# IMPLEMENTACIÓN DE UN ENTORNO DE SEGURIDAD PERIMETRAL EN GNU/LINUX MEDIANTE FIREWALL ENDIAN Y SEGMENTACIÓN LAN–DMZ–WAN

Omar Javier Aponte Navarrete
e-mail: ojaponten@unadvirtual.edu.co
Harryson Steven Baquero Castro
e-mail: hsbaqueroc@unadvirtual.edu.co
Ricardo Stid Ricardo Parra
e-mail: rsricardop@unadvirtual.edu.co
Luis David Huertas Redondo
e-mail: ldhuertasre@unadvirtual.edu.co
Johan Sebastian Moreno Ardila
e-mail: jsmorenoard@unadvirtual.edu.co

**RESUMEN:** *En esta actividad se implementó un entorno de seguridad perimetral utilizando GNU/Linux Endian como firewall central y VirtualBox como plataforma de virtualización. En la Temática 1, se configuraron las zonas Verde, Roja y Naranja, asegurando la segmentación LAN–WAN–DMZ. En la Temática 2, se establecieron reglas NAT para habilitar la comunicación entre LAN, DMZ e Internet, verificando la traducción de direcciones y el reenvío de puertos. En la Temática 3, se permitió y restringió tráfico específico mediante reglas para HTTP, FTP e ICMP, demostrando control granular de servicios. La Temática 4 fortaleció las políticas de acceso inter-zonas, validando la conectividad mediante pruebas de navegación. Finalmente, en la Temática 5 se implementó un Proxy HTTP con autenticación y listas negras, reforzando el control de navegación. Los resultados evidencian un entorno seguro, segmentado y administrado adecuadamente, aplicable a escenarios reales de protección perimetral.*

**PALABRAS CLAVE**: Endian, Firewall, GNU/Linux, Seguridad.

## 1 INTRODUCCIÓN

La ciberseguridad perimetral se ha vuelto fundamental en la administración de infraestructuras tecnológicas modernas. La necesidad de segmentar y controlar el tráfico entre distintas zonas de red permite mitigar riesgos, proteger servicios críticos y garantizar la integridad de la información. En este trabajo se implementa un entorno completo de seguridad utilizando el firewall GNU/Linux Endian (EFW), configurado en un escenario que incluye redes LAN, DMZ y WAN. A través de cinco temáticas, se desarrollan configuraciones de virtualización, reglas NAT, control de servicios, políticas inter-zona y un Proxy HTTP con autenticación y listas negras. El objetivo principal es fortalecer la arquitectura de seguridad mediante buenas prácticas basadas en Linux y firewalls perimetrales.

## 2 OBJETIVOS

### Objetivo General

Implementar un entorno de seguridad perimetral utilizando GNU/Linux Endian para segmentar redes, controlar servicios y gestionar políticas de acceso seguras entre la LAN, DMZ y WAN.

### Objetivos Específicos

Configurar la instancia de Endian en VirtualBox con sus zonas Verde, Roja y Naranja.

Implementar reglas NAT que permitan comunicación controlada entre LAN, DMZ e Internet.

Gestionar servicios desde la DMZ, permitiendo o denegando protocolos específicos.

Crear reglas de firewall inter-zona que garanticen el acceso seguro según los protocolos autorizados.

Implementar un Proxy HTTP con autenticación y políticas de filtrado mediante listas negras.

# 3 DESARROLLO DE LAS TEMÁTICAS

## 3.1 TEMÁTICA 1: CONFIGURACIÓN DE LA INSTANCIA ENDIAN EN VIRTUALBOX

Implementación de GNU/Linux Endian con las zonas verde, roja y naranja, así: Zona verde: Red interna (LAN), Zona roja: Acceso a internet (WAN) y Zona naranja: Servidores (DMZ).

