Implementación de mecanismos de seguridad en sistemas operativos GNU/Linux: estrategias, herramientas y buenas prácticas en entornos virtualizados

Deisy Viviana Blanco Gutiérrez
dvblancog@unadvirtual.edu.co
Genesis Edith Rincon Quintero
gerincon@unadvirtual.edu.co
Juan Nicolas Martinez Rocha
jnmartinezr@unadvirtual.edu.co
Karen Tatiana Veloza Rico
ktvelozar@unadvirtual.edu.co
Kevin Santiago Hernández Escobar
kshernandeze@unadvirtual.edu.co

RESUMEN: *Este artículo documenta la implementación práctica de una arquitectura de seguridad perimetral basada en Endian Firewall Community 3.3.2, desplegada sobre entornos de virtualización con Oracle VirtualBox. Se aborda la configuración de cinco temáticas fundamentales: instalación y configuración del firewall con segmentación en zonas de color (LAN, DMZ y WAN); implementación de Network Address Translation (NAT) con Source MASQUERADE; configuración de reglas para permitir servicios desde la zona DMZ; definición de reglas de acceso inter-zona para controlar el tráfico entre redes; y configuración del proxy HTTP con filtrado web. Los resultados demuestran que es posible establecer un entorno de seguridad funcional, escalable y sin hardware dedicado, validando el principio de mínimo privilegio mediante reglas de filtrado diferenciadas por zona.*

PALABRAS CLAVES: Aplicaciones web, DMZ, Endian Firewall, Proxy HTTP.

ABSTRACT: *This article documents the practical implementation of a perimeter security architecture based on Endian Firewall Community 3.3.2, deployed on virtualization environments with Oracle VirtualBox. Five fundamental topics are addressed: installation and configuration of the firewall with color-zone segmentation (LAN, DMZ, and WAN); implementation of Network Address Translation (NAT) with Source MASQUERADE; configuration of rules to allow services from the DMZ zone; definition of inter-zone access rules to control traffic between networks; and HTTP proxy configuration with web filtering. Results demonstrate that it is possible to establish a functional, scalable security environment without dedicated hardware, validating the principle of least privilege through zone-differentiated filtering rules.*

KEYWORDS: DMZ, Endian Firewall, HTTP Proxy, Web applications.

1. INTRODUCCIÓN

Las empresas deben proteger sus recursos internos de peligros externos al mismo tiempo, deben garantizar que los usuarios autorizados puedan acceder a los servicios. Usar software libre como Endian Firewall es una buena idea, es fuerte, flexible y no cuesta mucho, se puede usar para establecer reglas de seguridad en el borde de su red. Endian Firewall es un sistema basado en GNU/Linux se enfoca en la seguridad de redes permitiendo crear diferentes áreas para el tráfico. El área LAN o VERDE es para su red interna. El área WAN o ROJA es para el acceso a Internet. El área DMZ o NARANJA es para servidores públicos.

Tener estas tres áreas ayuda a crear reglas de acceso claras esto reduce los puntos débiles en su seguridad. También mejora la forma en que ve el tráfico en su red.

Este informe explica cómo configurar reglas NAT, estas reglas permiten que la LAN y la WAN se comuniquen también, permiten que la DMZ se comunique con Internet. Además, definimos reglas para los servicios HTTP y FTP entre áreas. Se limitó el protocolo ICMP bloqueándolo. También se realizó la configuramos un Proxy HTTP. Este proxy no es transparente y requiere que los usuarios se autentiquen. Incluimos listas para bloquear sitios web específicos.

Todo lo anterior se configuró en un entorno virtual usando VirtualBox, el artículo se organiza de la siguiente manera: primera parte configuración de reglas, configuración NAT, tercera, revisión de los servicios permitidos y bloqueados en la DMZ, cuarta sección

describe las reglas de acceso entre áreas y cómo se fueron probadas, quinta sección explica la configuración del Proxy HTTP con autenticación. Finalmente, se presentan las conclusiones y las referencias. [1]

2. FIREWALL ENDIAN

2.1 FIREWALL ENDIAN

Endian Firewall Community (EFW) es una solución de seguridad integral basada en el núcleo de Linux, diseñada bajo el concepto de Gestión Unificada de Amenazas (UTM). Esta plataforma permite la transformación de cualquier hardware x86 o entorno virtualizado en un dispositivo de seguridad perimetral robusto. Su arquitectura se fundamenta en la inspección de paquetes de estado (Stateful Packet Inspection) y la segregación de tráfico mediante zonas de colores (Verde, Naranja, Roja y Azul).

A través de una interfaz de gestión web (GUI), permite la administración de servicios críticos como firewalls de aplicación y redes privadas virtuales (VPN).[7]

2.2 ENTORNO DE VIRTUALIZACIÓN

Se utilizó Oracle VirtualBox como plataforma de virtualización sobre un sistema operativo Windows 11. Allí se crearon 3 máquinas virtuales:

- Ubuntu Desktop o Debian Desktop
- Ubuntu Server o Debian Server
- Endian con la versión 3.3.2

2.3 DEFINICIÓN Y CONFIGURACIÓN DE LA INFRAESTRUCTURA VIRTUAL

La implementación se realizó utilizando tres segmentos de red distintos para garantizar el aislamiento de funciones. El firewall Endian se configuró con tres adaptadores virtuales: eth0 para el acceso a internet (Zona Roja), eth1 para la red interna de clientes (Zona Verde) y eth2 para la zona de servicios (Zona Naranja). Se definió el siguiente esquema de direccionamiento IP para toda la red:

Tabla I.
Esquema de Direccionamiento IP para la Implementación de Firewall Endian

Zona	Interfaz	IP Endian	Adaptador VBox
Roja (WAN)	eth0	DHCP	NAT
Verde (LAN)	eth1	192.168.10.1/24	Red interna: LAN_ENDIAN
Naranja (DMZ)	eth2	192.168.20.1/24	Red interna: DMZ_ENDIAN

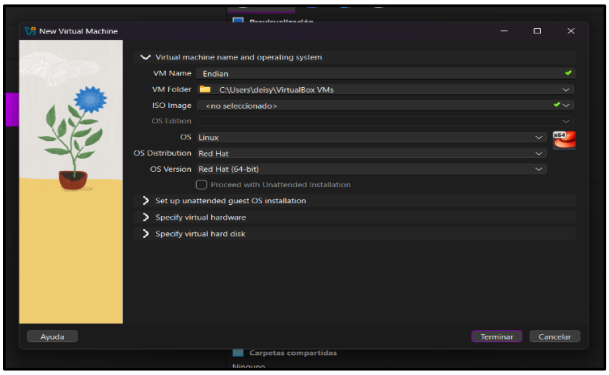
Fuente: Autoría propia

Nota. Esta tabla muestra la definición del direccionamiento IP utilizado en la Configuración de red en Endian.[6]

