# IMPLEMENTACIÓN DE SEGURIDAD PERIMETRAL CON ENDIAN FIREWALL EN ENTORNO GNU/LINUX

Anacona Anacona, Arley
e-mail:aanacona@unaadvirtual.edu.co
Giraldo Muñoz, Jhenifer
e-mail:jgiraldomun@unadvirtual.edu.co
Gomez Joaqui, Mabel Yurani
e-mail: mygomezj@unadvirtual.edu.co
Londoño Moscoso, Carlos Andrés
e-mail: calondonomos@unadvirtual.edu.co
Samboni Ruiz, Faber Herney
e-mail: fhsambonir@unadvirtual.edu.co

**RESUMEN:** *ESTE ARTÍCULO DESCRIBE la implementación de una solución de seguridad perimetral utilizando Endian Firewall en un entorno virtualizado con Oracle VirtualBox [4]. Se configuraron redes segmentadas en tres zonas (verde, roja y naranja) siguiendo las mejores prácticas de seguridad documentadas en el manual de Endian [7]. La segmentación demostró ser efectiva para aislar diferentes niveles de confianza, reduciendo la superficie de ataque y facilitando la aplicación de políticas de seguridad específicas por zona. La práctica permitió consolidar conocimientos sobre administración de sistemas GNU/Linux [1], configuración de redes virtuales [4], y principios de seguridad perimetral [7].*
*PALABRAS CLAVE: DMZ, Endian Firewall, GNU/Linux, Seguridad perimetral, Segmentación de red, VirtualBox.*

**PALABRAS CLAVE**: DMZ, Endian Firewall, GNU/Linux, Seguridad perimetral

## 1 INTRODUCCIÓN

**LA SEGURIDAD INFORMÁTICA** constituye un elemento esencial en el mantenimiento y operación de infraestructuras tecnológicas modernas [1]. En entornos donde convergen redes internas, redes externas y zonas de servicios expuestos como la DMZ, se requiere la implementación de mecanismos que garanticen la confidencialidad, integridad y disponibilidad de la información. Las distribuciones GNU/Linux orientadas a la seguridad, como Endian Firewall, permiten administrar de forma efectiva el tráfico entre zonas, aplicar políticas de acceso y proteger los servicios críticos [7].

Este artículo presenta la configuración inicial de Endian Firewall como solución de seguridad perimetral en un entorno virtualizado con Oracle VirtualBox [4]. La práctica se centróen establecer una arquitectura de tres zonas segmentadas que permita aislar diferentes tipos de tráfico y servicios según su nivel de confianza. Esta implementación constituye la base fundamental para configuraciones avanzadas de seguridad que se desarrollarán en las siguientes etapas del proyecto, consolidando conocimientos esenciales sobre administración de sistemas GNU/Linux [2], [3].

## 2. CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX

## 2.1 SEGMENTACIÓN DE RED CON ENDIAN FIREWALL

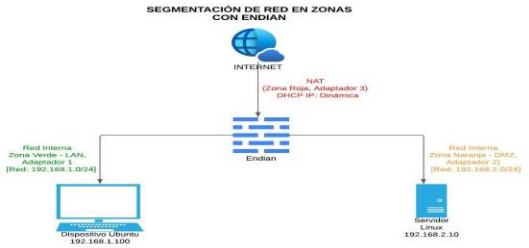
**LA SEGMENTACIÓN DE RED** constituye uno de los mecanismos fundamentales para aislar, controlar y gestionar de manera segura el flujo de información dentro de una infraestructura. En el contexto de esta práctica, Endian Firewall permite dividir la red en zonas lógicas con diferentes niveles de confianza y propósitos específicos [7]. Esta separación facilita la aplicación de políticas precisas, reduce la superficie de ataque y evita que una vulnerabilidad en un segmento comprometa a los demás.

Para esta implementación se configuraron tres zonas principales que representan una arquitectura de seguridad tradicional pero efectiva.

- **Zona Roja (WAN):** interfaz destinada a la conexión hacia Internet, considerada un entorno no confiable.
- **Zona Verde (LAN):** red interna que alberga los equipos de uso cotidiano, caracterizada por un nivel alto de confianza.
- **Zona Naranja (DMZ):** segmento intermedio utilizado para publicar servicios como HTTP o FTP sin exponer directamente la red interna.

Como muestra la Figura 1, esta arquitectura crea barreras lógicas que previenen la propagación lateral de amenazas.

Figura 1. Segmentación de la red en zonas verde, roja y naranja.




Fuente: Elaboración propia basada en documentación de Endian [7].

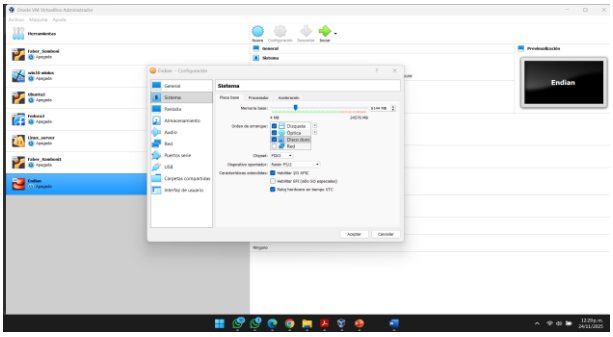
## 2.2 PREPARACIÓN DEL ENTORNO VIRTUAL EN VIRTUALBOX

**LA IMPLEMENTACIÓN** del laboratorio de seguridad se realizó utilizando Oracle VirtualBox como plataforma de virtualización, seleccionada por su amplia compatibilidad y disponibilidad gratuita [4]. Se descargó la imagen ISO de Endian Firewall Community desde el repositorio oficial de SourceForge.net, como se evidencia en la Figura 2, verificando la autenticidad del software. Se creó una máquina virtual con el nombre Endian asignando 6 GB de memoria RAM y 50 GB de espacio en disco, especificaciones adecuadas para las funciones de firewall en entorno de laboratorio. La configuración básica de la máquina virtual se presenta en la Figura 3.

Figura 2. página oficial de Endian.


Fuente: Elaboración propia basada en documentación de Endian [7].

Figura 3. Configuración de la máquina virtual para Endian.



Fuente: Elaboración propia con VirtualBox [4].

## 2.3 CONFIGURACIÓN DE ADAPTADORES DE RED

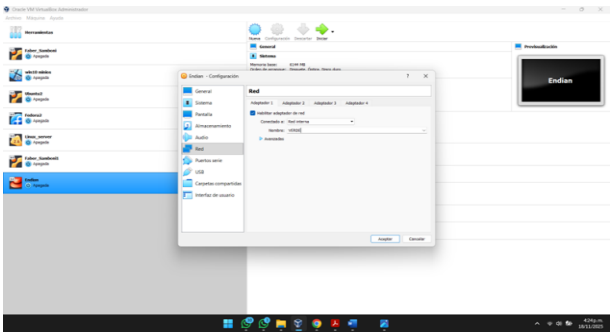
Una vez configurada la máquina virtual, se realizó la división lógica de las redes mediante la configuración de tres adaptadores de red virtuales en VirtualBox. El adaptador 1 se configuró en modo Red Interna con el nombre "Verde", destinado exclusivamente a la red interna confiable. El adaptador 2 se configuró en modo Red Interna con el nombre Naranja, creando un segmento separado para la zona DMZ. El adaptador 3 se configuró en modo NAT para simular la conexión a Internet, asignándose automáticamente a la zona roja. Esta configuración proporciona conectividad saliente a Internet mientras implementa traducción de direcciones de red (NAT) para ocultar la topología interna [4].

La configuración específica para cada adaptador se realizó desde la interfaz de VirtualBox, seleccionando el tipo de conexión correspondiente y asignando nombres descriptivos para cada zona. Como se muestra en las Figuras 4, 5 y 6, esta configuración de adaptadores establece los cimientos para la implementación de políticas de seguridad granular entre zonas, permitiendo el control exhaustivo del flujo de tráfico en todas las direcciones según las mejores prácticas de seguridad documentadas por Endian [7].

- Adaptador 1 > verde > red interna

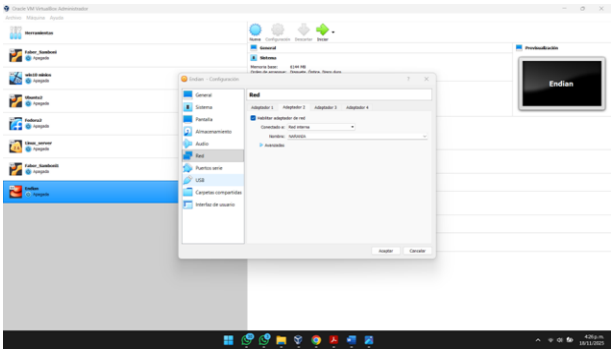
Adaptador 2 > Naranja > red interna
Adaptador 3 > Puente (LAN) – salida a internet

Figura 4. Configuración del adaptador para zona verde.



