Implementación de arquitectura de seguridad perimetral con Endian Firewall Community: segmentación de red y control de acceso en entornos virtualizados

Michael Stivens Arguello Lotero
msarguellol@unadvirtual.edu.co
Juan Carlos Vargas Pulido
jcvargaspu@unadvirtual.edu.co
Michael Alexander Reyes Acosta
mareyesaco@unadvirtual.edu.co
John Stive Acuña Valle
Jsacunav@unadvirtual.edu.co

RESUMEN: *El presente artículo documenta la implementación de una arquitectura de seguridad perimetral basada en el firewall UTM Endian Firewall Community, desplegado en un entorno virtualizado mediante Oracle VM VirtualBox. Se estableció una segmentación de red en tres zonas de seguridad —verde (LAN), naranja (DMZ) y roja (WAN)—, configurando reglas de traducción de direcciones (NAT), filtrado de servicios HTTP y FTP, control de tráfico interzona y un proxy HTTP con autenticación de usuarios y políticas de lista negra. Las pruebas de conectividad y funcionamiento confirmaron que la segmentación permite aislar servicios críticos, controlar el acceso a Internet desde la red interna y mitigar la exposición a amenazas externas. Los resultados evidencian que una correcta configuración de zonas de seguridad constituye la base para garantizar la integridad y disponibilidad de los servicios en infraestructuras de red basadas en GNU/Linux.*

PALABRAS CLAVE: Endian Firewall, NAT, seguridad perimetral, servidor, red, bloqueo.

ABSTRACT: *This article documents the implementation of a perimeter security architecture based on the Endian Firewall Community UTM firewall, deployed in a virtualized environment using Oracle VM VirtualBox. Network segmentation was established across three security zones — green (LAN), orange (DMZ), and red (WAN) — configuring network address translation (NAT) rules, HTTP and FTP service filtering, inter-zone traffic control, and an HTTP proxy with user authentication and blacklist policies. Connectivity and functionality tests confirmed that segmentation enables the isolation of critical services, control of Internet access from the internal network, and mitigation of exposure to external threats. The results demonstrate that proper configuration of security zones constitutes the foundation for ensuring the integrity and availability of services in GNU/Linux-based network infrastructures.*

KEYWORDS: Endian Firewall, NAT, perimeter security, server, network, blocking.

1 INTRODUCCIÓN

La protección de infraestructuras de red constituye uno de los pilares fundamentales en la administración de sistemas operativos modernos. En entornos donde coexisten servicios internos, aplicaciones web y acceso a Internet, resulta imprescindible establecer mecanismos que permitan controlar el flujo de información, aislar recursos críticos y mitigar la exposición ante amenazas externas. La seguridad perimetral, entendida como el conjunto de estrategias desplegadas en la frontera entre una red de área local y redes no confiables, adquiere relevancia particular en plataformas basadas en GNU/Linux, donde la flexibilidad del núcleo y la disponibilidad de herramientas de código abierto facilitan la construcción de soluciones robustas y adaptables a las necesidades organizacionales (Endian, 2024).

En este contexto, los firewalls de tipo UTM (Unified Threat Management) han emergido como una alternativa integral frente a los sistemas de filtrado tradicionales, al combinar en una sola plataforma funcionalidades de filtrado de paquetes, traducción de direcciones de red (NAT), proxy de aplicaciones, detección de intrusiones y control de contenido. Endian Firewall Community, distribución derivada de Debian GNU/Linux, representa una opción ampliamente documentada para la implementación de estas capacidades en entornos virtualizados, permitiendo la segmentación de la red en zonas de seguridad diferenciadas que limitan el alcance de posibles compromisos (Endian, s. f.).

El presente artículo reporta los resultados obtenidos por un grupo de trabajo colaborativo que implementó una arquitectura de seguridad perimetral mediante Endian Firewall Community 3.3.2 desplegado en Oracle VM VirtualBox. La actividad se estructuró en cuatro temáticas interdependientes: configuración de la instancia y segmentación de red en zonas verde, naranja y roja; establecimiento de reglas NAT para la comunicación de la LAN y la DMZ hacia Internet; habilitación de servicios HTTP y FTP en la zona desmilitarizada con denegación selectiva de tráfico ICMP; definición de reglas de acceso interzona para el control del tráfico entre la LAN, la DMZ

y la WAN; e implementación de un proxy HTTP no transparente con autenticación de usuarios y políticas de lista negra. Cada temática fue desarrollada de manera individual y posteriormente consolidada en este documento, con el fin de demostrar que una correcta configuración de firewall, apoyada en la segmentación lógica de redes, constituye una estrategia efectiva para garantizar la confidencialidad, integridad y disponibilidad de los servicios en infraestructuras de red.

2 METODOLOGÍA

El desarrollo de la actividad se apoyó en entornos de virtualización gestionados mediante Oracle VM VirtualBox, ejecutado sobre las estaciones de trabajo personales de cada integrante del grupo. Se dispuso de tres máquinas virtuales independientes que conformaron la topología lógica de la infraestructura: una instancia de Endian Firewall Community 3.3.2 (64-bit) que fungió como firewall UTM y gateway central; una máquina Ubuntu Desktop 22.04 LTS que representó la estación de trabajo de la zona LAN (Green); y una máquina Ubuntu Server 22.04 LTS destinada a albergar los servicios web y de base de datos en la zona DMZ (Orange). La conectividad hacia Internet se simuló mediante el modo NAT de VirtualBox en la interfaz Red del firewall, mientras que las comunicaciones internas se aislaron mediante redes internas (RedLan y RedDMZ) que operan de manera análoga a VLANs de capa 2, sin tráfico broadcast entre sí (Oracle, 2022).

La metodología de trabajo se organizó en cuatro fases secuenciales, cada una asignada a un integrante del grupo. La primera fase abordó la instalación de Endian y la definición del esquema de direccionamiento IP, el cual se publicó en el entorno colaborativo para garantizar la interoperabilidad de las configuraciones posteriores. Las fases siguientes abordaron la configuración de NAT, el filtrado de servicios en DMZ, las reglas de acceso interzona y el proxy HTTP con autenticación. Todas las pruebas de conectividad se ejecutaron mediante comandos de consola (ping, curl, ip addr, traceroute) y se documentaron con capturas de pantalla que registran fecha y hora del sistema.

3 DESARROLLO DE TEMÁTICAS

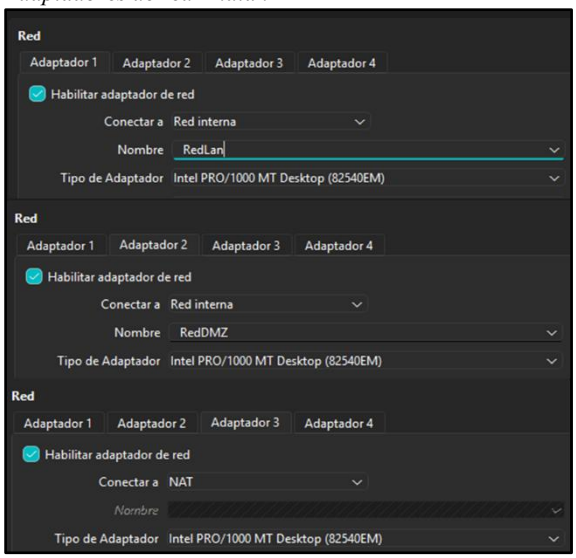
3.1 TEMÁTICA 1: CONFIGURACIÓN DE ENDIAN Y SEGMENTACIÓN DE RED

3.1.1 PREPARACIÓN DEL ENTORNO DE VIRTUALIZACIÓN

La materialización de la seguridad perimetral inició con la preparación del entorno de virtualización sobre el hipervisor Oracle VM VirtualBox. Se procedió a la creación de una nueva máquina virtual denominada Endian-Firewall, para la cual se asignaron 2048 MB de memoria RAM, dos núcleos de procesador y un disco duro virtual de tipo VDI (Virtual Disk Image) con capacidad de 10 GB, configurado con almacenamiento dinámicamente asignado. El tipo de sistema operativo seleccionado fue Linux 2.6 / 3.x / 4.x (64-bit), dado que Endian Firewall Community 3.3.2 se fundamenta en un núcleo Debian GNU/Linux optimizado para servicios de red y seguridad .

El aspecto crítico de esta fase residió en la definición de la topología de red virtual. A diferencia de las configuraciones convencionales donde una máquina virtual utiliza un único adaptador en modo NAT, el despliegue de un firewall UTM exige la separación física de los segmentos de red mediante interfaces independientes. Por tanto, se configuraron tres adaptadores de red: el Adaptador 1 se vinculó a una red interna exclusiva denominada RedLan, que materializa la zona de confianza (Green/LAN); el Adaptador 2 se asoció a una segunda red interna denominada RedDMZ, que representa la zona desmilitarizada (Orange/DMZ); y el Adaptador 3 se dejó en modo NAT, conectado a la interfaz física del equipo anfitrión, simulando así el enlace hacia el proveedor de servicios de Internet (Red/WAN). Esta configuración garantiza que el tráfico entre la LAN y la DMZ no circule directamente, sino que obligatoriamente atraviese el firewall, cumpliendo con el principio de defensa en profundidad [*Fig. 1*].