2.4 PROCESO DE INSTALACIÓN DE ENDIAN

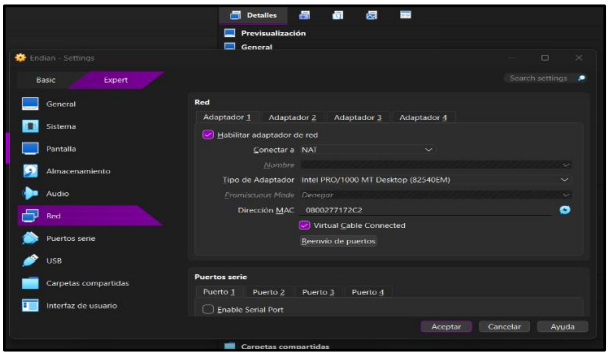
Para realizar la instalación de Endian, primero se crea una máquina virtual vacía, sin cargar inicialmente la imagen ISO del sistema. Luego, se configuran las tarjetas de red en la máquina virtual, asignándolas a las zonas roja (WAN), verde (LAN) y naranja (DMZ) teniendo en cuenta lo indicado en la Tabla I. Posteriormente, se carga la imagen ISO Community de Endian y se inicia la máquina virtual para comenzar el proceso de instalación.[9]

Figura 1.
Creación de la VM Endian mediante el asistente de VirtualBox



Fuente: Autoría Propia.

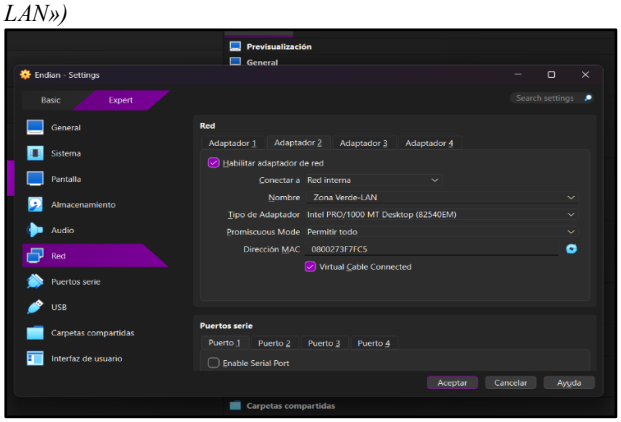
Figura 2.
Adaptador 1 → WAN/RED en modo NAT



Fuente: Autoría Propia.

Figura 3.

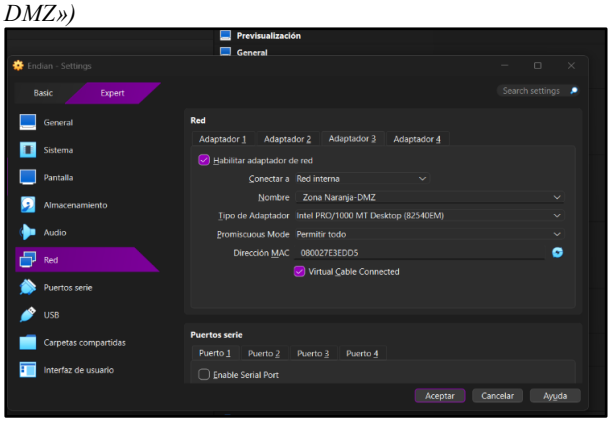
Adaptador 2 → LAN/VERDE (Red interna «Zona Verde-LAN»)



Fuente: Autoría Propia.

Figura 4.

Adaptador 3 → DMZ/Naranja (Red interna «Zona Naranja-DMZ»)

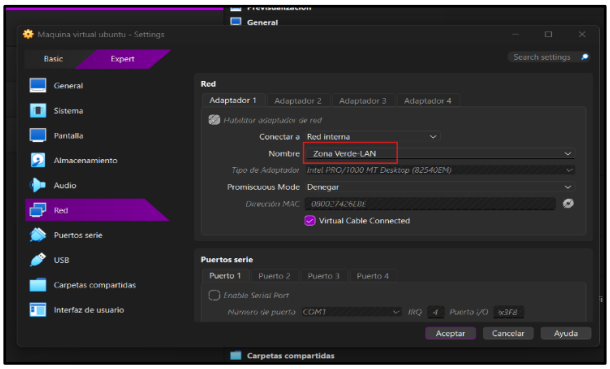


Fuente: Autoría Propia.

Se configura la máquina virtual desktop de Ubuntu (cliente) y la máquina virtual del servidor para que se comuniquen por la misma tarjeta de red.

Figura 5.

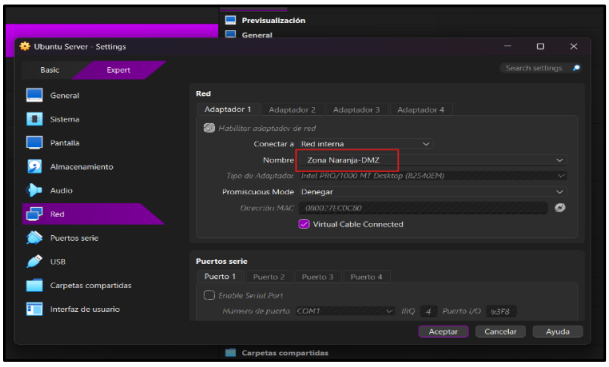
Configuración MV desktop de Ubuntu (cliente) para la red zona verde.



Fuente: Autoría Propia.

Figura 6.

Configurar MV servidor de Ubuntu para la red zona naranja.

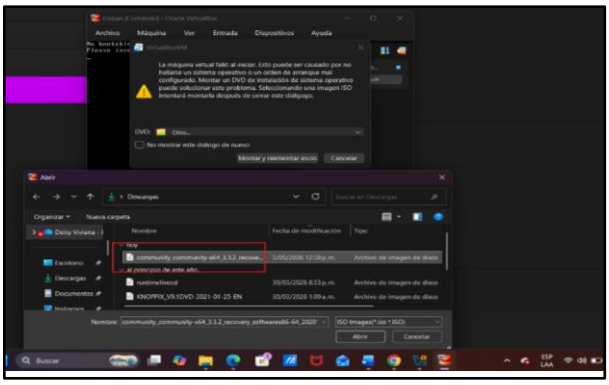


Fuente: Autoría Propia.

Se selecciona la imagen ISO de Endian y se inicia la máquina virtual.

Figura 7.

Seleccionar imágen ISO de Endian.

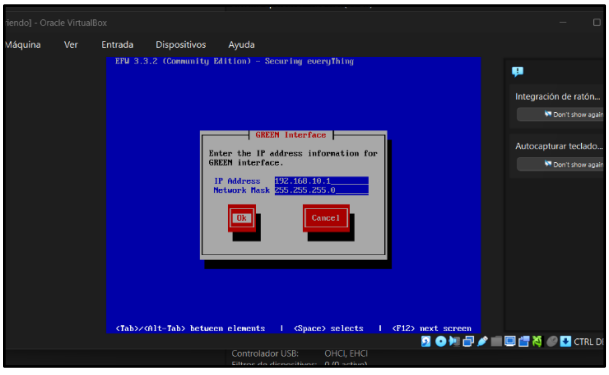


Fuente: Autoría Propia.