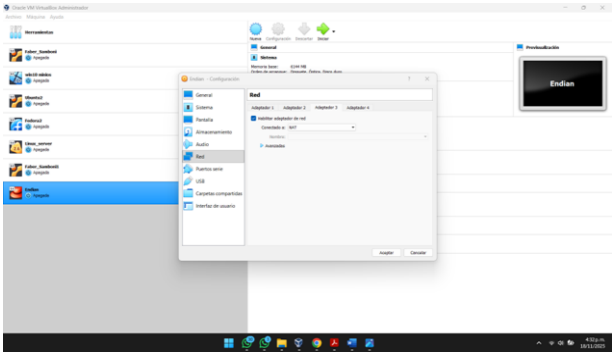
Fuente: Elaboración propia con VirtualBox [4].

Figura 5. Configuración del adaptador para zona Naranja.



Fuente: Elaboración propia con VirtualBox [4].

Figura 6. Configuración del adaptador para zona roja.

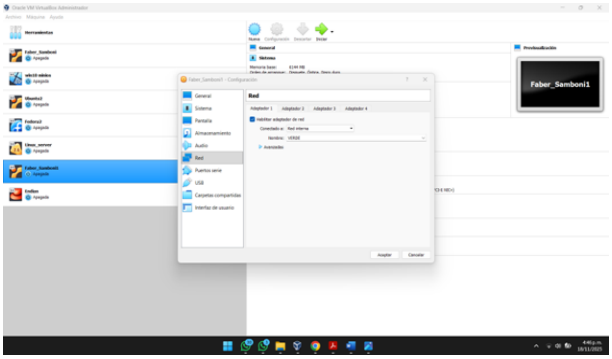


Fuente: Elaboración propia con VirtualBox [4].

## 2.4 INTEGRACIÓN DE ESTACIONES DE TRABAJO

Para completar la infraestructura de laboratorio, se integraron dos máquinas virtuales adicionales que representan los componentes típicos de una red empresarial. Una máquina con Ubuntu Desktop se configuró como estación de trabajo en la zona verde, asignándole el adaptador de red correspondiente [2]. Esta configuración, mostrada en la Figura 7, permite simular el acceso de usuarios finales a recursos internos a través del firewall.

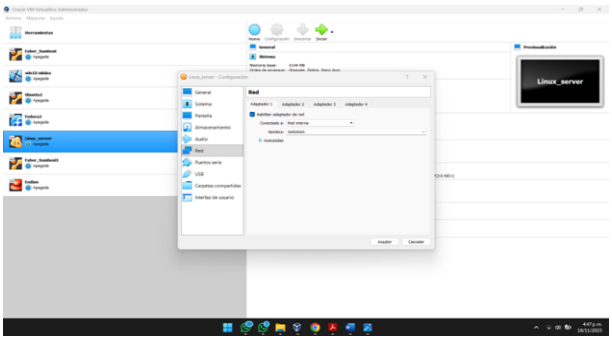
Figura 7. Asignación de adaptador para máquina Ubuntu en zona verde.



Fuente: Elaboración propia con Ubuntu Desktop [2].

De manera paralela, una máquina con Linux Server se configuró como servidor en la zona naranja (DMZ), asignándole el adaptador correspondiente [3]. Este servidor, presentado en la Figura 8, aloja los servicios HTTP y FTP que posteriormente se expondrán de manera controlada a diferentes zonas de red. La correcta asignación de adaptadores asegura que cada máquina quede confinada a su zona correspondiente, implementando efectivamente la segmentación de seguridad diseñada.

Figura 8. Asignación de adaptador para servidor Linux en zona naranja.



Fuente: Elaboración propia con Linux Server [3].

## 2.5 INSTALACIÓN Y CONFIGURACIÓN DE ENDIAN FIREWALL

La instalación de Endian Firewall se inició arrancando la máquina virtual desde la imagen ISO descargada. El instalador presentó un menú donde se seleccionó la opción Install Endian para iniciar el proceso completo. El sistema verificó automáticamente el hardware disponible, detectando correctamente los tres adaptadores de red configurados [4]. Posteriormente, solicitó confirmación para formatear el disco, advirtiendo que esta acción eliminaría cualquier dato existente. Una vez confirmado, procedió a copiar los archivos del sistema e instalar los paquetes base.

Al finalizar la copia de archivos, el instalador solicitó la definición de credenciales de administración robustas, siguiendo las recomendaciones de seguridad de LPI Linux Essentials [1]. Se estableció una contraseña compleja para el usuario root y credenciales para el usuario administrativo de la interfaz web. Finalmente, el sistema indicó la necesidad de reiniciar para completar la instalación y cargar el kernel con los módulos de seguridad necesarios.

## 2.6 CONFIGURACIÓN INICIAL DE RED POR ZONAS

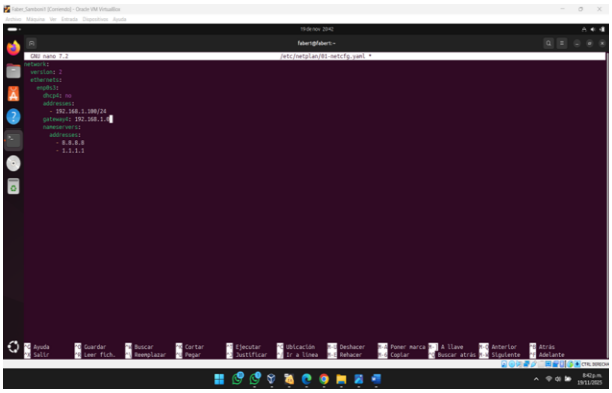
Para la zona verde (LAN) se asignó la dirección IP 192.168.1.1 con máscara 255.255.255.0, lo cual se realizó directamente desde el servidor Endian, estableciendo este segmento como red interna confiable, se evidencia en la Figura 9.

Figura 9. Asignación de IP verde en Endian (192.168.1.1).

Fuente: Autoría propia de la configuración web de Endian [7].

Para acceder a esta interfaz de Endian Fireball, se configuró temporalmente una estación de trabajo con Ubuntu Desktop [2] como se evidencia en la Figura 10, esto para que quedara en la misma red que la interfaz de administración del firewall, asignándole dirección IP 192.168.1.100/24. El asistente guió paso a paso la asignación de parámetros de red para cada zona según la documentación oficial de Endian [7].

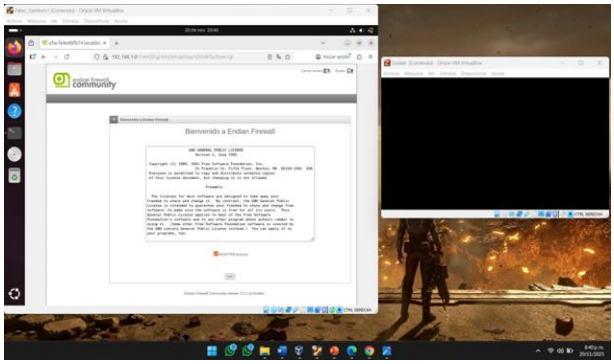
Figura 10. Configuración de IP estática en Ubuntu (192.168.1.100).



Fuente: Autoría propia captura de pantalla de Ubuntu Desktop [2].

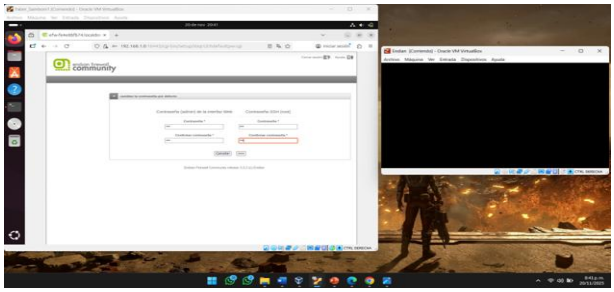
Una vez establecida la conectividad básica, se accedió a la interfaz web administrativa de Endian Firewall desde la estación de trabajo Ubuntu en la zona verde utilizando la dirección 192.168.1.1 a través del navegador web. Esta configuración asegura que la administración del firewall sea accesible únicamente desde la red interna, implementando una buena práctica de seguridad documentada en el manual de Endian [7]. El sistema presentó inicialmente un asistente de configuración que solicitó establecer parámetros básicos como idioma, aceptación de términos y condiciones, y definición de contraseña de administración, como se documenta en las Figuras 11 y 12.

