“Implementación del Firewall Endian en entorno virtualizado como estrategia de segmentación de red en GNU/Linux “

Fabian Andres Gonzalez Fuentes
fagonzalezfu@unadvirtual.edu.co
Juan David Saboya Jimenez
jdsaboyaj@unadvirtual.edu.co
Yerly Milena Vallejo Colmenares
ymvallejoco@unadvirtual.edu.co
Kevin Sting Garcia Corredor
ksgarciac@unadvirtual.edu.co

RESUMEN: *Este artículo presenta la implementación de una solución integral para la seguridad perimetral de redes corporativas utilizando la distribución Endian Firewall. El trabajo, desarrollado en un entorno virtualizado con VirtualBox, detalla la configuración de la infraestructura de red, incluyendo la definición de zonas de seguridad (Verde, Naranja, Roja) para la segmentación lógica de la LAN y una DMZ destinada a servidores. Se documentan los procedimientos para establecer reglas de Traducción de Direcciones de Red (NAT), configurar políticas de control de acceso para regular el flujo de tráfico entre las distintas zonas, permitir servicios específicos en la DMZ, y desplegar un proxy HTTP con capacidades de autenticación y filtrado de contenido. La implementación práctica demostró la efectividad de Endian Firewall como herramienta de código abierto para fortalecer la seguridad de la red, validar la segmentación de zonas y controlar el acceso a recursos internos y externos, consolidando las habilidades en diseño y despliegue de arquitecturas de red seguras.*

PALABRAS CLAVE: Firewall, Seguridad Perimetral, Segmentación de Redes, Virtualización, Efw.

1 INTRODUCCIÓN

En la actualidad, la seguridad informática representa un componente esencial en la administración de redes, especialmente en entornos que requieren la segmentación del tráfico para proteger servicios críticos. En este contexto, los firewalls se posicionan como herramientas fundamentales para mitigar riesgos y garantizar la confidencialidad, integridad y disponibilidad de la información.

El presente trabajo aborda la implementación del firewall Endian Community en un entorno virtualizado mediante VirtualBox, como parte de una estrategia académica orientada al fortalecimiento de competencias en GNU/Linux. a elección de Endian obedece a su enfoque en la seguridad perimetral, facilidad de configuración mediante interfaz web y su naturaleza como software libre, lo que lo convierte en una opción viable para instituciones educativas y entornos corporativos con recursos limitados

2 DESARROLLO DE ACTIVIDADES

Instalación y configuración de la distribución GNU/Linux Endian (EFW), así mismo seleccionar una de las siguientes cinco (5) temáticas y darle solución bajo esta distribución.

2.1 INSTALACIÓN Y CONFIGURACIÓN DE LA DISTRIBUCIÓN GNU/LINUX ENDIAN (EFW)

Para llevar a cabo la implementación del firewall de código abierto Endian, se optó por realizar el proceso dentro de un entorno controlado utilizando VirtualBox, se descarga de la figura ISO de Endian Firewall Community Edition desde su sitio oficial.

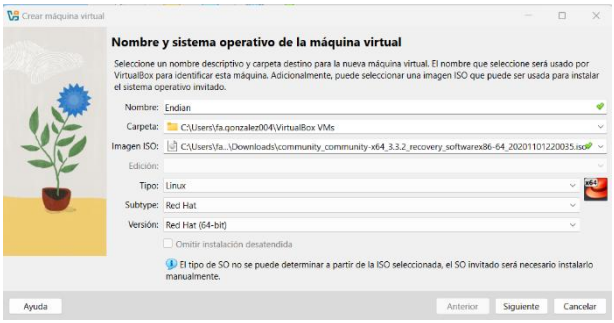

figura 1 Configuración de la máquina Virtual en VirtualBox Endian Fuente: Elaboración Propia – 2025.

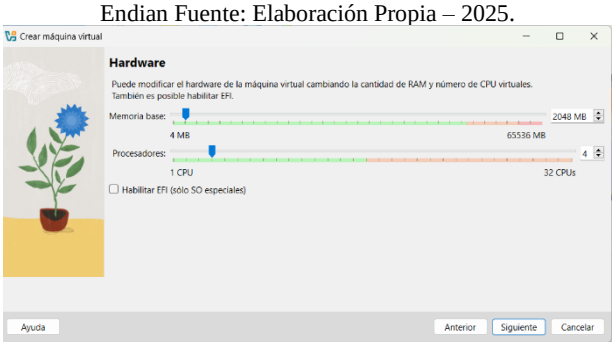

figura 2 Configuración Hardware Fuente: Elaboración Propia – 2025.

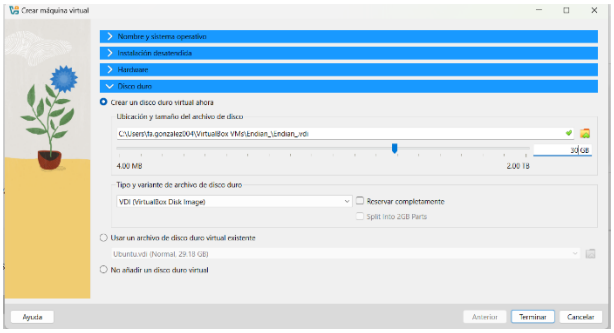

figura 3 Configuración Disco Duro Virtual Fuente: Elaboración Propia – 2025.

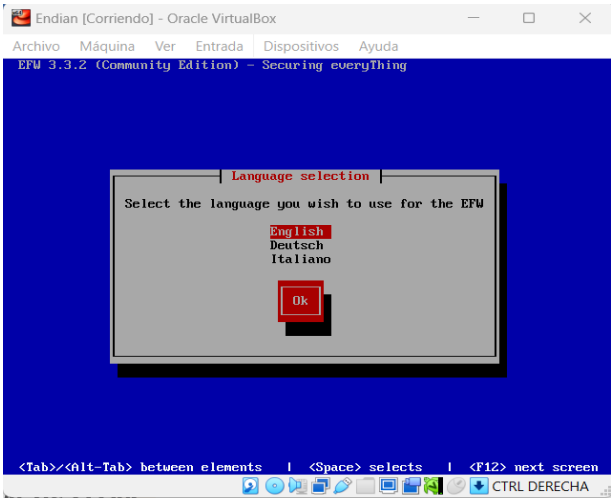

figura 4 Instalación del Endian selección de idioma Fuente: Elaboración Propia – 2025.

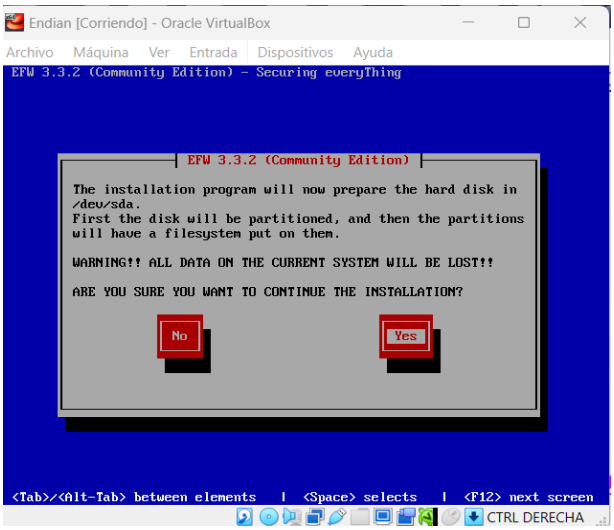

figura 5 Instalación del Endian selección de la partición del Disco Fuente: Elaboración Propia – 2025.