Durante el proceso de instalación, se Configura la IP para la interfaz (Verde), asignando 192.168.10.1 como se muestra en la siguiente imagen:

Figura 8.

Configurar dirección IP para la zona verde en Endian.



Fuente: Autoría Propia.

Al finalizar el proceso de instalación, se muestra la consola de Endian donde indica que la zona Verde se encuentra activa:

Figura 9.
Consola de Endian.

Fuente: Autoría Propia.

2.5 DIRECCIONAMIENTO Y CONECTIVIDAD LAN

Se configura el Ubuntu Desktop (Cliente) para que se pueda comunicar con el firewall Endian y así poder acceder a la interfaz de administración web. Para realizar la Configuración por la consola, se utiliza la herramienta nmcli.

Primero, se identifica el nombre de la interfaz de red en el sistema con el comando:

nmcli device

Al ejecutar el comando, se identifica que la interfaz se llama enp0s3 pero actualmente está en estado desconectada, porque no tiene un servidor DHCP activo. Para esto, se realiza la Configuración estática definiendo la IP 192.168.10.2 para el cliente y apuntando al Endian con la IP definida en la instalación (192.168.10.1) como salida.

Figura 10.
Identificar nombre de la interfaz de red en el cliente.

Fuente: Autoría Propia.

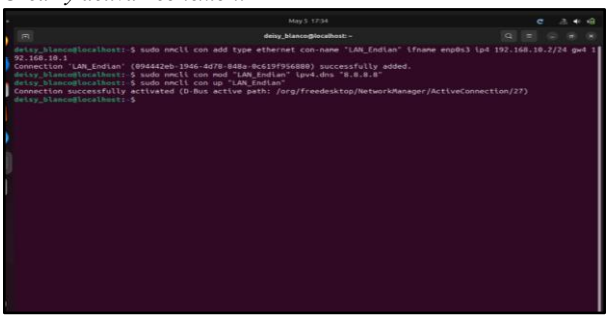
Para crear y activar la conexión, se ejecutan los siguientes comandos:

sudo nmcli con add type ethernet con-name "LAN_Endian" ifname enp0s3 ip4 192.168.10.2/24 gw4 192.168.10.1

sudo nmcli con mod "LAN_Endian" ipv4.dns "8.8.8.8"

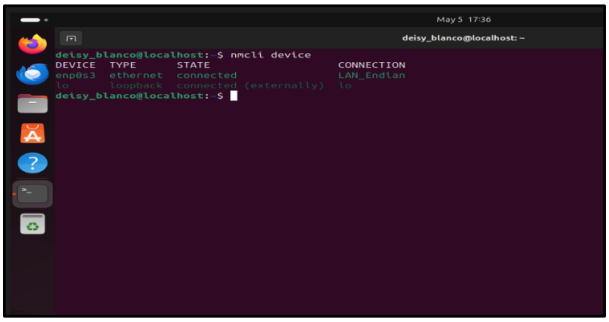
sudo nmcli con up "LAN_Endian"

Figura 11.
Crear y activar conexión.



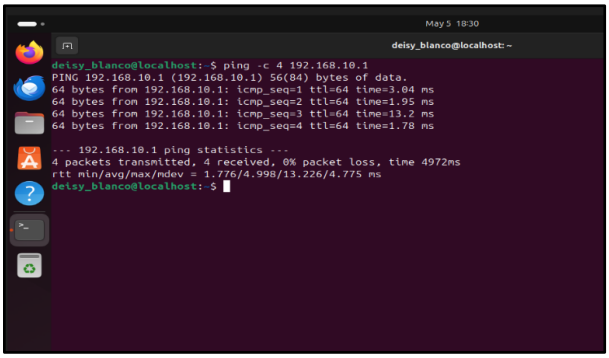
Fuente: Autoría Propia.

Figura 12.
Verificación de conexión activa con Endian al ejecutar nmcli device.



Fuente: Autoría Propia.

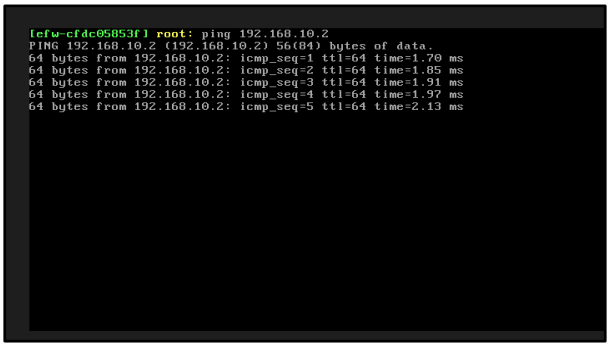
Figura 13.
Ejecución del ping -c 4 192.168.10.1 para validar comunicación con Endian.



Fuente: Autoría Propia.

La verificación muestra un 0% de paquetes perdidos, 4 paquetes permitidos y recibidos correctamente.

Figura 14.
Ejecución del ping 192.168.10.2 para validar comunicación con el cliente.



Fuente: Autoría Propia.

Nota: Se identificó un hallazgo crítico durante el desarrollo: la discrepancia en la asignación predeterminada de las interfaces en Endian, donde la IP de gestión 192.168.10.1 se encontraba inicialmente vinculada a eth0, requiriendo un reordenamiento de los adaptadores de la MV para coincidir con la topología planeada.

Para la Zona Naranja (DMZ), se asignó el segmento 192.168.20.0/24, vinculando la interfaz eth2 (identificada por la dirección MAC 08:00:27:E3:ED:D5) para servir como puerta de enlace del servidor de aplicaciones.

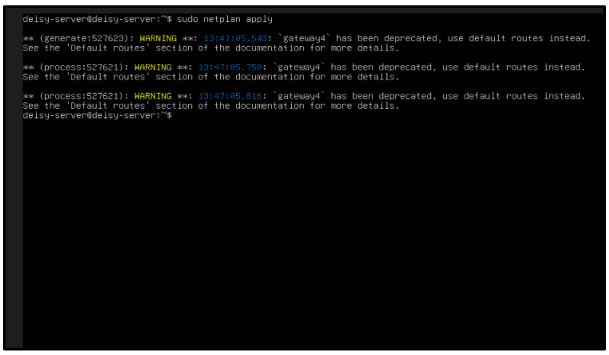
2.6 DESPLIEGUE DEL SERVIDOR EN ZONA NARANJA

En la máquina virtual de Ubuntu Server se integró a la DMZ mediante la Configuración del archivo Netplan, estableciendo la IP estática 192.168.20.10. Esta configuración permite al firewall actuar como un inspector de estado entre la zona Verde y la zona de servidores (Naranja), aplicando políticas de denegación por defecto para el tráfico originado en la DMZ hacia la LAN. [2]

Figura 15.
Configuración de la IP en el servidor de Ubuntu con sudo vi /etc/netplan/.yaml*

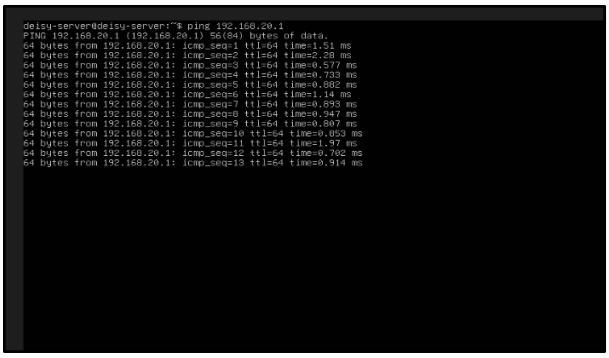
Fuente: Autoría Propia.