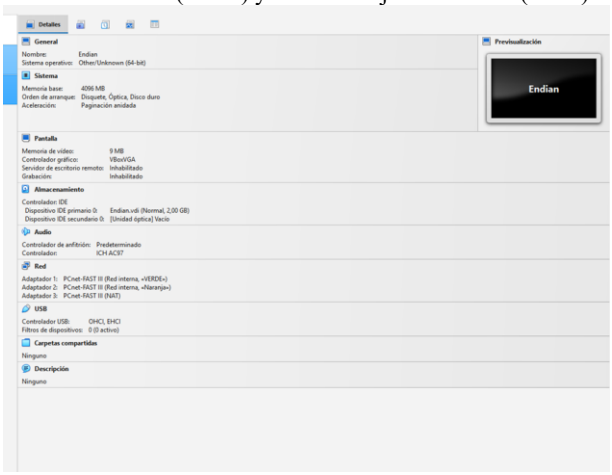



Imagen 1: Configuración Tarjetas de red Virtual Box

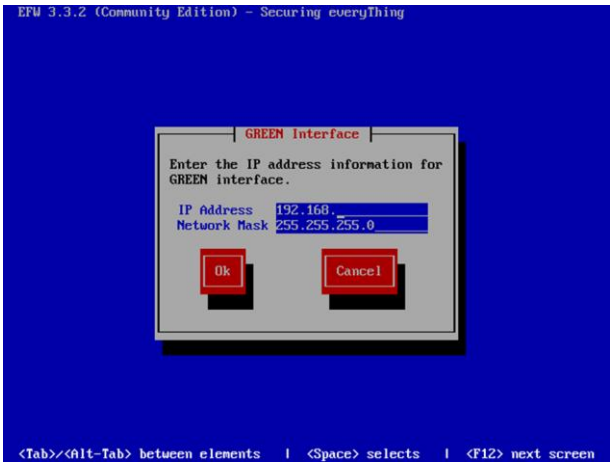



Imagen 2: Configuración instalación del ENDIAN Zona Verde

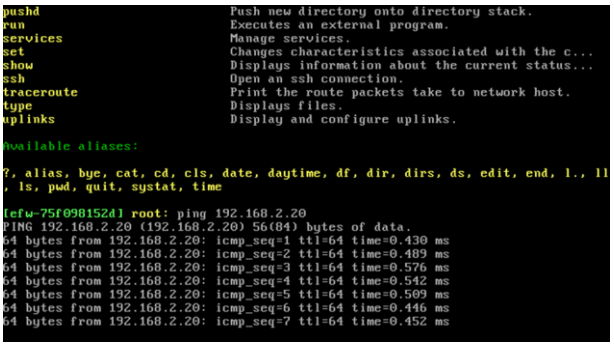



Imagen 3: ping ENDIAN Zona Verde Maquina Usuario

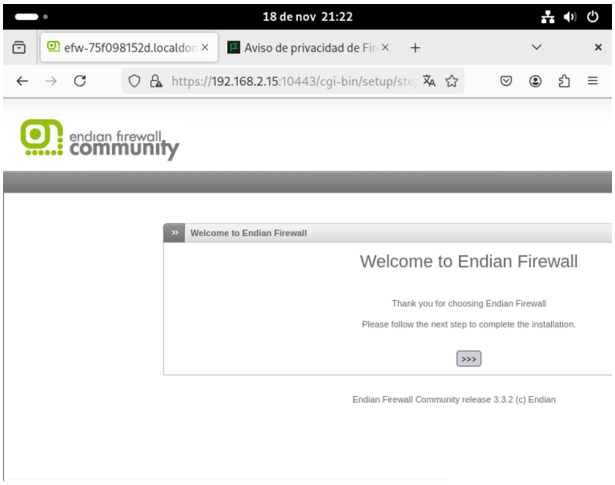



Imagen 4: Inicio sesión Instalación Endian desde equipo Usuario

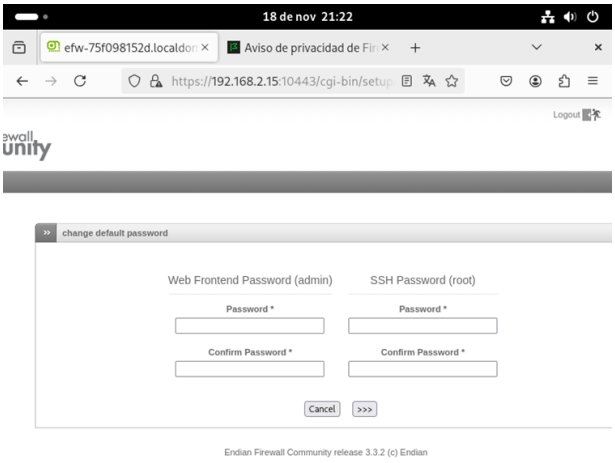



Imagen 5: Inicio sesión Endian desde equipo Usuario - Confirmación usuario admin

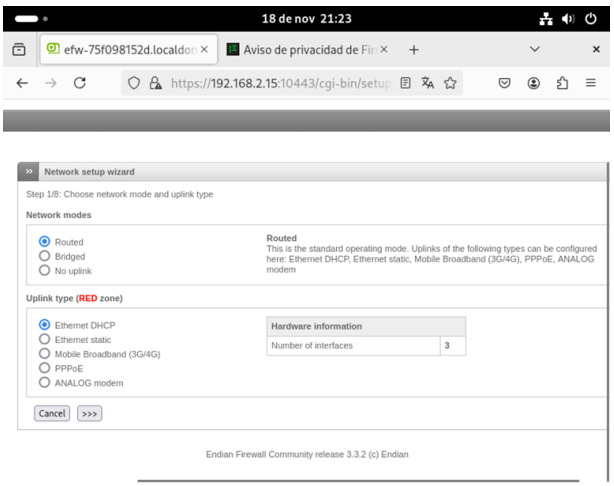



Imagen 6: Endian desde equipo Usuario - Configuración de zonas Roja – WAN

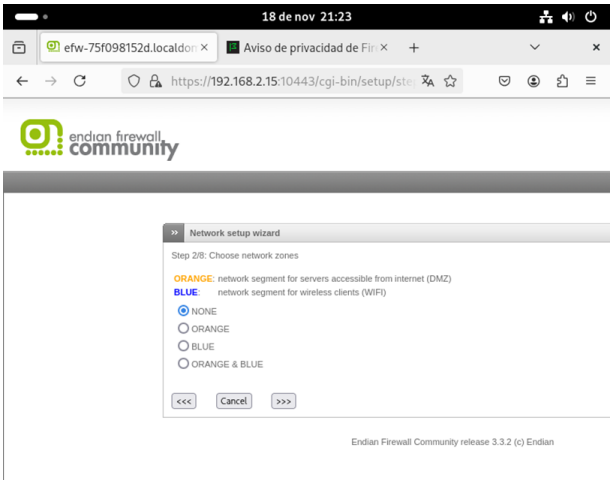



Imagen 7: Endian desde equipo Usuario - Configuración de zona Naranjada – DMZ

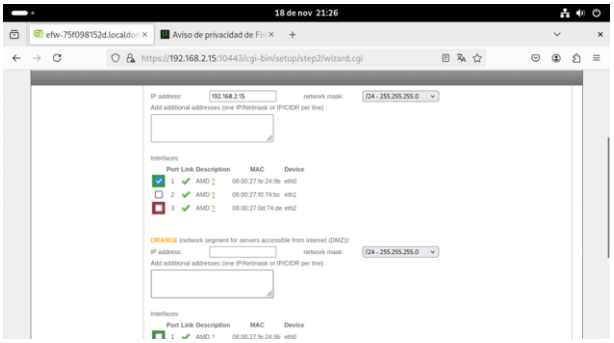



Imagen 8: Endian desde equipo Usuario - Configuración de zona Naranjada 2 – DMZ

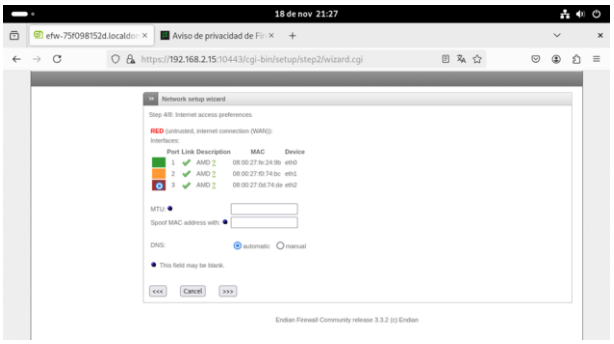



Imagen 9: Endian desde equipo Usuario - Configuración de zonas y activación de cada una

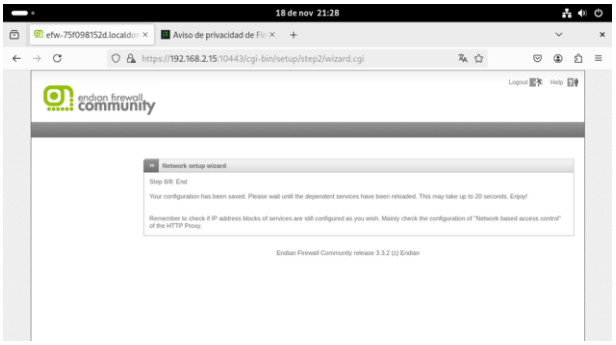



Imagen 10: Endian desde equipo Usuario - Configuracion culminada

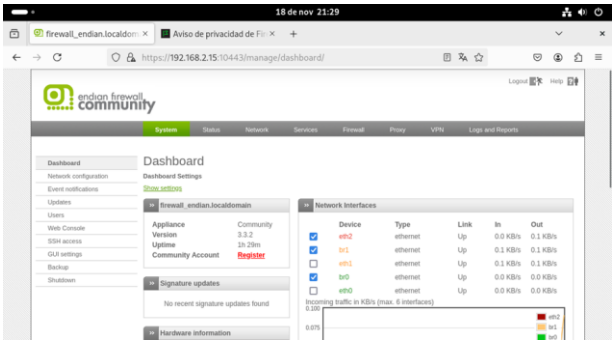



Imagen 11: Endian - Configuración resumida y coherente con lo solicitado VERDE -NARANJADA – ROJA

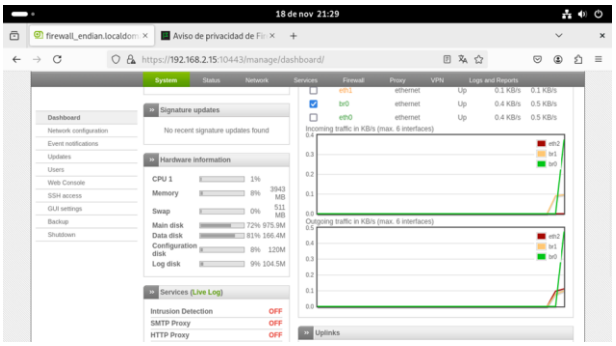



Imagen 12: Endian - VERDE -NARANJADA – ROJA Realizando Trafico Correspondiente

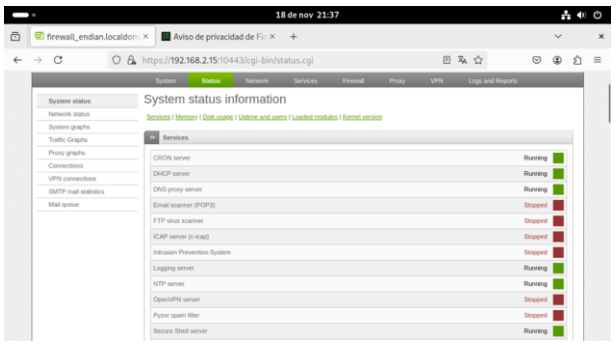



Imagen 13: Endian - Status System Information

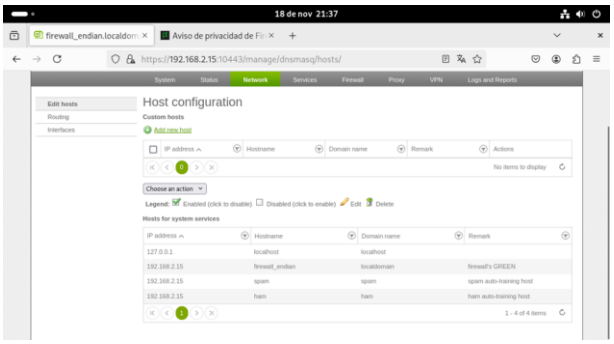



Imagen 14: Endian  Configuración de hosts

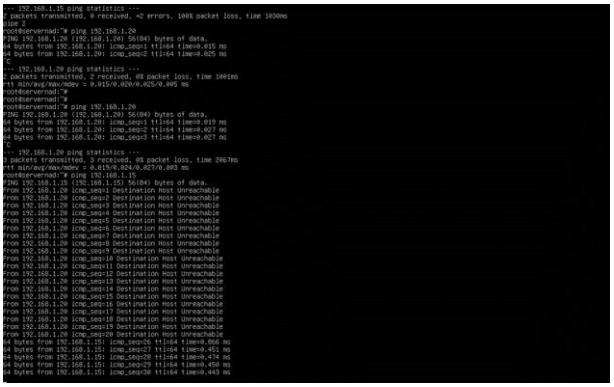


Imagen 15: Endian  Respuesta del servidor al Firewall exitosa

## 3.2 TEMÁTICA 2: CONFIGURACIÓN DE NAT

Configuramos la tarjeta de red como NAT desde VirtualBox:

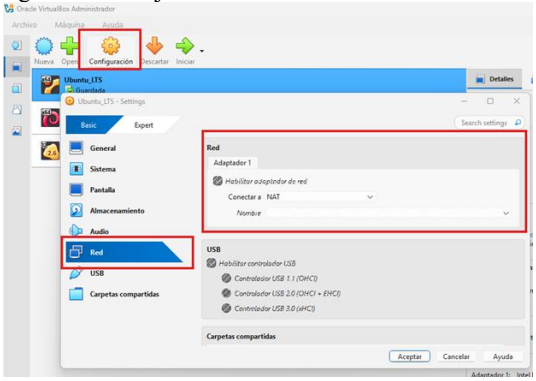


Ilustración 1. Configuración NAT en VirtualBox.