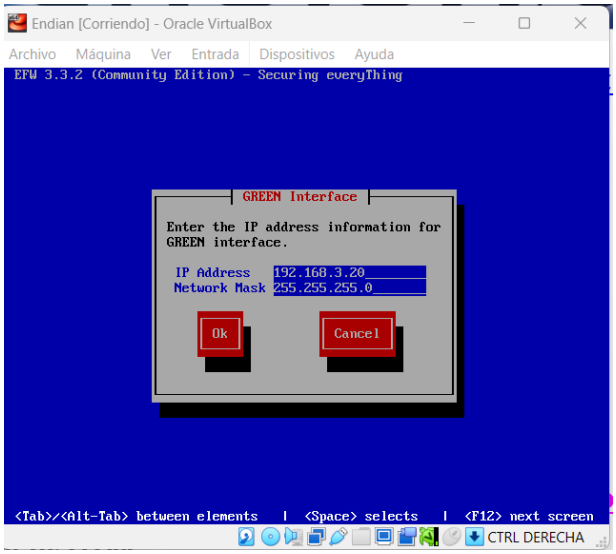

figura 6 Instalación del Endian selección de la IP para la zona Verde 192.168.3.20 Fuente: Elaboración Propia – 2025.

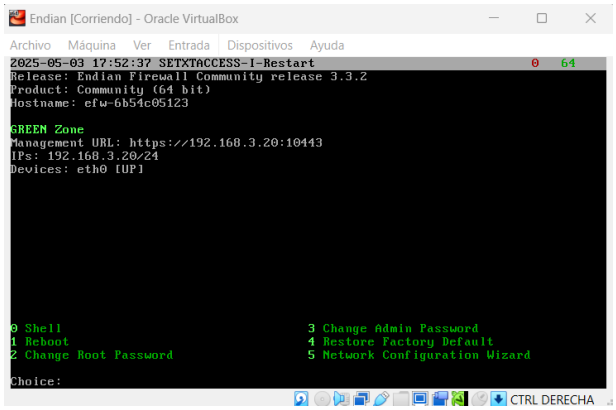

figura 7 Instalación completa del Endian Fuente: Elaboración Propia – 2025.

2.2 DESARROLLO DE LAS TEMÁTICAS

2.2.1 TEMÁTICA 1 CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX (TARJETAS DE RED) E INSTALACIÓN EFECTIVA DEL MISMO.

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).

La actividad se desarrolló en un entorno de virtualización controlado, utilizando Oracle VM VirtualBox, con el fin de evitar riesgos sobre el equipo anfitrión y facilitar la segmentación lógica de redes. Se descargó la figura ISO de Endian Firewall Community Edition desde su sitio oficial. Como se ilustra en las figuras de la 1 a la 4 posteriormente, se creó una máquina virtual asignándole 2 GB de RAM, un procesador virtual y un disco duro de 30 GB.

Posterior a esto se realiza la configuración de tres interfaces de red para la máquina virtual.

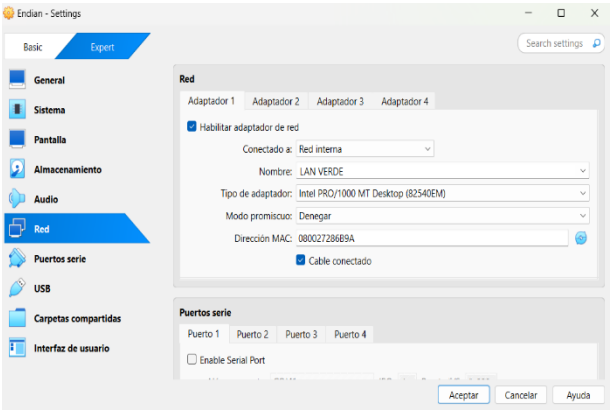

figura 8 Configuración de los adaptadores Red en la máquina virtual de Endian – LAN Verde Fuente: Elaboración Propia – 2025.

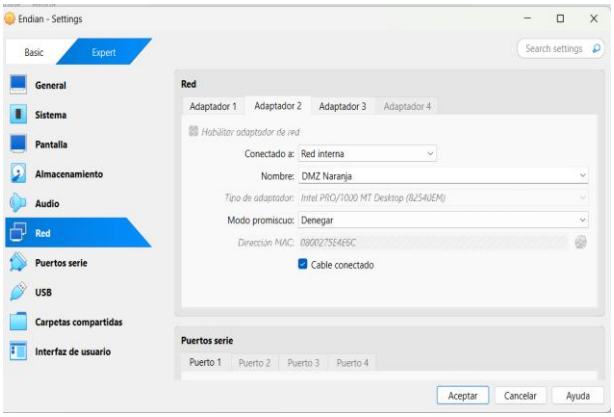

figura 9 Configuración de los adaptadores de Red en la máquina virtual de Endian – DMZ – Naranja Fuente: Elaboración Propia – 2025.

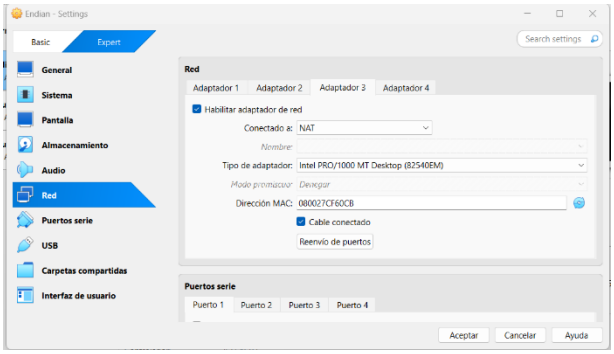

figura 10 Configuración de los adaptadores de Red en la máquina virtual de Endian – WAN – Roja. Fuente: Elaboración Propia – 2025.

Como se ilustra en las figuras de la 11 a la 13, seguidamente en cada una de las distribuciones se configuran los adaptadores a cada distribución.

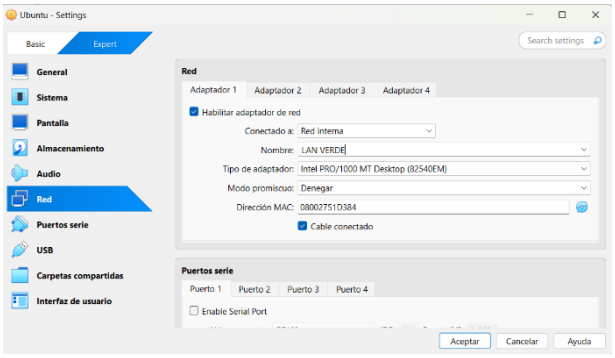

figura 11 Configuración del adaptador de la Red en el UBUNTU Desktop. Fuente: Elaboración Propia – 2025.

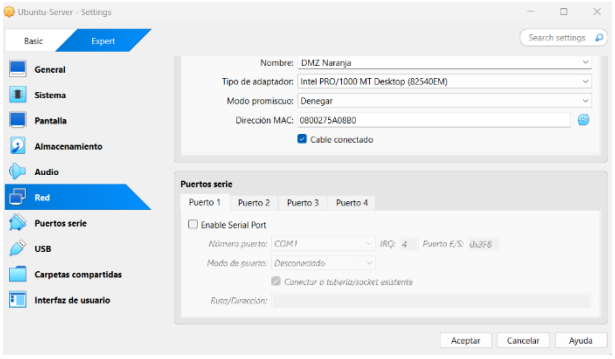

figura 12 Configuración del adaptador de la Red en el UBUNTU Server. Fuente: Elaboración Propia – 2025.