Figura 11. Términos y condiciones de Endian.



Fuente: Autoría propia captura de pantalla de Endian web interfaz [7].

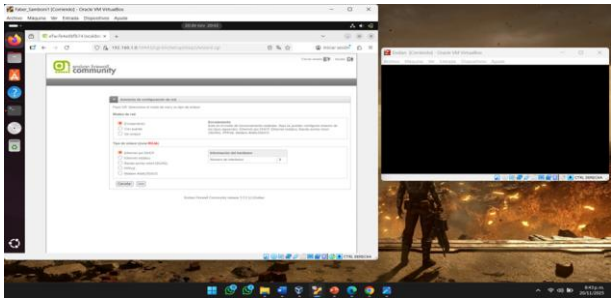
Figura 12. Establecimiento de contraseña de administración.



Fuente: Autoría propia captura de pantalla de Endian web interfaz [7].

La configuración se terminó de establecer basado en la segmentación, las direcciones IP finales para todas las interfaces del firewall: 192.168.1.1 para la interfaz de zona verde (configurada inicialmente durante la instalación), 192.168.2.1 para la interfaz de zona naranja (configurada desde la web), y dirección obtenida vía DHCP para la zona roja. La interfaz web de administración, presentada en las Figuras 13 y 14, proporciona acceso centralizado desde Ubuntu a todas las funcionalidades de seguridad del firewall, incluyendo monitoreo en tiempo real, configuración de reglas, y gestión de servicios, demostrando la efectividad de la administración remota desde sistemas cliente GNU/Linux [2]

Figura 13. Configuración de la red roja dada por el DHCP



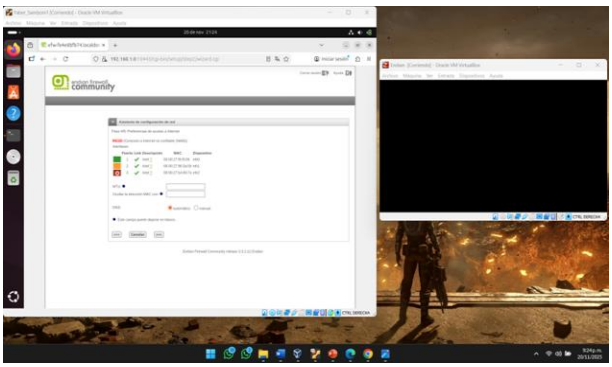
Fuente: Autoría propia captura de pantalla de Endian web interfaz [7].

Figura 14. Establecimiento de IP 192.168.2.1 para zona naranja.

Fuente: Autoría propia captura de pantalla de Endian web interfaz [7].

Una vez configuradas ambas zonas, el asistente web presentó una pantalla de resumen de configuración mostrando la zona verde (LAN) con dirección 192.168.1.1/24, servidor DHCP activado y política por defecto PERMITIR; la zona naranja (DMZ) con dirección 192.168.2.1/24, servidor DHCP activado y política por defecto DENEGAR; y la zona roja (WAN) con configuración DHCP obtenida automáticamente y NAT habilitado. Esta pantalla de resumen, documentada en la Figura 15.

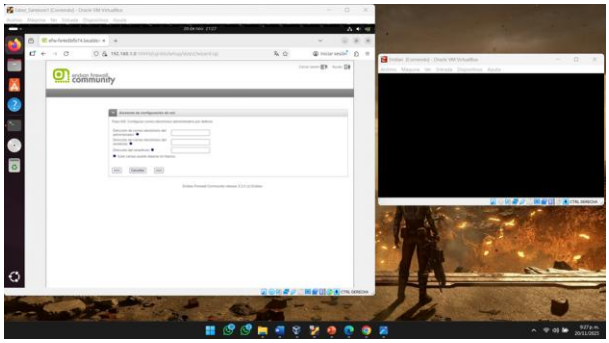
Figura 15. Resumen de configuración de Endian



Fuente: Autoría propia captura de pantalla de Endian web interfaz [7].

Posteriormente el asistente pidió una configuración opcional de registro mediante correo electrónico para notificaciones del sistema, incluyendo alertas de seguridad, actualizaciones disponibles y reportes periódicos con configuraciones de frecuencia diaria, semanal o mensual. Esta funcionalidad, recomendada en la documentación de Endian [7], permite al administrador recibir alertas tempranas sobre el estado del firewall y posibles incidencias de seguridad, aunque puede omitirse para continuar con la configuración como se evidencia en la Figura 16.

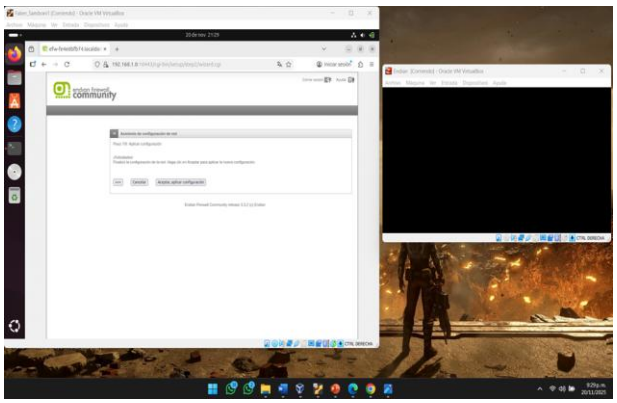
Figura 16. Solicitud del correo electrónico



Fuente: Autoría propia captura de pantalla de Endian web interfaz [7].

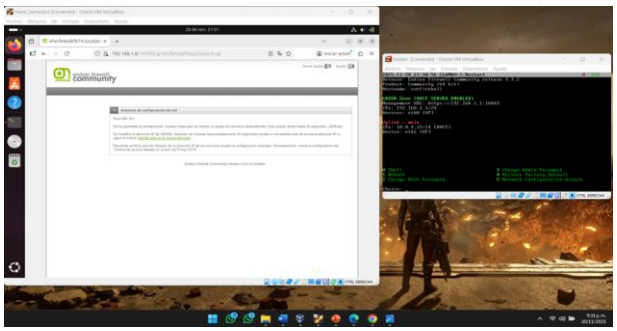
Finalmente, el sistema presentó una pantalla de confirmación final donde se solicitó aceptar y aplicar toda la configuración realizada en Endian Firewall. Al hacer clic en "Aceptar configuración", el sistema procesó todas las configuraciones establecidas en la segmentación de zonas, direccionamiento IP, políticas de acceso y servicios habilitados reiniciando los servicios necesarios para que los cambios surtieran efecto inmediatamente. Esta etapa confirmó la finalización exitosa del proceso de configuración inicial del firewall como se muestra en la figura 17 y 18.

Figura 17. Aceptar la configuración definida.



Fuente: Autoría propia captura de pantalla de Endian web interfaz [7].

Figura 18. Vista final de la configuración de Endian.

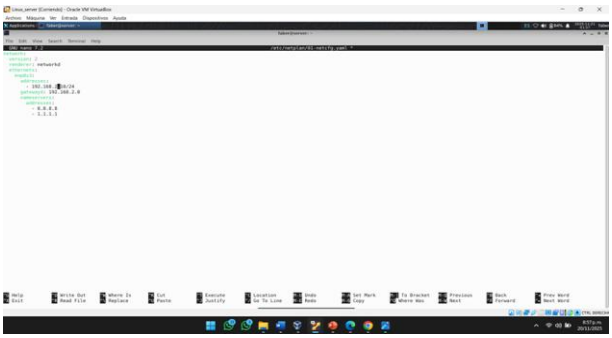


Fuente: Autoría propia captura de pantalla de Endian web interfaz [7].

## 2.7 CONFIGURACIÓN DE SERVIDOR EN ZONA NARANJA

Para validar la correcta configuración de la zona DMZ, se procedió a configurar el servidor Linux en la zona naranja asignándole dirección IP estática 192.168.2.10 con máscara 255.255.255.0 y gateway 192.168.2.1 [3]. Esta configuración, mostrada en la Figura 19, asegura que el servidor pueda comunicarse con el firewall para tráfico autorizado mientras permanece aislado de la red interna.

Figura 19. Establecimiento de dirección IP 192.168.2.10 en Linux server.

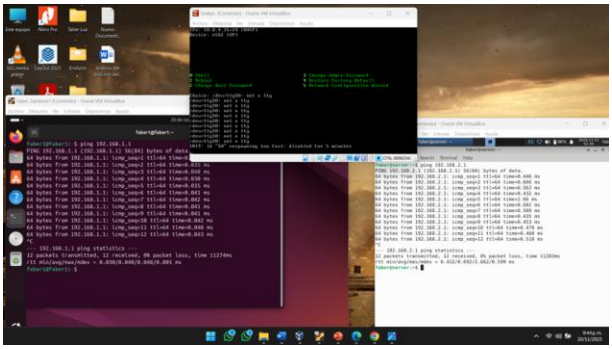


Fuente: Autoría propia captura de pantalla de Linux Server [7].

