# IMPLEMENTANDO SEGURIDAD EN GNU/LINUX

Laura Valeria Acosta Vélez
e-mail: lvacostav@unadvirtual.edu.co

**RESUMEN:** *La segmentación y el control del tráfico de red constituyen elementos fundamentales dentro de la seguridad informática en entornos GNU/Linux. En este artículo se presenta la implementación de Endian Firewall Community Edition en un entorno virtualizado mediante Oracle VM VirtualBox, configurando las zonas VERDE (LAN), NARANJA (DMZ) y ROJA (WAN) para la administración y control de las comunicaciones entre redes. Adicionalmente, se implementaron servicios HTTP y FTP sobre Ubuntu Server, aplicando reglas Inter-Zona y políticas NAT para permitir el acceso controlado entre las diferentes zonas de red. Finalmente, se realizaron pruebas de conectividad y validación de servicios que permitieron comprobar el funcionamiento de la infraestructura configurada y fortalecer conocimientos relacionados con Linux Essentials, administración de redes y seguridad informática en sistemas GNU/Linux.*

**PALABRAS CLAVE**: GNU/Linux, Endian Firewall, NAT, DMZ.

## 1 INTRODUCCIÓN

La seguridad informática en entornos GNU/Linux representa un componente fundamental dentro de la administración y protección de infraestructuras tecnológicas. Actualmente, el crecimiento de los servicios de red y la necesidad de controlar el acceso entre diferentes segmentos de comunicación hacen indispensable la implementación de mecanismos de filtrado, monitoreo y administración del tráfico de red.

En este contexto, los firewalls constituyen una de las principales herramientas para garantizar la seguridad y segmentación de redes, permitiendo establecer políticas de acceso entre zonas con diferentes niveles de confianza. Endian Firewall Community Edition ofrece funcionalidades orientadas a la administración de tráfico, control de acceso, configuración NAT y segmentación de redes mediante zonas como LAN, DMZ y WAN.

El presente artículo describe la implementación de Endian Firewall Community Edition dentro de un entorno virtualizado utilizando Oracle VM VirtualBox y sistemas GNU/Linux. Durante el desarrollo de la práctica se configuraron las zonas VERDE, NARANJA y ROJA, además de reglas Inter-Zona y políticas NAT para controlar la comunicación entre redes. Adicionalmente, se implementaron servicios HTTP y FTP sobre Ubuntu Server, validando posteriormente la conectividad y el funcionamiento de los servicios mediante diferentes pruebas de acceso y comunicación.

## 2 PROCEDIMIENTO TEMÁTICA 4

### 2.1 CONFIGURACIÓN DEL ENTORNO VIRTUALIZADO

Para el desarrollo de la temática se implementó un entorno virtualizado mediante Oracle VM VirtualBox, utilizando GNU/Linux Endian Firewall Community Edition como solución principal de seguridad perimetral. Adicionalmente, se crearon máquinas virtuales basadas en Ubuntu Server y Linux Mint Desktop para representar los servicios publicados en la DMZ y los clientes internos de la red LAN.

Durante la configuración del entorno se implementaron tres zonas principales dentro de Endian Firewall:

Zona VERDE (LAN): utilizada para representar la red interna de usuarios.

Zona NARANJA (DMZ): destinada a la publicación de servicios HTTP y FTP mediante Ubuntu Server.

Zona ROJA (WAN): utilizada para simular la conexión hacia Internet mediante un adaptador NAT.

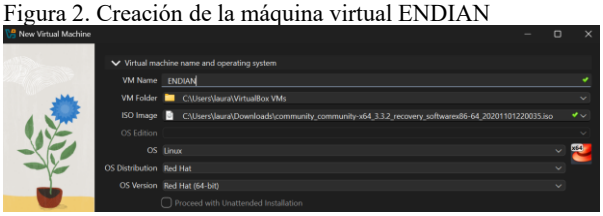
La correcta asignación de interfaces y direcciones IP permitió establecer comunicación entre las diferentes zonas de red y aplicar posteriormente las reglas de acceso y control de tráfico requeridas para la práctica.

Figura 1. Descarga de Endian Firewall Community Edition


*Fuente: Autoría propia.*

Una vez descargada la imagen ISO desde el repositorio oficial, se procedió a la creación de la máquina virtual que serviría como dispositivo principal de seguridad perimetral dentro del entorno virtualizado. Esta plataforma proporciona mecanismos para la segmentación de redes, control de acceso y administración del tráfico entre diferentes zonas de red [1].