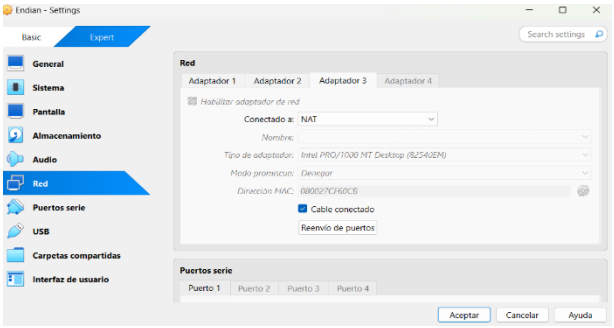

figura 13 Configuración del adaptador de la Red Endian. Fuente: Elaboración Propia – 2025.

Una vez realizado la instalación del Endian totalmente, en esta se realiza la configuración de la IP zona verde como lo podemos observar en la figura 6, la cual se le asigno la IP 192.168.3.20, esta configuración arroja una URL la cual debemos ingresar posteriormente para realizar la configuración mediante la interfaz web de Endian como se demuestra en la figura 14.

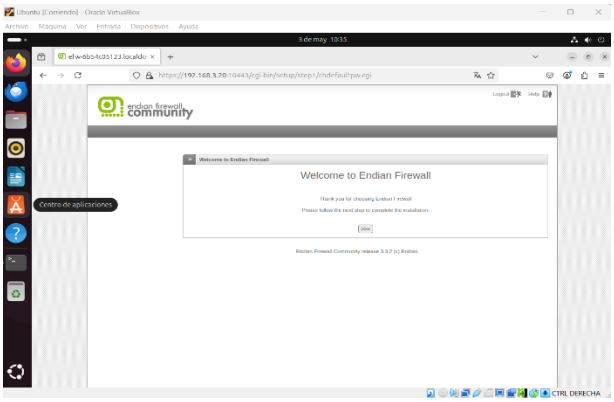

figura 14 Ingreso a la configuración del Endian por panel mediante la IP https://192.168.3.20:10443. Fuente: Elaboración Propia – 2025.

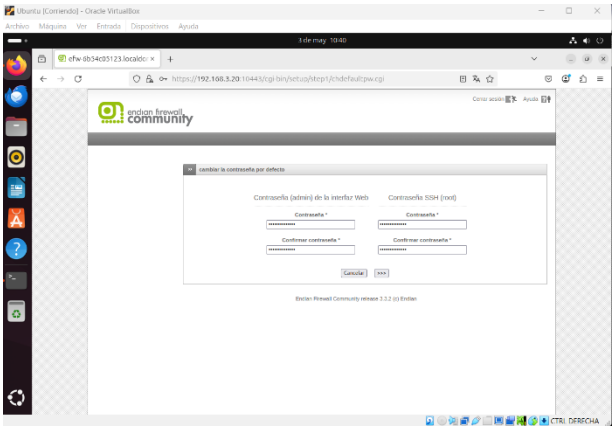

figura 17 Configuración de contraseña del Root y de la interfaz Web. Fuente: Elaboración Propia – 2025.

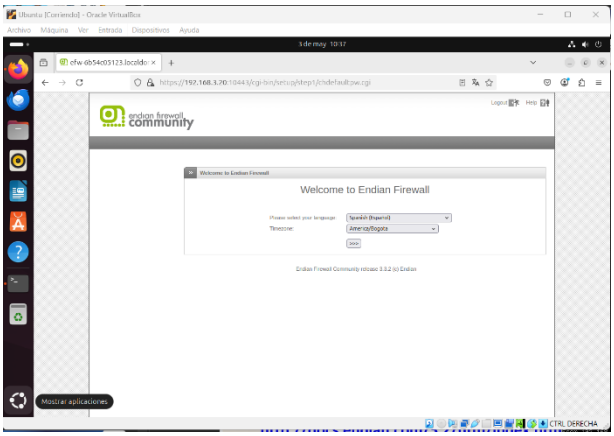

figura 15 Selección de idioma y zona. Fuente: Elaboración Propia – 2025.

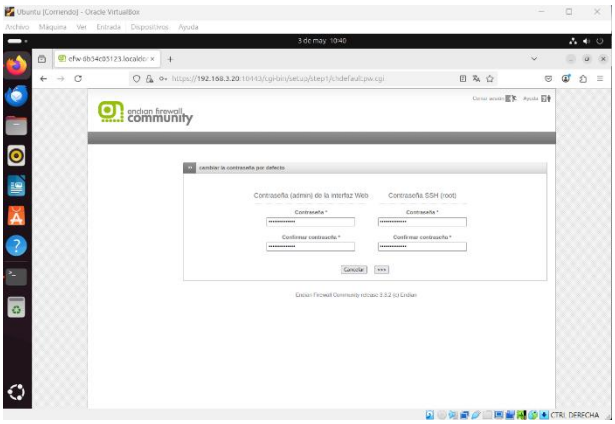

figura 18 Enrutamiento y tipo de enlace de la zona Roja este caso DHCP. Fuente: Elaboración Propia – 2025.

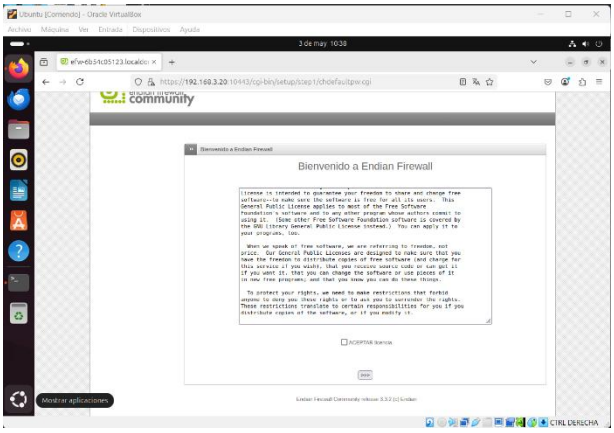

figura 16 Aceptación de términos y condiciones. Fuente: Elaboración Propia – 2025.

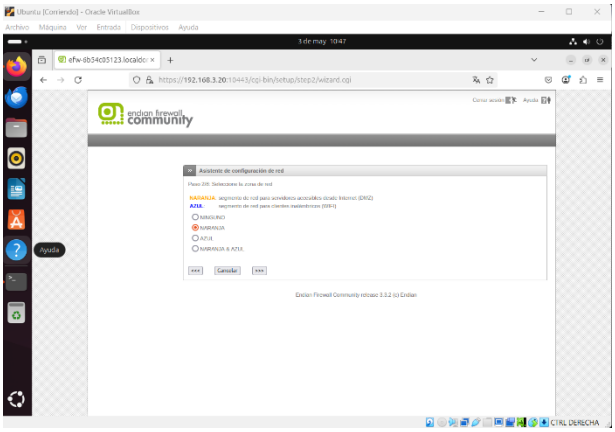

figura 19 Selección de configuración de la zona Naranja DMZ. Fuente: Elaboración Propia – 2025.

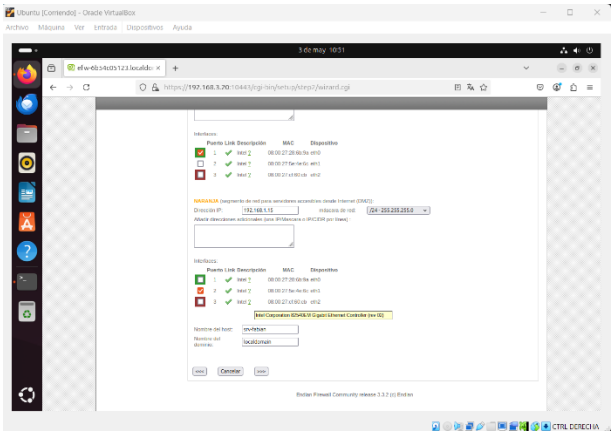

figura 20 Configuración de la zona Naranja DMZ, IP y nombre del host. Fuente: Elaboración Propia – 2025.