### 3.2.1 Configuración de la MV Ubuntu LTS (Gateway)

Activamos y ajustamos dos adaptadores:

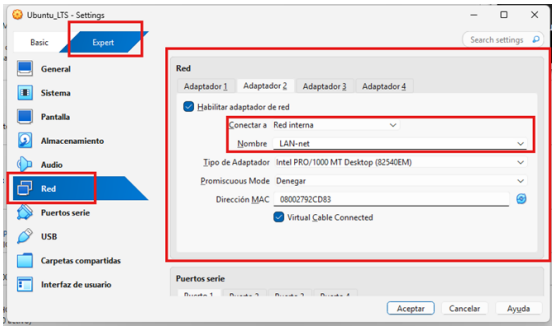


Ilustración 2. Activamos Adaptador 2.

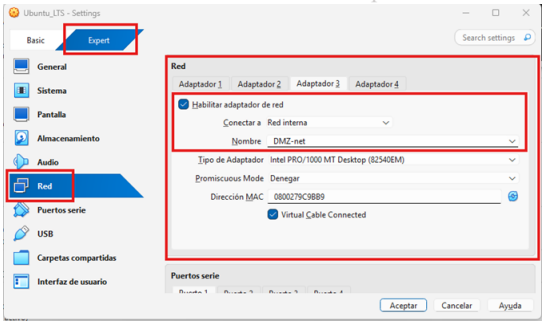


Ilustración 3. Activamos Adaptador 3.

Configuramos las IPs estáticas en los adaptadores que activamos:

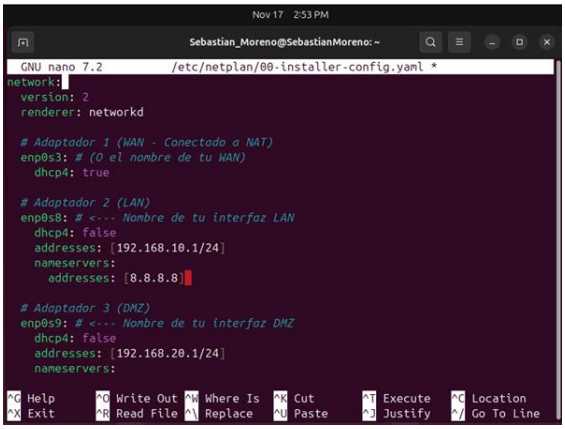



Ilustración 4. Archivo .yaml.

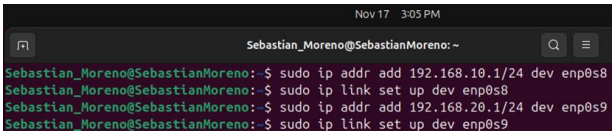



Ilustración 5. Ajustes de ip fija en Adaptadores.

Iniciamos la máquina de Debian y ajustamos dos adaptadores y ajustamos una ip de los mismos segmentos y hacemos una prueba de un ping:

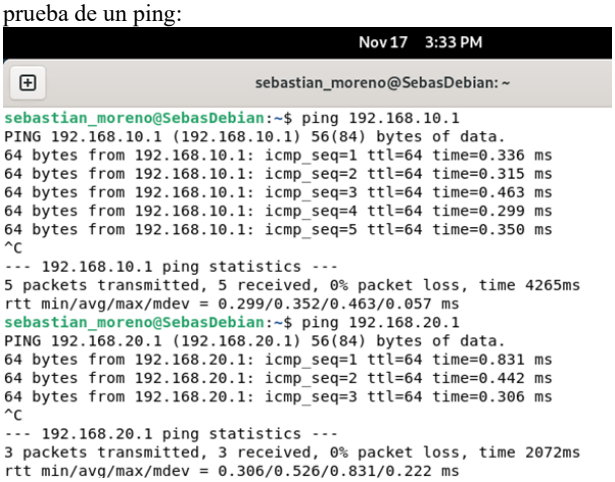



Ilustración 6. Prueba de ping desde Debian.

### 3.2.2: Configuración NAT con iptables

**Habilitar el Reenvío de Paquetes (IP Forwarding)**

Para que podamos mover el tráfico entre la red interna y la red externa debemos de permitir el reenvio de paquetes:

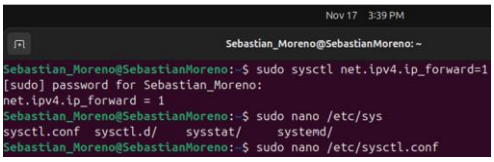



Ilustración 7. Habilitamos el Forward.

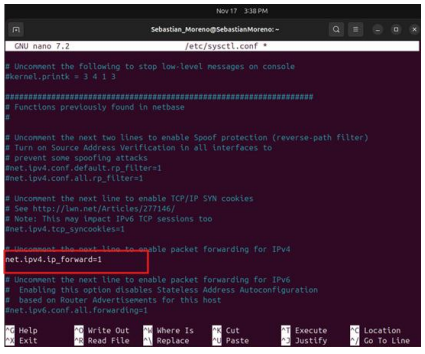



Ilustración 8. Eliminamos el #.

Limpiamos las reglas de NAT existentes:


Ilustración 9. Limpiamos las reglas NAT.

Configuramos la regla NAT:


Ilustración 10. Creamos regla NAT.

Verificamos desde Debian salida:

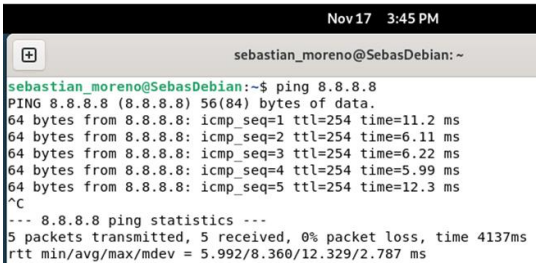



Ilustración 11. Ping a DNS de Google.

### 3.2.3 NAT de la DMZ hacia la WAN

Configuramos regla NAT:

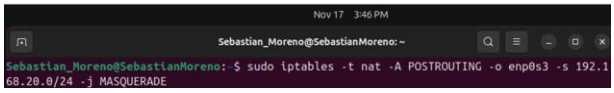



Ilustración 12. Regla NAT DMZ.

Comprobamos desde Ubuntu hacia Debian:

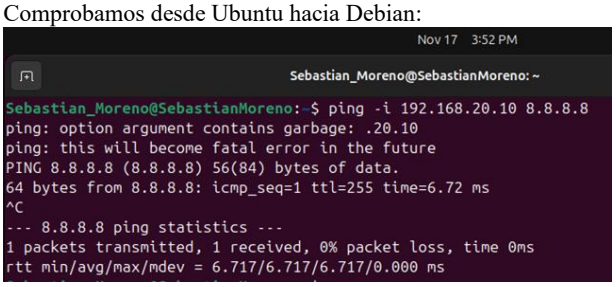



Ilustración 13. Confirmamos salida de internet por DMZ.

Configuramos la regla DNAT y FORWARD

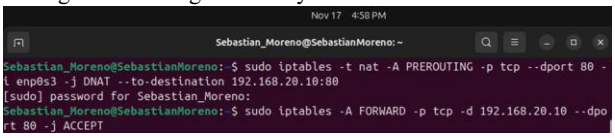



Ilustración 14. Regla DNAT y forward.