Figura 2. Creación de la máquina virtual ENDIAN

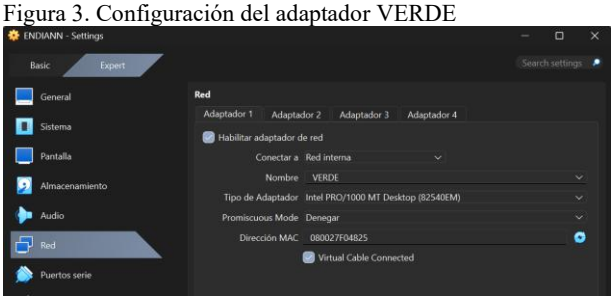



*Fuente: Autoría propia.*

Posteriormente, se realizó la configuración de las interfaces de red de la máquina virtual. Cada adaptador fue asociado a una zona específica con el fin de representar los diferentes segmentos de la infraestructura y permitir la aplicación de políticas de seguridad independientes.

La interfaz VERDE (LAN) fue destinada a la red interna de usuarios, proporcionando un entorno confiable desde el cual se realizaron las pruebas de acceso y comunicación hacia los servicios implementados.

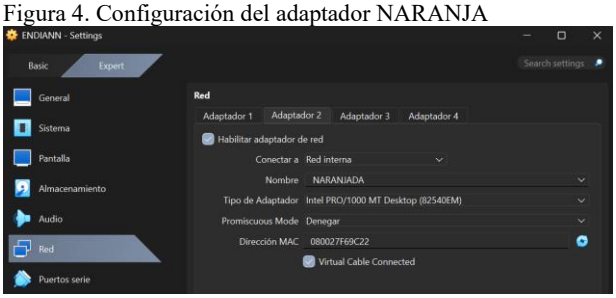
Figura 3. Configuración del adaptador VERDE




*Fuente: Autoría propia*

La interfaz NARANJA (DMZ) fue configurada para alojar los servicios públicos, permitiendo la publicación de los servidores HTTP y FTP de manera controlada y aislada de la red interna.

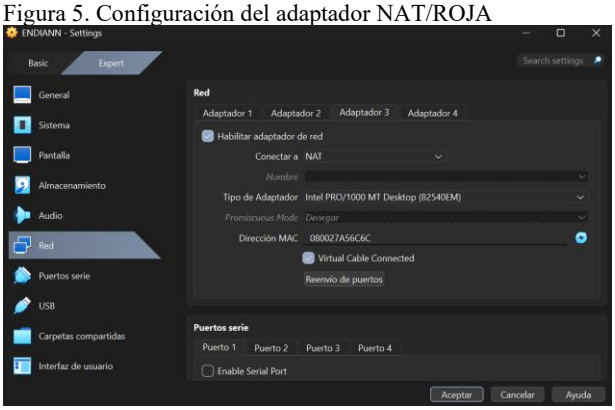
Figura 4. Configuración del adaptador NARANJA




*Fuente: Autoría propia*

La interfaz ROJA (WAN) se configuró mediante NAT para simular la conexión hacia Internet, permitiendo la comunicación externa necesaria para las pruebas de conectividad y acceso a servicios.

Figura 5. Configuración del adaptador NAT/ROJA




*Fuente: Autoría propia*

## 2.2 CONFIGURACIÓN DE ENDIAN FIREWALL

Una vez creada la infraestructura virtual y configuradas las interfaces de red, se procedió a la instalación de Endian Firewall Community Edition como solución principal de seguridad perimetral. Durante el proceso se definieron los parámetros básicos del sistema, incluyendo idioma, configuración inicial de red y servicios de administración. Endian proporciona funcionalidades orientadas al filtrado de tráfico, segmentación de redes, traducción de direcciones de red (NAT) y control de acceso, características fundamentales para la implementación de arquitecturas seguras en entornos GNU/Linux [1].

Figura 6. Instalación Endian Firewall


*Fuente: Autoría propia*

Finalizada la instalación, se verificó el correcto funcionamiento de la interfaz VERDE (LAN), destinada a representar la red interna de usuarios. Esta interfaz actúa como zona de confianza dentro de la arquitectura propuesta, permitiendo la administración inicial del firewall y la comunicación con los equipos ubicados en la red local.