## 2.8 PRUEBA DE CONECTIVIDAD

Para validar que la configuración se realizó correctamente, se ejecutaron pruebas de conectividad entre todos los componentes. Desde la estación de trabajo Ubuntu en la zona verde (192.168.1.100) se realizaron pruebas de ping hacia la interfaz del firewall en la misma zona (192.168.1.1), confirmando conectividad básica dentro del segmento LAN. Desde el servidor Linux en la zona naranja (192.168.2.10) se realizaron pruebas similares hacia la interfaz correspondiente del firewall (192.168.2.1) como se muestra en la figura 16.

Figura 20. Transmisión de paquetes de Ubuntu y Linux Server hacia el Firewall.



Fuente: Autoría propia captura de pantalla de pruebas de conectividad.

## 3. CONFIGURACIONES NAT

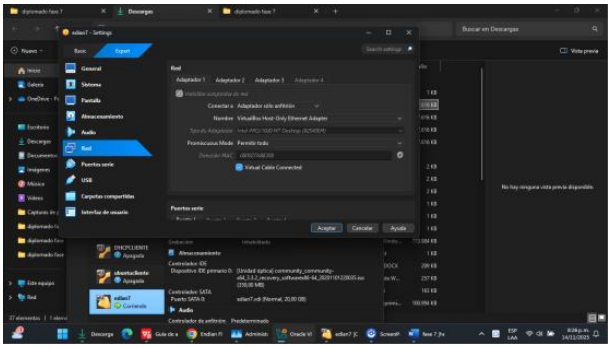
En esta sección se implementó la funcionalidad de traducción de direcciones de red (NAT) en un entorno de laboratorio usando Endian Firewall Community. La topología diseñada incluye tres zonas: GREEN (LAN), ORANGE (DMZ) y RED (WAN/Internet simulada). El objetivo fue permitir la comunicación de las redes internas hacia Internet, manteniendo la segmentación y seguridad de cada zona. Se configuraron dos reglas principales de Source NAT para garantizar que los dispositivos internos pudieran salir a redes externas utilizando una única dirección pública asociada a la zona RED. La aplicación de NAT es fundamental en redes modernas, ya que permite la conservación de direcciones IPv4, oculta la estructura interna de la red, reduce la superficie de ataque y facilita el control del tráfico que entra o sale de los segmentos protegidos [8]. Además, NAT funciona como una capa adicional de seguridad al impedir que hosts externos accedan directamente a equipos internos, reforzando el aislamiento entre LAN y DMZ. Su correcta implementación es esencial para garantizar comunicaciones eficientes sin comprometer la seguridad de la infraestructura.

### 3.1 CONFIGURACIÓN DE LA REGLA DE NAT DEMOSTRANDO EL ESTABLECIMIENTO DE LA COMUNICACIÓN DESDE LA LAN HACIA LA WAN

LAN → WAN:

La red GREEN (192.168.1.1/24) se configuró para salir hacia la WAN mediante *masquerading*, utilizando la dirección del firewall en la interfaz GREEN (192.168.1.1) como IP origen para las conexiones externas. Este mecanismo de *Source NAT* permite que múltiples hosts internos compartan una única dirección para acceder a redes públicas, optimizando el uso del espacio de direcciones IPv4 y proporcionando una capa adicional de ocultamiento y seguridad [9], [10]. La configuración de los adaptadores de red en la máquina perteneciente a la zona GREEN fue un paso fundamental para garantizar su correcta comunicación con el firewall Endian y para validar las funcionalidades de NAT en la LAN interna. En esta máquina se definieron dos interfaces de red: un adaptador conectado al segmento GREEN (192.168.1.0/24), configurado en modo *Red interna* según el entorno de virtualización, como se muestra en la figura 21, y un segundo adaptador en modo NAT, utilizado únicamente para suministrar conectividad temporal de Internet al sistema operativo durante su instalación y actualización inicial, como se muestra en la figura 22. El adaptador asociado a la red GREEN fue configurado con una IP estática 192.168.1.20, máscara 255.255.255.0 y puerta de enlace 192.168.1.1, correspondiente al firewall Endian. Esta configuración permitió que la máquina se integrara como un host legítimo dentro del segmento LAN, con acceso al WebAdmin de Endian mediante HTTPS y capacidad de realizar pruebas de conectividad, asegurando el correcto funcionamiento del enrutamiento y la traducción de direcciones en la red interna.

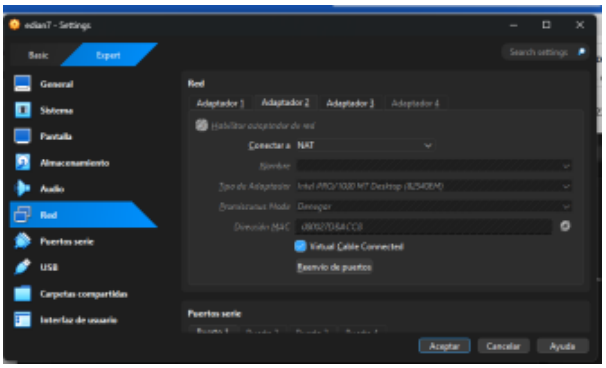
Figura 21. adaptador Green Zone



Fuente: Autoría propia captura de pantalla VirtualBox.

Desde la máquina cliente (Ubuntu Desktop) se accedió a la interfaz de administración del firewall mediante el navegador web, ingresando a la dirección https://192.168.1.1:10443, correspondiente a la IP de la interfaz GREEN del Endian. Al utilizar el protocolo HTTPS, el navegador mostró una advertencia relacionada con el certificado autofirmado, la cual fue aceptada temporalmente para permitir el ingreso seguro, como se evidencia en la figura 22. El sistema solicitó las credenciales previamente configuradas en Endian, y tras autenticarse correctamente, se obtuvo acceso al panel WebAdmin. Desde esta consola se verificó el estado de las interfaces y se ingresó a la sección Firewall → NAT, donde se revisaron y configuraron las reglas de *Source NAT* (masquerading) que habilitan la salida de tráfico tanto de la red LAN como de la DMZ hacia la red WAN. Cabe destacar que este acceso administrativo está limitado exclusivamente a la zona GREEN por razones de seguridad, ya que se considera la red de mayor confianza y esto reduce posibles vectores de ataque desde zonas menos seguras. Finalmente, luego de aplicar los ajustes correspondientes, se registraron evidencias como capturas de pantalla y pruebas de conectividad para validar el correcto funcionamiento de la traducción de direcciones.

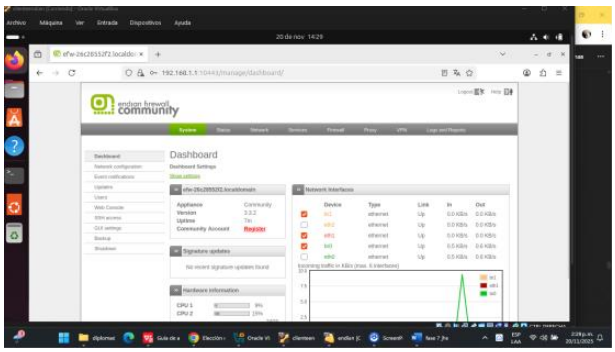
Figura 22. adaptador NAT



Fuente: Autoría propia captura de pantalla VirtualBox.

Desde la máquina cliente (Ubuntu Desktop) se accedió a la interfaz de administración del firewall mediante el navegador web, ingresando a la dirección https://192.168.1.1:10443, correspondiente a la IP de la interfaz GREEN del Endian. Al utilizar el protocolo HTTPS, el navegador mostró una advertencia relacionada con el certificado autofirmado, la cual fue aceptada temporalmente para permitir el ingreso seguro, como se evidencia en la figura 23. El sistema solicitó las credenciales previamente configuradas en Endian, y tras autenticarse correctamente, se obtuvo acceso al panel WebAdmin. Desde esta consola se verificó el estado de las interfaces y se ingresó a la sección Firewall → NAT, donde se revisaron y configuraron las reglas de *Source NAT* (masquerading) que habilitan la salida de tráfico tanto de la red LAN como de la DMZ hacia la red WAN. Cabe destacar que este acceso administrativo está limitado exclusivamente a la zona GREEN por razones de seguridad, ya que se considera la red de mayor confianza y esto reduce posibles vectores de ataque desde zonas menos seguras. Finalmente, luego de aplicar los ajustes correspondientes, se registraron evidencias como capturas de pantalla y pruebas de conectividad para validar el correcto funcionamiento de la traducción de direcciones.