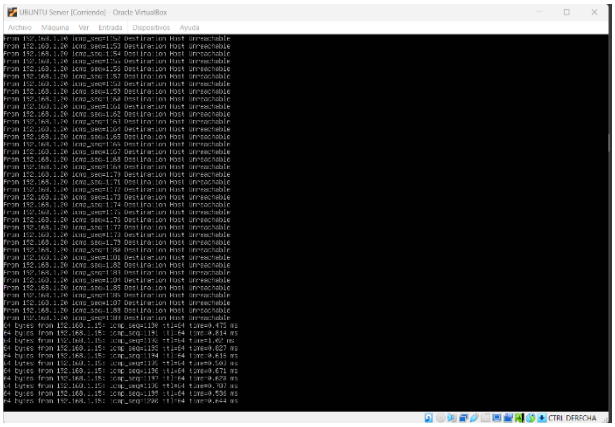

figura 23 Comprobación del ping realizado desde el servidor. Fuente: Elaboración Propia – 2025.

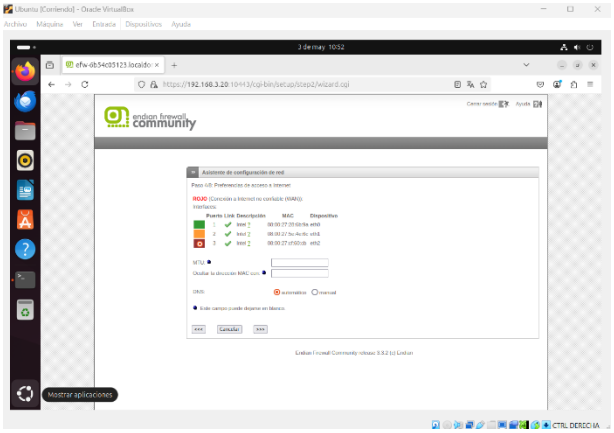

figura 21 Configuración de la zona roja. Fuente: Elaboración Propia – 2025.

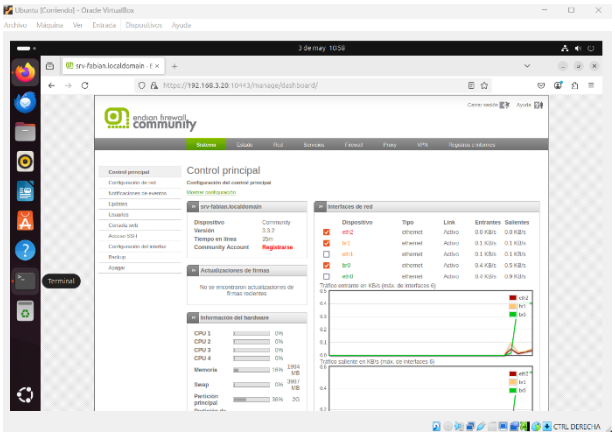

figura 24 Visualización del comportamiento de la red. Fuente: Elaboración Propia – 2025.

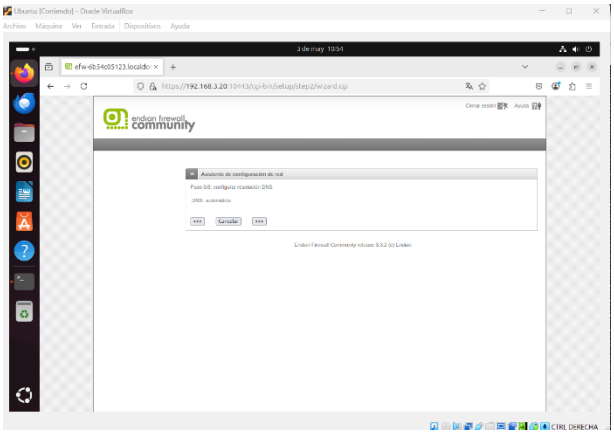

figura 22 Configuración del DNS para este caso automático. Fuente: Elaboración Propia – 2025.

La implementación del firewall Endian en una máquina virtual a través de VirtualBox permitió simular un entorno de red segmentado, seguro y funcional, replicando el comportamiento de una infraestructura perimetral en entornos reales. El uso de zonas diferenciadas (verde, roja y naranja) facilitó la gestión del tráfico, el aislamiento de servicios y la creación de políticas de seguridad específicas para cada segmento.

Por último, se entrega la tipología de la red diseñada, así como la podemos evidenciar en la figura 25:

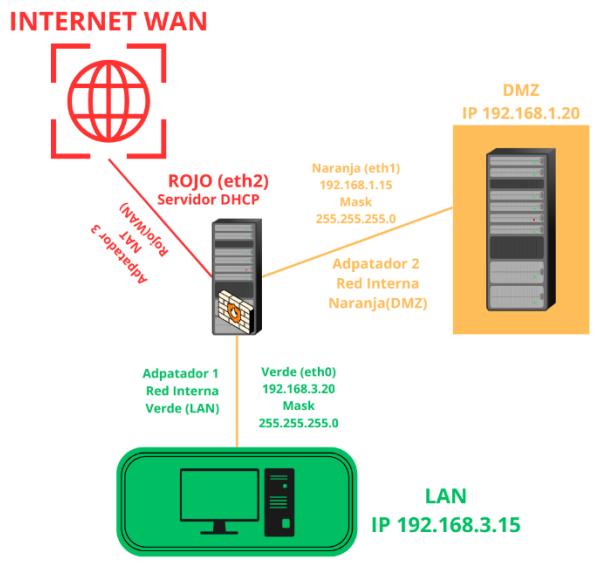

figura 25 Diseño de la red. Fuente: Elaboración Propia – 2025.

2.2.2 TEMÁTICA 2 CONFIGURACIÓN NAT.

CONFIGURACIÓN NAT

El proceso para configurar NAT, está determinado por agregar una IP virtual en una dirección pública en la cual es configurada la entrada se describe en Direcciones virtuales, posteriormente se va a Firewall > **Nat,** pestaña 1: 1, se hace click para agregar Nat en la parte superior de la lista, finalmente es configurado NAT, descrito en las opciones de regla NAT como se observa en la figura 26, se hace Click y se aplican cambios.

figura 26 Editando el NAT

Configuración de NAT para LAN hacia WAN:

1. Acceder al dispositivo de red: Accede al router o dispositivo de red que actuará como gateway para la LAN.
2. Crear una regla de NAT: Crea una regla de NAT que traduzca las direcciones IP privadas de la LAN a una dirección IP pública.
3. Especificar la interfaz: Especifica la interfaz que se utilizará para la conexión a Internet (WAN).
4. Configurar la dirección IP pública: Configura la dirección IP pública que se utilizará para la traducción.
5. Guardar la configuración: Guarda la configuración para que se aplique.

Configuración de NAT para DMZ hacia Internet:

1. Crear una zona DMZ: Crea una zona DMZ (Demilitarized Zone) en el dispositivo de red.
2. Crear una regla de NAT: Crea una regla de NAT que traduzca las direcciones IP de la DMZ a una dirección IP pública.
3. Especificar la interfaz: Especifica la interfaz que se utilizará para la conexión a Internet.
4. Configurar la dirección IP pública: Configura la dirección IP pública que se utilizará para la traducción.
5. Guardar la configuración: Guarda la configuración para que se aplique.

Verificar la configuración de NAT:

1. Verificar la tabla de NAT: Verifica la tabla de NAT para asegurarte de que las reglas se hayan aplicado correctamente.
2. Probar la conectividad: Prueba la conectividad desde la LAN y la DMZ hacia la Internet para asegurarte de que la configuración de NAT esté funcionando correctamente.
3.