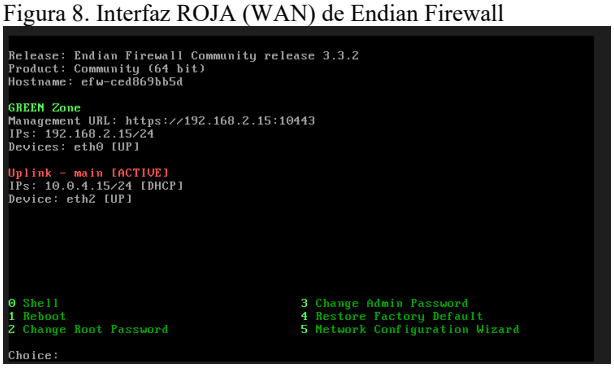
Figura 7. Interfaz VERDE de Endian Firewall


*Fuente: Autoría propia*

Posteriormente, se comprobó el estado operativo de la interfaz ROJA (WAN), configurada mediante direccionamiento dinámico DHCP a través del adaptador NAT de VirtualBox. Esta configuración permitió simular la conexión hacia Internet y validar los mecanismos de acceso

externo necesarios para el desarrollo de las pruebas de conectividad y publicación de servicios.

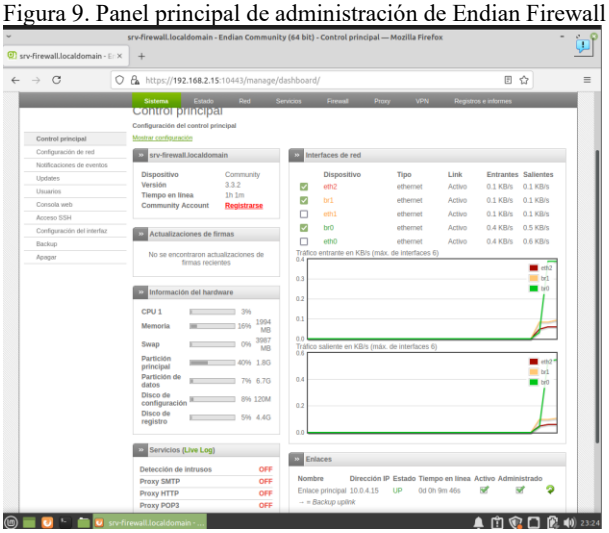
Figura 8. Interfaz ROJA (WAN) de Endian Firewall




*Fuente: Autoría propia*

Una vez verificadas las interfaces de red, se accedió al panel web de administración de Endian Firewall utilizando el protocolo HTTPS. Desde esta consola se realizaron las tareas de configuración de red, administración de servicios, creación de reglas de tráfico y monitoreo del estado general del sistema. La interfaz centraliza las principales funciones de gestión y facilita la supervisión de los recursos de seguridad implementados [2].

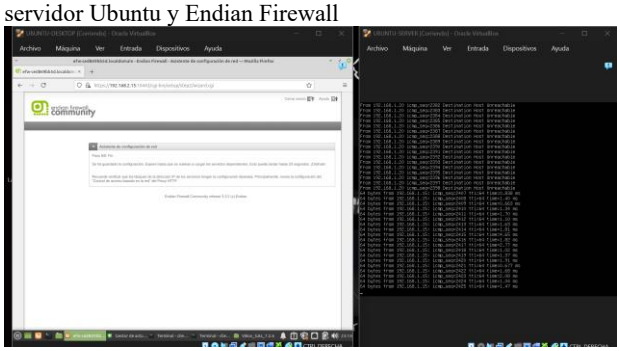
Figura 9. Panel principal de administración de Endian Firewall



*Fuente: Autoría propia*

Como etapa de validación inicial, se realizaron pruebas de conectividad mediante el protocolo ICMP entre el servidor Ubuntu Server y el firewall Endian. Estas pruebas permitieron comprobar la correcta comunicación entre segmentos de red, verificando que las direcciones IP configuradas y las interfaces asociadas a cada zona funcionaran de manera adecuada antes de continuar con la implementación de reglas de acceso y servicios adicionales.

Figura 10. Verificación de conectividad ICMP entre el servidor Ubuntu y Endian Firewall



*Fuente: Autoría propia*

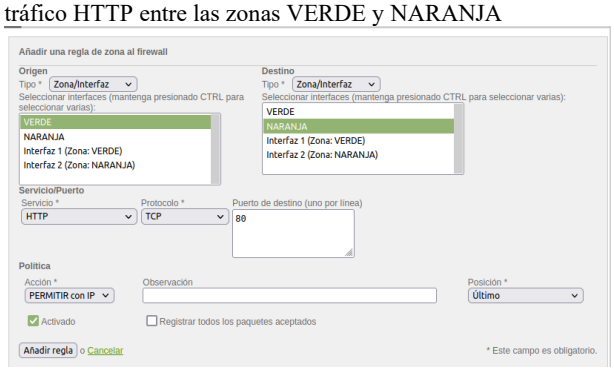
## 2.3 CONFIGURACIÓN DE REGLAS INTER-ZONA Y NAT

Con el entorno de red ya configurado, se procedió a implementar las reglas Inter-Zona y las políticas NAT en Endian Firewall, permitiendo el control del tráfico entre las zonas VERDE, NARANJA y ROJA. Para ello, se habilitaron los servicios HTTP y FTP mediante reglas específicas de acceso y traducción de direcciones de red.