Verificamos el reenvió:

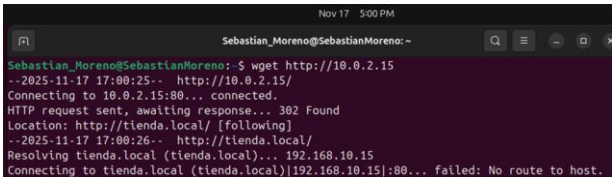



Ilustración 15. Confirmamos el forward.

### 3.2.4 Verificar la Creación de las Reglas

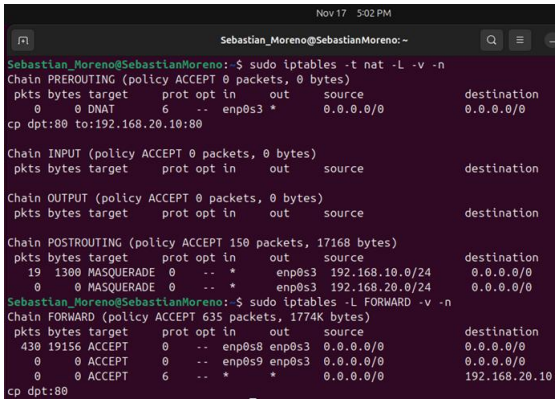
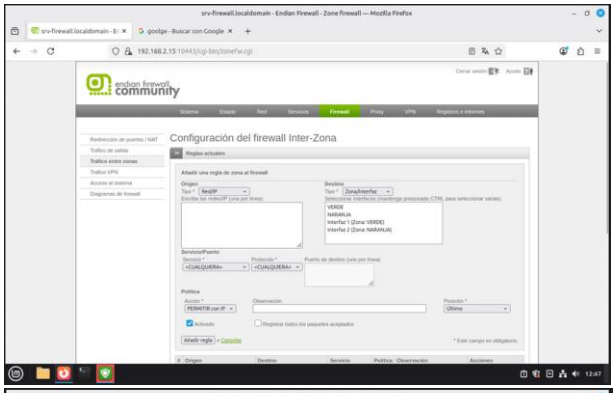
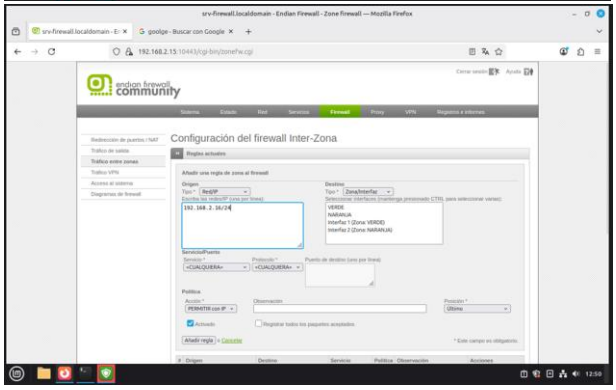



Ilustración 16. Confirmamos reglas.

## 3.3 TEMÁTICA 3: SERVICIOS DESDE LA DMZ

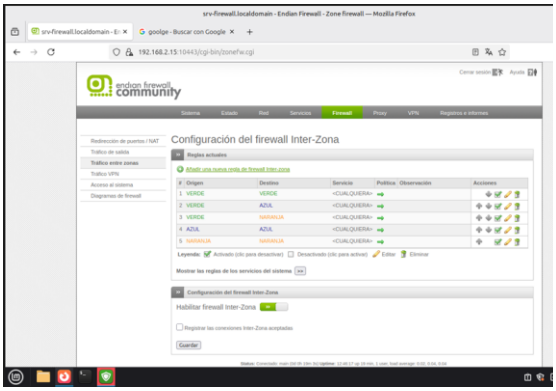
Permitir los servicios HTTP (Puerto 80) y FTP (Puerto 21) desde el servidor Web bajo Ubuntu Server.
2. Denegar el protocolo ICMP (Puerto 8 y puerto 30) para no permitir hacer ping en la red. Probar a través de una consola o terminal la no respuesta del comando ping hacia una IP de la red. Verificar en el tráfico de salida, la creación de las reglas.



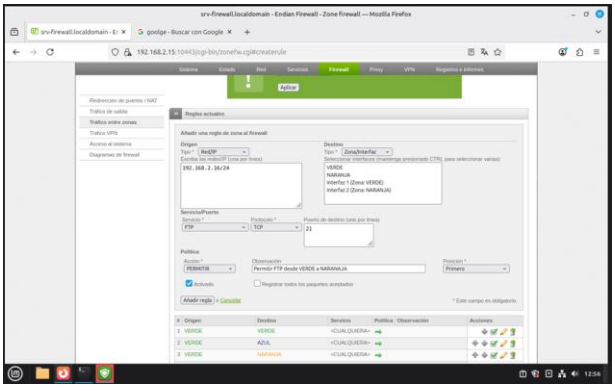

#### 3.3.1.1. — HTTP hacia el servidor DMZ (Permisos HTTP puerto 80)

- Origen: 192.168.2.16/24 (Linux Mint)
- Destino: Zona NARANJA
- Servicio: TCP/80 (HTTP)
- Acción: PERMITIR
- Propósito: Acceso a servicios web del servidor Ubuntu



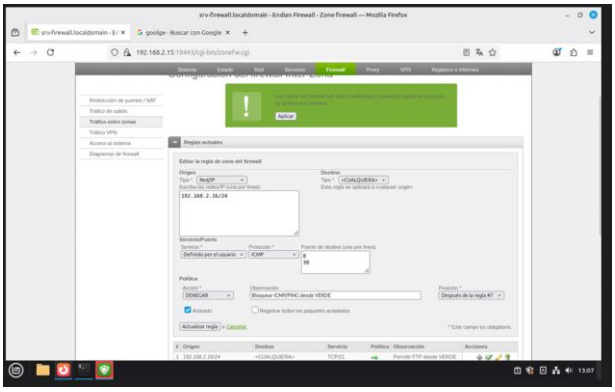

#### 3.3.1.2: Permiso FTP para (Puerto 21)

- Origen: 192.168.2.16/24 (Linux Mint)
- Destino: Zona NARANJA
- Servicio: TCP/21 (FTP)
- Acción: PERMITIR
- Propósito: Transferencia de archivos al servidor DMZ



#### 3.3.1.3. Bloqueo ICMP

- Origen: 192.168.2.16/24 (Linux Mint)
- Destino: Zona NARANJA
- Servicio: ICMP/8 (Echo Request)
- Acción: DENEGAR
- Propósito: Prevención de descubrimiento de hosts via ping



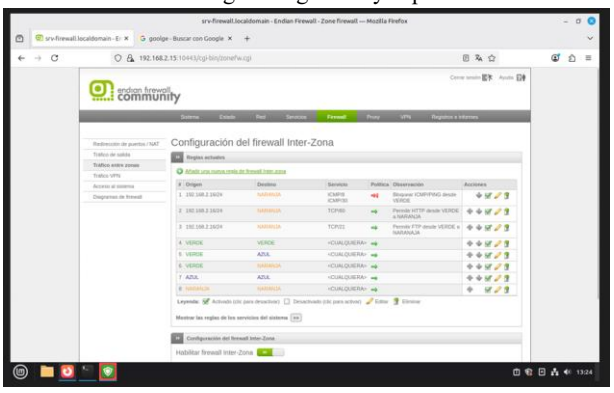
### 3.3.2. Implementación

#### 3.3.2.1. Configuración de Reglas

Las reglas se configuraron en la sección "Trafico entre zonas" del Endian Firewall Community 3.3.2, asegurando el orden de procesamiento correcto para la evaluación de políticas.