Figura 1.
Adaptadores de red Endian



Fuente: Autoría Propia

3.1.2 INSTALACIÓN DE ENDIAN FIREWALL COMMUNITY

La imagen ISO de instalación se obtuvo desde el portal oficial de la comunidad Endian (https://www.endian.com/community/downloads/), seleccionando la versión 3.3.2 de 64 bits. El archivo ISO se montó en la unidad óptica virtual de la máquina Endian-Firewall y se inició el proceso de arranque. El instalador de Endian opera en modo consola (texto), lo que exige la configuración manual de parámetros esenciales durante la instalación.

El asistente solicitó, en primera instancia, la definición de la dirección IP para la interfaz de zona verde

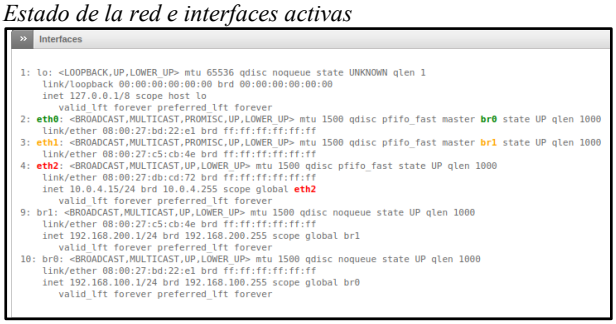
(Green). Se asignó la dirección estática 192.168.100.1 con máscara de subred 255.255.255.0 (/24). Esta decisión se fundamentó en la necesidad de evitar solapamientos con los rangos más comunes utilizados en redes residenciales —como 192.168.0.0/24 o 192.168.1.0/24— que podrían generar conflictos de enrutamiento en el equipo anfitrión. Posteriormente, el instalador requirió la configuración de la zona roja (Red/WAN), la cual se dejó en modo DHCP para que VirtualBox asignara automáticamente una dirección en el segmento 10.0.x.x. Finalmente, se configuró la zona naranja (Orange/DMZ) con la dirección estática 192.168.200.1/24, estableciendo así el gateway para los servidores de aplicaciones. Tras confirmar el formateo del disco virtual /dev/sda, el sistema procedió a la instalación de los paquetes base, servicios de red y módulos de seguridad, finalizando con un mensaje de confirmación que indicó la URL de acceso al panel web: https://192.168.100.1:10443.

3.1.3 CONFIGURACIÓN INICIAL MEDIANTE EL ASISTENTE WEB

Una vez finalizada la instalación y retirada la imagen ISO del almacenamiento virtual, se reinició la máquina Endian y se accedió al panel de administración desde la estación de trabajo Ubuntu Desktop (Scope), previamente ubicada en el segmento RedLan. El acceso se realizó mediante el protocolo HTTPS sobre el puerto no estándar 10443, aceptando el certificado de seguridad autofirmado que el sistema genera por defecto. El wizard de primer inicio solicitó la definición del idioma del sistema, la zona horaria y las contraseñas de los usuarios administrativos admin (panel web) y root (acceso SSH).

En el paso de configuración de red, el asistente detectó las tres interfaces previamente definidas en VirtualBox. Se verificó que el modo de red estaba establecido como Enrutamiento, lo cual permite que Endian opere como gateway entre los diferentes segmentos. Se seleccionó la zona naranja (Orange) como segmento adicional activo, descartando la zona azul (WiFi) dado que la actividad no contemplaba dispositivos inalámbricos. En la asignación de interfaces, se corroboró que eth0 correspondía a la zona Green (192.168.100.1/24), eth1 a la zona Orange (192.168.200.1/24) y eth2 a la zona Red mediante DHCP automático. El sistema internamente elevó las interfaces eth0 y eth1 a bridges de capa 2 (br0 y br1 respectivamente), permitiendo la gestión flexible de las zonas sin afectar la nomenclatura física de los adaptadores [*Fig. 2*].

Figura 2.
Estado de la red e interfaces activas



Fuente: Autoría Propia

3.1.4 DEFINICIÓN Y PUBLICACIÓN DEL ESQUEMA DE DIRECCIONAMIENTO

Como responsable de la Temática 1, se asumió la tarea de definir el esquema de direccionamiento IP que serviría de referencia obligatoria para los demás integrantes del grupo. La guía establece que las direcciones definidas de la instalación base, serán las mismas que deberán utilizar los demás participantes en el desarrollo de las siguientes temáticas, por lo que la coherencia y la documentación oportuna de este esquema resultaron críticas para evitar conflictos de conectividad en las fases posteriores (Oracle, 2022).

La *Tabla 1* presenta el esquema definitivo acordado y publicado en el foro del curso. Se optó por subredes clase C privadas (192.168.100.0/24 y 192.168.200.0/24) por su amplia documentación, facilidad de memorización y compatibilidad con las herramientas de virtualización. La zona Red se mantuvo en DHCP automático gestionado por VirtualBox, eliminando la necesidad de configuración manual del proveedor de Internet.

Tabla 1.
Esquema de direccionamiento IP de la infraestructura

Zona	Subred	Gateway	Dirección IP	Máscara
Green (LAN)	192.168.100.0/24	192.168.100.1	192.168.100.10	255.255.255.0
Orange (DMZ)	192.168.200.0/24	192.168.200.1	192.168.200.10	255.255.255.0
Red (WAN)	DHCP automático	Asignado por NAT	-	-

Fuente: Autoría Propia

3.1.5 CONFIGURACIÓN DE LOS NODOS DE RED

La estación de trabajo Ubuntu Desktop (Scope) se configuró con un único adaptador de red conectado a la red interna RedLan. Inicialmente, el sistema adquirió una dirección dinámica (192.168.100.2) mediante el servicio DHCP que Endian habilita por defecto en la zona Green. Sin embargo, para garantizar la estabilidad de las pruebas y la coherencia con el esquema publicado, se procedió a la configuración de una dirección IP estática persistente. Se editó el archivo /etc/netplan/00-installer-config.yaml mediante el editor de texto nano, definiendo la interfaz enp0s3 con dirección 192.168.100.10/24, gateway 192.168.100.1 y servidor DNS 8.8.8.8, desactivando explícitamente el cliente DHCP (dhcp4: no). Se identificó que existían archivos conflictivos (01 network manager all.yaml y 50 cloud init yaml) que forzaban asignaciones dinámicas secundarias; estos se trasladaron a un directorio de respaldo y se aplicó la configuración mediante sudo netplan apply y reinicio del servicio NetworkManager.

De forma análoga, el servidor Ubuntu destinado a la DMZ se configuró con un único adaptador en la red interna RedDMZ, eliminando cualquier conexión NAT previa que pudiera permitirle salir a Internet sin atravesar el firewall. Se aplicó la misma metodología de configuración persistente mediante Netplan, asignando la dirección 192.168.200.10/24, gateway 192.168.200.1 y DNS 8.8.8.8.

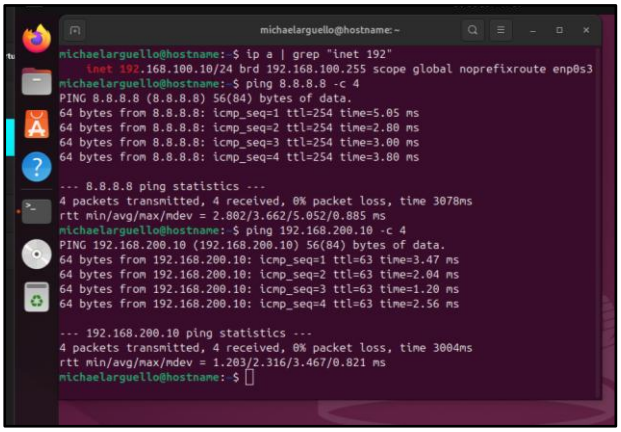
La verificación mediante el comando ip addr confirmó que ambos nodos mantenían sus direcciones estáticas tras reinicios del sistema, lo cual resulta indispensable para la continuidad de los servicios que se configurarán en las temáticas posteriores.

3.1.6 VERIFICACIÓN DE CONECTIVIDAD Y ANÁLISIS DE SEGMENTACIÓN

Se ejecutó una batería de pruebas de conectividad mediante el protocolo ICMP (comando ping) con el propósito de validar la integridad física y lógica de la segmentación. Desde la consola del firewall (acceso Shell, opción 0 del menú de administración), se verificó el alcance hacia el nodo Scope (192.168.100.10) y hacia el servidor (192.168.200.10), obteniendo respuesta exitosa en ambos casos con tiempos de latencia inferiores a 2 ms, lo que confirmó que Endian opera correctamente como gateway de ambos segmentos.