Adicionalmente, se configuraron reglas de tráfico de salida para permitir la comunicación desde las redes internas hacia Internet, habilitando servicios como HTTP, HTTPS y FTP. Finalmente, se realizaron pruebas de conectividad y validación de servicios desde los diferentes equipos virtualizados.

Con el fin de permitir la comunicación controlada entre la zona VERDE (LAN) y la zona NARANJA (DMZ), se configuraron reglas Inter-Zona para habilitar el tráfico HTTP. Estas reglas permiten que los equipos ubicados en la red interna puedan acceder a los servicios web publicados en la DMZ, manteniendo el aislamiento lógico entre segmentos y aplicando únicamente los permisos estrictamente necesarios para la operación de los servicios.

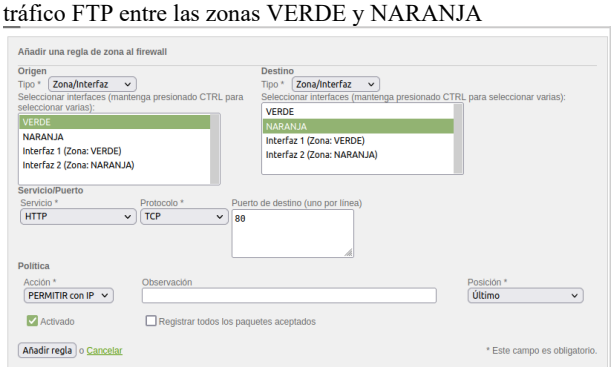
Figura 11. Configuración de regla Inter-Zona para permitir tráfico HTTP entre las zonas VERDE y NARANJA




*Fuente: Autoría propia*

Adicionalmente, se creó una regla Inter-Zona para permitir el tráfico FTP entre las zonas VERDE y NARANJA. Esta configuración fue necesaria para validar el funcionamiento del servidor FTP desplegado en la DMZ y comprobar el intercambio controlado de información entre los diferentes segmentos de la infraestructura.

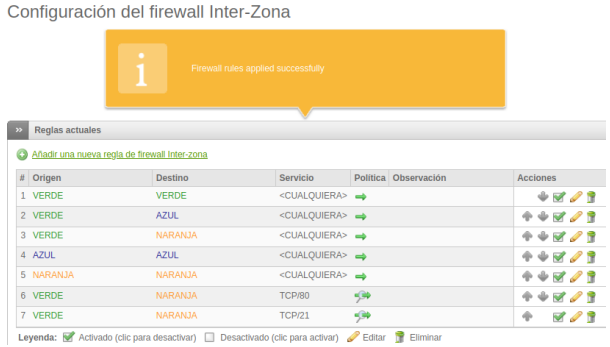
Figura 12. Configuración de regla Inter-Zona para permitir tráfico FTP entre las zonas VERDE y NARANJA




*Fuente: Autoría propia*

Una vez creadas las reglas de acceso, se verificó su correcta aplicación dentro del firewall. La validación permitió confirmar que las políticas configuradas se encontraban activas y disponibles para su utilización por parte de los servicios implementados durante la práctica.

Figura 13. Verificación de reglas Inter-Zona configuradas en Endian Firewall

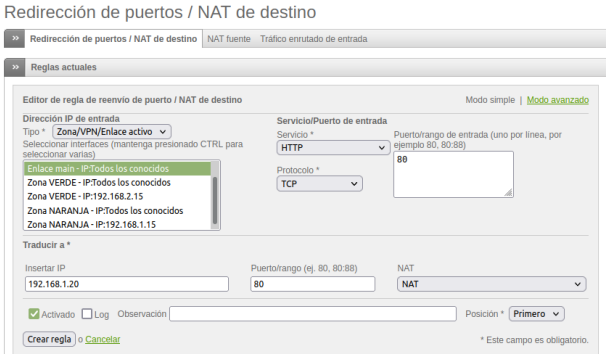



*Fuente: Autoría propia*

Posteriormente, se configuraron reglas NAT de destino con el propósito de publicar los servicios ubicados en la zona DMZ. Mediante estas reglas se realizó la redirección de peticiones provenientes de la red WAN hacia los servidores internos, permitiendo el acceso controlado a los servicios HTTP y FTP sin exponer directamente la infraestructura interna [1].