El proceso para configurar NAT, está determinado por agregar una IP virtual en una dirección pública en la cual es configurada la entrada se describe en Direcciones virtuales, posteriormente se va a Firewall>**Nat,** pestaña 1: 1, se hace click para agregar Nat en la parte superior de la lista, finalmente es configurado NAT, descrito en las opciones de regla NAT, se hace Click y se aplican cambios.

Reenvío de puertos / NAT:

1. Crear una regla de re-envío de puertos: Crea una regla de re-envío de puertos que permita el tráfico entrante hacia un servidor o dispositivo específico en la LAN o DMZ.
2. Especificar el puerto: Especifica el puerto que se utilizará para el re-envío.
3. Especificar la dirección IP: Especifica la dirección IP del servidor o dispositivo que recibirá el tráfico.
4. Guardar la configuración: Guarda la configuración para que se aplique.

Ejemplo:

Tenemos un router con la siguiente configuración:

- Interfaz WAN: eth0 con dirección IP pública 200.100.50.25
- Interfaz LAN: eth1 con dirección IP privada 192.168.1.1
- Zona DMZ: eth2 con dirección IP privada 10.10.10.1

La configuración de NAT para la LAN hacia la WAN sería la siguiente:

- -Router(config)# ip nat inside source list 1 interface eth0 overload
- -Router(config)# ip nat inside source static tcp 192.168.1.100 80 200.100.50.25 80

La configuración de NAT para la DMZ hacia la Internet sería:

- -Router(config)# ip nat inside source list 2 interface eth0 overload
- -Router(config)# ip nat inside source static tcp 10.10.10.100 80 200.100.50.25 8080

Nota: la configuración específica puede variar dependiendo del dispositivo de red y del software que estés utilizando.

Configuración de NAT para LAN hacia WAN:

Si tenemos un router con la siguiente configuración:

- Interfaz WAN (Internet): GigabitEthernet0/0 con dirección IP pública 200.100.50.25/24
- Interfaz LAN: GigabitEthernet0/1 con dirección IP privada 192.168.1.1/24
- Red LAN: 192.168.1.0/24

Queremos configurar NAT para que los dispositivos de la LAN puedan acceder a Internet. Para ello, crearemos una regla de NAT que traduzca las direcciones IP privadas de la LAN a la dirección IP pública de la interfaz WAN.

Paso 1: Configurar la interfaz WAN:

- Router(config)# interface GigabitEthernet0/0
- Router(config-if)# ip address 200.100.50.25 255.255.255.0
- Router(config-if)# no shutdown

Paso 2: Configurar la interfaz LAN:

- Router(config)# interface GigabitEthernet0/1
- Router(config-if)# ip address 192.168.1.1 255.255.255.0

Paso 3: Crear una lista de acceso para la LAN

- Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255

Paso 4: Configurar la regla de NAT:

- Router(config)# ip nat inside source list 1 interface GigabitEthernet0/0 overload

Paso 5: Aplicar la regla de NAT a la interfaz LAN:

- Router(config)# interface GigabitEthernet0/1
- Router(config-if)# ip nat inside

Paso 6: Aplicar la regla de NAT a la interfaz WAN:

- Router(config)# interface GigabitEthernet0/0
- Router(config-if)# ip nat outside

Configuración de NAT para DMZ hacia Internet:

Si tenemos una zona DMZ con la siguiente configuración:

- Interfaz DMZ: GigabitEthernet0/2 con dirección IP privada 10.10.10.1/24
- Red DMZ: 10.10.10.0/24

Con la configurar NAT para que los dispositivos de la DMZ puedan acceder a Internet. Para ello, crearemos una regla de NAT que traduzca las direcciones IP de la DMZ a la dirección IP pública de la interfaz WAN.

Paso 1: Configurar la interfaz DMZ:

- Router(config)# interface GigabitEthernet0/2
- Router(config-if)# ip address 10.10.10.1 255.255.255.0
- Router(config-if)# no shutdown

Paso 2: Crear una lista de acceso para la DMZ:

- Router(config)# access-list 2 permit 10.10.10.0 0.0.0.255

Paso 3: Configurar la regla de NAT:

- Router(config)# ip nat inside source list 2 interface GigabitEthernet0/0 overload

Paso 4: Aplicar la regla de NAT a la interfaz DMZ:

- Router(config)# interface GigabitEthernet0/2
- Router(config-if)# ip nat inside

Re-envío de puertos / NAT:

Si queremos permitir el acceso a un servidor web en la LAN con dirección IP 192.168.1.100 y puerto 80. Queremos que el

tráfico entrante hacia la dirección IP pública 200.100.50.25 y puerto 80 sea re-enviado al servidor web.

- Router(config)# ip nat inside source static tcp 192.168.1.100 80 200.100.50.25 80

De esta manera, cuando alguien acceda a la dirección IP pública 200.100.50.25 y puerto 80, el tráfico será re-enviado al servidor web en la LAN con dirección IP 192.168.1.100 y puerto 80.

2.2.3 TEMÁTICA 4: REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO.

Las reglas de firewall en Endian Firewall que permiten el tráfico controlado entre zonas de red críticas (LAN, DMZ e Internet), asegurando comunicaciones seguras para servicios HTTP y FTP como se relaciona en las figuras de la 27 a la 33.

Para permitir que los dispositivos ubicados en la zona DMZ accedan a Internet, es necesario configurar reglas de NAT en el firewall como se relaciona en la figura 34, esto se realiza mediante la creación de reglas de NAT.

Detallamos el proceso de conectividad y reglas de firewall, monitoreo y configuración avanzada de reglas Endian firewall como se relaciona desde la figura 36 a la 45 centralizando la conectividad entre zonas, la aplicación de servicios HTTP y FTP y validación de tráfico.

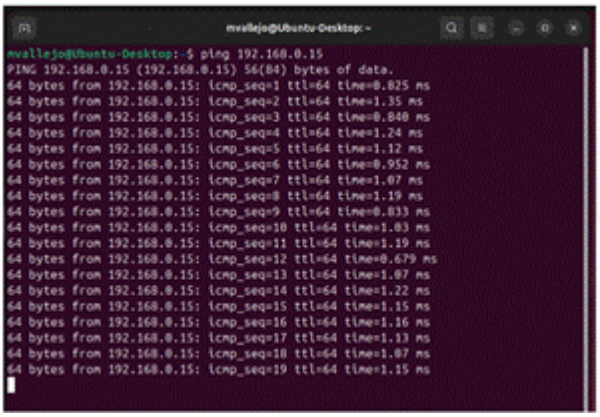

figura 27 Verificar la conectividad de red hacia el host 192.168.0.15 mediante el comando ping Fuente: Elaboración Propia – 2025.

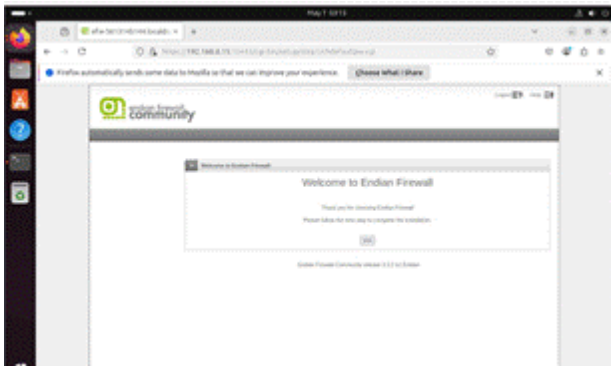

figura 28 Endian Firewall, para comenzar con la configuración y administración Fuente: Elaboración Propia – 2025.


figura 29 Definir la segmentación de red para clientes inalámbricos Fuente: Elaboración Propia – 2025.


figura 30 Asistente de configuración inicial para definir los parámetros de red para las zonas verde (LAN) y Naranja (DMZ). Fuente: Elaboración Propia – 2025.

figura 31 Asistente de configuración inicial, Configurado correctamente. Fuente: Elaboración Propia – 2025.