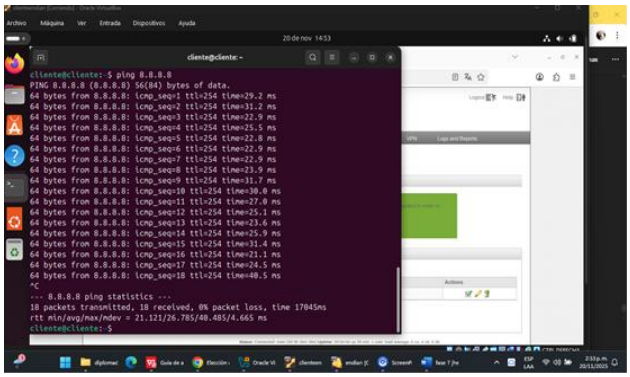
Figura 23. Ingreso a https://192.168.1.1:10443



Fuente: Autoría propia captura de pantalla Ubuntu Desktop.

La conectividad se verificó, como se muestra en la figura 21, desde una máquina Ubuntu ubicada en la zona GREEN, realizando pruebas de *ping* hacia direcciones públicas (8.8.8.8) y consultas DNS a dominios como *google.com*. Estas pruebas confirmaron la correcta traducción de direcciones y la funcionalidad del proceso de NAT dentro del entorno segmentado [11] como se evidencia en la figura 23.

Figura 24. probar conexión LAN hacia WAN



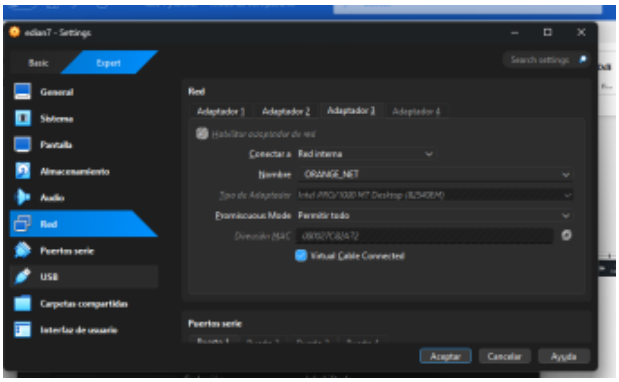
Fuente: Autoría propia captura de pantalla de Linux Server.

## 3.2 CONFIGURACIÓN DE LA REGLA DE NAT, DEMOSTRANDO EL ESTABLECIMIENTO DE LA

## COMUNICACIÓN DE LA ZONA DMZ HACIA LA INTERNET

La red ORANGE (192.168.2.0/24), correspondiente a la zona DMZ, se configuró para permitir la salida hacia la WAN mediante *masquerading*, empleando como dirección de origen la IP del firewall asignada a la interfaz ORANGE (192.168.2.1). La aplicación de NAT en redes DMZ es esencial para controlar y restringir el flujo de tráfico hacia Internet, evitando la exposición directa de los servidores o servicios ubicados en esta zona y reduciendo así la superficie de ataque [9], [10]. En la red ORANGE (DMZ) se configuró un adaptador de red dedicado exclusivamente a esta zona, cuyo propósito es aislar servicios expuestos sin comprometer la seguridad de la LAN. En la máquina Ubuntu destinada a la DMZ, el adaptador fue configurado en VirtualBox como Red Interna como se muestra en la figura 24, seleccionando la misma red interna utilizada por la interfaz ORANGE del Endian Firewall. Esto garantiza que la máquina solo pueda comunicarse con el firewall y otros equipos de la DMZ, sin acceder directamente a la LAN (GREEN). Dentro del sistema operativo Ubuntu, se asignó manualmente la dirección IP 192.168.2.20, con máscara 255.255.255.0, gateway 192.168.2.1 (correspondiente a la interfaz ORANGE del Endian) y DNS público 8.8.8.8, permitiendo operar como un cliente DMZ típico. Esta configuración de adaptadores facilita la implementación de reglas de Source NAT, asegurando que el tráfico generado en la DMZ sea correctamente traducido y encaminado hacia la WAN, mientras se mantiene el aislamiento estructural característico de una zona perimetral.

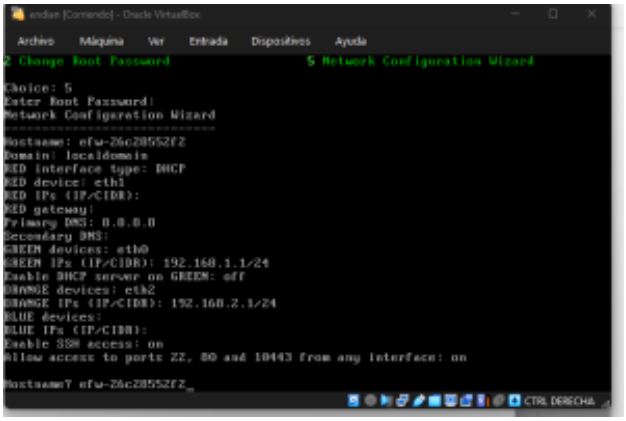
Figura 25. adaptador Orange Zone




Fuente: Autoría propia captura de pantalla VirtualBox.

En la máquina Endian Firewall se configuró la zona ORANGE (DMZ) asignándole la dirección IP 192.168.2.1, como se muestra en la figura 25, la cual actúa como puerta de enlace para todos los dispositivos ubicados en esta red perimetral. Esta interfaz fue habilitada y definida como DMZ durante el proceso de instalación o desde la sección *Network → Interfaces* del WebAdmin. Su función principal es proporcionar un punto de conexión controlado entre los servicios expuestos y el firewall, manteniendo siempre una separación estricta respecto a la red interna (GREEN). La IP 192.168.2.1 permite que Endian gestione y supervise el tráfico proveniente de la DMZ, aplicando políticas de seguridad, reglas de NAT y filtrado antes de permitir el acceso a la WAN. Esta configuración asegura que los equipos en la zona ORANGE puedan comunicarse hacia el exterior, mientras que permanecen aislados de la LAN para minimizar riesgos de seguridad.

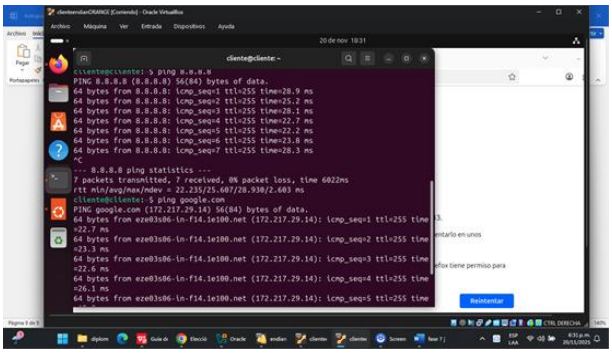
Figura 26. Configuracion Orange Zone.




Fuente: Autoría propia captura de pantalla de Linux Server.

La verificación operativa se realizó desde una máquina Ubuntu ubicada en ORANGE, comprobando conectividad hacia la WAN mediante *pings* y consultas DNS a dominios públicos, como se muestra en la figura 26. Estos resultados confirmaron la correcta traducción de direcciones, así como la capacidad de la DMZ de acceder a servicios externos sin comprometer la seguridad interna [11]. Toda la configuración se efectuó desde el WebAdmin de Endian accesible únicamente a través de la zona GREEN, dado que la administración del firewall está restringida a dicha interfaz. Esta limitación evita que la DMZ tenga acceso directo a la plataforma administrativa, reforzando el aislamiento y la seguridad de la red.

Figura 27. probar conexión DMZ hacia WAN




Fuente: Autoría propia captura de pantalla de Linux Server.

## 4.CONFIGURACIÓN DE LA INFRAESTRUCTURA

Para la práctica se creó una infraestructura virtual en Oracle VirtualBox compuesta por:
- Adaptador NAT (internet)
- Adaptador solo anfitrión (administración local)
- Red interna (DMZ)

A Endian Firewall se le asignaron las zonas predeterminadas:
- Verde: red interna
- Roja: red externa
- Naranja: DMZ

Figura 28. Configuración de adaptadores de red en Endian.

*Nota: Se observa la asignación de los tres adaptadores de red para la máquina virtual.*

*Fuente: Autoría Propia*

Endian Firewall: NAT, adaptador solo anfitrión y red interna DMZ.

