# IMPLEMENTACIÓN DE SEGURIDAD EN GNU/LINUX MEDIANTE LA CONFIGURACIÓN DE INTERFACES, SERVICIOS ESENCIALES Y ARQUITECTURAS DMZ USANDO ENDIAN FIREWALL

Avila Viatela, Johana Katherine c.c. 1014221129
e-mail: jkavilav@unadvirtual.edu.co
Caminos Arias, Guillermo Alberto c.c. 80747822
e-mail: gacaminosa@unadvirtual.edu.co
Herrera, Bibiana Paola c.c. 1019060432
e-mail: bpherrera@unadvirtual.edu.co
Velandia Rubio, Miller Damián c.c. 1007297752
e-mail: mdvelandiar@unadvirtual.edu.co

**RESUMEN:** *En este artículo se describe la implementación de un esquema integral de seguridad en sistemas GNU/Linux mediante el uso de la distribución Endian Firewall (EFW) como plataforma central para la administración de zonas LAN, WAN y DMZ. Se configuraron interfaces de usuario, servicios esenciales y reglas de seguridad orientadas a proteger servidores internos y aplicaciones desplegadas en entornos corporativos. La metodología incluyó la instalación de EFW en VirtualBox, configuración de NAT, establecimiento de reglas de tráfico entre zonas, habilitación controlada de servicios y la implementación de un proxy HTTP con autenticación. Los resultados muestran una infraestructura segura, segmentada y funcional, capaz de proteger bases de datos y servicios web bajo GNU/Linux. Este enfoque permite fortalecer la integridad, disponibilidad y confidencialidad dentro de intranets y extranet corporativas.*

**PALABRAS CLAVE**: DMZ, Endian Firewall, GNU/Linux, Seguridad informática, SSH, NAT, LAN, puerto

## 1 INTRODUCCIÓN

En la actualidad, la evolución constante de las amenazas cibernéticas obliga a las organizaciones a implementar estrategias sólidas de seguridad perimetral, orientadas a proteger la integridad, la disponibilidad y la confidencialidad de sus infraestructuras tecnológicas. La correcta segmentación de redes internas (LAN) y la creación de Zonas Desmilitarizadas (DMZ) se ha convertido en una práctica fundamental para controlar los riesgos asociados a accesos no autorizados y ataques dirigidos [1]. En este sentido, los sistemas basados en GNU/Linux representan una opción robusta, flexible y segura para la administración de firewalls avanzados, destacándose soluciones como Endian Firewall (EFW), reconocida por su capacidad de gestionar tráfico, aplicar políticas de filtrado y fortalecer la protección perimetral [2].

No obstante, muchas empresas carecen de una arquitectura segmentada correctamente o de configuraciones perimetrales definidas, incrementando la vulnerabilidad frente a ataques externos, intrusiones laterales o explotación de servicios expuestos. Este panorama plantea la necesidad de diseñar e implementar infraestructuras de red que integren firewalls especializados, políticas de control de acceso y mecanismos de autenticación para garantizar un entorno seguro [3].

El propósito de este artículo es analizar y documentar la implementación de una solución de seguridad perimetral basada en GNU/Linux Endian Firewall, abordando configuraciones relacionadas con segmentación de red, reglas NAT, acceso entre zonas y políticas de navegación mediante proxy HTTP. La propuesta se desarrolló en un entorno virtualizado con Oracle VirtualBox, en el cual se configuraron máquinas virtuales que representan una LAN corporativa, una zona DMZ con servidor web y un firewall como punto de control central.

A través de un enfoque práctico y colaborativo, se configuraron las zonas Verde (LAN), Naranja (DMZ) y Roja (WAN), estableciendo reglas de tráfico, listas negras de navegación y autenticación de usuarios. Estas configuraciones permitieron verificar la efectividad del filtrado, el bloqueo de protocolos como ICMP, la habilitación controlada de servicios HTTP y FTP, y la funcionalidad de la infraestructura bajo un modelo seguro. Los resultados obtenidos demuestran que Endian Firewall permite consolidar una arquitectura de red segmentada, eficiente y controlada, capaz de proteger servidores críticos y gestionar el acceso a recursos internos y externos.

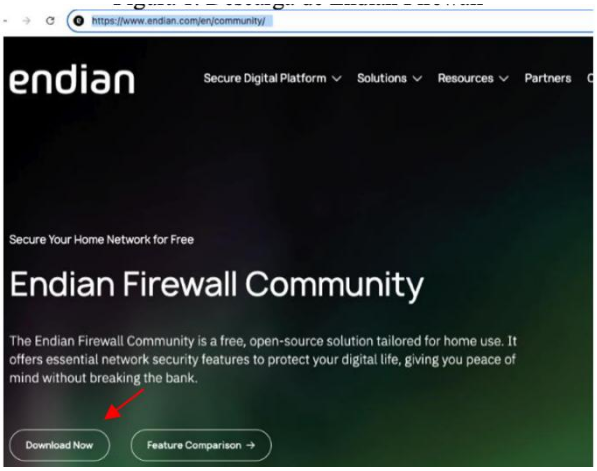
La experiencia desarrollada aporta conocimientos relevantes para estudiantes y profesionales interesados en la protección de infraestructuras de red utilizando software libre. Asimismo, evidencia la importancia del uso de herramientas especializadas para fortalecer la seguridad perimetral, reforzando el papel de GNU/Linux en la administración de redes corporativas. A continuación, se detalla la arquitectura diseñada, los procedimientos realizados en cada temática y los resultados alcanzados en este estudio.

## 2 PREPARACIÓN E INSTALACIÓN DEL SISTEMA ENDIAN FIREWALL

Para dar inicio al desarrollo de las temáticas, se procedió a descargar la versión Community de Endian Firewall desde su sitio oficial en https://www.endian.com/en/community/. Antes de ello, fue necesario preparar el entorno de virtualización instalando Oracle VirtualBox, herramienta que permite emular

equipos de cómputo mediante la creación y ejecución de máquinas virtuales dentro de cualquier sistema operativo anfitrión. Endian, como distribución Linux de código abierto, funciona en este proyecto como un sistema de firewall, actuando como un mecanismo de protección perimetral capaz de filtrar el tráfico y resguardar los servicios implementados

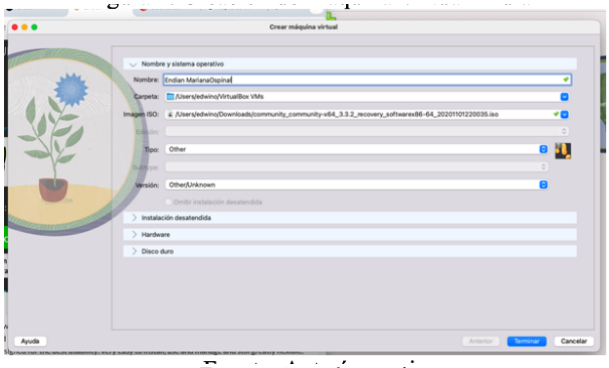
Figura 1. Proceso de Descarga de Endian Firewall Community




Fuente: Autoría propia

Después de completar la descarga de Endian, se procedió a crear la máquina virtual correspondiente y, en la sección destinada a la "imagen ISO", se incorporó el archivo ISO previamente obtenido.