Para la publicación del servicio web se configuró una regla NAT de destino orientada al puerto 80, permitiendo redirigir las solicitudes provenientes de la red WAN hacia el servidor ubicado en la DMZ.

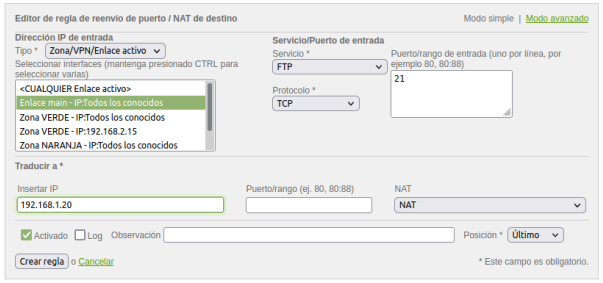
Figura 14. Configuración de regla NAT para acceso HTTP hacia el servidor ubicado en la DMZ




*Fuente: Autoría propia*

De manera complementaria, se implementó una regla NAT para el servicio FTP, habilitando el acceso controlado al puerto correspondiente y manteniendo el aislamiento de la red interna.

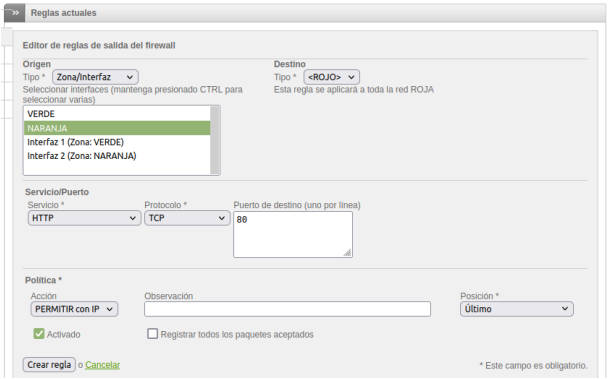
Figura 15. Configuración de regla NAT para acceso FTP hacia el servidor ubicado en la DMZ




*Fuente: Autoría propia*

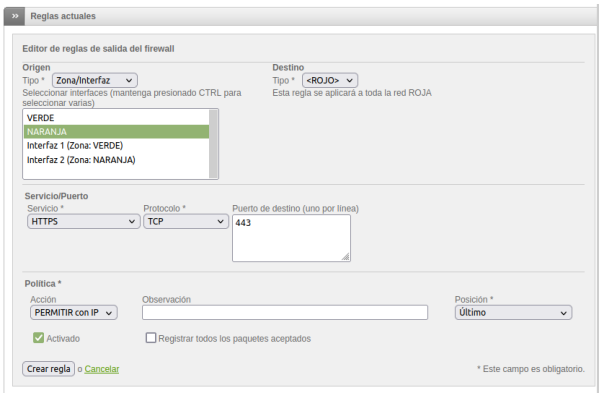
Para garantizar la conectividad de los equipos internos hacia Internet, se definieron reglas de salida desde las zonas VERDE y NARANJA hacia la zona ROJA (WAN). Estas políticas permitieron habilitar servicios esenciales como HTTP y HTTPS, necesarios para la descarga de paquetes, actualizaciones del sistema y acceso a recursos externos.

Figura 16. Configuración de regla de salida HTTP hacia la red WAN




*Fuente: Autoría propia*

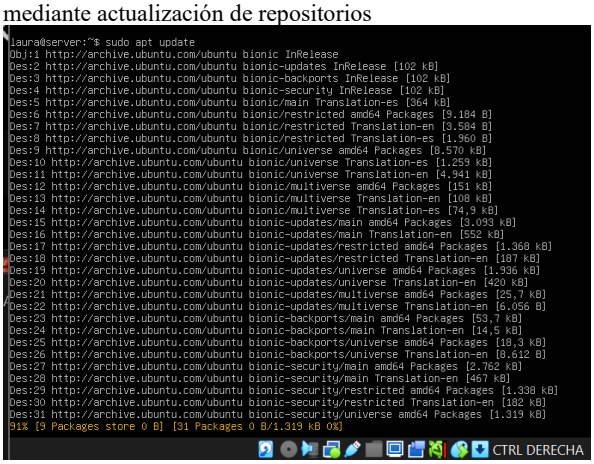
Figura 17. Configuración de regla de salida HTTPS hacia la red WAN




*Fuente: Autoría propia*

Finalmente, se realizaron pruebas de conectividad para validar el funcionamiento de las reglas de salida configuradas. La ejecución del comando apt update permitió comprobar el acceso exitoso a repositorios externos, confirmando que las políticas de filtrado y las configuraciones NAT implementadas operaban correctamente dentro de la arquitectura propuesta.