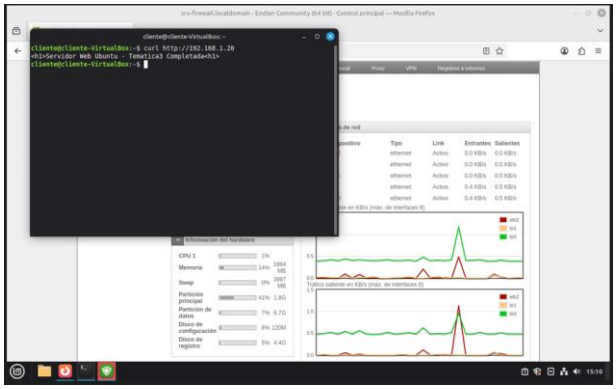
### 3.3.3 Servicios Implementados

- Servidor Web: Python HTTP Server en puerto 80
- Servidor FTP: Netcat listener en puerto 21
- Cliente de pruebas: Linux Mint 22.2
- Todas las Reglas en general ya aplicadas

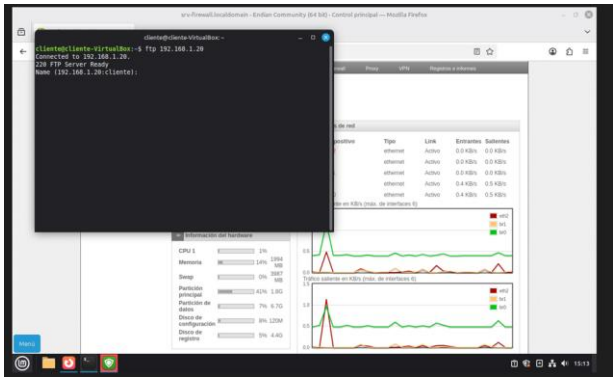


### 3.3.4. Resultados y Verificación

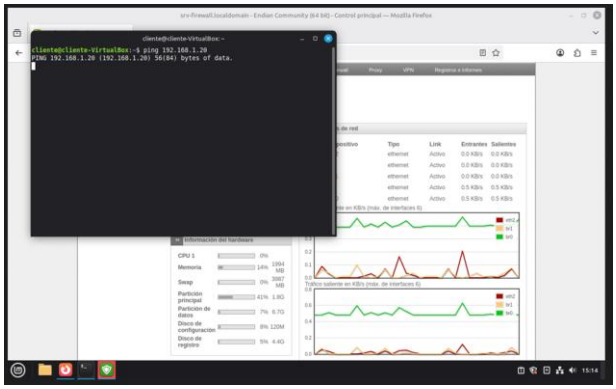
3.**3.4.1. Permitir HTTP (Puerto 80)** – FUNCIONAL



3.3.4.2. Permitir FTP – FUNCIONAL



3.3.4.3. Denegar PING – NO FUNCIONAL



No arroja ningún ping ni paquetes enviados, por ende podemos concluir que se bloqueó el PING

### 3.3.5. Análisis de Seguridad

#### 3.3.5.1 Efectividad de las Políticas

- La configuración implementada demuestra:
- Control granular sobre servicios permitidos
- Bloqueo efectivo de protocolos no esenciales
- Aislamiento adecuado de la zona DMZ

#### 3.3.5.2 Cumplimiento de Objetivos

- Servicios HTTP y FTP accesibles desde red interna
- Protocolo ICMP completamente bloqueado
- Reglas de firewall verificadas y operativas

## 3.4 TEMÁTICA 4: REGLAS ENTRE ZONAS

La seguridad perimetral es esencial para proteger la integridad de los sistemas y aplicaciones en entornos corporativos. En esta temática se implementan reglas de acceso en Endian Firewall para controlar la comunicación entre zonas críticas (LAN, DMZ e Internet), asegurando que solo los servicios autorizados puedan establecer conexión.

Se utilizó Endian Community Firewall instalado en VirtualBox, configurando tres interfaces:

- Zona Verde (LAN): Red interna para estaciones de trabajo.
- Zona Naranja (DMZ): Servidor Ubuntu con servicios HTTP y FTP.
- Zona Roja (WAN): Acceso a Internet.

Se configuró los adaptadores de red en VirtualBox de la siguiente manera para cada una de las máquinas virtuales:

- Endian
  - Adaptador 1: Red interna “VERDE”
  - Adaptador 2: Red interna “NARANJA”
  - Adaptador 3: NAT
- Ubuntu Desktop
  - Adaptador 1: NAT
  - Adaptador 2: Red interna “VERDE”
- Ubuntu Server
  - Adaptador 1: NAT
  - Adaptador 2: Red interna “NARANJA”

Figura 1. Configuración de redes para la MV Endian


Configuración de IP estáticas:

- LAN: 192.168.2.20
- DMZ: 192.168.1.20

Figura 2. Configuración de la IP estática para la red LAN

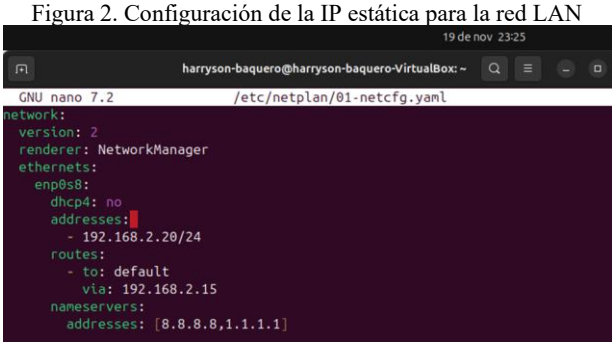
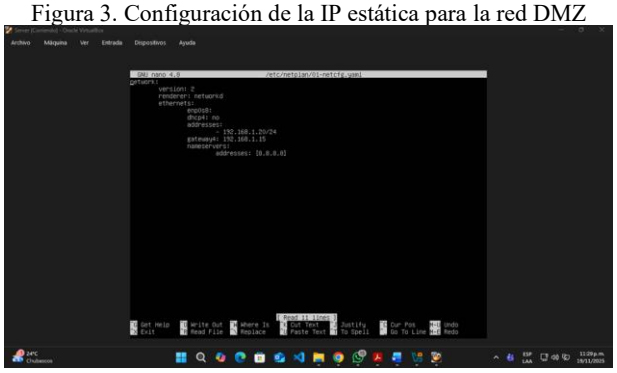
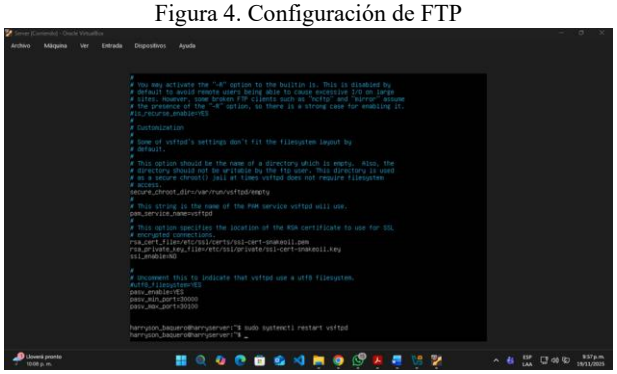



Figura 3. Configuración de la IP estática para la red DMZ



Instalación y configuración de Apache y FTP (vsftpd) en el servidor DMZ. La herramienta Apache HTTP nos permite tener un servicio disponible para realizar pruebas de acceso, y la herramienta FTP con su respetiva configuración permitirá soportar conexiones FTP estándar y pasivas.

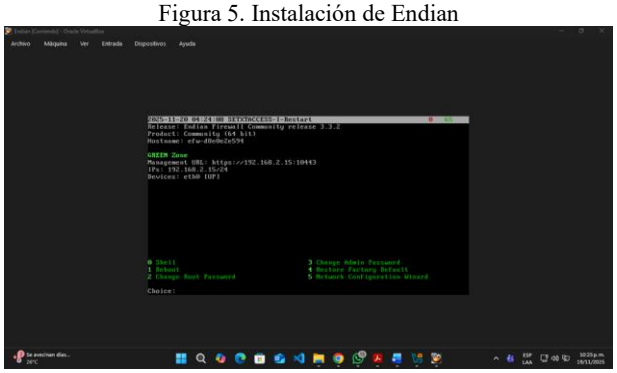
Figura 4. Configuración de FTP



En esta instancia se desactiva la red NAT para las máquinas virtuales Ubuntu Desktop y Ubuntu Server en VirtualBox, dejando solo activas las redes internas de cada MV para que no haya problemas de conexión.

Con las máquinas virtuales apagadas, se procede a la instalación y configuración de Endian. En esta instalación se pide la direción IP LAN (zona verde), la cual para el ejercicio fue 192.168.2.15.

Figura 5. Instalación de Endian



Con la ruta configurada que nos da Endian: https://192.168.2.15:10443, ingresamos desde el navegador de Ubuntu Desktop para configurar las redes desde el dashboard de Endian.