Desde la estación Scope, se ejecutó ping 192.168.100.1 para validar la comunicación con el gateway de la LAN, ping 192.168.200.10 para verificar la conectividad interzona (LAN hacia DMZ), y ping 8.8.8.8 para comprobar la salida a Internet. Los tres casos arrojaron respuesta positiva, evidenciando que Endian, en su configuración por defecto, ya establece el ruteo entre zonas internas y aplica NAT automático desde los segmentos Green y Orange hacia la zona Red. Desde el servidor en DMZ se replicaron las pruebas hacia su gateway (192.168.200.1) y hacia Internet (8.8.8.8), con resultados igualmente satisfactorios [*Fig. 3*].

Figura 3.
Conectividad interzona



Fuente: Autoría Propia

Resultó particularmente relevante constatar que, aunque la comunicación ICMP entre LAN y DMZ funcionaba, esto no implicaba que todos los protocolos estuvieran abiertos por defecto. El firewall Endian aplica una política de denegación implícita (default deny) para servicios de capa superior no autorizados, lo cual significa que, si bien los paquetes de eco ICMP son respondidos, cualquier intento de acceso HTTP, FTP o SSH entre zonas, requerirá la creación explícita de reglas de acceso. Este comportamiento fue documentado como observación técnica, dado que constituye la base sobre la cual se desarrollarán las reglas de filtrado específicas en las temáticas siguientes.

3.1.7 SINCRONIZACIÓN GRUPAL Y ENTREGA DE LA INFRAESTRUCTURA BASE

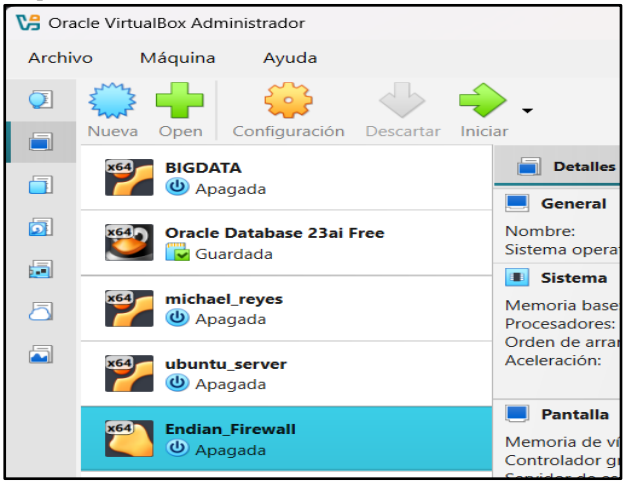
La última fase de la Temática 1 consistió en la publicación formal del esquema de direccionamiento y la confirmación de la operatividad de la red. Se elaboró un mensaje estructurado que incluía la tabla de direccionamiento, la configuración de adaptadores en VirtualBox para cada máquina, las credenciales de acceso al dashboard de Endian y las instrucciones de verificación inicial (ping 192.168.100.1). Esta comunicación permitió que los responsables de las temáticas siguientes iniciaran sus configuraciones sobre una infraestructura estable y estandarizada, evitando retrabajos por inconsistencias en los segmentos de red. Se confirmó, mediante pruebas finales ejecutadas tras reinicios simultáneos de las tres máquinas virtuales, que la asignación de IPs persistentes y la conectividad entre zonas se mantenían invariantes, cerrando así el ciclo de implementación de la infraestructura base de seguridad perimetral.

3.2 TEMÁTICA 2: CONFIGURACIÓN NAT

En el desarrollo de la presente práctica se implementó un entorno virtualizado orientado a la administración y segmentación de redes mediante el uso del firewall Endian. La actividad consistió en la configuración de las zonas GREEN, ORANGE y RED, permitiendo establecer comunicación controlada entre una red local, una DMZ y la red externa. Adicionalmente, se aplicaron reglas de NAT y port forwarding para gestionar el tráfico de red y habilitar el acceso a servicios alojados en la zona desmilitarizada. Como evidencia de funcionamiento, se implementó un servicio web básico en un servidor Ubuntu ubicado en la DMZ, validando la conectividad y el control de acceso entre las diferentes zonas configuradas. Los resultados obtenidos permitieron comprender la importancia de la segmentación de redes y el uso de firewalls en entornos de seguridad informática.

La seguridad en redes es un aspecto fundamental en la protección de la información y en el control del tráfico dentro de las infraestructuras tecnológicas. En este trabajo se desarrolló un entorno virtualizado utilizando Endian Firewall y máquinas virtuales Ubuntu, con el propósito de implementar una arquitectura segmentada compuesta por las zonas GREEN, ORANGE y RED. A través de la configuración de reglas de firewall, NAT y redireccionamiento de puertos, se logró establecer una comunicación controlada entre las diferentes redes, simulando un escenario real de seguridad perimetral y acceso a servicios en una DMZ.

Figura 4.
Máquinas Virtuales



Fuente: Autoría Propia

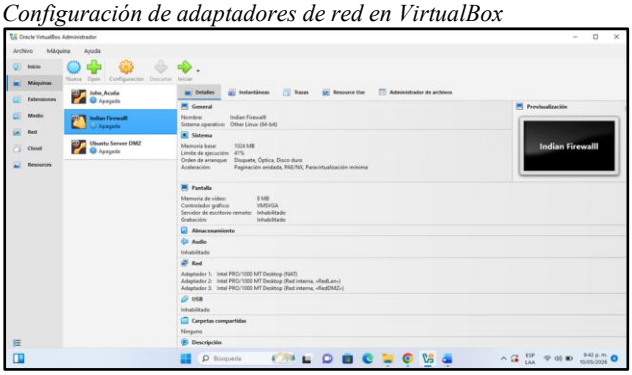
Se implementó un entorno virtualizado utilizando Endian Firewall y sistemas Ubuntu para segmentar redes y controlar el tráfico mediante reglas NAT y acceso a una DMZ."

3.2.1 CONFIGURACIÓN DEL ENTORNO VIRTUAL

Inicialmente se crearon las máquinas virtuales necesarias para el desarrollo de la práctica, utilizando VirtualBox como plataforma de virtualización. Se implementaron tres máquinas virtuales correspondientes a Endian Firewall, Ubuntu Desktop y Ubuntu Server.
Posteriormente se configuraron los adaptadores de red para representar las diferentes zonas de red utilizadas por el firewall:

- GREEN: red interna LAN
- ORANGE: zona DMZ.
- RED: salida hacia Internet.

Figura 5.
Configuración de adaptadores de red en VirtualBox



Fuente: Autoría Propia

La máquina Endian fue configurada con múltiples interfaces de red para permitir la comunicación entre las diferentes zonas.

3.2.2 CONFIGURACIÓN DEL FIREWALL ENDIAN

Después de instalar Endian Firewall, se accedió a la interfaz web de administración para realizar la configuración de las interfaces de red y asignar las direcciones IP correspondientes a cada zona.
La configuración implementada fue la siguiente:

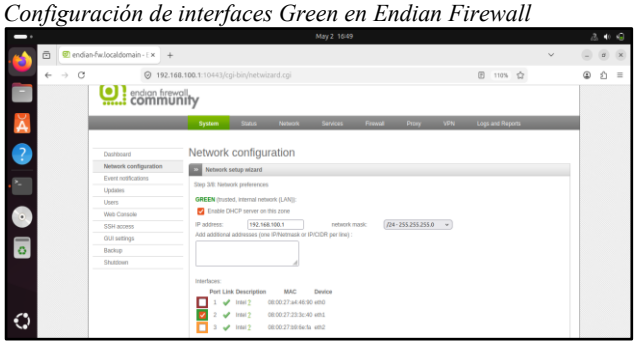
Tabla 2
Configuración de interfaces en Endian Firewall.

Zona	Dirección Ip
Green	192.168.100.1
Orange	192.168.300.1
Red	10.0.2.15

Fuente: Autoría Propia

La zona GREEN fue utilizada para la red interna de usuarios y la zona ORANGE para alojar el servidor DMZ y la zona RED como interfaz de salida hacia Internet

Figura 6.
Configuración de interfaces Green en Endian Firewall



Fuente: Autoría Propia

La interfaz GREEN fue configurada como la red interna LAN, utilizada para conectar los equipos de usuarios internos. Esta zona permitió la comunicación segura dentro de la red local y el acceso controlado hacia Internet mediante el firewall Endian.

Figura 7.
Configuración de interfaces Orange en Endian Firewall

Fuente: Autoría Propia

La interfaz ORANGE fue configurada como la zona DMZ, destinada a alojar el servidor Ubuntu donde se implementó el servicio web. Esta red funciona como una zona intermedia de seguridad para aislar servicios y evitar el acceso directo a la red interna.