Figura 18. Verificación de conectividad y reglas de salida mediante actualización de repositorios



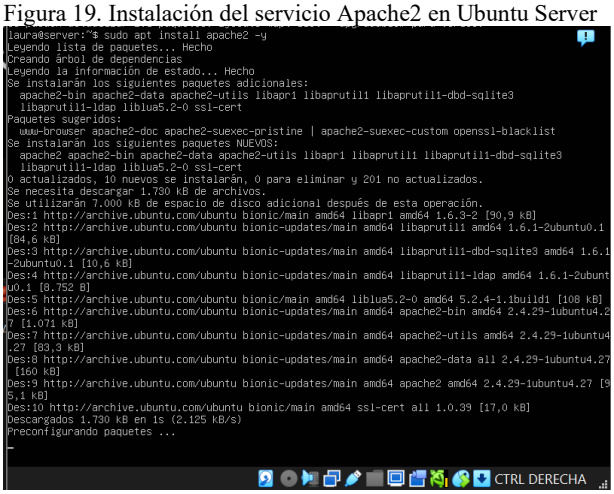

*Fuente: Autoría propia*

## 2.4 IMPLEMENTACIÓN DE SERVICIOS HTTP Y FTP

Una vez implementadas las reglas Inter-Zona y las políticas NAT en Endian Firewall, se procedió a la instalación de servicios de red dentro de la zona NARANJA (DMZ). Para ello se utilizó Ubuntu Server como plataforma de publicación, configurando los servicios Apache2 para el acceso web y VSFTPD para la transferencia de archivos. Esta implementación permitió validar el funcionamiento de la arquitectura propuesta y comprobar la interacción controlada entre las diferentes zonas de red definidas durante la práctica.

Inicialmente, se ejecutó la actualización de repositorios del sistema y posteriormente la instalación del servidor Apache2 mediante comandos de administración de paquetes en GNU/Linux. Este proceso permitió descargar e instalar los componentes necesarios para habilitar el servicio web dentro de la zona DMZ, garantizando la disponibilidad de los recursos requeridos para la publicación de contenido mediante el protocolo HTTP. Apache2 es ampliamente utilizado en entornos GNU/Linux debido a su estabilidad, flexibilidad y facilidad de administración [2].

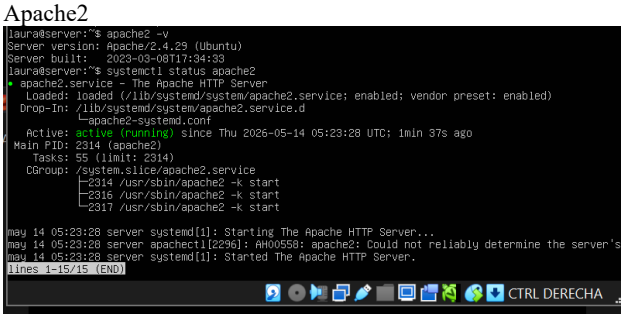
Figura 19. Instalación del servicio Apache2 en Ubuntu Server




*Fuente: Autoría propia*

Una vez completada la instalación, se verificó el estado operativo del servicio utilizando la herramienta systemctl. Esta validación permitió comprobar que Apache2 se encontraba activo y ejecutándose correctamente, asegurando que el servidor estaba preparado para atender solicitudes provenientes de los equipos autorizados dentro de la infraestructura de red implementada.

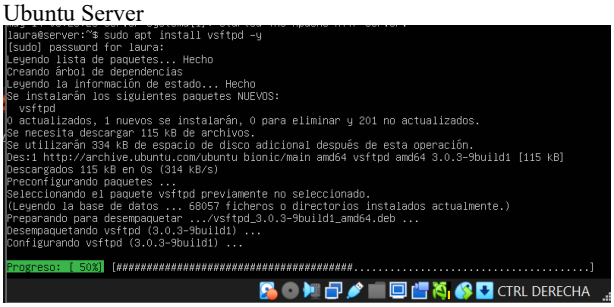
Figura 20. Validación del estado operativo del servicio Apache2




*Fuente: Autoría propia*

Posteriormente, se realizó la instalación del servicio FTP mediante VSFTPD (Very Secure FTP Daemon), una de las soluciones más utilizadas para la transferencia de archivos en sistemas GNU/Linux. La configuración de este servicio permitió habilitar mecanismos de autenticación y acceso controlado para los usuarios autorizados dentro de la red segmentada.