Figura 6. Comprobación de lectura sobre las tres intefaces

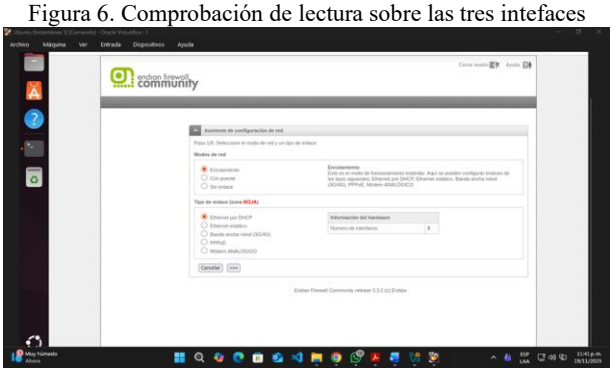
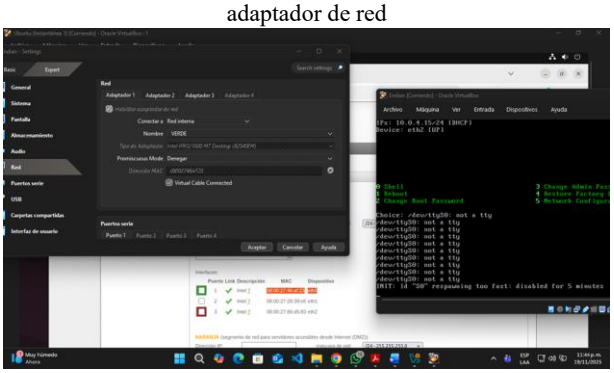
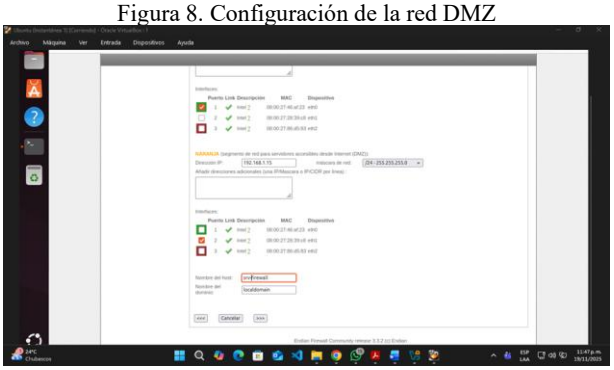


Figura 7. Comprobación de las direcciones MAC para cada adaptador de red



La zona DMZ se configura directamente en Endian, para este ejercicio se configuró la IP 192.168.1.15.

Figura 8. Configuración de la red DMZ

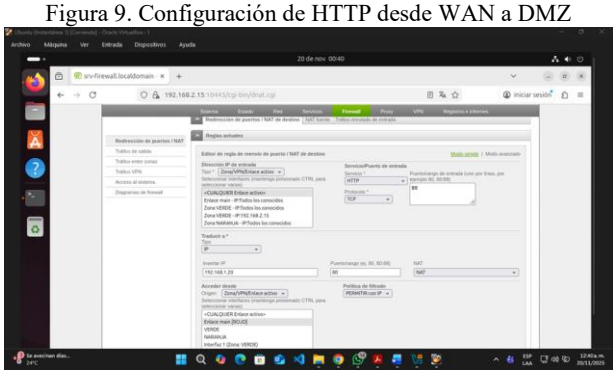


Una vez configuradas las conexiones y lotaje de IP para cada zona, se procede con las reglas a implementar para el desarrollo de las pruebas.

**Reglas implementadas:**

1. **Permitir HTTP y FTP entre Zona Verde y Zona Naranja**:
    a. GREEN → ORANGE (HTTP, FTP, FTP pasivo).
2. **Permitir tráfico desde DMZ hacia Internet**.
3. **Permitir HTTP, FTP y FTP pasivo desde WAN hacia DMZ**.

Figura 9. Configuración de HTTP desde WAN a DMZ



Al finalizar se verifica en logs Inter-Zona para confirmar aplicación de reglas.

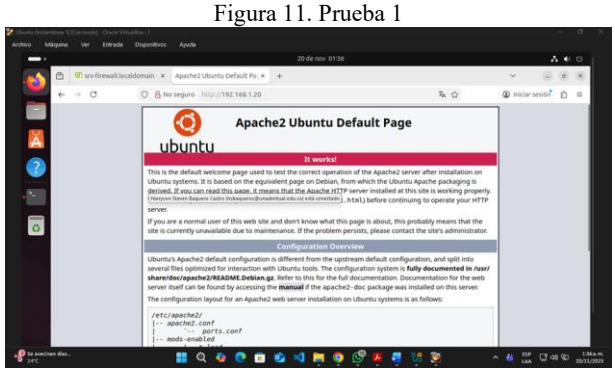
Figura 10. Verificación de reglas para tráfico entre zonas

Figura 10. Verificación de reglas para tráfico de salida

Una vez configuradas las reglas de conexión entre las zonas, se procede a realizar las pruebas.

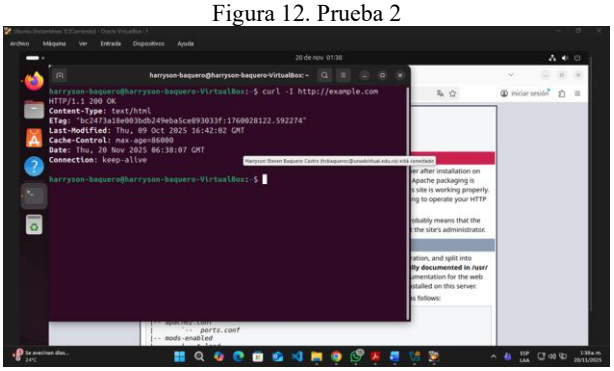
**Prueba 1:** HTTP desde LAN → DMZ Desde el navegador en desktop: http://192.168.1.20

Figura 11. Prueba 1



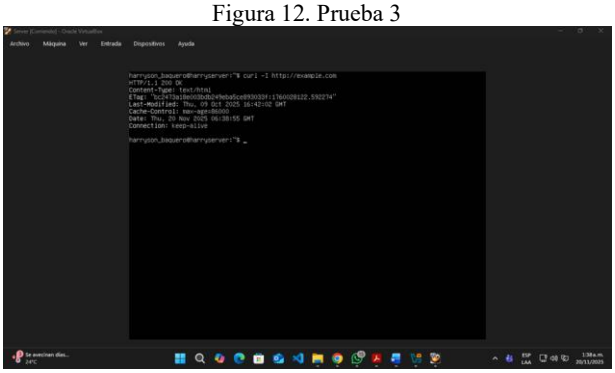
**Prueba 2:** HTTP desde LAN → WAN Desde el shell de desktop ejecutar curl -I http://example.com

Figura 12. Prueba 2



**Prueba 3:** HTTP desde DMZ → WAN Desde el shell de Ubuntu Server ejecutar curl -I http://example.com

Figura 12. Prueba 3



**Registro en tiempo real:** Observación de conexiones activas en el panel Live Connections. Donde se logra evidenciar nuevamente las conexiones entre las tres zonas configuradas.

Figura 13. Registro de conexiones activas

Las pruebas realizadas confirmaron la correcta aplicación de las reglas de acceso configuradas en el firewall Endian. Cada escenario validó la comunicación entre las zonas según lo establecido: acceso HTTP y FTP entre LAN y DMZ, conectividad desde DMZ hacia Internet y tráfico controlado desde WAN hacia DMZ. Además, la visualización en tiempo real de las conexiones activas y la revisión de los registros Inter-Zona evidenciaron que las políticas implementadas cumplen con los objetivos de segmentación y seguridad definidos para esta práctica.

## 3.5 TEMÁTICA 5: PROXY HTTP CON AUTENTICACIÓN

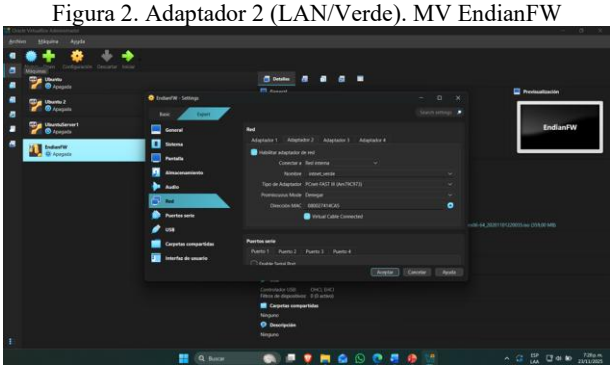
**Pasos previos:**

- Descargar recursos (ISO): Endian Firewall Community (EFW) y Cliente GNU/Linux.
- Configuración de VirtualBox, Aquí configuraremos las "zonas" que exige la guía (Verde, Roja, Naranja).