Figura 2. Configuración Inicial de la Máquina Virtual para Endian

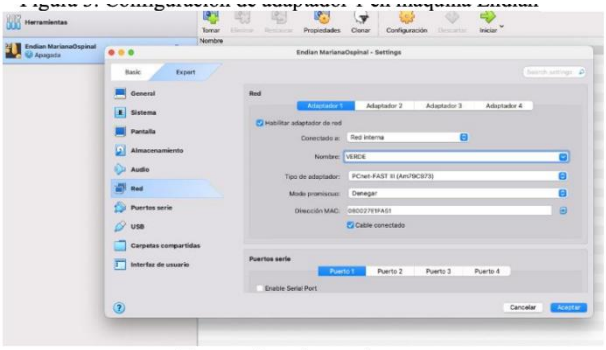


Fuente: Autoría propia

Posteriormente, se realizaron los ajustes correspondientes en las interfaces de red, quedando organizadas de la siguiente forma:

El Adaptador 1 se configuró como *zona verde* utilizando el modo de red interna; el Adaptador 2 se asignó a la *zona naranja* también bajo red interna; y el Adaptador 3 se estableció en modo *puente*, permitiendo la conexión hacia la red LAN y el acceso a Internet.

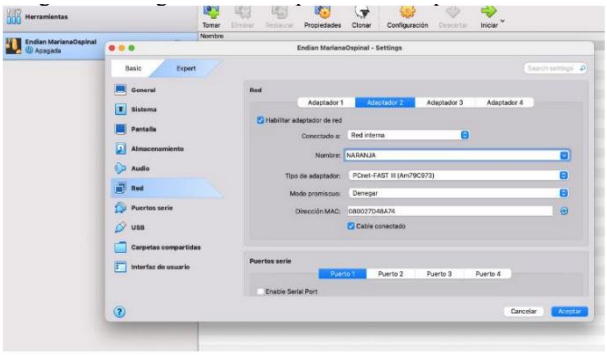
Figura 3. Ajuste del adaptador de red 1 en la máquina virtual Endian



Fuente: Autoría propia

La configuración inicial del sistema Endian Firewall corresponde al adaptador 1, el cual es asignado a la Zona Verde dentro de la estructura de red.

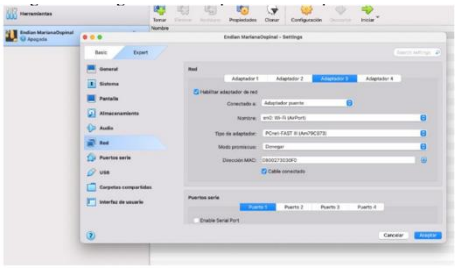
Figura 4. Definición de la interfaz de red 2 en el entorno VirtualBox para Endian



Fuente: Autoría propia

Adaptador 2 en Endian Firewall, configurado para operar como la Zona Naranja.

Figura 5. Ajuste del tercer adaptador de red en la máquina virtual Endian



Fuente: Autoría propia

Adaptador 3 en Endian Firewall, configurado como interfaz de salida hacia Internet mediante el modo *Adaptador puente*.

Posteriormente, se inició la máquina virtual realizando el arranque desde la imagen ISO. Durante el asistente de instalación, se seleccionó el idioma y se aprobó la creación automática de la partición y del disco. A continuación, el sistema identificó la primera interfaz correspondiente a la Zona

Verde, por lo que se solicitó ingresar la dirección IP y la máscara de subred asignadas a esta red: 192.169.100.1 con 255.255.255.0.

Figura 6. Configuración de la Dirección IP para la Zona Verde en Endian

Fuente: Autoría propia

Después de confirmar y aplicar todas las configuraciones previas, se verifica que la instalación de Endian se ha completado correctamente, mostrándose la información correspondiente a la Zona Verde, incluida su dirección IP y el puerto habilitado para la conexión.

En el paso siguiente, se seleccionó la opción 0 del menú con el fin de acceder al Shell dentro del sistema Endian. En este punto, se inició sesión utilizando la contraseña predeterminada *endian*. Al ingresar, el sistema notificó que la Zona Roja había recibido automáticamente una dirección IP mediante DHCP. Esto se debe a que, durante la configuración del adaptador 3 en la máquina virtual, se eligió el modo Adaptador puente**,** permitiendo que Endian obtenga una dirección IP pública de manera automática desde el proveedor de red. Esta configuración favorece la conectividad con Internet, ya que posibilita que múltiples dispositivos internos accedan a la red externa utilizando una única dirección IP asignada por el servicio de Internet.

En la última fase, las configuraciones adicionales de Endian se realizaron desde una máquina cliente con Linux Mint.

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

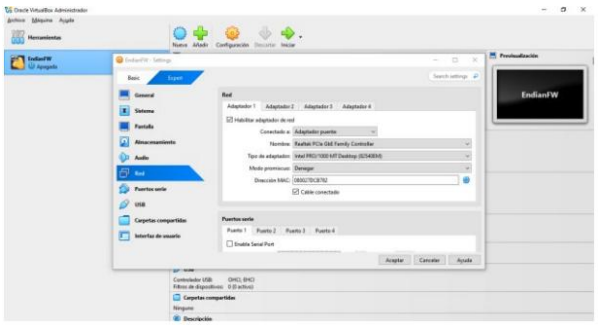
En la temática 1 se configuraron las zonas de red de Endian Firewall dentro del entorno virtual. Estas zonas verde (LAN), naranja (DMZ) y roja (WAN) representan diferentes niveles de seguridad y permiten separar el tráfico y proteger servicios esenciales.

La configuración se hizo desde VirtualBox, asignando un adaptador de red distinto para cada zona. En esta parte se describen de forma breve los pasos utilizados para definir las interfaces correspondientes a cada segmento [4].

La zona verde corresponde a la red interna segura donde se ubican los equipos cliente. En VirtualBox, el Adaptador 1 se configuró como Adaptador interno con el nombre LAN_zVerde.

En Endian, esta zona quedó asignada a eth0, con la IP 192.168.0.15 y su máscara. Esto permite que los equipos internos se comuniquen a través del firewall y accedan a servicios o internet según las reglas establecidas.
La Figura 7 muestra la configuración del adaptador para la zona verde.

Figura 7. Ajuste del Adaptador de Red Correspondiente a la Zona Verde en el Entorno Virtual

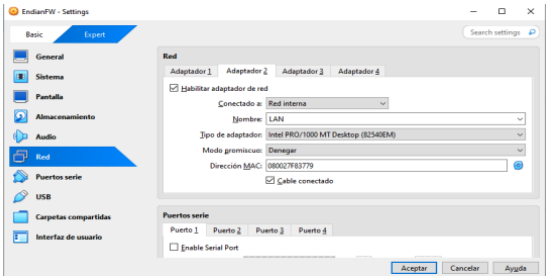


Fuente: Autoría propia

La zona naranja se destinó a los servicios que deben ser accesibles desde el exterior, como servidores web o FTP, manteniéndolos separados de la red interna pero con acceso controlado.