## 4.1 CREACIÓN DE REGLAS DE FIREWALL EN ENDIAN

### 4.1.1 Regla para permitir HTTP (puerto 80)

Se habilitó el tráfico HTTP desde la DMZ hacia cualquier destino.
- Origen: ORANGE
- Servicio: TCP/80
- Acción: ACEPTAR
- Registro: habilitado

Figura 29. Crear Regla para permitir HTTP desde DMZ

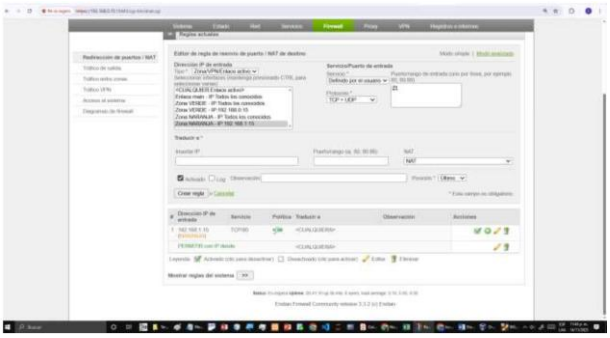

*Notas: Reglas creadas en Endian para permitir tráfico HTTP originado en la DMZ hacia el exterior.*

*Fuente: Autoría Propia*

### 4.1.2 Regla para permitir FTP (puerto 21)

Se permitió el tráfico FTP desde la DMZ hacia redes externas.
- Origen: ORANGE
- Servicio: TCP/21
- Acción: ACEPTAR

Figura 30. Crear regla para permitir FTP desde DMZ



*Nota: Regla "Allow_DMZ_FTP" configurada para permitir tráfico FTP (puerto 21) desde la zona DMZ hacia cualquier destino en Endian Firewall.*

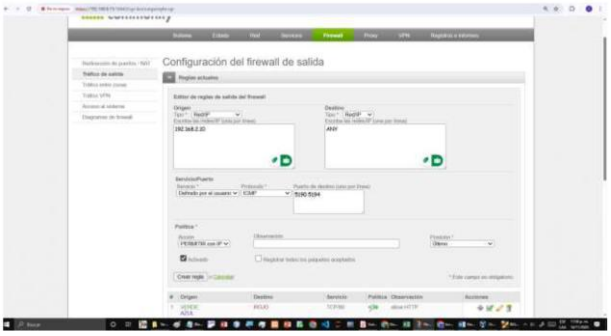
*Fuente: Autoría Propia*

### 4.1.3 Regla para denegar ICMP

Se configuraron dos reglas:
1. Bloquear ICMP desde la DMZ hacia cualquier destino.
2. Bloquear ICMP hacia la DMZ desde cualquier zona.

Ambas reglas utilizando acción DROP para evitar respuesta alguna.

Figura 31. .Regla A (denegar salida ICMP desde DMZ)




*Nota: Configuración de reglas del firewall para bloquear tráfico ICMP de entrada y salida entre la zona DMZ y otras redes en Endian Firewall.*

*Fuente: Autoría Propia*

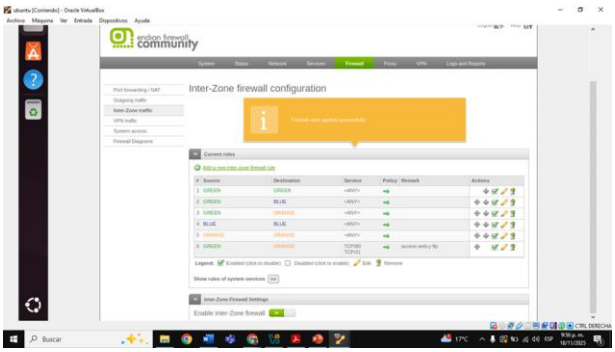
## 5. REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRAFICO

Un **firewall basado en GNU/Linux (Endian Firewall)** para gestionar el tráfico de red entre distintas zonas de seguridad: **Verde (LAN), Naranja (DMZ) e Internet (WAN/Roja)**. El objetivo principal es establecer y verificar directivas de seguridad que permitan o denieguen el flujo de protocolos clave como **HTTP y FTP** a través de las diferentes zonas.

## 5.1 Comunicación entre la zona Verde y la zona Naranja mediante HTTP y FTP

Esta regla se configuró para permitir (acción **ALLOW**) el tráfico que utiliza el protocolo **TCP** para los servicios **HTTP** y **FTP**, indicando explícitamente los puertos de destino correspondientes: el puerto **80** para el servicio web HTTP y el puerto **21** para el servicio de transferencia de archivos FTP. Esta configuración asegura que los usuarios o sistemas de la red interna y confiable (Verde) puedan acceder y consumir los servicios (como un servidor web o FTP) que se encuentran alojados en la zona semicontrolada (DMZ).

Figura 32. Comunicación de Zonas



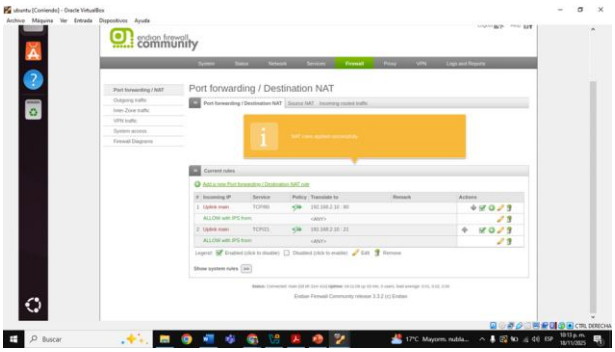

*Nota: Reglas agregadas correctamente para HTTP y FTP*

*Fuente: Autoria Propia*

## 5.2 Comunicar la zona Internet con la zona DMZ.

Se gestiona principalmente a través de la funcionalidad de **Port Forwarding** o **Destination NAT** en el Endian Firewall. Este mecanismo es crucial, ya que el firewall bloquea por defecto el tráfico entrante desde la WAN por seguridad; para permitir el acceso externo a los servicios alojados en la DMZ (como el servidor web HTTP en el puerto 80 y el servidor FTP en el puerto 21), se configuró una regla que intercepta las peticiones dirigidas a la dirección IP pública de la interfaz WAN/Roja del firewall y las **traduce** y **redirige** transparentemente hacia la dirección IP privada del servidor específico dentro de la Zona Naranja (DMZ), asegurando que el tráfico solo alcance los puertos y servicios autorizados

Figura 33. Comunicación de Zonas



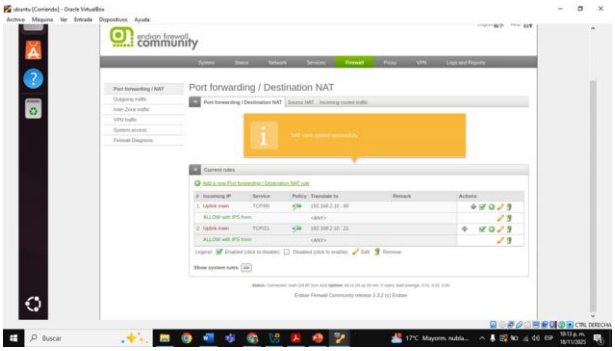

*Nota: Se agregan las 2 reglas de port forwarding tanto de http*

*Fuente: Autoría Propia*

## 5.3 Verificar en el tráfico Inter - Zona, la creación de las reglas

Estas reglas son esenciales para que los usuarios de la LAN puedan navegar por la web (utilizando **HTTP** en el puerto 80 y **HTTPS** en el 443) y para que los servidores en la DMZ puedan buscar actualizaciones, resolver nombres de dominio o enviar datos a la WAN (incluyendo potencialmente el servicio **FTP** en el puerto 21), configurándose de forma explícita las directivas **Out-going** para controlar y permitir únicamente el tráfico saliente deseado desde cada zona hacia el exterior.

Figura 34. Creación de reglas



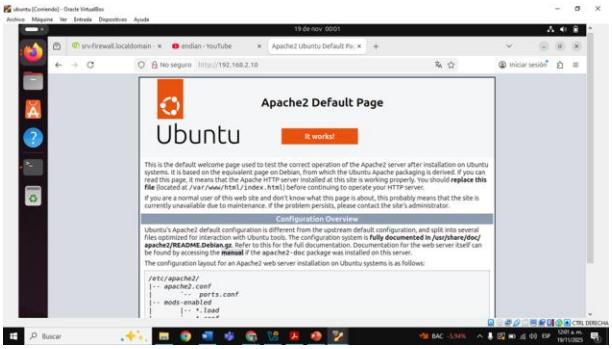

*Nota: Se agregan las 2 reglas de port forwarding de ftp*

*Fuente: Autoría Propia*

## 5.4 Servicio HTTP desde la LAN hacia la zona DMZ

Al establecer la acción en **PERMITIR (ALLOW)**, se garantizó que los usuarios o sistemas ubicados en la red interna de confianza (LAN) pudieran iniciar y completar exitosamente la conexión para acceder a cualquier servicio web que estuviera alojado en el servidor de la DMZ, verificando el acceso al servidor HTTP con una prueba desde un navegador web.