Figura 16.
Aplicar cambios en el archivo con sudo netplan apply.



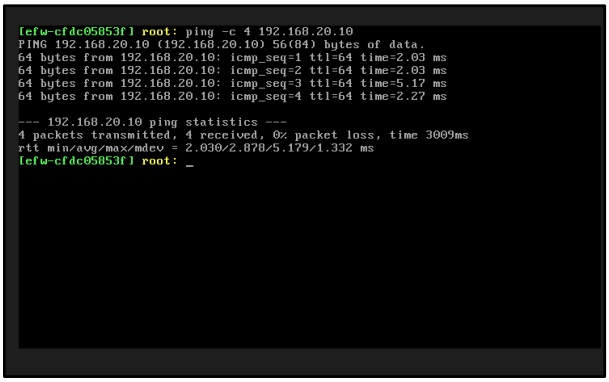
Fuente: Autoría Propia.

Figura 17.
Validar conectividad desde el servidor de Ubuntu.



Fuente: Autoría Propia.

Figura 18.
Validar conectividad desde Endian.



Fuente: Autoría Propia.

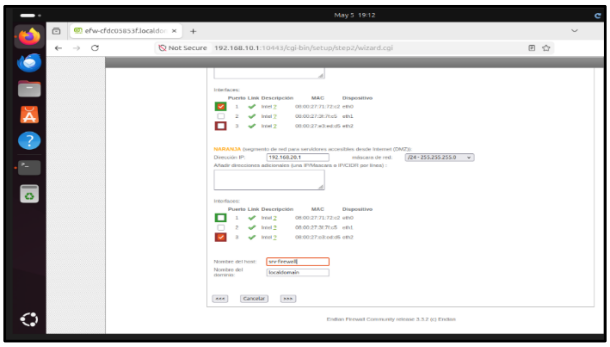
2.7 RESULTADOS

2.7.1 Ingreso a la Interfaz de Administración de Endian

Para acceder a la web de Endian, desde la máquina virtual desktop Ubuntu (cliente) en el navegador se ingresa a https://192.168.10.1:10443. Se navega por el asistente de

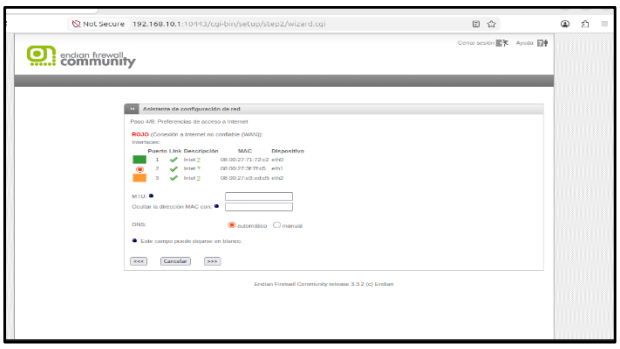
Configuración y se configuran la zona Naranja y zona Roja, seleccionando su interfaz teniendo en cuenta la dirección MAC en la Configuración de la máquina virtual.

Figura 19.
Configuración zona Naranja.



Fuente: Autoría Propia.

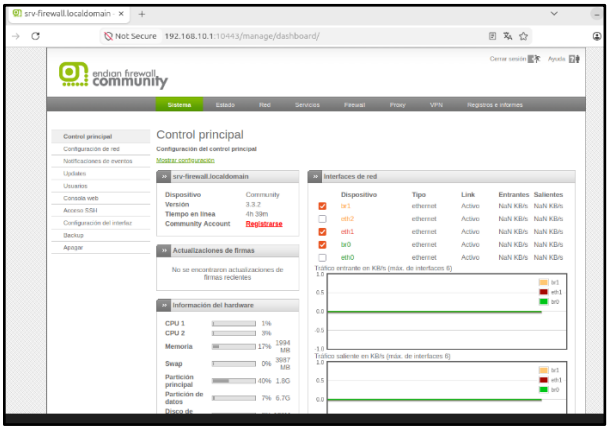
Figura 20.
Configuración zona Roja.



Fuente: Autoría Propia.

Al finalizar la Configuración, se inicia sesión con el usuario admin y se observa el panel de administración web de Endian, evidenciando las interfaces en estado activo.

Figura 21.
Panel de administración web de Endian.



Fuente: Autoría Propia.

Desde la terminal de Ubuntu Desktop (cliente), se verifica si tiene salida a internet a través del firewall haciendo ping -c 4 google.com, lo cual responde confirmando que la Zona Roja está realizando el enmascaramiento de red (NAT).

Figura 22.
Verificar salida a internet a través del firewall Endian.

Fuente: Autoría Propia.

3. NETWORK ADDRESS TRANSLATION (NAT)

3.1 NETWORK ADDRESS TRANSLATION (NAT)

El NAT es una técnica de red definida en el RFC 3022 que modifica la información de direccionamiento IP en los encabezados de los paquetes mientras estos transitan por un dispositivo de enrutamiento. Existen tres variantes principales: NAT estático (mapeo 1:1), NAT dinámico (pool de IPs) y MASQUERADE (muchos a uno), siendo esta última la más utilizada en entornos donde la IP pública es dinámica [4]

El MASQUERADE sustituye la dirección IP de origen del paquete saliente por la dirección IP de la interfaz de salida del router, manteniendo una tabla de traducciones que permite redirigir las respuestas al host interno correspondiente. En GNU/Linux, esta funcionalidad es implementada por el módulo

de iptables a través de la cadena POSTROUTING de la tabla NAT.

3.2 ARQUITECTURA DE SEGURIDAD PERIMETRAL

La arquitectura de seguridad perimetral con tres zonas define niveles de confianza diferenciados. La zona verde (LAN) incluye los equipos internos de la organización y tiene el mayor nivel de confianza. La zona roja (WAN) representa la red externa, generalmente Internet, considerada no confiable. La zona naranja (DMZ) es una red intermedia que alberga los servidores accesibles desde el exterior, actuando como buffer entre la LAN y la WAN [5]

3.3 GNU/LINUX ENDIAN FIREWALL COMMUNITY

Endian Firewall es una distribución GNU/Linux basada en Red Hat/CentOS diseñada específicamente para funciones de firewall y seguridad de red. La versión Community 3.3.2 incluye gestión de interfaces de red por zonas de color, NAT y reenvío de puertos, proxy HTTP/HTTPS, servidor VPN y sistema de detección de intrusos (IDS). Su administración se realiza a través de una interfaz web accesible por HTTPS en el puerto 10443 [3]

3.4 METODOLOGÍA

La implementación se realizó siguiendo una metodología de despliegue incremental por fases, partiendo desde la configuración del entorno de virtualización hasta la verificación funcional del NAT en ambas zonas internas.