En VirtualBox, el Adaptador 2 se configuró como Adaptador interno usando el nombre DMZ_zNaranja. En Endian, esta zona se vinculó a la interfaz eth1, asignándole la IP 192.168.10.1. Esta red será utilizada por la máquina virtual que funcionará como servidor, la cual deberá tener una IP del mismo rango para permitir la comunicación directa.

Figura 8. Ajuste del Adaptador de Red Correspondiente a la Zona Naranja (DMZ) en VirtualBox



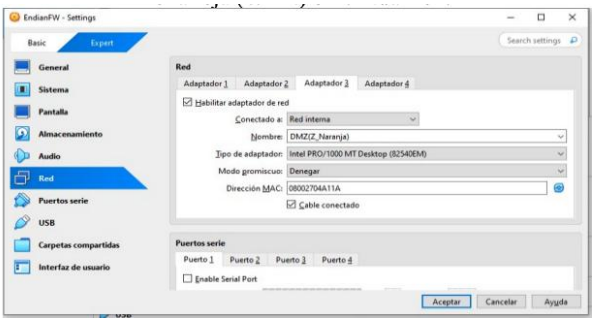

Fuente: Autoría propia

La zona roja corresponde al acceso externo, es decir, la simulación de la conexión a Internet. En VirtualBox, el Adaptador 3 se configuró como Adaptador puente (o NAT, según disponibilidad), lo que permite que Endian obtenga automáticamente una dirección IP vía DHCP desde la red real del equipo anfitrión.

Dentro de Endian, esta zona se asignó a la interfaz eth2, sin requerir la configuración manual de una IP. Gracias a esta

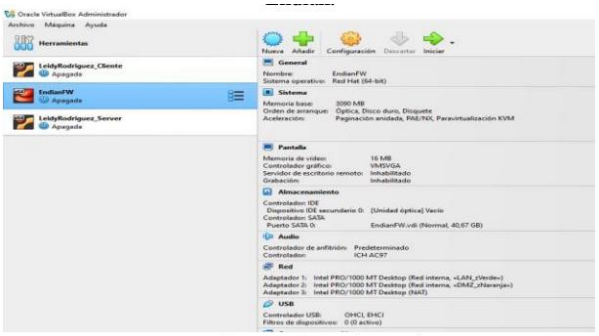
conexión, será posible realizar pruebas de navegación desde la LAN y permitir que los servidores en la DMZ se actualicen, siempre y cuando existan reglas de red adecuadas.

Figura 9. Asignación del Adaptador Puente/NAT para la Zona Roja (WAN) en VirtualBox.




Fuente: Autoría propia

Figura 10. Interfaces configuradas para las zonas Verde, Naranja y Roja en Endian.




Fuente: Autoría propia

La configuración adecuada de las zonas de red en Endian Firewall es esencial para lograr una segmentación segura y eficiente. Definir adaptadores específicos para cada zona, asignar las direcciones IP correspondientes y verificar la comunicación garantiza un manejo controlado del tráfico entre las redes internas y externas. Esta base sólida permite que posteriormente el sistema implemente funciones como NAT, proxy y gestión de servicios sobre una arquitectura confiable.

# 4 TEMÁTICA 2: CONFIGURACIÓN NAT

Superado el tema de la creación, instalación y configuración de Endian (EFW) y habiendo segmentado los adaptadores y redes internar para los diferentes propósitos, se debe comenzar con esta temática definiendo términos que se abordaran para el desarrollo de aquí en más:

NAT (Network Address Translation) técnica que permite que múltiples dispositivos en una red privada compartan una única dirección IP pública para acceder a Internet [5].

LAN (Local Area Network) Una LAN es una red de computadoras y dispositivos interconectados en un área geográfica limitada, como una casa, oficina o edificio [6].

WAN (Wide Area Network) Una WAN es una red que conecta múltiples redes locales (LAN) a través de grandes distancias geográficas, como ciudades o países [7].

DMZ (Demilitarized Zone) Una DMZ es una subred perimetral que agrega una capa de seguridad entre la red interna (LAN) y redes externas como Internet (Achotech, 2024).

SSH (Secure Shell) SSH es un protocolo de red que permite acceder y administrar sistemas informáticos de forma remota y segura mediante cifrado. Es ampliamente usado para conexiones a servidores Linux y Unix [8].

Teniendo lo anterior claro el movimiento de estar en función primero de las tres redes (Verde, Naranja y roja) y luego de creación tanto de la NAT como de las reglas para la administración de puertos y servicios:

Con la utilización de tres maquinas una con el ENDIAN (roja), otra con el Ubuntu server (Naranja) y el Ubuntu desktop (verde) como se observa a continuación

Tabla 1. Conectividad de las máquinas virtuales según la zona de red configurada.

| Red | ENDIAN | Ubuntu Desktop | Ubuntu Server |
|---|---|---|---|
| Verde | ✅ | ✅ | ❌ |
| Naranja | ✅ | ❌ | ✅ |
| NAT | ✅ | ❌ | ❌ |

Fuente: Autoría propia

Se comienza configurando la regla de NAT para la red verde, demostrando el establecimiento de la comunicación desde la LAN hacia la WAN (Red simulada de Internet).

La segmentación ya es conocida, pero vamos a recordarla:

Red Verde (verde)

- Red: 192.168.100.1/24
- Máscara: 255.255.255.0
- Equipo Ubuntu desktop: 192.168.100.2
- Rango usable: 192.168.100.2 – 192.168.100.254

Red Naranja (naranja)

- Red: 10.0.0.1/24
- Máscara: 255.255.255.0
- Server 10.0.0.2
- Rango usable: 10.0.0.2 – 10.0.0.254

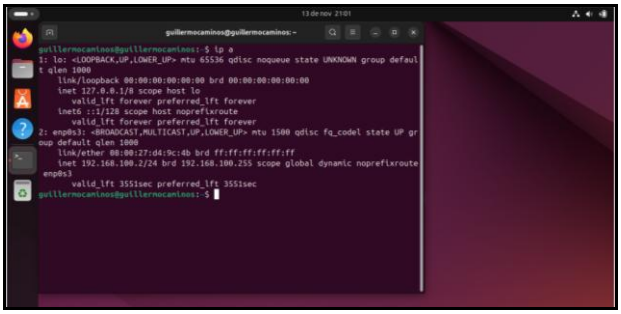
La red roja la vamos a descubrir más adelante.

Primero y muy aconsejable es configura el NAT de la red verde, esto con el fin de acceder desde el navegador al panel de control de ENDIAN en donde hay que hacer otras configuraciones para la red naranja y la creación de reglas.