Figura 35. Servicio HTTP




*Nota: **ingreso del servicio HTTP desde la LAN hacia la zona DMZ** creando una regla de tráfico **Inter-Zona** explícita en el firewall, permitiendo el protocolo **TCP** en el puerto **80** desde la **Zona Verde** hacia la **Zona Naranja***

*Fuente: Autoria Propia*

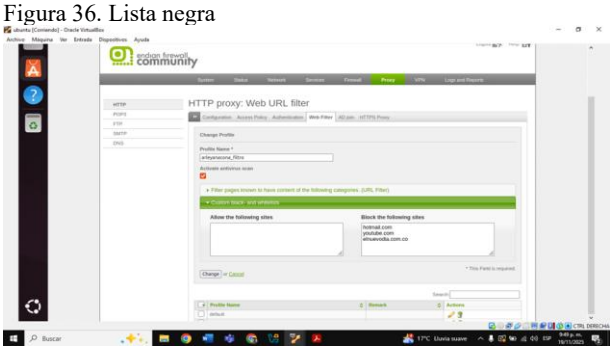
# 6. Implementar un Proxy HTTP con políticas de autenticación para navegación en Internet.

la configuración de un **Proxy HTTP No Transparente** utilizando un firewall perimetral basado en GNU/Linux (**Endian Firewall Community Edition**), con el objetivo de controlar la navegación de los usuarios de la red local (LAN). La implementación se centra en establecer políticas de **autenticación por usuario** y aplicar un **filtro de contenido (Lista Negra)** para restringir el acceso a sitios web específicos, mejorando así la seguridad y la productividad de la red.

## 6.1 Crear un perfil y establecer una lista negra bloqueando los siguientes sitios

Se centró en establecer las restricciones de navegación que aplicará el proxy, lo cual se logró mediante la creación de un **Perfil de Filtrado** específico dentro de la configuración del servicio Proxy HTTP. A este perfil se le asoció una **Lista Negra de URLs Denegadas** (Blacklist), que actúa como un filtro de contenido, donde se incluyeron explícitamente los dominios `www.hotmail.com`, `www.youtube.com` y `www.elnuevodia.com.co` para asegurar que el acceso a estos portales fuera bloqueado de manera efectiva para los usuarios que utilicen dicho perfil.

Figura 36. Lista negra




*Nota: Parametrización del servicio proxy en modo "not transparent".*

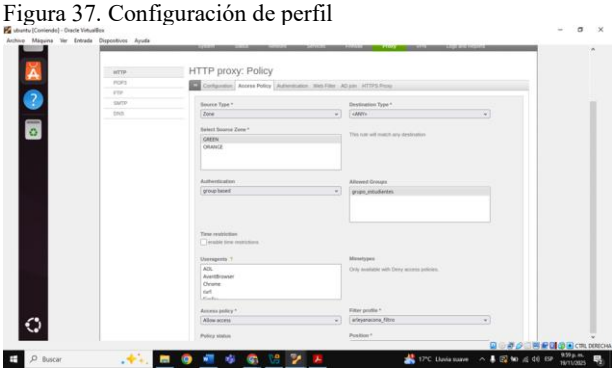
*Fuente: Autoría Propia*

## 6.2 Autenticación por usuario

Se establecio la **Política de Acceso (Access Policy)** del proxy para aplicar el control de usuarios, lo cual se logró enlazando dos componentes clave: primero, el sistema se configuró para requerir **Autenticación por Usuario/Grupo**, asegurando que solo los usuarios registrados (como *usuario_proxy*) pudieran

utilizar el servicio; y segundo, esta política fue vinculada directamente al **Perfil de Filtrado** previamente creado (que contiene la Lista Negra de sitios denegados), garantizando que las restricciones de contenido se aplicaran exclusivamente a aquellos usuarios que se identificaran y fueran autorizados a navegar a través del proxy.

Figura 37. Configuración de perfil



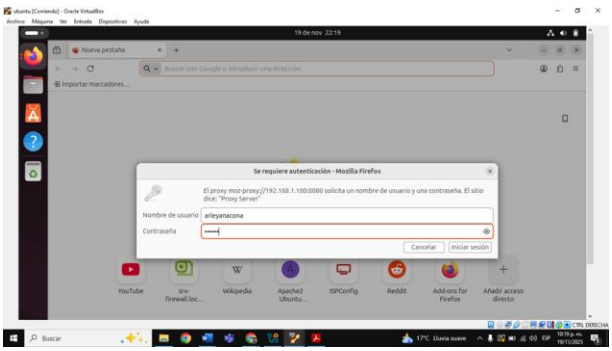

*Nota: Establecimiento de la política de control de acceso.*

*Fuente: Autoría Propia*

## 6.3 Probar desde la LAN a través de un navegador Web, el acceso a los portales referenciados en la lista negra.

Realizando pruebas directas desde un equipo de la **LAN** (Zona Verde) a través de un navegador web, el cual fue configurado previamente para usar el firewall como servidor proxy (ej. IP del firewall:puerto 8080). Esta prueba de verificación consistió en intentar acceder a cada uno de los sitios web que habían sido añadidos a la Lista Negra ; el resultado esperado y comprobado fue que, tras la autenticación exitosa del usuario, el proxy interceptó las peticiones y denegó el acceso, mostrando un mensaje de **"Acceso Denegado"** (*Forbidden*) generado por el propio proxy, confirmando la aplicación efectiva de la política de filtrado de contenido y autenticación sobre el tráfico saliente.

Figura 38. Navegador del cliente LAN




*Nota: Credenciales previamente configuradas en Endian Firewall.*

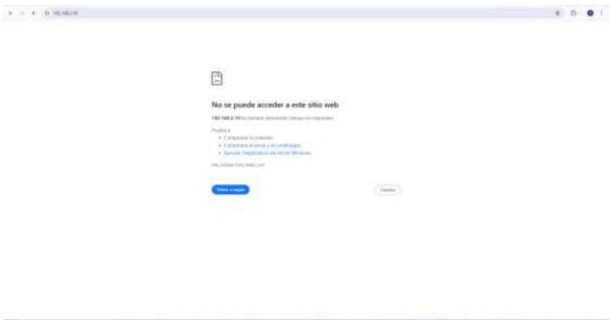
*Fuente: Autoría Propia*

# 7 RESULTADOS

Los resultados obtenidos evidenciaron que la configuración realizada permitió establecer correctamente la comunicación entre las diferentes zonas de la red. La LAN logró acceder a la WAN mediante la regla de NAT configurada, y la zona DMZ también pudo comunicarse con Internet sin interrupciones. Las pruebas de conectividad, como ping y navegación, confirmaron que el enmascaramiento de direcciones se aplicó de manera adecuada y que el tráfico fluye según lo previsto en el diseño de red.

Las pruebas realizadas confirmaron el acceso correcto a los servicios habilitados (HTTP y FTP), con códigos de respuesta exitosos. Asimismo, las pruebas de ping generaron tiempo de espera, validando la correcta denegación del protocolo ICMP.