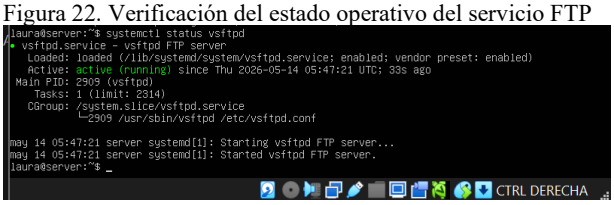
Figura 21. Instalación del servicio FTP mediante VSFTPD en Ubuntu Server




*Fuente: Autoría propia*

Finalmente, se verificó el estado operativo del servicio FTP mediante herramientas de administración del sistema, confirmando que VSFTPD se encontraba activo y disponible para recibir conexiones. Esta comprobación constituyó un paso previo indispensable antes de realizar las pruebas de acceso desde los equipos cliente ubicados en la zona VERDE.

Figura 22. Verificación del estado operativo del servicio FTP




*Fuente: Autoría propia*

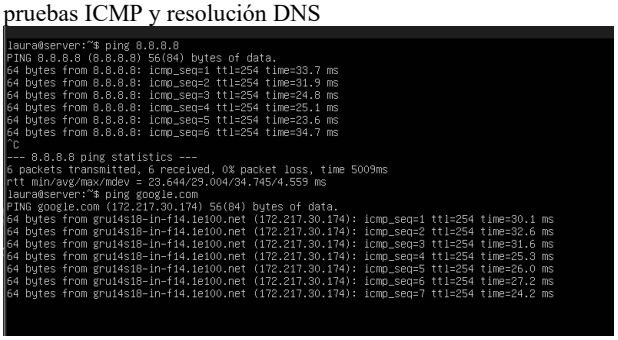
## 2.5 VALIDACIÓN DE CONECTIVIDAD Y SERVICIOS

Una vez implementados los servicios y configuradas las políticas de acceso en Endian Firewall, se realizaron diferentes pruebas de conectividad y validación con el fin de comprobar el correcto funcionamiento de la infraestructura virtualizada. Inicialmente, se verificó la comunicación entre los equipos mediante pruebas ICMP (ping) desde las diferentes zonas de red configuradas.

Posteriormente, se validó la salida a Internet desde Ubuntu Server mediante pruebas hacia direcciones públicas y resolución de nombres de dominio, confirmando el correcto funcionamiento de la interfaz ROJA (WAN) y de las reglas de tráfico de salida configuradas en el firewall.

Adicionalmente, se ejecutó el comando sudo apt update para comprobar el acceso a repositorios externos desde el servidor, verificando el funcionamiento adecuado de las reglas HTTP y HTTPS configuradas en Endian Firewall. Finalmente, se comprobó el acceso exitoso a los servicios implementados, validando la disponibilidad del servidor web Apache2 mediante navegador web y realizando pruebas de autenticación y conexión FTP desde el cliente Linux Mint hacia el servidor ubicado en la zona NARANJA (DMZ).

Figura 23. Validación de conectividad hacia Internet mediante pruebas ICMP y resolución DNS

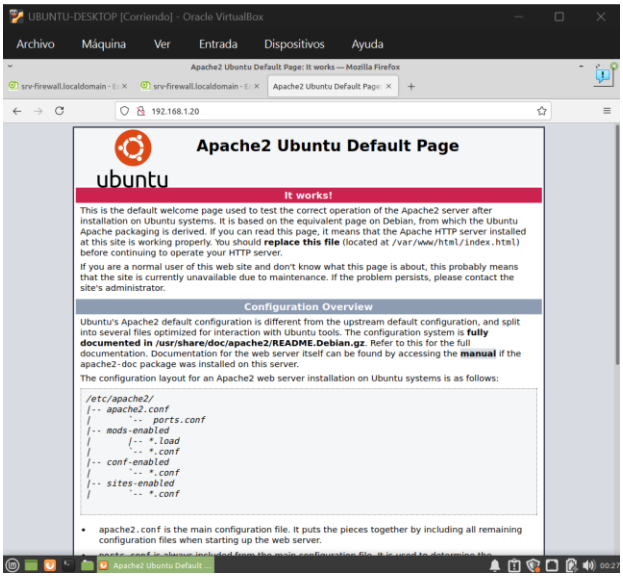



*Fuente: Autoría propia*

Los resultados obtenidos evidenciaron respuesta satisfactoria tanto hacia direcciones IP públicas como hacia dominios externos, confirmando el correcto funcionamiento de los mecanismos de enrutamiento, resolución DNS y acceso a Internet configurados previamente en la interfaz WAN del firewall. Estas pruebas permitieron verificar la conectividad del servidor hacia recursos externos necesarios para la operación normal de los servicios implementados.