Nota. Estas configuraciones también se pueden hacer desde la CLI (Command Line Interface) de ENDIAN pero es para un nivel de experticia más avanzado.

Entonces para configurar la red verde y que LAN tenga comunicación a través de la NAT hacia WAN (internet), primero se debe configurar ENDIAN (puedes ser desde la instalación) como el Gateway de la red verde, asignando lo como IP la dirección destinada para tal fin 192.168.100.1 y además después de varios ajustes desde el Ubuntu desktop, es mejor que endian preste el servicio DHCP y se le asigne la IP de manera automática al equipo de escritorio.

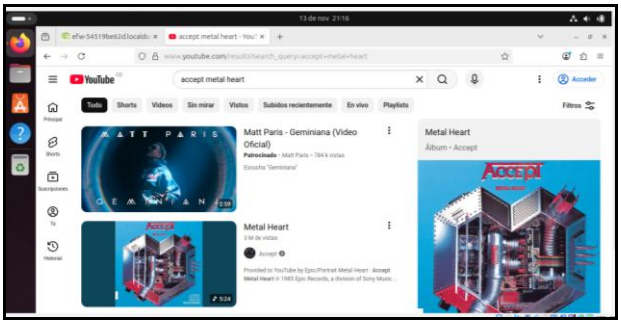
Figura 11. Visualización de las interfaces de red en Ubuntu mediante el comando *ip a*.



Fuente: Autoría propia

Consultando la IP desde la terminal de Ubuntu desktop se puede evidenciar que la IP ha sido asignada por el ENDIAN y corresponde a 192.168.100.2; para comprobar esto se pueden realizar ping a ENDIAN, pero que mejor evidencia que intentar desde el navegador del equipo acceder a un sitio web.

Figura 12. Navegación en YouTube desde Ubuntu para verificar conectividad externa.



Fuente: Autoría propia

La navegación a través de la NAT proporcionada por ENDIAN para la red verde se encuentra comprobada, lo que confirma el correcto funcionamiento del acceso externo. Aún más relevante es que ahora es posible ingresar al panel de administración de ENDIAN, lo que permite implementar configuraciones adicionales orientadas a fortalecer la seguridad de la red naranja.

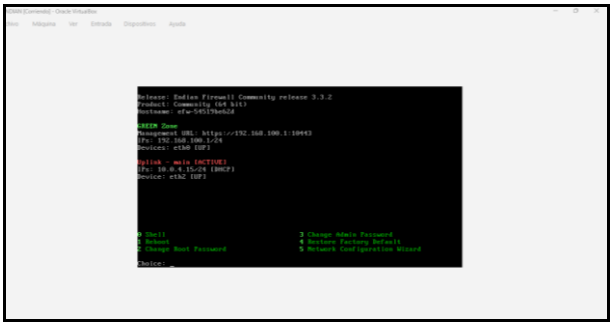
Aunque en este ejercicio únicamente se utiliza EFW para gestionar servicios como NAT, segmentación de redes y monitoreo del tráfico, es importante resaltar las múltiples ventajas que ofrece esta herramienta de código abierto basada en Linux, entre ellas servicios VPN, proxy y filtrado web, así como antivirus y antispam.

En la segunda parte de la temática, se solicita configurar la regla de NAT correspondiente a la DMZ (red naranja), demostrando la comunicación hacia Internet y verificando el funcionamiento del reenvío de puertos mediante la creación de las reglas correspondientes.

El establecimiento de la comunicación hacia la Internet, además verificar en el re-envió de puertos / NAT, mediante la creación de las reglas.

Para comenzar con esta el espacio de trabajo del ENDIAN:

Figura 13. Vista del panel de estado inicial de Endian Firewall en la consola de VirtualBox.



Fuente: Autoría propia

Es notorio como ya identifica dos de las tres redes (verde y roja) entre ellas la red que tiene conexión a internet y cuya IP es asignada de manera DHCP por el prestador de servicios de internet (ISP) en este caso 10.0.4.15/24.

Entonces para comenzar con la configuración de la red naranja desde el panel de ENDIAN se realizó desde el panel de ENDIAN, asistente de configuración de red, se comienza seleccionando la red que se va a configurar, NARANJA en este caso, se agregó la IP para la red que se relacionó en la segmentación como Gateway(10.0.0.1) y luego se selecciona la interface a la cual corresponde en este caso la que esta identificada con la MAC 080027A2E884, la cual se obtiene de la asignación de las redes a la maquina de ENDIAN en el virtual box.

Figura 14. Configuración del asistente de red para la zona roja (WAN) en la interfaz web de Endian Firewall.

Fuente: Autoría propia

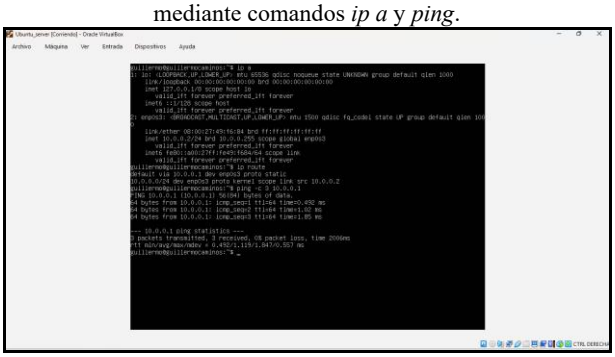
Una vez configurada la NAT en ENDIAN se debe configurar la IP fija para el SERVER, no está de más aclarar que dicha IP tiene que estar dentro del rango de direcciones descrita en la segmentación, entonces se accede al CLI del

SEVER y con ayuda del editor de texto simple "nano" configuro la IP fija 10.0.0.2 y al Gateway el cual es el que se le asignó a ENDIAN 10.0.0.1 y se aplica la configuración de red en el SERVER y esto debería de ser suficiente para que podamos establecer contacto con ENDIAN desde el SERVER.

Figura 15. Configuración de red estática en Ubuntu Server mediante el archivo *netplan*

Fuente: Autoría propia

Figura 16. Verificación de conectividad en Ubuntu Server mediante comandos *ip a* y *ping*.

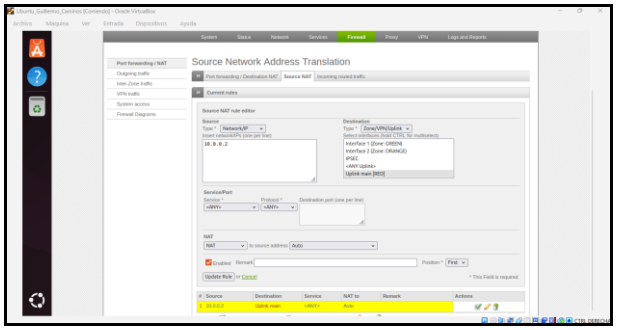


Fuente: Autoría propia

Para comprobar la conectividad, basta con revisar la dirección IP asignada y ejecutar un ping hacia ENDIAN. Tal como se evidencia, los tres paquetes enviados fueron recibidos correctamente, lo que confirma que la comunicación entre el servidor y el firewall funciona de manera adecuada.