3.4.1 Entorno de virtualización

Se utilizó Oracle VirtualBox como plataforma de virtualización sobre un sistema operativo base Windows 10. La Tabla II presenta las especificaciones de las máquinas virtuales implementadas.

Tabla II.
Especificaciones de las Máquinas Virtuales

VM	SO	Red
Endian	EFW 3.3.2 (64-bit)	NIC1:NAT NIC2:LAN NIC3:DMZ
Desktop	Ubuntu 22.04	LAN_ENDIAN

Fuente: Autoría propia

Nota. La Configuración de cada NIC se realiza desde el CMD del host base (Windows).

3.4.2 Esquema de direccionamiento IP

La Tabla III presenta el esquema de direccionamiento IP definido para la implementación, consistente con los requisitos de la arquitectura de tres zonas.

Tabla III.
Esquema de Direccionamiento IP

Zona	Iface	IP Endian	Red
Roja (WAN)	eth0	DHCP	Internet
Verde (LAN)	eth1	192.168.10.1/24	192.168.10.0/24
Naranja (DMZ)	eth2	192.168.20.1/24	192.168.20.0/24

Fuente: Autoría propia

Nota. La Configuración en Endian de los parámetros de red se realiza desde la opción 5 del menú.

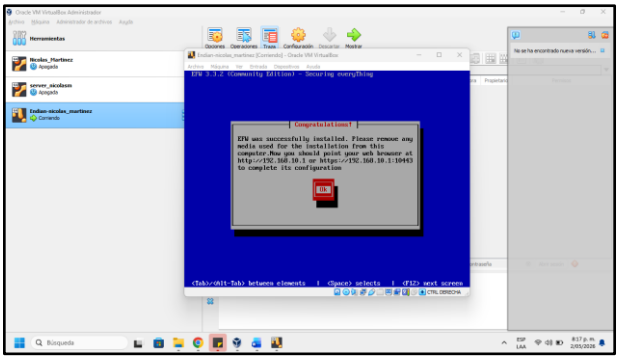
3.4.3 Proceso de instalación

La instalación de Endian Firewall se realizó desde la imagen ISO community_community-x64_3.3.2. Antes de iniciar la VM, se Configuraron los tres adaptadores de red mediante VBoxManage:

```
VBoxManage modifyvm "Endian" --nic1 nat
VBoxManage modifyvm "Endian" --nic2 intnet --intnet2 "LAN_ENDIAN"
VBoxManage modifyvm "Endian" --nic3 intnet --intnet3 "DMZ_ENDIAN"
```

El instalador de Endian solicitó la Configuración de la IP de la interfaz Verde durante el proceso de instalación. Se asignó 192.168.10.1/24 como se muestra en la Figura 23.

Figura *23.*
Instalación exitosa de Endian Firewall Community 3.3.2.



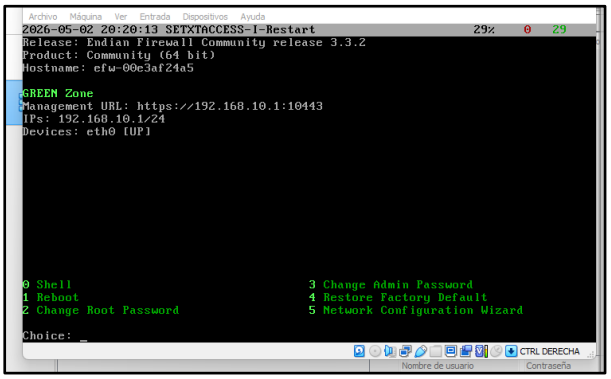
Fuente: Autoría Propia.

3.4.4 Configuración de interfaces de red

Tras la instalación, se ejecutó el Network Configuration Wizard desde la opción 5 del menú de consola de Endian para asignar correctamente las tres interfaces. Los parámetros clave Configurados fueron:

- ROJA (WAN): eth0, tipo DHCP
- VERDE (LAN): eth1, IP 192.168.10.1/24
- NARANJA (DMZ): eth2, IP 192.168.20.1/24
- DNS primario: 8.8.8.8 / secundario: 8.8.4.4

Figura 24.
Consola de Endian con Zona VERDE asignada a eth1 [UP].



Fuente: Autoría Propia.

3.5 RESULTADOS

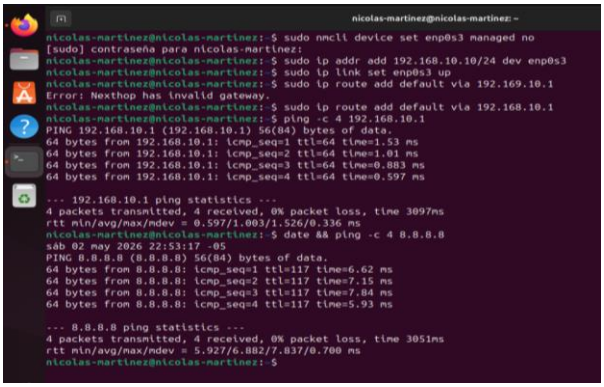
3.5.1 Configuración del cliente lan

La VM de Ubuntu Desktop fue Configurada con IP estática en la red LAN mediante los siguientes comandos, previa deshabilitación del gestor NetworkManager:

```
sudo nmcli device set enp0s3 managed no
sudo ip addr add 192.168.10.10/24 dev enp0s3
sudo ip link set enp0s3 up
sudo ip route add default via 192.168.10.1
```

La verificación de conectividad con el gateway LAN de Endian (192.168.10.1) arrojó 0% de pérdida de paquetes, confirmando la correcta operación de la red interna.

Figura 25.
Ping exitoso desde el cliente LAN al gateway Endian.

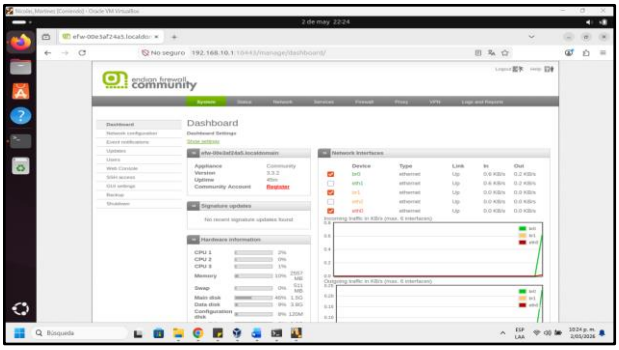


Fuente: Autoría Propia.

3.5.2 Acceso a la interfaz web de endian

Desde la VM cliente LAN se accedió a la interfaz web de administración de Endian Firewall en https://192.168.10.1:10443. El dashboard confirmó que las tres interfaces de red estaban activas: br0/eth1 (VERDE), br1/eth2 (NARANJA) y eth0 (ROJA), con tráfico activo en la zona LAN.

Figura 26.
Dashboard de Endian Firewall con las tres interfaces activas.