Figura 8.
Configuración de interfaces

Fuente: Autoría Propia

La interfaz RED fue configurada como la conexión hacia Internet o red externa. Esta interfaz permite la salida del tráfico desde las redes internas hacia Internet mediante las reglas NAT configuradas en el firewall Endian.

3.2.3 CONFIGURACIÓN DEL SERVIDOR UBUNTU EN LA DMZ

La configuración fue realizada editando el archivo YAML de Netplan con los siguientes parámetros:

Figura 9.
Configuración YAML del servidor Ubuntu Server

Fuente: Autoría Propia

Para la implementación de la DMZ se utilizó un servidor Ubuntu Server configurado manualmente mediante Netplan. Se asignó una dirección IP estática perteneciente a la red ORANGE para permitir la comunicación con el firewall.

3.2.4 CONFIGURACIÓN DE REGLAS NAT

Con el objetivo de permitir la salida hacia Internet desde las redes internas, se configuraron reglas Source NAT en Endian Firewall, asímismo las reglas implementadas permitieron que las redes GREEN y ORANGE pudieran acceder a Internet utilizando la interfaz RED del firewall. Este proceso permitió traducir las direcciones IP privadas internas para habilitar la comunicación externa.

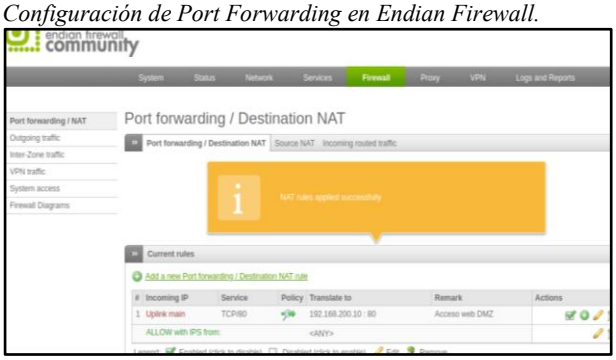
Figura 10.
Configuración de reglas Source NAT en Endian Firewall.

Fuente: Autoría Propia

3.2.5 CONFIGURACIÓN DE PORT FORWARDING

Posteriormente se configuró una regla de port forwarding para permitir el acceso al servicio web alojado en el servidor ubicado en la DMZ, así mismo y se creo una regla de port forwarding para permitir el acceso al servicio web alojado en el servidor ubicado en la DMZ. Esta configuración permitió redireccionar las solicitudes recibidas hacia el servidor Ubuntu Server configurado con dirección IP 192.168.200.10.

Figura 11.
Configuración de Port Forwarding en Endian Firewall.



Fuente: Autoría Propia

3.2.6 IMPLEMENTACIÓN DEL SERVICIO WEB

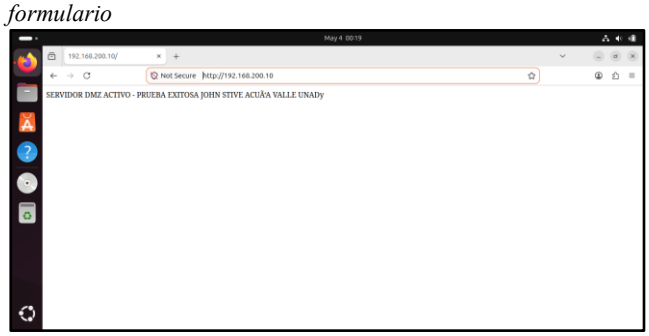
Con el propósito de validar el funcionamiento de la DMZ, se implementó un servicio web básico utilizando Python en el servidor Ubuntu Server.
El servicio fue iniciado mediante el siguiente comando *python3 -m http.server 80.* Este comando permitió habilitar temporalmente un servidor HTTP sobre el puerto 80 para comprobar el acceso desde otras zonas de red.

Figura 12.

Ejecución del servicio web mediante Python HTTP Server.

Fuente: Autoría Propia

Figura 13.
Ejecución del servicio web modificando los datos del formulario

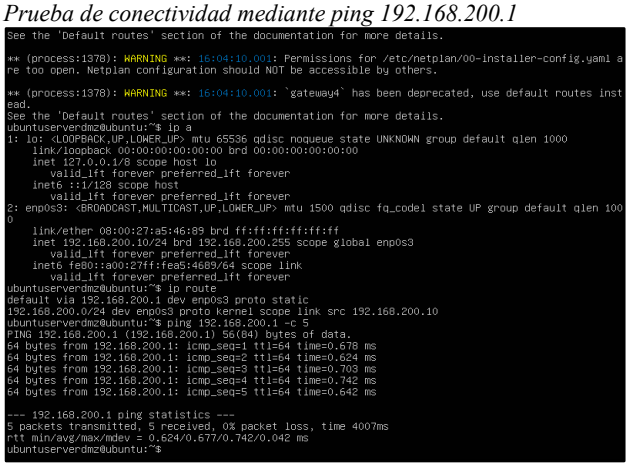


Fuente: Autoría Propia

3.2.7 PRUEBAS DE CONECTIVIDAD Y FUNCIONAMIENTO

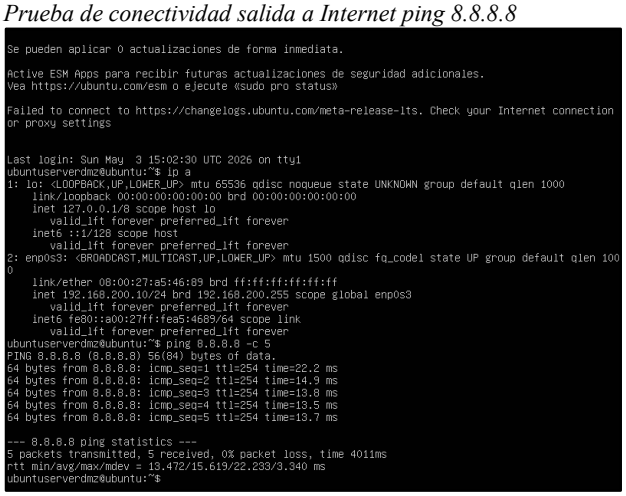
Una vez configurado el entorno, se realizaron pruebas de conectividad entre las diferentes zonas de red para verificar el correcto funcionamiento del firewall y las reglas implementadas, inicialmente se comprobó la comunicación entre el servidor de la DMZ y el firewall utilizando el comando ping 192.168.200.1 y posteriormente se validó la salida hacia Internet mediante ping 8.8.8.8, finalmente, desde la máquina Ubuntu Desktop se accedió al servicio web implementado en la DMZ utilizando la siguiente dirección http://192.168.200.10

Figura 14.
Prueba de conectividad mediante ping 192.168.200.1



Fuente: Autoría Propia

Figura 15.
Prueba de conectividad salida a Internet ping 8.8.8.8



Fuente: Autoría Propia

Las pruebas realizadas permitieron verificar la conectividad entre redes y el correcto funcionamiento de las reglas NAT y port forwarding configuradas en Endian Firewall.

3.2.8 VALIDACIÓN DEL FUNCIONAMIENTO DEL ENTORNO

Durante el desarrollo de la práctica se logró implementar correctamente un entorno de red segmentado utilizando Endian Firewall. Las configuraciones realizadas permitieron establecer comunicación entre las diferentes zonas de red y habilitar acceso controlado a un servicio ubicado en la DMZ.

Asimismo, se comprobó el funcionamiento de las reglas NAT para la salida hacia Internet y la correcta operación del servicio web implementado en el servidor Ubuntu Server.

3.3 TEMÁTICA 3: PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED.

La implementación desarrollada en esta temática tiene como propósito demostrar, de manera práctica, cómo funciona una arquitectura segmentada —basada en el diseño trabajado en la temática 1— utilizando Endian Firewall Community 3.3.2 como punto central de control **[1]**. Para este escenario se configuraron dos redes internas: GREEN, donde opera una máquina tipo desktop que actúa como cliente interno, y ORANGE (DMZ), destinada a alojar servicios públicos como HTTP y FTP en un servidor Ubuntu 26.04.

El objetivo principal es evidenciar cómo el firewall administra y regula el tráfico entre ambas redes, aplicando reglas explícitas de control que permiten únicamente los servicios autorizados **[2]** y bloquean cualquier comunicación no contemplada. De esta manera se simula un entorno real donde la DMZ queda expuesta para servicios públicos, pero siempre bajo supervisión del firewall.

Esta sección documenta el proceso completo: diseño de la arquitectura, configuración de cada componente, ejecución de pruebas, validación del comportamiento del firewall y análisis de los resultados obtenidos, destacando los elementos clave que permiten mantener separadas las redes y asegurar que cada zona funcione de manera controlada y protegida. (Oracle, 2022)

3.3.1 ARQUITECTURA DE RED

La arquitectura *Tabla 3* se compone de tres máquinas virtuales interconectadas a través de VirtualBox, donde Endian actúa como puente de control entre las redes internas y la DMZ.