Posteriormente, es necesario regresar al panel de administración de ENDIAN, donde se gestionan todos los aspectos relacionados con la red. En este punto corresponde configurar la NAT para permitir que la DMZ tenga acceso a Internet. Esta tarea se realiza desde la opción *Source NAT*, donde, mediante una configuración sencilla, se habilita el servicio correspondiente para esta red.

Figura 17. Configuración de la regla de Source NAT para la red DMZ en Endian Firewall.




Fuente: Autoría propia

Con la configuración ya aplicada y operativa, se procede a verificar la salida a Internet desde la DMZ. Para ello, se ejecuta un *ping* primero al DNS de Google y luego a una dirección específica. Ambas pruebas muestran respuesta completa, lo que confirma que la DMZ tiene acceso exitoso a Internet y que la primera parte del ejercicio queda finalizada.

Figura 18. Verificación de conectividad a Internet desde la DMZ mediante pruebas de *ping*.

Fuente: Autoría propia

A continuación, inicia la segunda parte del ejercicio, en la cual se debe crear una regla para el monitoreo de servicios basados en puertos. Para ello, se configura una nueva regla desde el panel de administración de ENDIAN, enfocada en este caso en el servicio SSH, que opera por defecto sobre el puerto 22

Figura 19. Creación de la regla de redirección de puertos (Destination NAT) para el servicio SSH en Endian Firewall

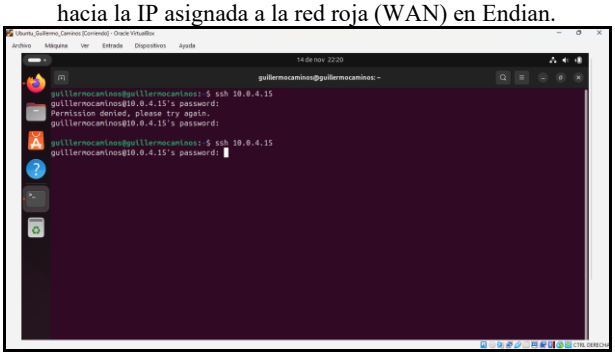

Fuente: Autoría propia

Para este proceso se utiliza la sección *Port forwarding / Destination NAT*, que permite redirigir el tráfico entrante desde la red externa (Roja/WAN) hacia un servicio ubicado en

la red interna (LAN o DMZ). Esta función es fundamental para habilitar y supervisar servicios expuestos de forma segura.

Para comprobar que la regla funciona, se emplea un equipo fuera de la red naranja; en este caso, Ubuntu Desktop. Desde su terminal se intenta acceder por SSH al servidor interno. La IP utilizada para la prueba corresponde a la red roja, es decir, la dirección asignada al ENDIAN por el ISP: 10.0.4.15, ya que es la que recibe las conexiones externas que luego serán redirigidas.

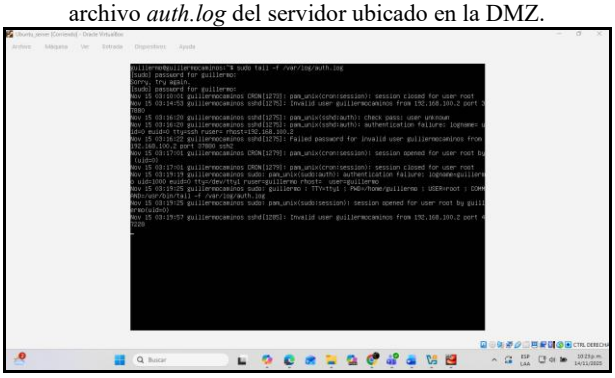
Figura 20. Intento de conexión SSH desde Ubuntu Desktop hacia la IP asignada a la red roja (WAN) en Endian.




Fuente: Autoría propia

Si la regla está funcionando correctamente, debe generarse un rastro en el servidor ubicado en la DMZ. Esto se valida verificando el intento de acceso por SSH y revisando los registros correspondientes almacenados en /var/log/auth.log.

Figura 21. Registros de intentos de autenticación SSH en el archivo *auth.log* del servidor ubicado en la DMZ.



Fuente: Autoría propia

El registro existe y tiene información como fecha, hora, IP del usuario remoto y el evento en este caso acceso de denegado por un password incorrecto.

Es importante implementar la seguridad en nuestros sistemas Linux y considerar que lo que no se monitorea, no se controla y que una forma de minimizar riesgos es segmentando la red y controlando el tráfico por los puertos y el uso de los servicios.

# 5 TEMÁTICA 3: PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

La regla de NAT de salida permite que los equipos ubicados en la zona Verde (LAN) y en la zona Naranja (DMZ) accedan a Internet mediante la traducción de sus direcciones privadas hacia la dirección pública de la zona Roja (WAN) [9]. Como parte de la configuración realizada, se habilitaron los servicios esenciales dentro de la DMZ, instalando un servidor web que opera por HTTP en el puerto 80 y un servidor FTP en el puerto 21, ambos ejecutados en Ubuntu Server. Estas configuraciones se gestionaron desde el Firewall Endian, donde además se bloqueó el protocolo ICMP en los puertos 8 y 30, con el fin de evitar pruebas de ping y reforzar la seguridad de la red interna.

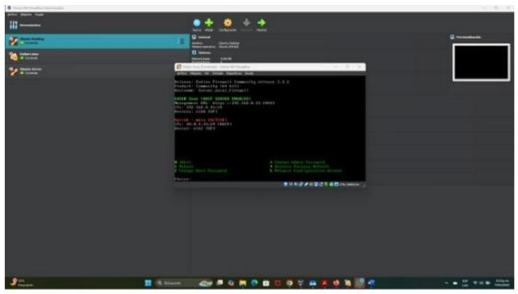
## 5.1 CONFIGURACIÓN DE RED

La configuración de red, como se muestra en la tabla 1, permitió definir las zonas Roja, Verde y Naranja con sus respectivas direcciones y puertas de enlace. La zona Verde fue establecida con la gateway 192.168.0.15 y la red 192.168.0.20/24, donde se ubicó un equipo con Ubuntu Desktop 24.04. En la zona Naranja se configuró la gateway 192.168.1.0.1 y la red 192.168.1.0.20/24, asignada a un Ubuntu Server 24.04. La zona Roja quedó asociada al firewall Endian, encargado del control externo. Esta distribución permitió organizar la comunicación interna y delimitar las funciones de cada segmento, asegurando una estructura de red coherente y funcional.