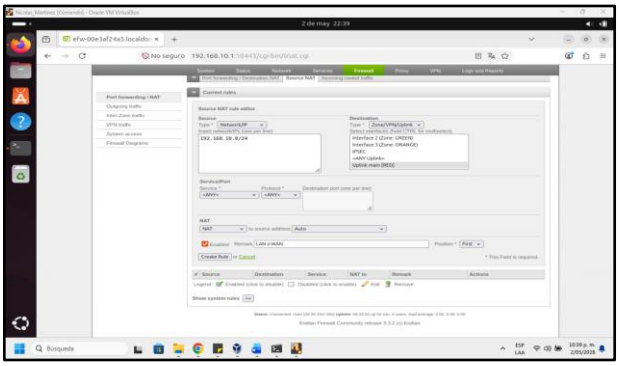
Fuente: Autoría Propia.

3.5.3 Regla nat – zona lan hacia wan

La primera regla Source NAT se creó en Firewall → Port Forwarding / NAT → Source NAT, con los siguientes parámetros:

- Source: Network/IP → 192.168.10.0/24
- Destination: Uplink main [RED]
- Service/Protocol: ANY/ANY
- NAT to source address: Auto (MASQUERADE)
- Remark: LAN a WAN

Figura 27.
Formulario Source NAT Configurado para LAN → WAN.



Fuente: Autoría Propia.

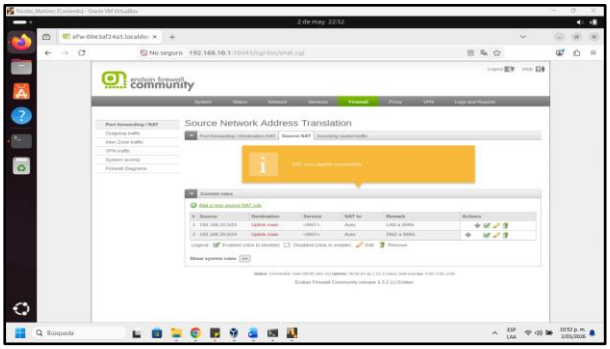
3.5.4 Regla nat – zona dmz hacia wan

La segunda regla Source NAT se creó con los mismos parámetros, modificando únicamente la red de origen:

- Source: Network/IP → 192.168.20.0/24
- Destination: Uplink main [RED]
- Remark: DMZ a WAN

Ambas reglas fueron aplicadas exitosamente, como lo confirma el mensaje "NAT rules applied successfully" mostrado por Endian tras ejecutar la acción Apply.

Figura 28.
Ambas reglas Source NAT aplicadas exitosamente.



Fuente: Autoría Propia.

3.5.5 Verificación de conectividad lan → wan

Se ejecutaron pruebas de verificación desde la terminal del cliente LAN. La Tabla IV resume los resultados obtenidos.

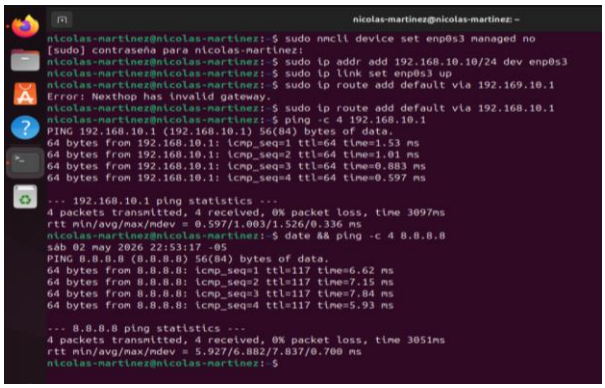
Tabla IV.
Resultados de Verificación NAT LAN → WAN

Comando	Resultado	Estado
ping -c 4 192.168.10.1	0% packet loss	✓ OK
ping -c 4 8.8.8.8	0% packet loss	✓ OK
ip route show	GW: 192.168.10.1	✓ OK
nslookup google.com	172.217.30.174	✓ OK
traceroute 8.8.8.8	1er salto: 192.168.10.1	✓ OK

Fuente: Autoría propia

Nota. Algunos intentos de conexión fallaron, por lo cual es importante tener presente cada paso realizado para revertirlos si es necesario.

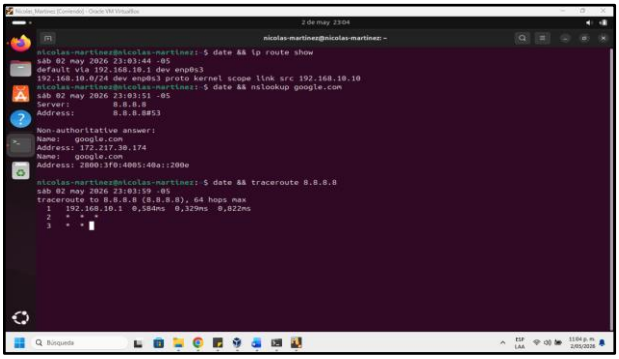
Figura 29.
Ping exitoso a Internet (8.8.8.8) con 0% de pérdida.



Fuente: Autoría Propia.

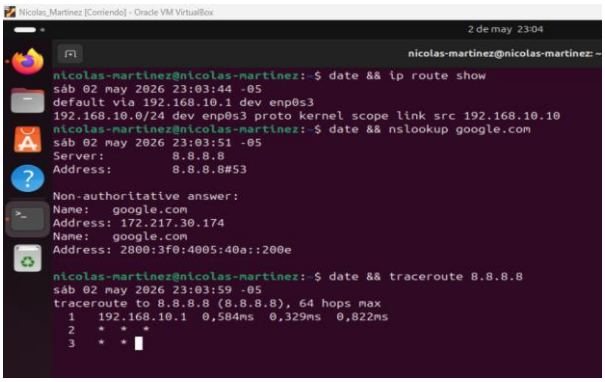
Figura 30.

Resolución DNS de google.com a través del NAT.



Fuente: Autoría Propia.

Figura 31.
Traceroute confirmando a Endian como primer salto NAT



Fuente: Autoría Propia.

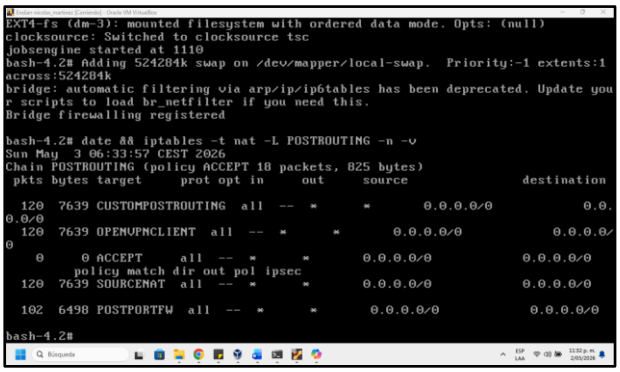
3.5.6 Verificación de Reglas iptables

Desde el shell de administración de Endian se ejecutó la inspección directa de las reglas NAT en las tablas iptables, confirmando la presencia de la cadena SOURCENAT en la cadena POSTROUTING:

iptables -t nat -L POSTROUTING -n -v

La salida mostró las cadenas CUSTOMPOSTROUTING, SOURCENAT y POSTPORTFW activas, confirmando que Endian gestiona correctamente las reglas NAT Configuradas desde la interfaz web mediante iptables en el kernel Linux.