Tabla 3
Estructura firewall (Wan, Lan, DMZ)

Componente	Rol	Red	Dirección IP
Endian Firewall	Gateway / Controlador	GREEN	192.168.100.1
Endian Firewall	Gateway / Controlador	ORANGE	192.168.200.1
Cliente Desktop	Usuario interno	GREEN	192.168.100.2
Servidor DMZ	Servicios HTTP/FTP	ORANGE	192.168.200.2

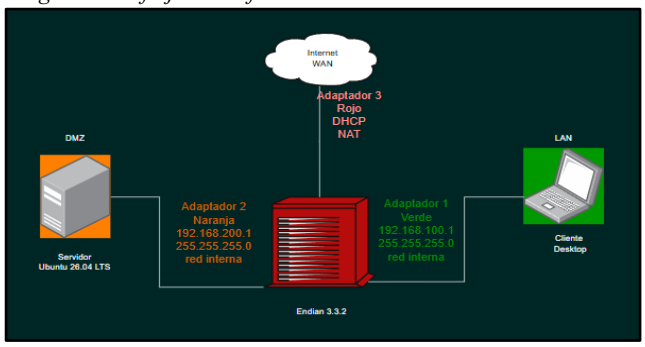
Fuente: Autoría Propia

La asignación de direcciones sigue un principio fundamental:
las IP terminadas en .1 se reservan para el firewall [5], ya que actúa como gateway en cada red. Los hosts principales utilizan la terminación .2, lo que simplifica la administración y evita conflictos.

3.3.2 DIAGRAMA FLUJO DE COMUNICACIÓN CÓDIGO

Este diagrama *[Fig 16]* resume el flujo básico: el cliente solicita acceso para algunos de los servicios HTTP, FTP o ICMP **[6]**, Endian evalúa las reglas, y solo si están permitidas, el tráfico llega al servidor, a su vez el server puede solicitar la validación y comunicación por ICMP.

Figura 16.
Diagrama de flujo de trafico

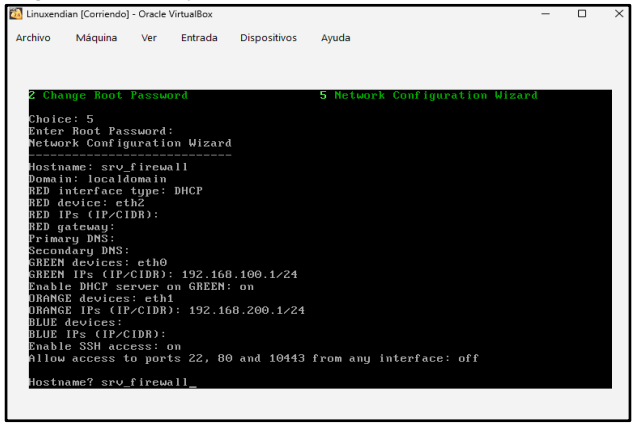


Fuente: Autoría Propia

3.3.3 IMPLEMENTACIÓN TÉCNICA

En esta etapa, Endian [Fig 17] queda configurado como el punto obligatorio de paso entre GREEN y la DMZ **[1]**, con reglas claras que habilitan únicamente HTTP, FTP e ICMP para validación. Su función es filtrar, permitir o bloquear el tráfico según lo definido, y esa lógica es la que demuestra cómo cada servicio del servidor en ORANGE solo funciona cuando Endian lo autoriza. Todo el proceso gira alrededor de cómo el firewall controla y ordena la comunicación entre redes.

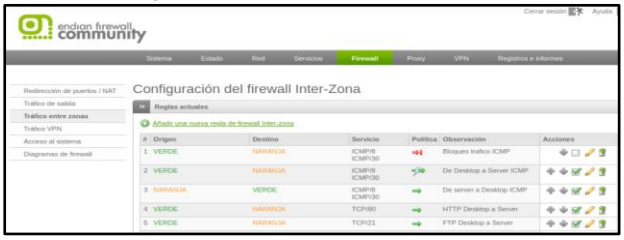
Figura 17.
Asignación de interfaces



Fuente: Autoría Propia

Como evidenciamos en *[Fig 18]*, estas reglas representan el núcleo del proyecto: solo se permite lo estrictamente necesario, manteniendo el resto del tráfico bloqueado.

Figura 18.
Creación de Reglas



Fuente: Autoría Propia

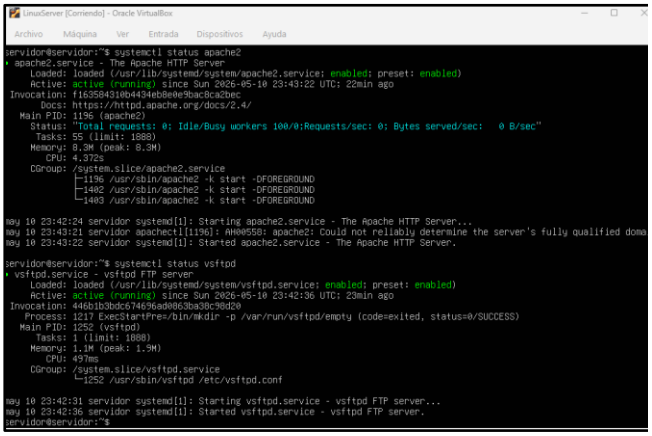
3.3.4 CONFIGURACIÓN DEL SERVIDOR DMZ

La máquina ubicada en la red ORANGE cumple el rol de servidor dentro de la DMZ. Su función principal es ofrecer servicios accesibles desde la red GREEN bajo el control del firewall. Para este proyecto se utilizó un servidor Ubuntu Server 26.04 **[7]**, configurado con la dirección IP 192.168.200.2, la cual se mantiene fija para garantizar estabilidad en las pruebas y coherencia con las reglas del firewall.

El servidor quedó preparado para responder solicitudes HTTP, FTP y ICMP provenientes de la red GREEN, siempre y cuando el firewall lo permitiera. Esta configuración permitió validar el comportamiento del tráfico web dentro de la DMZ (Oracle, 2022) y comprobar cómo Endian controla el acceso a este servicio.

La configuración del servidor en la *[Fig 19]* en esta zona no solo permite ofrecer servicios, sino que también cumple un papel clave en la simulación de un entorno real. La DMZ actúa como una zona intermedia **[8]** donde se alojan servicios que deben ser accesibles desde redes internas o externas, pero sin exponer directamente la red principal.

Figura 19.
Servicios activos en el servidor DMZ



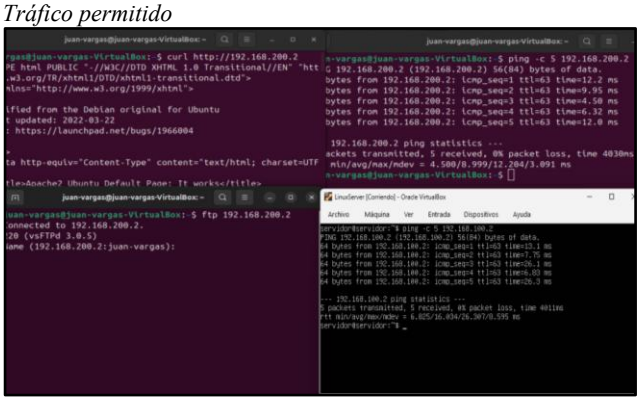
Fuente: Autoría Propia

Ambos servicios quedan escuchando en la IP 192.168.200.2, listos para ser consumidos desde la red GREEN.

3.3.5 EJECUTANDO LA IMPLEMENTACIÓN

En esta etapa se ejecutan las cuatro validaciones en la Fig 20 y Fig 21 que permiten comprobar cómo Endian controla el tráfico entre GREEN y la DMZ (Endian, 2024). El proceso se divide en dos fases: primero se realizan todas las pruebas con el firewall sin reglas, donde el tráfico debe ser completamente bloqueado; luego se habilitan las reglas específicas y se repiten exactamente las mismas validaciones para demostrar el cambio de comportamiento.

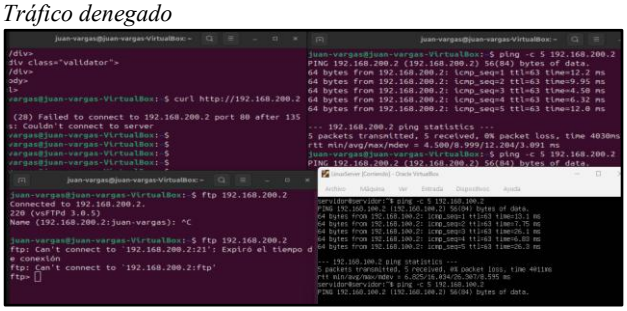
Figura 20.
Tráfico permitido



Fuente: Autoría Propia

Las pruebas incluyen tres verificaciones desde el cliente hacia el servidor **[6]** (ICMP, HTTP y FTP) y una validación adicional desde el servidor hacia el cliente, donde se comprueba exclusivamente el tráfico ICMP de retorno, ya que es la única regla configurada en sentido inverso. Esta ejecución comparativa es la que evidencia, de forma práctica, cómo Endian decide qué pasa y qué no dentro de la arquitectura, controlando ambos sentidos de comunicación según las reglas definidas.

