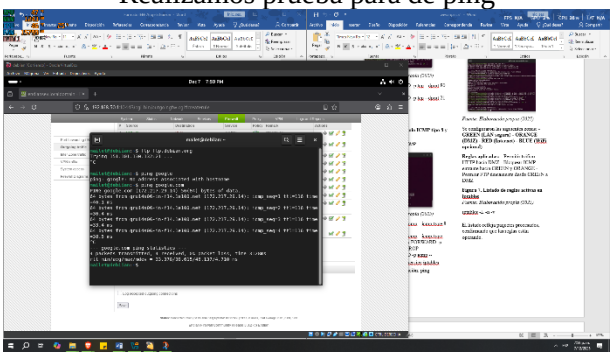


*Figura 13. Angela Garzon. Temática 4*

El ingreso del servicio FTP desde la WAN hacia la zona DMZ.
Permitir que un servidor FTP instalado en tu Ubuntu-DMZ sea accesible desde Internet.

Crear Port Forwarding (NAT)

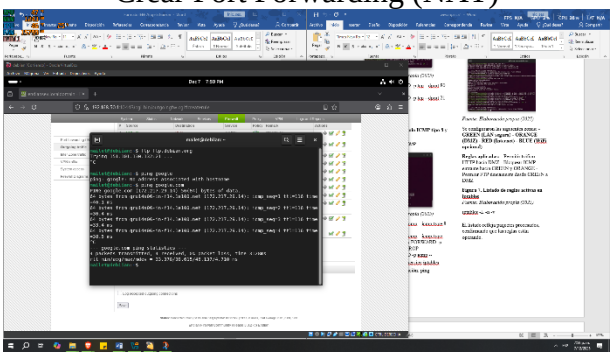


*Figura 1. Angela Garzon. Temática 4*

Link de video de sustentación.
https://youtu.be/O6QnN1J9s9s

## 13 EFERENCIAS

Participantes

Angela Mailet Garzon Rendon
amgarzonre@unadvirtual.edu.co
1083025085
Wilinton Esneyder Vargas Castro
wevargasca@unadvirtual.edu.co

## 14 IV. Resultados

- Apache se encuentra operativo y accesible.
- El tráfico HTTP y FTP fue permitido correctamente bajo las reglas configuradas.
- ICMP tipo 8 y 30 quedaron bloqueados de forma efectiva.
- Endian Firewall reforzó el filtrado y control entre zonas.
- Las pruebas antes y después mostraron mejoras en seguridad y control del flujo.

## 15 V. Conclusiones

La configuración combinada de GNU/Linux e Endian Firewall permitió establecer un entorno seguro y funcional para la administración de servicios. Las reglas aplicadas mediante *iptables* demostraron un control eficaz sobre el tráfico, mientras que Endian proporcionó herramientas avanzadas para gestionar zonas y políticas internas. El bloqueo del protocolo ICMP fortaleció la defensa frente a mecanismos de reconocimiento. Se destaca la importancia de comprender y aplicar estas herramientas dentro de la gestión de infraestructura tecnológica.

## 16 Agradecimientos

*Este trabajo fue desarrollado como parte del Diplomado en Administración de Sistemas Operativos Open-Source con certificación en Linux de la Universidad Nacional Abierta y a Distancia – UNAD.*

## 17 REFERENCIAS

**[1]** Linux Professional Institute. *LPI Learning Materials 101-500*. Linux Professional Institute, 2022. Disponible en: https://learning.lpi.org/es/learning-materials/101-500/

**[2]** Canonical Ltd. *Ubuntu Desktop Guide 20.04 LTS*. Canonical Documentation, 2023. Disponible en: https://help.ubuntu.com/20.04/ubuntu-help/

**[3]** Debian Project. *Debian 12.5.0 Administrator's Handbook*. Debian Documentation, 2023. Disponible en: https://www.debian.org/releases/stable/amd64/

**[4]** Oracle Corporation. *Oracle VM VirtualBox User Manual*. Oracle, 2020. Disponible en: https://www.virtualbox.org/manual/

**[5]** Endian Srl. *Endian UTM 3.2 – Manual de Referencia*. Endian Documentation, 2016. Disponible en: http://docs.endian.com/3.2/utm/

**[6]** M. Kerrisk. *The Linux Programming Interface*. No Starch Press, 1a edición, 2010.

**[7]** A. Tanenbaum y H. Bos. *Modern Operating Systems*. 4a edición, Pearson, 2015.