Figura 32.
Reglas iptables NAT activas en la cadena POSTROUTING.



Fuente: Autoría Propia.

3.6 DISCUSIÓN

Los resultados obtenidos demuestran que GNU/Linux Endian Firewall es una plataforma efectiva para la implementación de seguridad perimetral con NAT en entornos virtualizados. La separación en zonas de color facilita la comprensión y gestión del modelo de seguridad, mientras que la interfaz web provee una capa de abstracción sobre la complejidad de iptables.

Un aspecto relevante observado durante la implementación fue la necesidad de configurar correctamente los adaptadores de red de VirtualBox antes de la instalación de Endian, dado que el instalador detecta y asigna las interfaces en el orden en que las encuentra. La Configuración mediante VBoxManage desde la línea de comandos del host demostró ser el método más fiable para garantizar la asignación correcta de NIC1→NAT, NIC2→LAN_ENDIAN y NIC3→DMZ_ENDIAN

La verificación de las reglas NAT a nivel de iptables es fundamental para confirmar que la Configuración realizada desde la interfaz web fue correctamente traducida a reglas de kernel, cerrando el ciclo de validación desde la capa de usuario hasta la capa del sistema operativo.

4. PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

Como parte de la formación práctica en Administración de Servicios en Red, se desarrolló un conjunto de actividades orientadas a la configuración de redes segmentadas y a la implementación de políticas de seguridad mediante herramientas basadas en GNU/Linux. En este contexto, se realizó la Configuración de una red segmentada utilizando el firewall Endian Firewall Community, abarcando desde la instalación del sistema hasta la validación de servicios permitidos y restringidos entre las diferentes zonas de red.[8]

4.1 CREACIÓN DE LA MÁQUINA VIRTUAL ENDIAN FIREWALL

Para la implementación del entorno de pruebas se utilizó Oracle VM VirtualBox, donde se creó la máquina virtual denominada Endian_Firewall. Esta fue Configurada con un sistema operativo Linux de 64 bits, 1024 MB de memoria RAM y un disco duro virtual tipo VDI con capacidad de 20 GB.

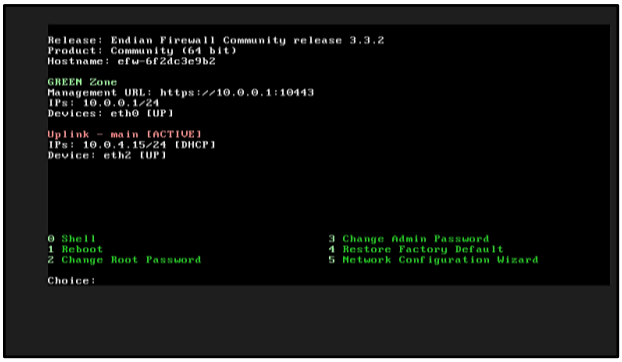
Adicionalmente, se Configuraron tres adaptadores de red con el fin de segmentar el entorno de comunicación:

- Adaptador 1: red interna denominada LAN-Verde.
- Adaptador 2: red interna denominada DMZ-Naranja.
- Adaptador 3: modo NAT para acceso a Internet.

4.2 INSTALACIÓN DEL SISTEMA ENDIAN FIREWALL

Se montó la ISO EFW-COMMUNITY-3.3.2.iso en la VM y se procedió con la instalación. Durante la Configuración inicial, se asignó la zona verde con IP estática 10.0.0.1/24. Luego se accedió a la interfaz gráfica desde un navegador en una máquina cliente LAN.

Figura 33.
Interfaz principal de Endian Firewall.



Fuente: Autoría Propia.

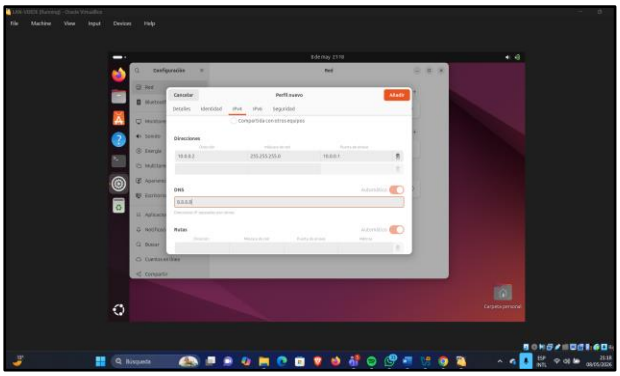
4.3 CREACIÓN DE CLIENTE LAN Y SERVIDOR DMZ

Se crearon dos nuevas máquinas virtuales:

- Desktop-LAN con IP 10.0.0.2, red interna LAN.
- Server-DMZ con IP 172.16.0.2, red interna DMZ.

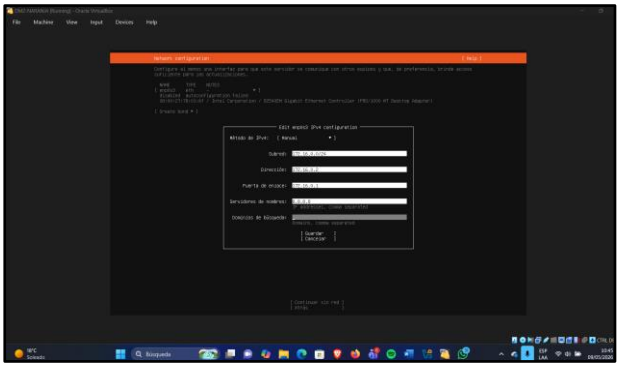
Ambas sin ISO, utilizando Ubuntu Desktop y Server previamente instalados.

Figura 34.
Configuración de IPv4 en máquina LAN



Fuente: Autoría Propia.

Figura 35.
Configuración de IPv4 en máquina DMZ. Fuente: Autoría Propia.



Fuente: Autoría Propia.

4.4 ACCESO AL DASHBOARD Y CONFIGURACIÓN BÁSICA

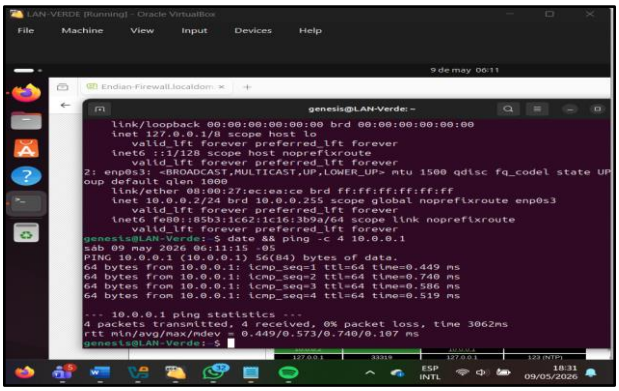
Desde el navegador de la máquina cliente (con IP 10.0.0.2), se accedió a la dirección https://10.0.0.1 para iniciar sesión en el dashboard de Endian. Se completó el asistente de Configuración inicial, se estableció zona roja como ETH02, zona verde como ETH00 y zona naranja como ETH01. Se Configuraron las interfaces con IPs:

- Verde: 10.0.0.1/24
- Naranja: 172.16.0.1/24
- Roja: automática por DHCP

4.5 PRUEBAS DE CONECTIVIDAD

- Ping desde Endian Firewall hacia LAN-verde (Ubuntu Desktop) 10.0.0.2 y DMZ-naranja (Ubuntu server) 172.16.0.2.