Figura 21.
Tráfico denegado



Fuente: Autoría Propia

3.3.6 ANALIZANDO LA IMPLEMENTACIÓN

La implementación permitió comprobar que Endian cumple su función como firewall de capa de red (Endian, s. f.), bloqueando todo tráfico no autorizado y permitiendo únicamente los servicios definidos en las reglas. ICMP

sirvió como herramienta de diagnóstico para validar la conectividad y el comportamiento del firewall, mientras que la DMZ quedó correctamente aislada [8], evitando accesos directos desde el cliente sin pasar por el control de Endian. En conjunto, la arquitectura replicó un entorno real y dejó claro cómo cada servicio depende de las políticas aplicadas. Con esta base ya validada y operativa, queda todo preparado para continuar con las siguientes temáticas.

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

La segmentación de red establecida en la Temática 1 y la configuración de NAT desarrollada en la Temática 2 constituyen la infraestructura física y lógica sobre la cual se materializan las políticas de seguridad. Sin embargo, la mera separación en zonas no garantiza el control del tráfico: es necesario definir reglas explícitas que determinen qué protocolos, puertos y direcciones pueden comunicarse entre los segmentos. Endian Firewall Community implementa una política de denegación implícita (default deny) para el tráfico interzona, lo que significa que cualquier paquete que no coincida con una regla de permiso específica será descartado [7].

Como se evidenció en la sección 3.1.6, la conectividad ICMP entre zonas internas opera por defecto en la configuración inicial de Endian, pero los servicios de capa superior —HTTP, FTP, SSH— requieren la creación manual de reglas de acceso. Esta temática aborda la configuración de reglas que permiten la comunicación selectiva entre la zona LAN (Green), la DMZ (Orange) y la WAN (Red), habilitando los servicios HTTP y FTP en la DMZ, bloqueando selectivamente el protocolo ICMP entre zonas internas, y verificando la operatividad de las reglas NAT para acceso externo. El objetivo es demostrar que el firewall opera como árbitro del tráfico, aplicando el principio de mínimo privilegio y garantizando que solo las comunicaciones autorizadas transcurren entre los segmentos de red.

3.4.1 FUNDAMENTOS DE LAS REGLAS INTERZONA EN ENDIAN FIREWALL

Endian Firewall Community organiza el control de tráfico en dos categorías principales: el tráfico de salida (Outgoing), que regula la comunicación desde una zona hacia Internet o hacia otras zonas, y el tráfico interzona (Interzona), que controla específicamente el paso de paquetes entre dos segmentos definidos. La evaluación de las reglas sigue un orden secuencial descendente (top-down): el sistema compara cada paquete contra las reglas en el orden en que aparecen en la lista, y ejecuta la acción de la primera coincidencia, sin evaluar las reglas posteriores.

Esta característica hace crítica la posición relativa de las reglas. Una regla de permiso ubicada antes de una regla de denegación para el mismo tráfico prevalecerá, mientras que el orden inverso bloqueará la comunicación. Por esta razón, las reglas más específicas deben posicionarse antes que las reglas generales, y las reglas de denegación explícita deben colocarse estratégicamente para no interferir con el tráfico legítimo.

La interfaz web de administración presenta las reglas interzona mediante matrices que cruzan cada zona de origen con cada zona de destino. Para la arquitectura implementada en esta actividad, las combinaciones relevantes son Green → Orange (LAN hacia DMZ), Green → Red (LAN hacia WAN), Orange → Red (DMZ hacia WAN) y Red → Orange (WAN hacia DMZ). Cada celda de esta matriz permite definir múltiples reglas con granularidad hasta el nivel de dirección IP individual, subred completa o servicio específico.

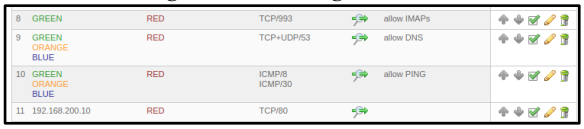
3.4.2 CONFIGURACIÓN DE REGLAS LAN → DMZ (HTTP Y FTP)

La primera fase de configuración abordó la habilitación de la comunicación desde la estación de trabajo Ubuntu Desktop (zona Green, 192.168.100.10) hacia el servidor Ubuntu Server (zona Orange, 192.168.200.10). El acceso al panel de administración se realizó mediante navegador web desde la máquina Scope, ingresando la URL https://192.168.100.1:10443 y autenticándose con las credenciales establecidas durante la instalación.

Inicialmente, se creó una regla de prueba con servicio ANY que permitía todo el tráfico desde Green hacia Orange. Esta regla, aunque funcional para verificar la conectividad básica, contraviene los principios de seguridad por mínimo privilegio, pues expone la DMZ ante cualquier protocolo originado en la LAN. Por tanto, se procedió a su eliminación y se sustituyó por reglas específicas para los servicios requeridos.

La configuración de la regla HTTP se estableció mediante los siguientes parámetros: origen Green, dirección de origen Cualquiera, destino Orange, dirección de destino 192.168.200.10, servicio HTTP (puerto 80 TCP), acción Permitir, y registro activado. De forma análoga, la regla FTP se configuró con los mismos parámetros de origen y destino, seleccionando el servicio FTP (puerto 21 TCP). Ambas reglas se posicionaron en la parte superior de la lista de reglas Green → Orange para garantizar su evaluación prioritaria [Fig. 22].

Figura 22.
Panel Endian: reglas Green-Orange



Fuente: Autoría Propia

Panel de reglas interzona Green → Orange en Endian Firewall. Se observan las reglas específicas para HTTP (puerto 80) y FTP (puerto 21) hacia el servidor DMZ.

La verificación de la regla HTTP se ejecutó desde el navegador Firefox de la máquina Scope, ingresando la dirección http://192.168.200.10. El servidor Apache2 instalado en la DMZ respondió con la página por defecto "It

works!", confirmando que el tráfico HTTP atravesaba el firewall y alcanzaba el servicio web Fig. 23.

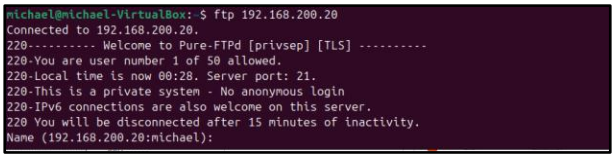
Figura 23
Navegador mostrando Apache

Fuente: Autoría Propia

Navegador Firefox en Ubuntu Desktop (192.168.100.10) mostrando la página por defecto de Apache2 al acceder a http://192.168.200.10.

Para la verificación del servicio FTP, se abrió una terminal en la máquina Scope y se ejecutó el comando ftp 192.168.200.10. El sistema solicitó credenciales de usuario; tras ingresar un usuario local válido del servidor Ubuntu Server, se estableció la sesión y se ejecutó el comando ls para listar el contenido del directorio home del usuario. El listado se completó exitosamente, evidenciando que la regla FTP permitía tanto el canal de control (puerto 21) como la negociación del canal de datos [Fig. 24].

Figura 24.
Terminal con sesión FTP



Fuente: Autoría Propia

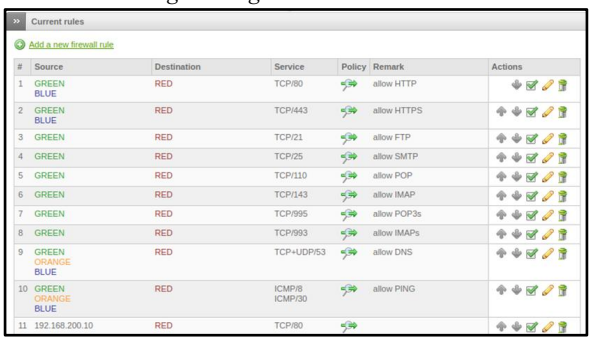
Terminal en Ubuntu Desktop mostrando sesión FTP exitosa hacia 192.168.200.10, con autenticación y listado de directorio.

3.4.3 DENEGACIÓN SELECTIVA DEL PROTOCOLO ICMP

El requerimiento de bloqueo del protocolo ICMP entre zonas internas implicó la creación de una regla de denegación explícita. Aunque, como se documentó en 3.1.6, Endian permite por defecto el tráfico ICMP entre Green y Orange para facilitar el diagnóstico inicial, la política de seguridad de la actividad exigía la inhibición del comando ping como mecanismo de reconocimiento de red.