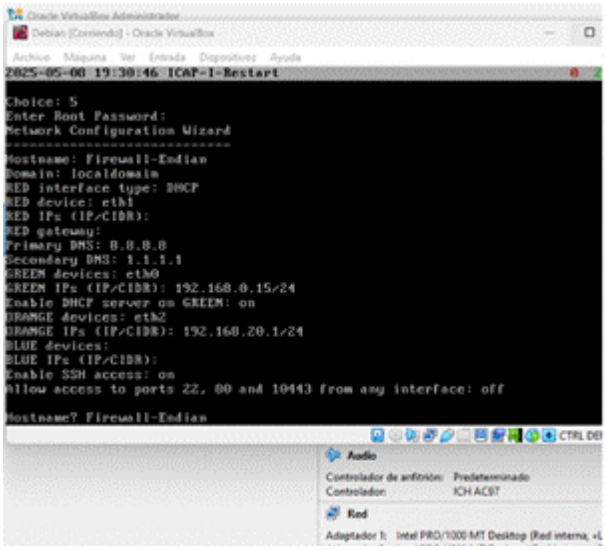

figura 32 Configuración la red para el firewall. Fuente: Elaboración Propia – 2025.

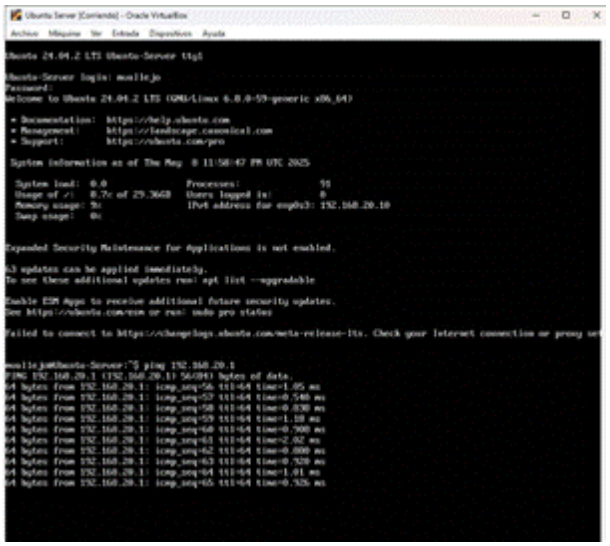

figura 33 Monitoreo el estado del sistema y su conectividad. Fuente: Elaboración Propia – 2025.

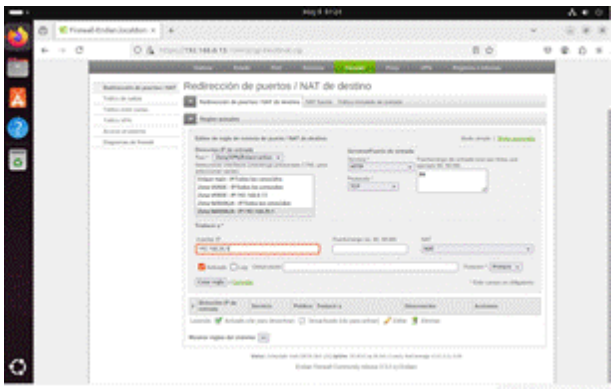

figura 34 Configurar NAT de destino (redirección de puertos) en el firewall Endian para permitir tráfico entrante hacia un servidor interno Fuente: Elaboración Propia – 2025.

figura 35 Configurando reglas para manejar tráfico entrante hacia servidores internos. Fuente: Elaboración Propia – 2025.

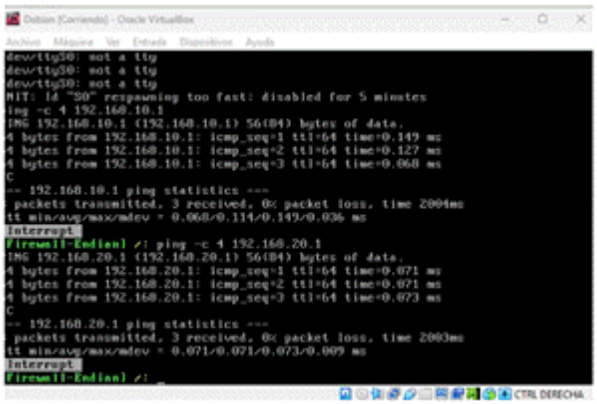

figura 36 Probando la conexión de la red. Fuente: Elaboración Propia – 2025.

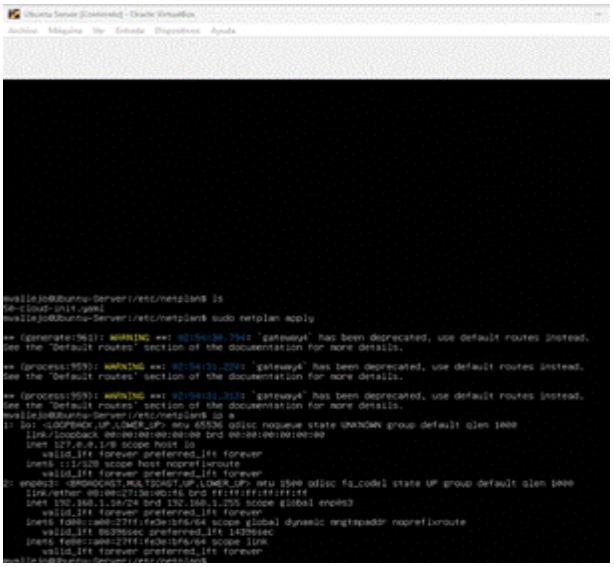

figura 37 Configurar la red en Ubuntu Server Fuente: Elaboración Propia – 2025.

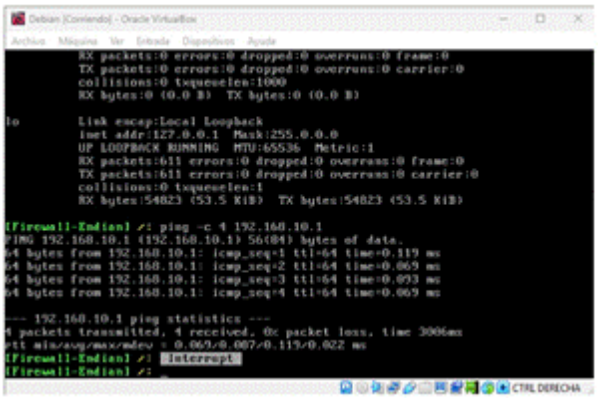

figura 38 Monitoreando la red y validando conectividad desde el firewall Endian. Fuente: Elaboración Propia – 2025.

figura 39 Reglas de firewall en el Firewall Endian, Reglas de filtrado, validación de reglas de entrada, con el comando iptables -L -n -v Fuente: Elaboración Propia – 2025.

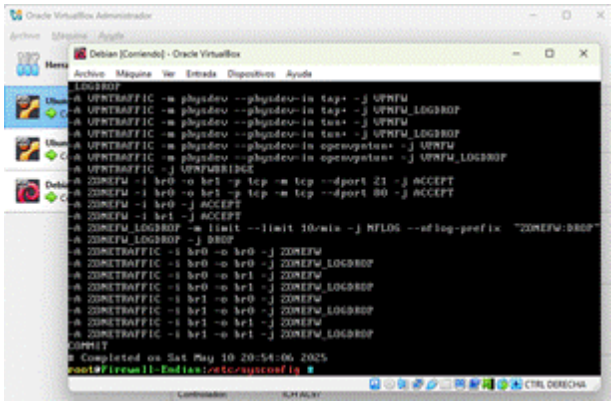

figura 40 Validación de las reglas de filtrado de un Firewall Endian, tráfico VPN, Comunicación entre zonas (LAN - DMZ), Registro de tráfico bloqueado para seguridad. Fuente: Elaboración Propia – 2025.