Figura 1. Adaptador 1 (WAN/Roja). MV EndianFW

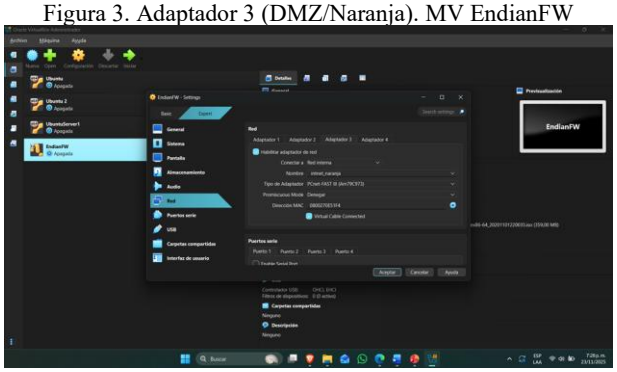
Fuente: Autoría Propia

Figura 2. Adaptador 2 (LAN/Verde). MV EndianFW



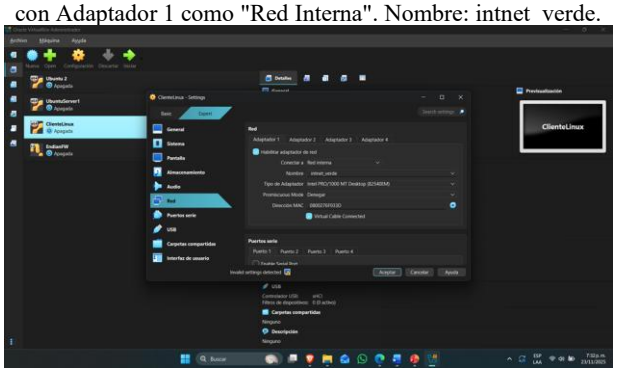
Fuente: Autoría Propia

Figura 3. Adaptador 3 (DMZ/Naranja). MV EndianFW



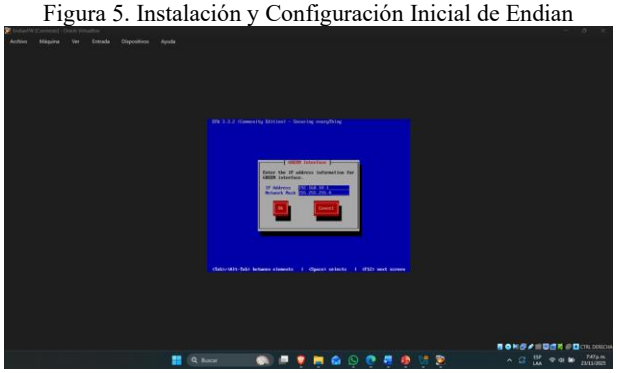
Fuente: Autoría Propia

Figura 4. Crear Máquina Virtual para el Cliente (El Usuario) con Adaptador 1 como "Red Interna". Nombre: intnet_verde.



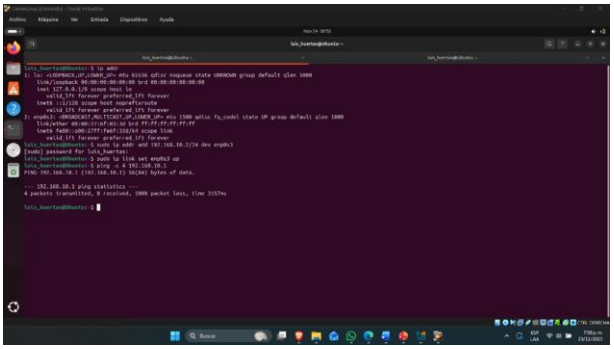
Fuente: Autoría Propia

Figura 5. Instalación y Configuración Inicial de Endian



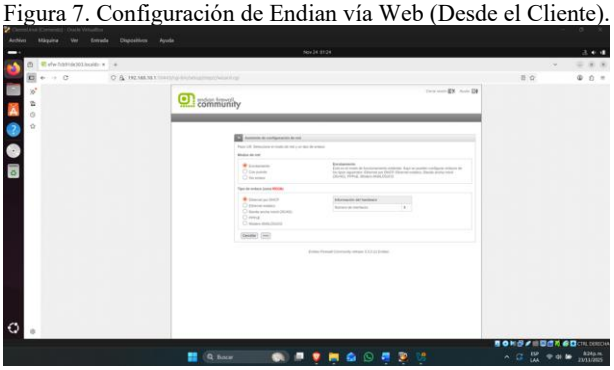
Fuente: Autoría Propia

Figura 6. Configuración del Cliente Linux para generar conexión con Endian



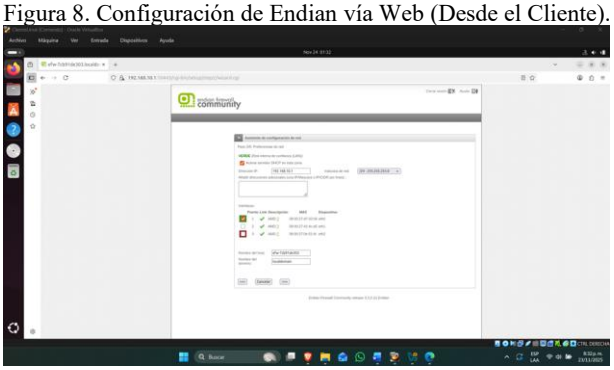
Fuente: Autoría Propia

Figura 7. Configuración de Endian vía Web (Desde el Cliente).



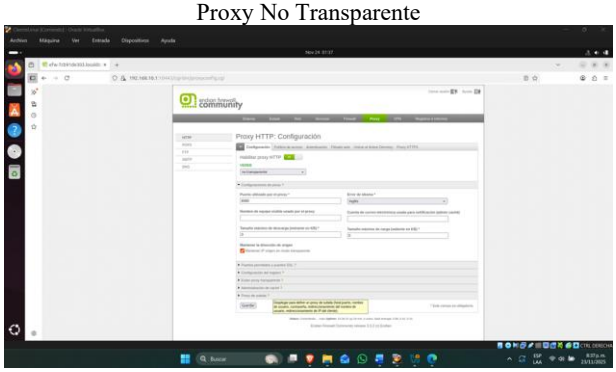
Fuente: Autoría Propia

Figura 8. Configuración de Endian vía Web (Desde el Cliente).



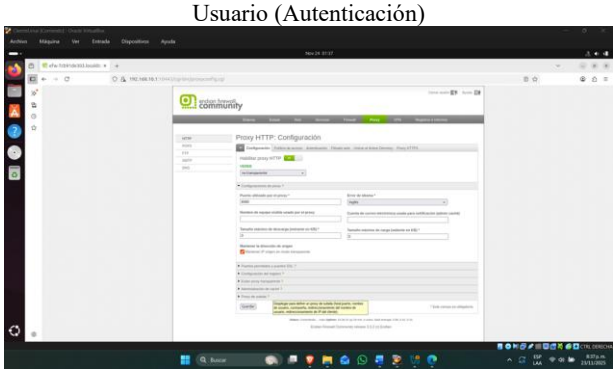
Fuente: Autoría Propia

Figura 9. Desarrollo de la Temática 5 (El Proxy). Habilitar Proxy No Transparente



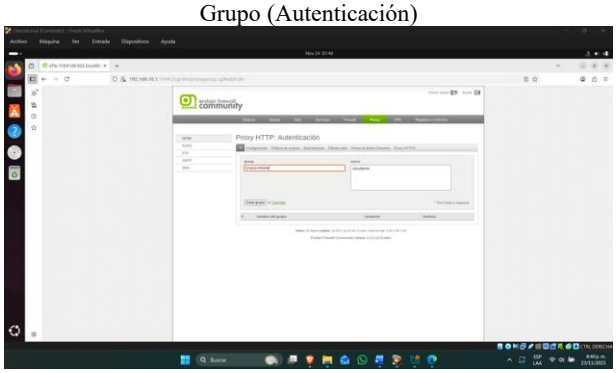
Fuente: Autoría Propia

Figura 10. Desarrollo de la Temática 5 (El Proxy). Crear Usuario (Autenticación)