Figura 39. Respuesta curl o navegador mostrando la página

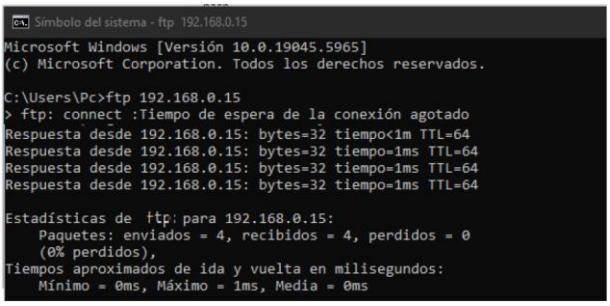



*Nota: Prueba de acceso HTTP al servidor ubicado en la DMZ. Respuesta*

*HTTP con código 200 indica que el servicio web está accesible a través de la regla permitida*

*Fuente: Autoría Propia*

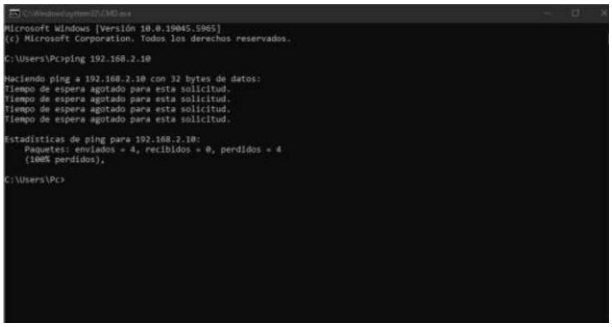
Figura 40. Probar FTP




*Nota: Conexión FTP exitosa al servidor en DMZ desde la red de pruebas. Nota. Puerto 21 abierto y permitido por la regla Allow_DMZ_FTP.*

*Fuente: Autoría Propia*

*Figura 41. Probar ping (ICMP)*



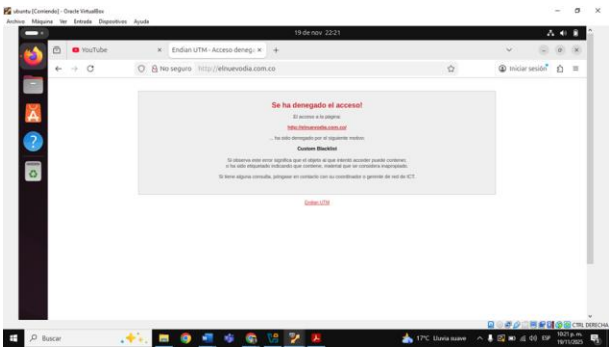

*Nota: Prueba de ping hacia el servidor DMZ que evidencia la denegación de ICMP. Se observa tiempo de espera (timeout) y ausencia de respuesta, confirmando la regla Deny_DMZ_ICMP.*

*Fuente: Autoría Propia*

El correcto funcionamiento de las reglas de firewall implementadas, verificándose exitosamente el ingreso de los servicios. Y validando la comunicacion, demostrando que la configuración de port forwarding y las políticas inter-zona aplicadas en Endian Firewall permitieron el tráfico autorizado mientras mantuvieron el aislamiento de seguridad entre los diferentes segmentos de red. Todas las pruebas realizadas desde el navegador web evidenciaron la efectividad de la configuración implementada para los servicios tanto HTTP como FTP.

al intentar acceder desde el navegador en la LAN (previamente configurado y autenticado), la imagen debe mostrar que el acceso fue **bloqueado** por el sistema. El resultado concreto es un mensaje de **"Acceso Denegado"** o *Forbidden*, generado directamente por el servidor proxy, confirmando la aplicación efectiva de la política de filtrado sobre el tráfico HTTP saliente y demostrando el control de navegación.

*Figura 42. Comprobación del acceso*




*Nota: Revisión del comportamiento del portal elnuevodia.com.co*

*Fuente: Autoría Propia*

# 8 DISCUSIÓN

La configuración de NAT en este entorno demostró cómo la traducción de direcciones permite mantener la segmentación entre las zonas GREEN y ORANGE, garantizando al mismo tiempo el acceso controlado a la red WAN. Aunque la implementación fue funcional, se evidenció que la administración del firewall requiere acceso exclusivo desde la red GREEN, lo cual refuerza buenas prácticas de seguridad, pero limita la gestión desde otras zonas como la DMZ. Asimismo, el uso de reglas de Source NAT simplificó la salida a Internet desde ambas redes internas; sin embargo, este enfoque debe complementarse con políticas de firewall más estrictas en escenarios reales para evitar fugas de tráfico no deseado o accesos no autorizados. En conjunto, los resultados muestran que NAT es un componente esencial, pero debe integrarse con medidas adicionales para lograr una arquitectura de red realmente segura.

Los resultados demostraron la importancia de la segmentación de redes mediante zonas de seguridad y la aplicación de reglas precisas que controlen el tráfico permitido y denegado. El bloqueo de ICMP evita procesos de reconocimiento en la red, mientras que la habilitación controlada de servicios HTTP y

La implementación exitosa de las reglas de firewall en Endian valida la eficacia de la segmentación de red para equilibrar accesibilidad y seguridad, aplicando el principio de mínimo privilegio. Sin embargo, la experiencia evidenció que la complejidad en la configuración exige un conocimiento sólido de fundamentos de red y protocolos para evitar errores críticos. Esta práctica nos refuerza que, más allá del uso de interfaces gráficas, la comprensión subyacente de las herramientas de seguridad en Linux es indispensable para una administración robusta y la resolución efectiva de problemas.

El Proxy HTTP no transparente funcionó de manera satisfactoria, aplicando correctamente la lista negra y exigiendo autenticación previa. La política configurada garantizó que solo los usuarios registrados accedieran a Internet y que los dominios restringidos permanecieran inaccesibles. Además, los registros del sistema permitieron auditar los intentos de acceso denegados.

# 9 CONCLUSIONES

**1**. La implementación de la arquitectura de red mediante las zonas Verde (LAN), Roja (WAN) y Naranja (DMZ) permitió establecer una segmentación adecuada que facilita el control del tráfico, mejora la administración y refuerza la seguridad de la infraestructura. Esta división, junto con la correcta creación de reglas en Endian Firewall, permitió habilitar servicios esenciales como HTTP y FTP entre la LAN y la DMZ sin comprometer la protección del sistema.

**2.** Asimismo, la configuración de traducciones de dirección (NAT y Port Forwarding) aseguró que tanto la LAN como la DMZ pudieran acceder de manera controlada y segura a la red WAN. Esta funcionalidad también posibilitó la exposición de servicios de la DMZ hacia el exterior bajo criterios estrictos de seguridad, sentando las bases para la creación de políticas más avanzadas en futuras fases del proyecto.

**3.** El bloqueo del protocolo ICMP representó una medida adicional de defensa frente a intentos de reconocimiento o escaneo, reafirmando la importancia de las reglas de acceso y filtrado dentro de una política de seguridad perimetral.

**4.** Durante la práctica también se implementó un servidor Proxy HTTP No Transparente con autenticación y filtrado de contenido mediante listas negras. Esta configuración demostró un nivel de control superior sobre el acceso a Internet, permitiendo aplicar políticas granulares por usuario o grupo, aspecto fundamental en entornos corporativos y educativos que requieren regular el uso de los recursos y mitigar riesgos.

**5.** A nivel formativo, la actividad fortaleció significativamente las competencias en administración de sistemas GNU/Linux, configuración de seguridad perimetral y diagnóstico de redes. El uso de entornos virtualizados facilitó la recreación de escenarios reales de forma segura, favoreciendo la experimentación, el análisis y la comprensión de los conceptos aplicados.

## 10 REFERENCIAS


[1] LPI Linux Essentials, “Tema 5: Seguridad y sistema de permisos de archivos,” 2022.

[2] Canonical, Guía del Ubuntu Desktop 20.04 LTS, 2023.

[3] Debian, Manual del Administrador Debian 12.5.0, 2023.

[4] Oracle, VirtualBox User Manual, 2020.

[5] P. Hernández y J. Sánchez, “Monitoreo y administración de sistemas Linux,” UNAD, 2022.

[6] P. Hernández y J. Sánchez, “Servidores para administración remota y compartir recursos,” UNAD, 2022.

[7] Endian srl. (2008). Manual de referencia del firewall Endian r. 2.2.1.9. https://docs.endian.com/archive/2.2/efw.system.html

[8] Cisco Systems, *Cisco Networking Academy: CCNA Routing and Switching – NAT Fundamentals*. Cisco Press, accesso académico.

[9] P. Srisuresh and K. Egevang, “Traditional IP Network Address Translator (Traditional NAT),” *RFC 3022*, IETF, Jan. 2001.

[10] W. Stallings, *Data and Computer Communications*, 10th ed. Upper Saddle River, NJ, USA: Pearson, 2013.

[11] J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach*, 7th ed. Boston, MA, USA: Pearson, 2017.

[12] T. Berners-Lee, R. Fielding, y H. Frystyk, "Hypertext Transfer Protocol -- HTTP/1.1," *IETF RFC 2068*, Ene. 1997.

[13] P. P. F. Srisuresh y D. Egevang, "Traditional IP Network Address Translator (Traditional NAT)," *IETF RFC 3022*, Ene. 2001

[14] L. W. S. Fan, M. W. S. Al'fiyah, y R. M. F. B. Mohamad, "Implementation of content filtering system using proxy server," en *Proc. 2nd Int. Conf. on Comput. and Commun. Eng.*, Malasia, 2008, pp. 1111-1115.

[15] D. J. M. Snelders y P. M. T. L. A. Snelders, *Implementing and Administering Linux: Security, Servers, and Advanced Topics*. Pearson Education, 2018.