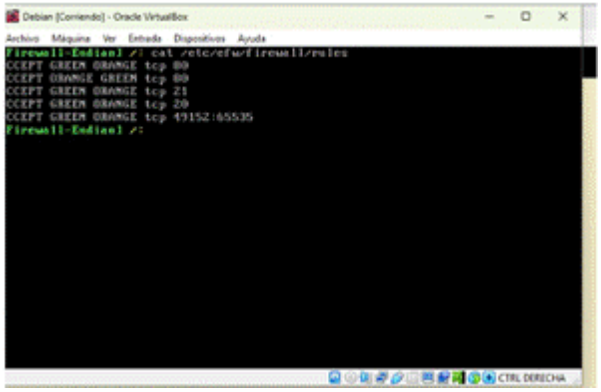

figura 41 Se evidencia el firewall configurado, Permitir HTTP y FTP entre la LAN GREEN y la DMZ -ORANGE. Fuente: Elaboración Propia – 2025.

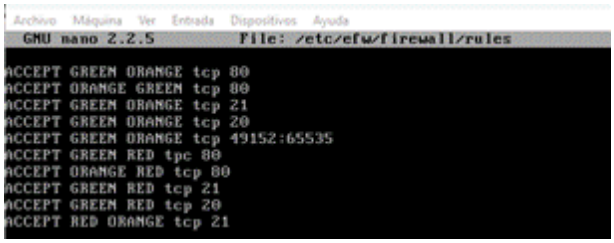

figura 42 Se evidencia el firewall configurado, Permitir HTTP y FTP Fuente: Elaboración Propia – 2025. Fuente: Elaboración Propia – 2025.

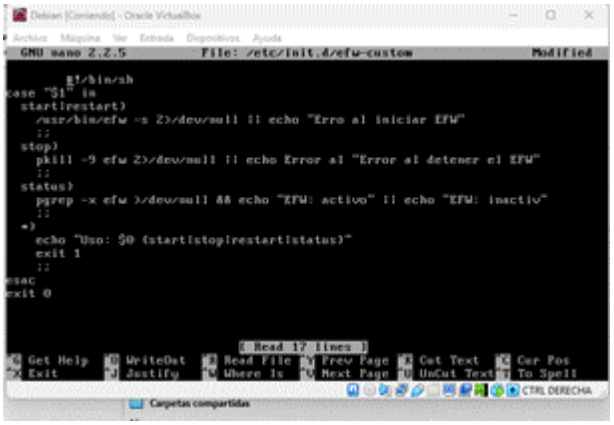

figura 43 Se crea un script de inicio para gestionar el servicio efw (Endian Firewall). Fuente: Elaboración Propia – 2025.

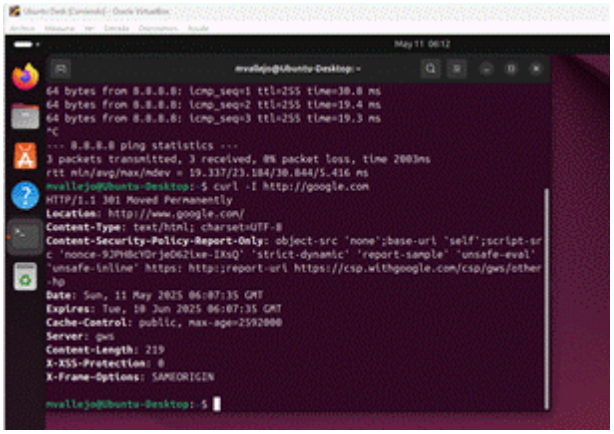

figura 44 Ingreso del servicio HTTP desde la zona DMZ hacia la WAN Fuente: Elaboración Propia – 2025.

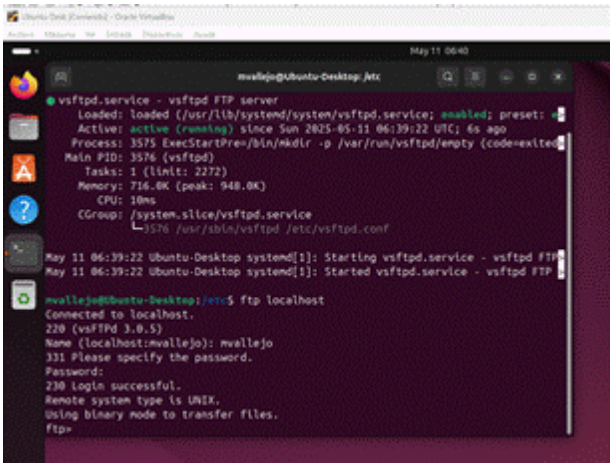

figura 45 Comunicar la zona Verde con la zona Naranja usando FTP, el puerto 21 está en funcionamiento Fuente: Elaboración Propia – 2025.

En las reglas de acceso en endian firewall nos permite conectar de forma segura las zonas LAN, DMZ y WAN, siguiendo mejores prácticas de seguridad perimetral. La segmentación adecuada reduce el riesgo de ataques transversales, también permitiendo que las reglas específicas para HTTP/FTP permiten comunicaciones necesarias mientras se bloquea tráfico no autorizado.

2.2.4 TEMÁTICA 5: IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE) CON POLÍTICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET.

La implementación practica de un proxy HTTP no transparente utilizando el firewall Endian Community como se relaciona en las figuras 46 y 47 para aplicar navegación autenticada y filtrado de contenido en una red de área local (LAN).

La creación de usuario, grupos y políticas permite la segmentación granular de bloqueos o permisos específicos de acuerdo con las necesidades de las compañías como podemos validar en la figura 48 – 50.

El estudio detalla el proceso de configuración, incluyendo la creación de un perfil de navegación asociado a una lista negra de sitios web específicos (www.hotmail.com, www.youtube.com y www.elnuevodia.com.co) como se observa en las figuras 51 – 53.

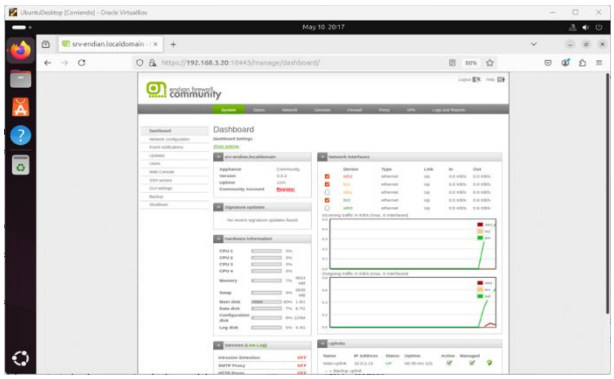

figura 46 Accediendo al dashboard Fuente: Elaboración Propia – 2025.

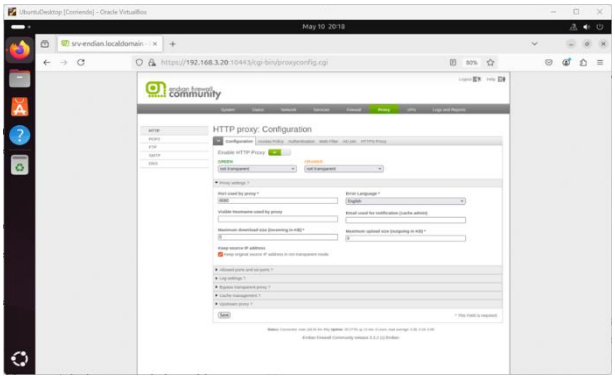

figura 47 Habilitando el Proxy HTTP Fuente: Elaboración Propia – 2025.