Tabla 2. Asignación de zonas y parámetros de red

| Zona | Zona Roja | Zona verde | Zona Naranja |
|---|---|---|---|
| Gateway | | 192.168.0.15 | 192.168.10.1 |
| Dirección IP | | 192.168.0.20/24 | 192.168.10.20/24 |
| Host | Endian | Ubuntu Desktop 24.04 | Ubuntu Server 24.04 |

Figura 22. Configuración de las zonas Verde (LAN) y Roja (WAN) en Endian Firewall



Fuente: Autoría propia

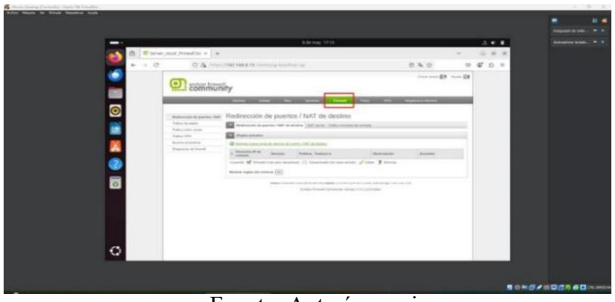
La interfaz de Endian ejecutándose en VirtualBox, donde se visualizan los parámetros asignados a las zonas Verde y Roja. La zona Verde corresponde a la red interna (LAN), encargada de gestionar los dispositivos locales, mientras que la zona Roja funciona como la interfaz WAN hacia Internet. En la pantalla se observan las direcciones IP, estados de conexión y opciones básicas del firewall. Esta configuración permite

establecer y controlar la comunicación entre la red interna y la red externa.

## 5.2 IMPLEMENTACIÓN DE LOS SERVICIOS WEB (HTTP) Y DE TRANSFERENCIA DE ARCHIVOS (FTP)

Para habilitar los servicios HTTP y FTP en la DMZ fue necesario instalar sus gestores en el servidor ubicado en esta zona, lo cual requirió primero permitir el acceso a Internet desde la zona Naranja hacia la zona Roja. Con esta conexión se pudieron descargar e instalar los paquetes necesarios. El proceso comenzó ingresando al Firewall Endian desde el navegador del equipo en la zona Verde. Allí se creó una regla NAT para enlazar las zonas definidas y traducir la IP del servidor a una IP pública en la zona Roja. La Figura 23 muestra el acceso a la sección del firewall donde se configura dicha regla.

Figura 23. Interfaz del Firewall Endian para configuración de NAT



Fuente: Autoría propia

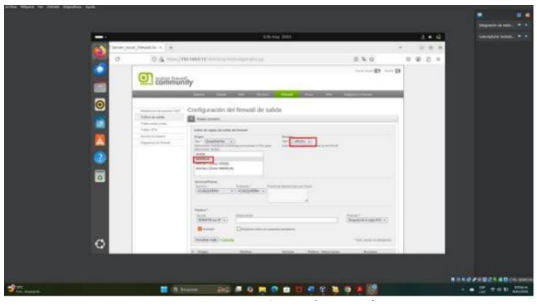
Desde la opción Fuente NAT, se especifica la dirección IP correspondiente al servidor ubicado en la DMZ, indicando que esta será la IP de origen para la traducción. Posteriormente, se define que el tráfico generado por dicho servidor debe dirigirse hacia la zona Roja, que actúa como destino y salida hacia Internet. Esta configuración permite que las solicitudes del servidor sean traducidas correctamente y puedan alcanzar la red externa. Además, garantiza que el firewall gestione la comunicación de forma segura y controlada. La figura muestra la interfaz donde se realiza este procedimiento.

Figura 24. Panel de configuración de NAT de origen hacia la zona Roja

Fuente: Autoría propia

La configuración de la regla que habilita el tráfico desde la zona Naranja hacia la zona Roja, permitiendo que el servidor en la DMZ tenga salida a la WAN, se muestra en la Figura 25. Esta regla define que todo el flujo proveniente de la zona Naranja sea redirigido correctamente hacia la zona Roja, garantizando el acceso a Internet y permitiendo la instalación y funcionamiento de los servicios necesarios.

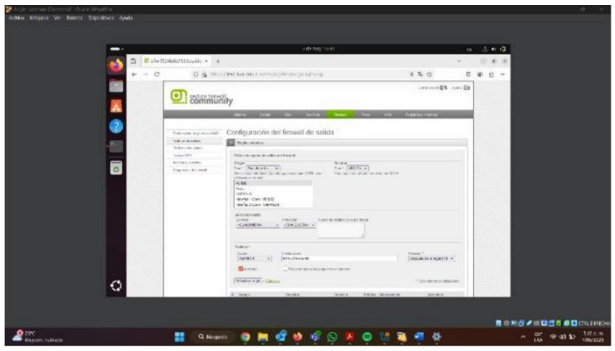
Figura 25. Configuración de salida de tráfico desde la zona Naranja hacia la zona Roja



Fuente: Autoría propia

La sección de configuración del firewall de salida en Endian, accedida desde un entorno Ubuntu Desktop. En esta pantalla se define la política que controla el tráfico saliente desde las distintas zonas de la red. Se observa la selección de la zona de origen, la especificación de servicios permitidos y la asignación de destinos autorizados. También se visualizan las opciones para permitir o bloquear conexiones según protocolos y puertos definidos. Esta configuración garantiza un control detallado del tráfico que sale de la red interna hacia el exterior.

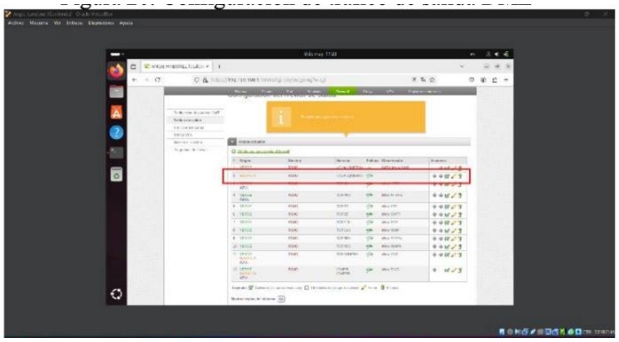
Figura 26. Panel de configuración del tráfico saliente en Endian Firewall



Fuente: Autoría propia

Posteriormente en la figura 27 presenta el listado de reglas del firewall de salida en Endian, donde se resalta la regla correspondiente a la zona Naranja (DMZ). En dicha regla se observa que el origen es la DMZ y el destino es la zona Roja, permitiendo la comunicación hacia la red WAN. La interfaz muestra también los servicios asociados, los puertos permitidos y el estado de cada regla activa. Los iconos laterales permiten administrar cada configuración, como editar, activar o eliminar. Esta visualización confirma que la DMZ tiene acceso autorizado hacia Internet mediante la política establecida.