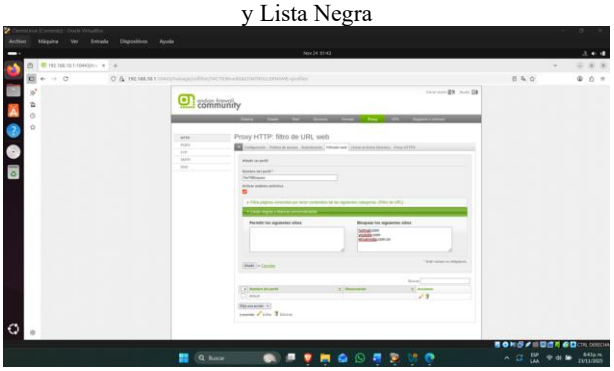
Fuente: Autoría Propia

Figura 11. Desarrollo de la Temática 5 (El Proxy). Crear Grupo (Autenticación)



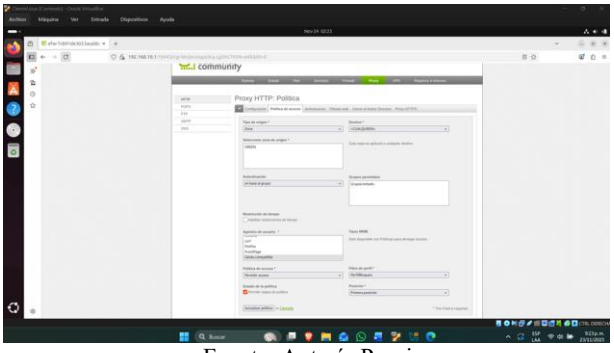
Fuente: Autoría Propia

Figura 12. Desarrollo de la Temática 5 (El Proxy). Crear Perfil y Lista Negra



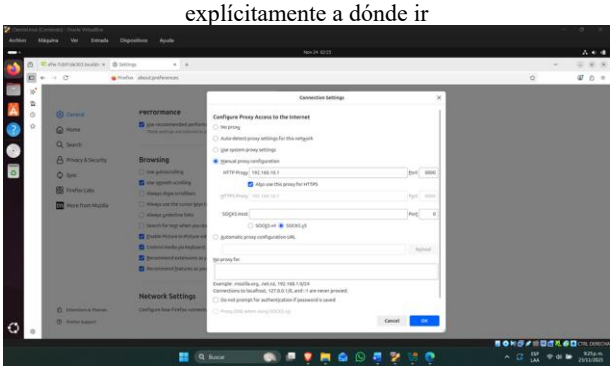
Fuente: Autoría Propia

Figura 13. Desarrollo de la Temática 5 (El Proxy). Crear Política de Acceso



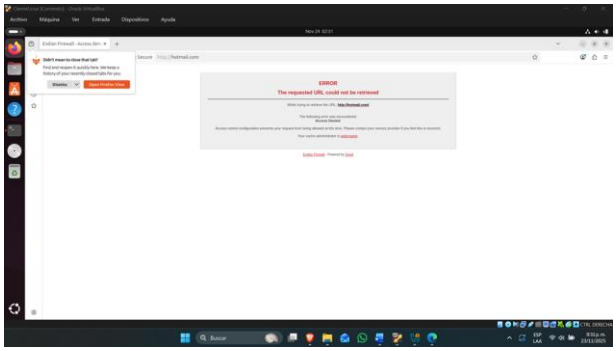
Fuente: Autoría Propia

Figura 14. Configurar el Proxy en el Sistema/Navegador: Como es "No Transparente", el cliente debe saber explícitamente a dónde ir



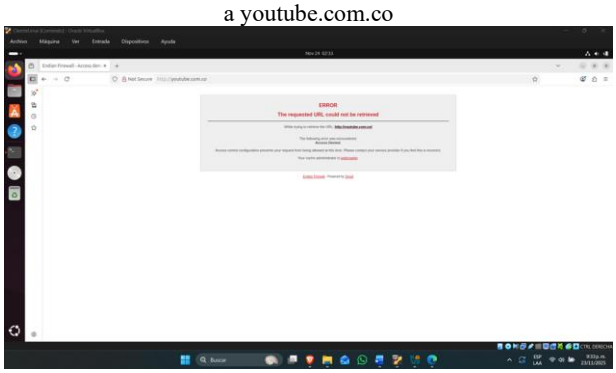
Fuente: Autoría Propia

Figura 15. Prueba de Navegación y Bloqueo: Intento de entrar a hotmail.com



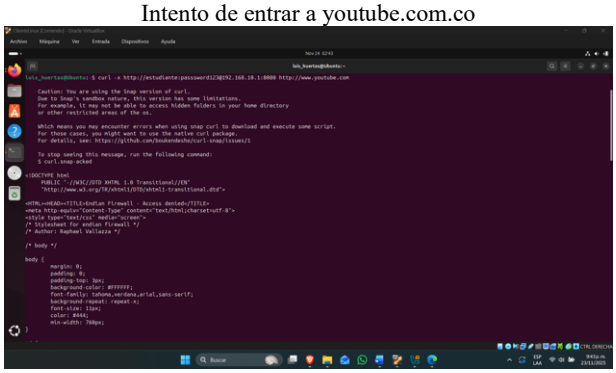
Fuente: Autoría Propia

Figura 16. Prueba de Navegación y Bloqueo: Intento de entrar a youtube.com.co



Fuente: Autoría Propia

Figura 17. Prueba de Navegación y Bloqueo desde consola: Intento de entrar a youtube.com.co



Fuente: Autoría Propia

# 4 CONCLUSIONES

La configuración de la instancia de GNU/Linux Endian en VirtualBox permitió establecer la base estructural del entorno de seguridad perimetral. La correcta definición de las zonas Verde, Roja y Naranja aseguró una segmentación clara entre la red interna, la DMZ y el acceso a Internet, garantizando un aislamiento que reduce riesgos y fortalece la arquitectura de seguridad. Este proceso evidenció el papel fundamental de la virtualización en la creación de escenarios controlados para implementar y validar configuraciones críticas sin impactar infraestructuras reales. Asimismo, demostró cómo la precisión en la asignación de interfaces, direcciones IP y parámetros de red influye directamente en la efectividad de las políticas y servicios aplicados en las siguientes temáticas. En síntesis, esta primera etapa no solo consolidó conocimientos esenciales en administración de redes y firewalls perimetrales, sino que estableció los cimientos necesarios para la implementación exitosa del resto de mecanismos de seguridad.

**Temática 4:** La implementación de reglas de acceso en el firewall Endian demostró ser una solución efectiva para garantizar la seguridad perimetral en entornos GNU/Linux. La correcta segmentación de las zonas LAN, DMZ y WAN, junto con la aplicación de políticas específicas para protocolos HTTP y FTP, permitió controlar el flujo de tráfico de manera segura y eficiente. Las pruebas y verificaciones realizadas confirman que la configuración propuesta cumple con los principios de protección y disponibilidad de servicios, fortaleciendo la arquitectura de red frente a posibles riesgos

La implementación de la **Temática 5: Proxy HTTP No Transparente** fue exitosa, validando el cumplimiento de los objetivos de seguridad y filtrado requeridos. El requisito de un Proxy No Transparente se cumplió obligando al cliente a configurar manualmente su navegador y, simultáneamente, se verificó el requisito de seguridad al requerir la autenticación por usuario/grupo antes de permitir el tráfico. El perfil de filtro, con la lista negra personalizada, se aplicó correctamente a través de la política de acceso, bloqueando de manera efectiva el acceso a los sitios prohibidos (como www.youtube.com), lo cual fue demostrado con la respuesta "Acceso Denegado" del Proxy.

# 5 REFERENCIAS


- LPI Linux Essentials. (2022). Tema 1: La Comunidad Linux y una carrera en el mundo del código abierto . https://learning.lpi.org/es/learning-materials/010-160/1/

- LPI Linux Essentials.(2022). Tema 2: Encontrando el camino en un sistema Linux . https://learning.lpi.org/es/learning-materials/010-160/2/

- LPI Linux Essentials.(2022). Tema 3: El poder de la línea de comandos . https://learning.lpi.org/es/learning-materials/010-160/3/

- Free Software Foundation (2016). Software Libre y educación. El sistema operativo GNU . http://www.gnu.org/education/education.html

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

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

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

- LPI Linux Essentials. (2022). Tema 1: La Comunidad Linux y una carrera en el mundo del código abierto. https://learning.lpi.org/es/learning-materials/010-160/1/

- Free Software Foundation (2016). Software Libre y educación. El sistema operativo GNU. http://www.gnu.org/education/education.html

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

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

- Oracle (2020), Manual de usuario VirtualBox. VirtualBox. https://www.virtualbox.org/manual/

- Guzman Arevalo, D. ( 20,01,2017). OVI Unidad I_Nivelacion. [Archivo de video]. Repositorio UNAD. http://hdl.handle.net/10596/10570