Una vez validada la conectividad externa, se procedió a comprobar el acceso al servicio web Apache2 desde un equipo cliente ubicado en la zona VERDE. Esta prueba permitió verificar el correcto funcionamiento de las reglas Inter-Zona y NAT previamente configuradas, garantizando la publicación controlada del servicio en la zona DMZ.

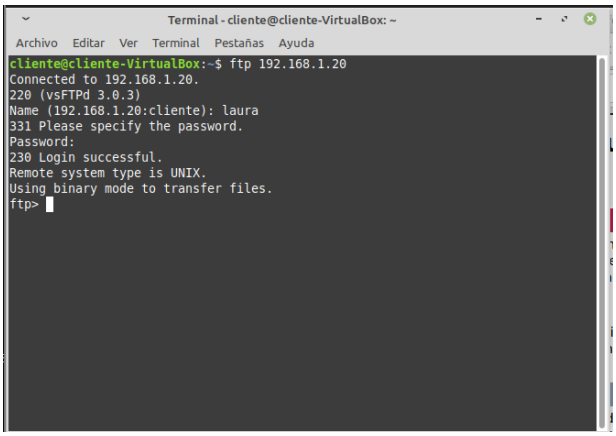
Figura 24. Validación del acceso HTTP desde la red interna hacia el servidor web en la DMZ




*Fuente: Autoría propia*

Finalmente, se realizó una prueba de autenticación y conexión FTP desde el cliente Linux Mint hacia el servidor ubicado en la zona NARANJA. La conexión exitosa confirmó el correcto funcionamiento del servicio VSFTPD, así como la adecuada aplicación de las políticas de acceso definidas dentro de la arquitectura de red implementada.

Figura 25. Validación del acceso FTP desde la zona VERDE hacia el servidor ubicado en la DMZ




*Fuente: Autoría propia*

# 3 RESULTADOS

La implementación del entorno de seguridad perimetral en GNU/Linux mediante Endian Firewall Community Edition permitió segmentar correctamente la red virtualizada en las zonas VERDE (LAN), NARANJA (DMZ) y ROJA (WAN), logrando controlar el tráfico entre los diferentes segmentos configurados. Las pruebas realizadas evidenciaron el correcto funcionamiento de las políticas de acceso Inter-Zona y de las reglas NAT implementadas, permitiendo la comunicación controlada entre los equipos virtualizados y el acceso hacia servicios específicos publicados en la DMZ.

Adicionalmente, se logró la implementación y validación de los servicios HTTP y FTP sobre Ubuntu Server, verificando su disponibilidad desde el cliente Linux Mint mediante pruebas de navegación web, autenticación FTP y conectividad ICMP. De igual manera, se comprobó el acceso exitoso a Internet desde el servidor utilizando reglas de salida configuradas en Endian Firewall. Estos resultados permitieron evidenciar el correcto funcionamiento de la infraestructura propuesta y fortalecer conocimientos relacionados con administración de redes GNU/Linux, segmentación de redes, configuración de firewalls, traducción de direcciones NAT y validación de servicios en entornos virtualizados.

# 4 CONCLUSIONES

La implementación de Endian Firewall Community Edition en un entorno virtualizado permitió comprender y aplicar conceptos fundamentales relacionados con la seguridad perimetral, la segmentación de redes y el control del tráfico en infraestructuras GNU/Linux. Mediante la configuración de las zonas VERDE (LAN), NARANJA (DMZ) y ROJA (WAN), fue posible establecer mecanismos de comunicación controlada entre diferentes segmentos de red, aplicando políticas de acceso, reglas Inter-Zona y traducción de direcciones de red (NAT) para garantizar un funcionamiento seguro de los servicios implementados. Asimismo, la instalación y validación de los servicios Apache2 y VSFTPD permitió comprobar la correcta publicación de recursos en la zona DMZ, mientras que las pruebas de conectividad, resolución DNS, acceso a Internet y autenticación FTP evidenciaron el adecuado funcionamiento de la arquitectura propuesta. Finalmente, el desarrollo de la práctica fortaleció competencias relacionadas con virtualización, administración de sistemas GNU/Linux, configuración de servicios de red y aplicación de mecanismos básicos de seguridad informática, integrando de manera efectiva los conocimientos teóricos y prácticos adquiridos durante el diplomado.

# 5 REFERENCIAS

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

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