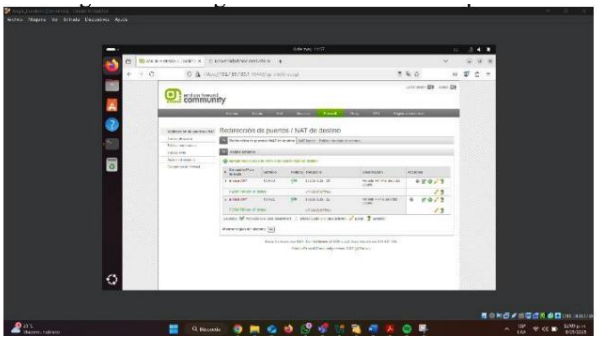
Figura 27. Permisos de salida de la DMZ hacia la WAN en Endian Firewall



Fuente: Autoría propia

En el servidor Ubuntu Server se instalaron los servicios apache2 para el funcionamiento del servidor web y vsftpd para habilitar las transferencias FTP. Luego, en Endian Firewall se crearon reglas de Destination NAT que redirigen las solicitudes externas recibidas en los puertos 80 y 21 hacia el servidor ubicado en la DMZ. También se configuraron políticas de firewall que permiten el acceso a estos servicios desde la zona Verde (LAN). Esta estructura asegura un control adecuado del tráfico y mantiene separadas las zonas según los principios de seguridad perimetral.

Figura 28. Parámetros de reenvío de tráfico hacia la DMZ



Fuente: Autoría propia

# 6 TEMÁTICA 4: REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO

En este apartado se describe la configuración, verificación y prueba de las reglas de acceso establecidas entre las distintas zonas de la red: Zona Verde (LAN), Zona Naranja (DMZ) y Zona Roja/WAN (Internet). El propósito es asegurar una conectividad segura mediante los servicios HTTP (puerto 80) y FTP (puerto 21) [10].

A. Comunicación entre la Zona Verde y la Zona Naranja mediante HTTP y FTP
Se implementaron reglas que permiten:

Tráfico HTTP (TCP/80) desde la LAN hacia la DMZ.
Tráfico FTP (TCP/21) desde la LAN hacia la DMZ.

B. Comunicación entre la Zona WAN y la Zona DMZ
Se configuraron reglas para autorizar:

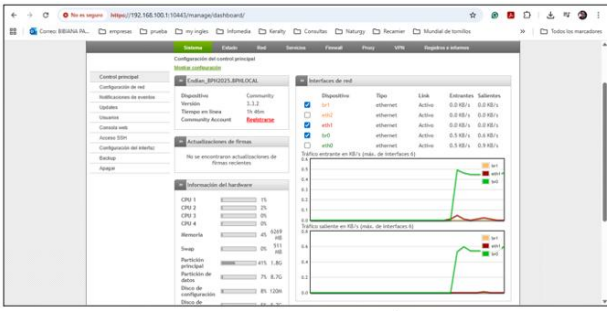
Acceso HTTP desde la WAN hacia la DMZ.
Acceso FTP desde la WAN hacia la DMZ.

C. Verificación del tráfico entre zonas

La validación se realizó mediante:

1. El monitor de tráfico del firewall.
2. La revisión de los registros de eventos (logs).
3. Pruebas funcionales ejecutadas desde cada una de las zonas.

Figura 29. Monitoreo de interfaces de red y tráfico en tiempo real desde el panel de administración de Endian Firewall.

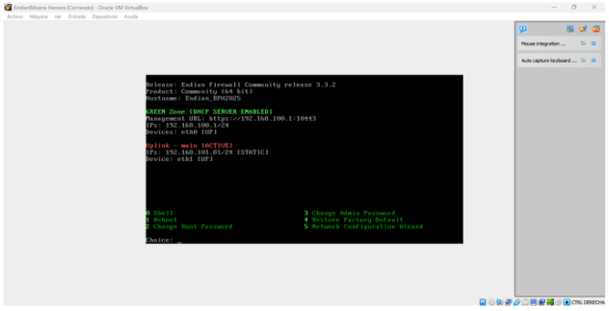


Fuente: Autoría propia

La configuración de reglas de acceso y las pruebas funcionales se realizaron sobre un servidor Linux, un equipo Linux de escritorio y un firewall Endian. Esta infraestructura permitió verificar de manera práctica el control del tráfico entre las zonas LAN, DMZ y WAN.

Las pruebas demostraron la correcta identificación de servicios y protocolos, así como el funcionamiento adecuado del firewall, la gestión de puertos y la aplicación de políticas de seguridad. La interacción entre los sistemas confirmó una comunicación segura y controlada entre todas las zonas de la red.

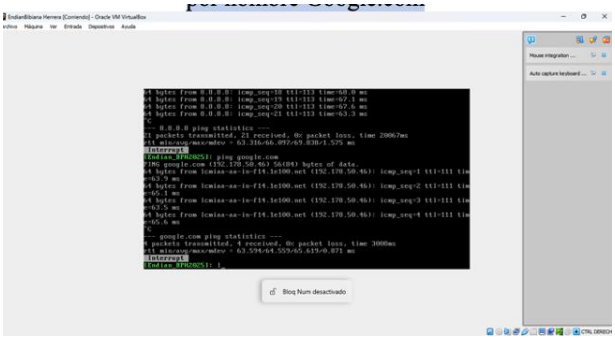
Figura 30. Estado de las interfaces de red y parámetros iniciales del sistema en la consola de Endian Firewall



Fuente: Autoría propia

Se verifica la conectividad de nuestro Endian al IP 8.8.8.8 y por nombre Google.com

Figura 31. Pruebas de conectividad desde Endian Firewall mediante comandos *ping* hacia redes internas y externas.

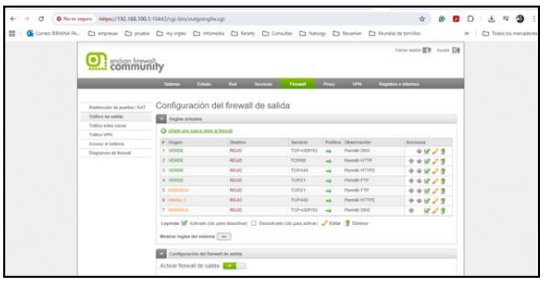


Fuente: Autoría propia

En esta sección se muestra el *Firewall de salida* de Endian Firewall, donde se controlan las reglas que permiten o bloquean el tráfico desde las zonas internas hacia la zona ROJA (Internet). Las reglas indican que la zona VERDE (LAN) puede acceder a servicios como DNS (53), HTTP (80), HTTPS (443) y FTP (21). La zona NARANJA (DMZ) y otra interfaz adicional cuentan con permisos similares.

Cada regla detalla el origen, destino, servicio o puerto, y la acción aplicada, que corresponde a *Permitir* (ACCEPT). Las anotaciones describen la función de cada permiso, como "Permitir HTTP". El firewall de salida está habilitado, garantizando que solo el tráfico autorizado tenga salida hacia Internet.

Figura 32. Reglas configuradas en el firewall de salida de Endian Firewall para las zonas LAN, DMZ y WAN.