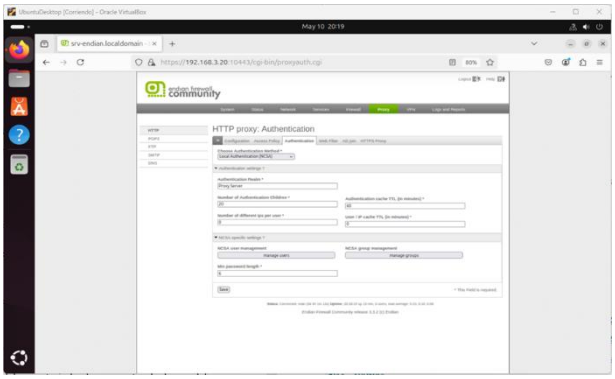

figura 48 Habilitando autenticación local Fuente: Elaboración Propia – 2025.

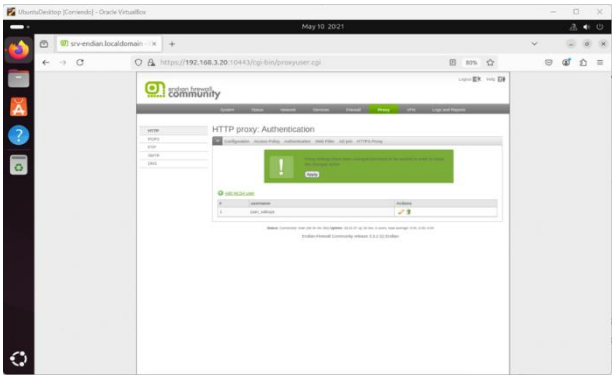

figura 49 Creando Usuarios Fuente: Elaboración Propia – 2025.

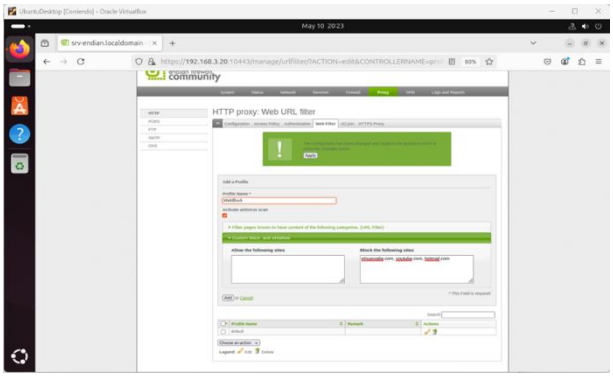

figura 50 Creando la lista de bloqueo. Fuente: Elaboración Propia – 2025.

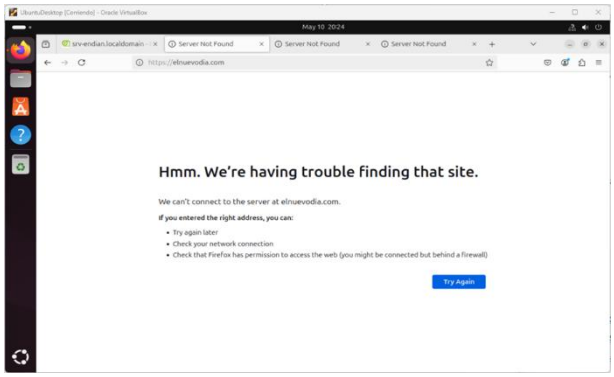

figura 51 Bloqueando elnuevodia.com Fuente: Elaboración Propia – 2025.

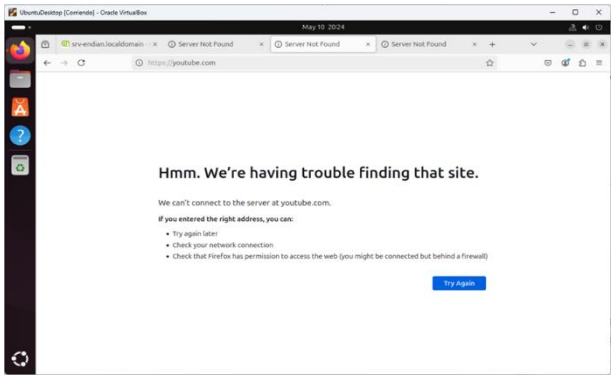

figura 52 Bloqueando youtube.com Fuente: Elaboración Propia – 2025.

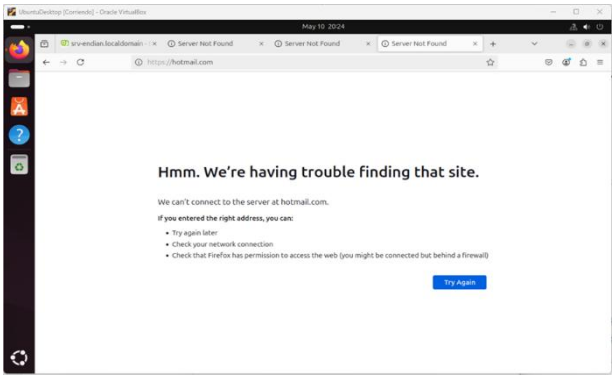

figura 53 Bloqueando hotmail.com Fuente: Elaboración Propia – 2025.

Endian emerge como una solución robusta y flexible para implementar un control de acceso a internet granular y seguro mediante un proxy HTTP no transparente con autenticación y listas negras.

3 CONCLUSIONES

En el desarrollo de esta actividad, valoramos especialmente el avance logrado en nuestra comprensión aplicada de la seguridad en GNU/Linux. Pasar de la teoría a la práctica con herramientas como Endian, ha sido una experiencia de aprendizaje muy enriquecedora.

Hemos podido experimentar directamente, gracias a los entornos virtualizados, cómo se endurece un sistema y se monitorean sus servicios críticos, lo cual reafirma el potencial de GNU/Linux para construir entornos seguros.

En síntesis, el proyecto cumplió con los objetivos de formación del diplomado, proporcionando a los participantes una experiencia integral que les permite comprender y aplicar soluciones de seguridad informática sobre plataformas GNU/Linux, promoviendo el uso de tecnologías abiertas para la protección de la información..

4 REFERENCIAS

[1] A. C. Morales y D. R. López, "Análisis comparativo de soluciones de firewall en software libre para redes LAN," *Revista Científica Ciencia y Tecnología*, vol. 29, no. 3, pp. 85–94, 2023. https://revistascientificas.edu.co

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

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

[4] Deka, G. C., & Das, P. K. (2018). Virtual Network With Virtual Router/Firewall Using Endian Firewall Community (EFW). In Design and Use of Virtualization Technology in Cloud Computing (pp. 260-276). IGI Global.

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

[6] 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.

[7] J. Medina et al., "Entornos virtualizados con VirtualBox para prácticas de seguridad perimetral en GNU/Linux," *Revista Educación y Tecnología*, vol. 6, no. 2, pp. 110–121, 2022.

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

[9] O. Nieto y L. Torres, "Fortalecimiento de la seguridad perimetral en entornos virtualizados: estudio de caso con Endian Firewall," *Revista de Seguridad Informática*, vol. 12, no. 2, pp. 35–42, 2022

[10] Rincon Pineda, J. A., Quintana Rendón, H. D. J., & Jiménez Parra, S. E. Instalación y configuración de nethserver para la Implementación y administración de servicios de red.