Se accedió nuevamente a la matriz Interzona Green → Orange y se creó una regla con los siguientes parámetros: origen Green, destino Orange, servicio ICMP (tipos 8 Echo Request y 30 Traceroute), acción Denegar. La regla se posicionó inmediatamente después de las reglas HTTP y FTP, garantizando que el tráfico de estos servicios no fuera afectado. La política de denegación implícita al final de la lista se mantiene como respaldo, pero la regla explícita permite el registro auditable de los intentos de ICMP bloqueados [Fig. 25].

Figura 25.
Panel Endian: regla denegar ICMP

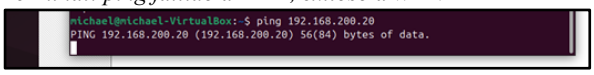


Fuente: Autoría Propia

Regla de denegación ICMP en la matriz Green → Orange. La acción "Denegar" se aplica a los tipos ICMP 8 y 30, posicionada después de las reglas de permiso HTTP y FTP.

La verificación se ejecutó mediante el comando ping 192.168.200.10 desde la terminal de la máquina Scope. El sistema respondió con el mensaje "Destination port unreachable" tras el timeout, indicando que el firewall descartó los paquetes ICMP sin generar respuesta al emisor. Como control positivo, se ejecutó simultáneamente ping 8.8.8.8 hacia Internet, el cual respondió correctamente, confirmando que la denegación afecta exclusivamente al tráfico interzona y no a la salida hacia la WAN [Fig. 26].

Figura 26.
Terminal: ping fallido a DMZ, exitoso a WAN



Fuente: Autoría Propia

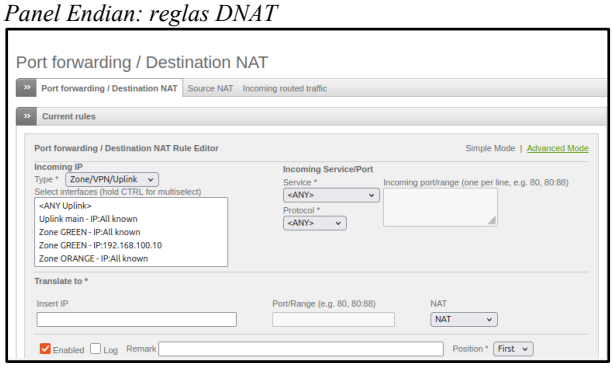
Terminal mostrando bloqueo de ping hacia DMZ (192.168.200.10) y respuesta exitosa hacia WAN (8.8.8.8), evidenciando la selectividad de la regla ICMP.

3.4.4 CONFIGURACIÓN DE ACCESO WAN → DMZ MEDIANTE NAT Y PORT FORWARDING

La publicación de servicios desde la DMZ hacia la red externa requirió la implementación de traducción de direcciones de destino (Destination NAT o Port Forwarding). Dado que la zona Orange utiliza direccionamiento privado (192.168.200.0/24), los equipos en la WAN no pueden direccionar directamente al servidor DMZ; en su lugar, deben dirigirse a la interfaz pública del

firewall (zona Red, asignada por DHCP en el segmento 10.0.x.x de VirtualBox), la cual redirige el tráfico al nodo interno mediante reglas DNAT.
Se accedió a la sección Firewall → Port Forwarding / NAT y se creó una regla de reenvío para el servicio HTTP: protocolo TCP, origen Red, puerto origen 80, destino Orange, dirección destino 192.168.200.10, puerto destino 80, IP traducida 192.168.200.10, puerto traducido 80. De forma similar, se estableció la regla para FTP: protocolo TCP, origen Red, puerto origen 21, destino Orange, dirección destino 192.168.200.10, puerto destino 21 como se evidencia en la Fig. 27.

Figura 27.
Panel Endian: reglas DNAT



Fuente: Autoría Propia

Configuración de Port Forwarding en Endian Firewall. Reglas DNAT para HTTP (puerto 80) y FTP (puerto 21) desde la zona Red hacia el servidor DMZ.

La regla de firewall asociada se configuró en la matriz Interzona Red → Orange, permitiendo el servicio FTP desde cualquier origen hacia 192.168.200.10. Para el modo pasivo de FTP, que requiere canales de datos adicionales, se editó el archivo /etc/vsftpd.conf en el servidor Ubuntu Server, estableciendo los parámetros pasv_enable=YES, pasv_min_port=40000, pasv_max_port=50000, y pasv_address=192.168.200.10. Se reinició el servicio vsftpd mediante systemctl restart vsftpd y se verificó su estado [Fig. 28].

Figura 28.
Terminal: nano /etc/vsftpd.conf

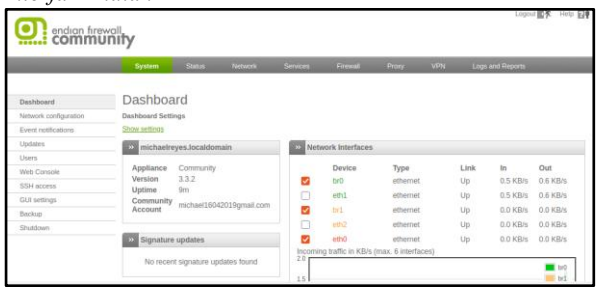
Fuente: Autoría Propia

Configuración del archivo /etc/vsftpd.conf en Ubuntu Server, mostrando parámetros para modo pasivo (puertos 40000-50000) y dirección de escucha.

3.4.5 VERIFICACIÓN DE CONECTIVIDAD WAN → DMZ

Las pruebas de acceso desde la zona WAN se ejecutaron desde la máquina anfitriona del hipervisor VirtualBox, la cual comparte la interfaz NAT con la zona Red del firewall. Para el servicio HTTP, se abrió un navegador e ingresó la dirección IP asignada por DHCP a la interfaz Red de Endian (10.0.2.15 en la configuración de prueba). El firewall redirigió la petición al servidor DMZ, respondiendo con la página por defecto de Apache2 como se evidencia en la Fig. 29.

Figura 29.
Interfaz Endian

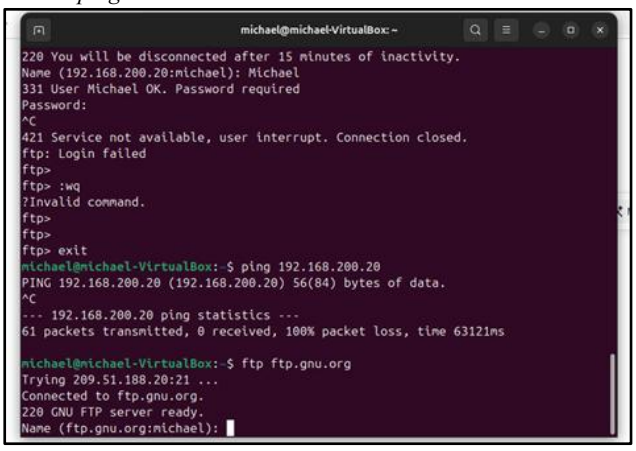


Fuente: Autoría Propia

Navegador desde máquina anfitriona accediendo vía NAT al servicio HTTP publicado en la DMZ. La URL corresponde a la IP de la interfaz Red de Endian.

Para la verificación del servicio FTP desde WAN, se utilizó el cliente de línea de comandos ftp desde una terminal externa, conectando a la IP de la zona Red. Tras la autenticación, se ejecutaron comandos de listado y transferencia de archivos de prueba, confirmando que tanto el canal de control (puerto 21) como los canales de datos pasivos (puertos 40000-50000) operaban correctamente a través del mecanismo DNAT como se evidencia en la Fig. 30.

Figura 30.
Prueba ping a Internet



Fuente: Autoría Propia

Sesión FTP establecida desde máquina externa (WAN) hacia la IP pública de Endian, con listado de directorios en el servidor DMZ mediante modo pasivo.

3.4.6 MATRIZ DE PRUEBAS DE CONECTIVIDAD

Con el fin de consolidar la verificación de todas las políticas configuradas, se diseñó una matriz de pruebas que abarca las combinaciones de origen, destino y servicio especificadas en los requerimientos de la actividad. La figura presenta los resultados obtenidos, diferenciando entre comunicaciones permitidas explícitamente, denegadas por regla específica, y bloqueadas por la política de denegación implícita.