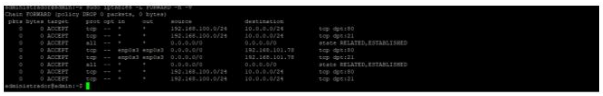


Fuente: Autoría propia

La interfaz del módulo *Firewall Inter-Zona* de Endian Firewall muestra las reglas actualmente activas entre las zonas VERDE (LAN), NARANJA (DMZ) y AZUL (WiFi/Invitados). Las reglas visibles permiten el tráfico entre estas zonas utilizando el servicio configurado como <CUALQUIERA>, lo que indica que todo tipo de tráfico está autorizado según el origen y destino definidos. Cada regla dispone de opciones para editarla, eliminarla o modificar su orden. El firewall Inter-Zona se encuentra habilitado, de modo que las políticas establecidas se aplican para controlar la comunicación entre las diferentes zonas de la red.

En esta práctica, los protocolos permitidos corresponden a HTTP y FTP, mientras que el resto del tráfico permanece bloqueado por defecto, garantizando así un control más estricto sobre las comunicaciones interzonales.

Figura 33. Reglas activas de *iptables* en la cadena FORWARD para el control del tráfico entre zonas en Endian Firewall

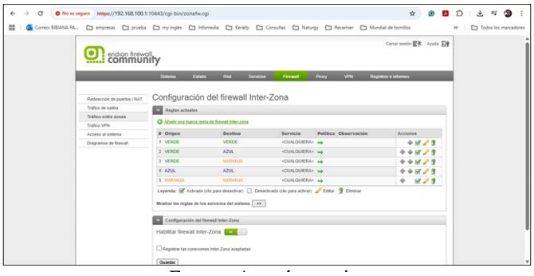


Fuente: Autoría propia

Las reglas activas del firewall UFW, basado en iptables, muestran en la cadena *ufw-user-input* permisos de entrada para los puertos 22 (SSH), 21 (FTP) y 80 (HTTP), aceptando tráfico desde cualquier origen.

La cadena *ufw-user-limit* aplica limitación de intentos de conexión, registrando la actividad y bloqueando automáticamente las solicitudes cuando se excede el número permitido.

Figura 34. Reglas activas del firewall Inter-Zona en Endian Firewall para el control del tráfico entre zonas LAN, DMZ y WiFi.



Fuente: Autoría propia

Se presenta un conjunto de reglas orientadas a permitir únicamente tráfico controlado entre las diferentes zonas, garantizando que las comunicaciones cumplan con las políticas establecidas.

En conjunto, la configuración evidencia un firewall activo que habilita solo los servicios esenciales y aplica controles de tráfico, reforzando así la seguridad entre las zonas de la red.

Figura 35. Reglas activas del firewall UFW basadas en iptables para el control del tráfico en el equipo Linux.

Fuente: Autoría propia

# 8 CONCLUSIONES

La puesta en marcha de Endian Firewall dentro de una infraestructura virtualizada se evidencia como una alternativa eficiente y formativa para comprender los fundamentos de la segmentación de red, la defensa perimetral y la administración de servicios. El entorno diseñado permite recrear el comportamiento de una red corporativa protegida, facilitando la apropiación de conceptos como NAT, DMZ, reglas de firewall y control de acceso entre zonas.

La configuración de las reglas NAT y las políticas de filtrado en Endian probó ser un mecanismo altamente efectivo para gestionar la conectividad y la seguridad entre los diferentes segmentos de la red, especialmente en las comunicaciones desde la LAN y la DMZ hacia la WAN. Mediante la creación de reglas de Source NAT y el control del tráfico saliente, fue posible ocultar las direcciones IP privadas y aplicar restricciones precisas que permitieron validar el sistema tanto en escenarios de acceso autorizado como bloqueado. Las pruebas confirmaron la capacidad, flexibilidad y solidez de esta arquitectura, lo que la convierte en una opción pertinente para laboratorios, entornos empresariales o actividades académicas que requieran separación clara del tráfico y control detallado de la salida hacia redes externas.

Se consolidó así una infraestructura de red virtual completa y segmentada utilizando Endian Firewall Community. Entre los resultados más relevantes se encuentran: ingreso exitoso a la interfaz web de Endian desde la zona Verde, verificación de conectividad a Internet desde la zona Verde (Desktop) y la zona Naranja (Server), acceso correcto a la página web y al servicio FTP alojado en Ubuntu Server desde los clientes ubicados en la zona Verde, redireccionamiento del tráfico mediante reglas NAT de forma adecuada, la práctica fortaleció las competencias en redes, seguridad perimetral y uso de entornos virtuales para simular escenarios operativos reales.

Asimismo, la configuración de reglas de acceso entre la zona Verde y la zona Naranja, habilitando exclusivamente los servicios HTTP (puerto 80) y FTP (puertos 20 y 21), evidencia la capacidad de segmentar el tráfico y permitir únicamente los servicios necesarios entre zonas diferenciadas, manteniendo un nivel de seguridad adecuado dentro de la infraestructura.

El módulo Port Forwarding / Destination NAT en Endian Firewall permite exponer servicios internos de forma segura hacia el exterior, controlando qué tráfico entra desde la red WAN hacia servidores en la LAN o DMZ. Es esencial para publicar servicios como SSH, HTTP o correo sin comprometer la seguridad de la red interna (Endian.com, s.f.).

# 9 REFERENCIAS


[1] Hernández, C., Palacios, R. H., & de Jesús Núñez-Cárdenas, F. (2023). Instalación y configuración de Pfsense en máquina virtual con VirtualBox. *Ciencia Huasteca Boletín Científico de la Escuela Superior de Huejutla*, *11*(22), 22-31.

[2] Gomes, J. R. D. F. (2023). Segurança de redes de computadores: um estudo sobre o Endian Firewall.

[3] Mokrani Gallego, O. (2021). Diseño y manejo de infraestructuras de red cumpliendo con los estándares de ciberseguridad.

[4] Garcia, E. A., Jaramillo, P. A. R., Acevedo, C. M. S., Delgado, F. N. G., & Clavijo, C. A. M. (2022). Implementación y configuración bajo NethServer solucionando necesidades especificas con GNU/Linux.

[5] Jiménez, J. (2025, septiembre 29). Qué significa NAT y cómo actúa en la red. RedesZone. https://www.redeszone.net/tutoriales/redes-cable/que-es-nat-red/

[6] RedesInformaticas.org. (s.f.). Redes LAN: ¿Qué son? Características, ventajas y desventajas. https://redesinformaticas.org/red-lan/

[7] Concepto.de. (s.f.). Red WAN. https://concepto.de/red-wan/

[8] Achotech. (2024, marzo 18). ¿Qué es una red DMZ? Cómo funciona y su rol en la protección de redes. https://achotech.com/que-es-dmz-red/

[9] Fasyah, T. I., Putra, J. C., Chaiyadi, R. T., Andreas, J., & Pakpahan, T. W. (2024). SIMULASI JARINGAN UNTUK SISTEM TERDISTRIBUSI OPENSTACK DENGAN GNS3. *Jurnal Ilmu Komputer dan Sistem Informasi*, *12*(2).

[10] Velurtas, F., Diaz, J., & Luengo, M. (2009). *Optimización de Enlaces en redes IP. Control de tráfico* (Doctoral dissertation, Tesis de Posgrado).