Figura 31.
Matriz de pruebas de conectividad interzona y NAT

Origen	Destino	Servicio	Puerto	Protocolo	Resultado	Mecanismo de control
Green (LAN)	Orange (DMZ)	HTTP	80	TCP	✅ Permitido	Regla Inter-Zona Green→Orange
Green (LAN)	Orange (DMZ)	FTP	21	TCP	✅ Permitido	Regla Inter-Zona Green→Orange
Green (LAN)	Orange (DMZ)	ICMP	8, 30	ICMP	❌ Denegado	Regla explícita Denegar ICMP
Green (LAN)	Red (WAN)	HTTP	80	TCP	✅ Permitido	NAT automático Outgoing
Green (LAN)	Red (WAN)	FTP	21	TCP	❌ Denegado	Política implícita (no se creó regla)
Orange (DMZ)	Red (WAN)	HTTP	80	TCP	✅ Permitido	NAT automático Outgoing
Red (WAN)	Orange (DMZ)	HTTP	80	TCP	✅ Permitido	Port Forwarding DNAT + Regla Red→Orange
Red (WAN)	Orange (DMZ)	FTP	21	TCP	✅ Permitido	Port Forwarding DNAT + Regla Red→Orange

Fuente: Autoría Propia

El análisis de la matriz revela patrones consistentes con la política de mínimo privilegio. La comunicación desde la LAN hacia la DMZ está restringida exclusivamente a HTTP y FTP; cualquier otro protocolo, incluyendo ICMP, es bloqueado. La salida hacia Internet desde la LAN opera por defecto para HTTP, pero el servicio FTP requiere una regla explícita de salida que no fue configurada en esta temática, quedando como observación para implementaciones posteriores. La DMZ mantiene acceso HTTP hacia Internet, coherente con la necesidad de actualizaciones y repositorios. Finalmente, los servicios publicados mediante NAT desde la WAN responden correctamente, validando que el mecanismo de traducción de direcciones opera sin exponer la topología interna.

3.4.7 ANÁLISIS DE RESULTADOS Y COMPORTAMIENTO DEL FIREWALL

La implementación de las reglas interzona demostró que la segmentación física de la red, materializada mediante adaptadores independientes en VirtualBox, adquiere valor de seguridad únicamente cuando se complementa con políticas de filtrado explícitas. El firewall Endian actúa como punto de control obligatorio (choke point) donde todo el tráfico entre zonas es inspeccionado, registrado y autorizado o denegado según criterios definidos por el administrador.

Un hallazgo relevante fue la diferencia de comportamiento entre ICMP y los servicios de capa de aplicación. Mientras que el protocolo ICMP fluye entre zonas internas en la configuración por defecto —facilitando el diagnóstico durante la instalación—, los servicios TCP como HTTP y FTP requieren reglas manuales desde el inicio. Esta dualidad evidencia que Endian prioriza la operatividad inicial para protocolos de control, pero mantiene una postura restrictiva para servicios que implican transferencia de datos o acceso a recursos.

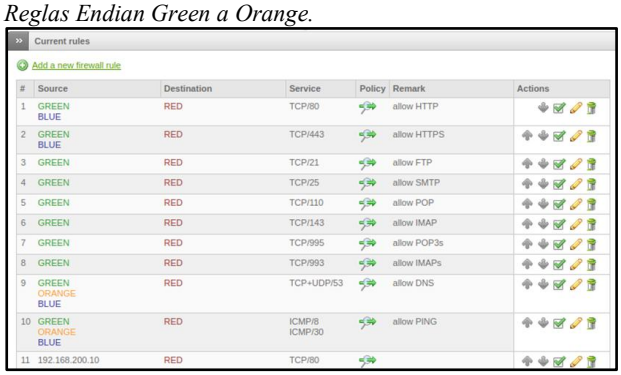
La configuración de Port Forwarding para acceso WAN→DMZ introdujo la complejidad adicional del modo pasivo FTP. A diferencia de HTTP, que opera sobre un único puerto bien conocido, FTP requiere la coordinación de un canal de control y múltiples canales de datos dinámicos. La solución implementada —definir un rango estático de puertos pasivos en vsftpd y reenviarlos mediante reglas DNAT adicionales— representa una práctica estándar en entornos con firewalls stateful, donde el seguimiento de conexiones (connection tracking) permite asociar los canales de datos con la sesión de control establecida previamente [9].

El orden de evaluación de las reglas se confirmó como factor crítico. Durante las pruebas, una regla de permiso ANY posicionada antes de la regla ICMP bloqueada anulaba el efecto de esta última. Tras reordenar las reglas colocando las específicas de permiso primero, la denegación ICMP segunda, y eliminando la regla ANY, el comportamiento se ajustó a los requerimientos. Esta experiencia valida la recomendación de mantener reglas granulares y evitar permisos genéricos en producción.

Finalmente, la matriz de pruebas consolidada demuestra que la arquitectura implementada cumple con el objetivo de aislamiento selectivo. La DMZ permanece accesible para servicios públicos desde la WAN, pero protegida contra reconocimiento ICMP y accesible solo mediante protocolos autorizados desde la LAN. El servidor web y FTP en la zona Orange opera como punto de publicación controlado, mientras que la estación de trabajo en la zona Green mantiene conectividad saliente hacia Internet sin exponerse a conexiones entrantes no solicitadas. Esta configuración constituye una materialización práctica del principio de defensa en profundidad, donde múltiples capas de control —segmentación física, filtrado de paquetes, traducción de direcciones y políticas de

servicio— se superponen para mitigar riesgos de compromiso como se evidencia en la Fig. 32.

Figura 32.
Reglas Endian Green a Orange.



Fuente: Autoría Propia

Vista consolidada del panel de reglas Interzona en Endian Firewall, mostrando la configuración completa de permisos y denegaciones para las zonas Green, Orange y Red.

4. CONCLUSIONES

La configuración base de la infraestructura demostró que la segmentación física de la red en tres zonas de seguridad —Green (LAN), Orange (DMZ) y Red (WAN)— constituye el pilar sobre el cual se sustentan las demás capas de protección. La correcta asignación de adaptadores de red en el hipervisor, la definición de un esquema de direccionamiento IP estático coherente y la verificación de conectividad entre todos los nodos garantizaron que el firewall Endian operara como único punto de interconexión desde el inicio del proyecto, evitando que el tráfico entre la LAN y la DMZ circulara por rutas alternas no controladas.

La implementación de las reglas de traducción de direcciones de red (NAT) confirmó que es posible otorgar salida a Internet a múltiples segmentos internos sin exponer la topología ni las direcciones privadas de la infraestructura. Tanto la zona LAN como la DMZ accedieron a servicios externos mediante el enmascaramiento de sus IPs en la interfaz Red del firewall, lo cual evidenció que Endian no solo segmenta, sino que también gestiona eficientemente el tránsito hacia redes no confiables preservando la confidencialidad del direccionamiento interno.

La habilitación de servicios HTTP y FTP dentro de la zona desmilitarizada validó que la DMZ puede albergar servicios públicos sin comprometer la seguridad de la red interna, siempre que dichos servicios permanezcan bajo la supervisión directa del firewall. Paralelamente, la denegación selectiva del protocolo ICMP permitió controlar con precisión las pruebas de reconocimiento de red, dejando en evidencia la diferencia entre alcanzar al firewall como destino y atravesarlo hacia otros segmentos, lo cual reafirmó su doble rol como gateway y como barrera de contención.

Finalmente, la definición de reglas de acceso interzonal puso de manifiesto que la comunicación entre la LAN, la DMZ y la WAN no es automática ni bidireccional por defecto, sino que requiere políticas explícitas basadas en el principio de mínimo privilegio. Las validaciones de tráfico ICMP, HTTP y FTP en ambos sentidos confirmaron que Endian Firewall Community opera como árbitro efectivo del tránsito entre segmentos, permitiendo únicamente las conexiones autorizadas y denegando implícitamente todo lo demás, lo que reduce la superficie de ataque y garantiza la integridad de la infraestructura.

5. REFERENCIAS

[1] Endian. (2024). Endian Firewall Community (Versión 3.3.2) [Software]. SourceForge. https://sourceforge.net/projects/efw/

[2] Endian. (s. f.). Getting started — Endian UTM 5.0 reference manual. Endian Documentation. Recuperado el 25 de mayo de 2026, de https://docs.endian.com/5.0/reference-manual/en/

[3] Oracle. (2022). Oracle VM VirtualBox user manual (versión 6.1). Oracle Documentation. https://www.virtualbox.org/manual/UserManual.html

[4] Wikipedia contributors. (2015, 12 de abril). Endian Firewall. En Wikipedia, The Free Encyclopedia. Recuperado el 25 de mayo de 2026, de https://en.wikipedia.org/wiki/Endian_Firewall

[5] Internet Engineering Task Force. (2024). RFC database. RFC Editor. https://www.rfc-editor.org/

[6] Canonical Ltd. (2024). Ubuntu Server Guide: Networking and firewall. Ubuntu Documentation. https://ubuntu.com/server/docs/networking-and-firewall

[7] Endian. (s. f.). Endian Firewall Community administrator's guide (Versión 3.3). Endian Documentation. Recuperado el 25 de mayo de 2026, de https://www.endian.com/community/docs/

[8] Cheswick, W. R., Bellovin, S. M., & Rubin, A. D. (2003). Firewalls and Internet security: Repelling the wily hacker (2.ª ed.). Addison-Wesley Professional.

[9] Postel, J., & Reynolds, J. (1985). File Transfer Protocol (FTP) (RFC 959). Internet Engineering Task Force. https://doi.org/10.17487/RFC0959