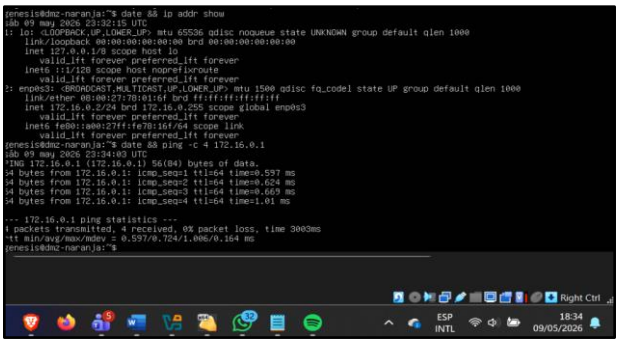
Figura 36.
Ping exitoso desde Endian_Firewall.



Fuente: Autoría Propia.

- Ping desde LAN-verde (Ubuntu desktop) hacia Endian Firewall.

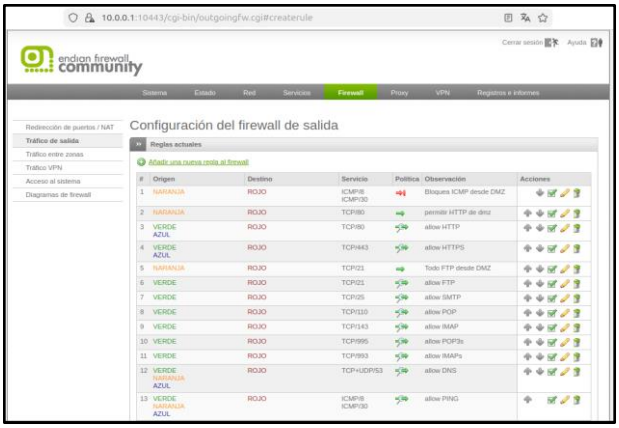
Figura 37.
Ping exitoso desde LAN-Desktop.



Fuente: Autoría Propia.

- Ping desde DMZ naranja (Ubuntu server) hacia Endian (Ubuntu Desktop).

Figura 38.
Ping exitoso desde DMZ-Server.



Fuente: Autoría Propia.

4.6 REGLAS DE FIREWALL Y FILTRADO DE SERVICIOS

Configuración y comprobación de la Temática 3: Permitir servicios de la Zona DMZ para la red.

- Regla 1: Permitir los servicios HTTP (Puerto 80).
- Regla 2: Permitir FTP (puerto 21) desde NARANJA.
- Regla 3: Bloquear ICMP tipo 8 (ping) desde NARANJA.
- Regla 4: Bloquear ICMP tipo 30 (traceroute) desde NARANJA.

Figura 39.
Reglas Temática 3.

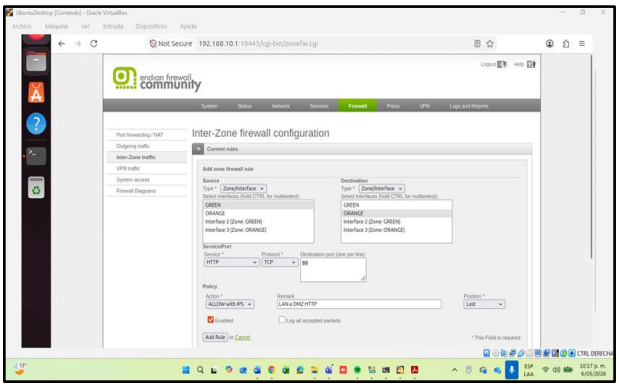
Fuente: Autoría Propia.

4.7 VERIFICACIÓN DE LAS REGLAS APLICADAS

- La primera prueba verificó el bloqueo del protocolo ICMP desde la zona DMZ mediante un comando ping hacia 8.8.8.8. El resultado fue 100% de pérdida de paquetes, confirmando el correcto bloqueo Configurado en Endian Firewall Community.

- La segunda prueba validó el acceso HTTP desde la zona DMZ utilizando el comando curl -I hacia Google. La respuesta obtenida confirmó que el tráfico TCP por el puerto 80 se encuentra permitido correctamente.

Figura 40.
Verificación de reglas mediante DMZ-Server.



Fuente: Autoría Propia.

5. REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO

En esta temática se Configuraron reglas de control de acceso inter-zona sobre Endian Firewall Community desplegado en Oracle VirtualBox, segmentando la infraestructura en tres zonas: Zona Verde (LAN), Zona Naranja (DMZ) y Zona Roja (WAN), asignadas mediante las interfaces br0 y br1. [11]

5.1 ENTORNO DE VIRTUALIZACIÓN

Se utilizó Oracle VirtualBox como plataforma de virtualización sobre Windows 11.

Tabla V.
Especificaciones de las Máquinas Virtuales

Máquina Virtual	Zona	Dirección IP
Endian 1	Firewall	192.168.10.1 192.168.20.1
Ubuntu Desktop	LAN (VERDE)	192.168.10.3
Server	DMZ (NARANJA)	192.168.20.2

Fuente: Autoría Propia.

Nota: La Tabla V presenta las especificaciones de las máquinas virtuales

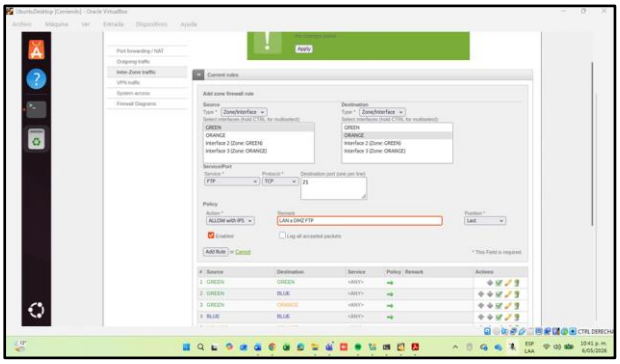
5.2 PROCESO DE INSTALACIÓN Y CONFIGURACIÓN BASE

La configuración lógica se basó en la creación de puentes de red (bridges). La interfaz eth1 se vinculó al puente br0, representando la zona VERDE (LAN) con la IP 192.168.10.1/24. De forma análoga, la interfaz eth2 se asoció al puente br1, que define la zona NARANJA (DMZ) con el segmento 192.168.20.1/24. El acceso a la administración web se realizó a través de la IP virtual del puente de la LAN en https://192.168.10.1:10443.

5.3 REGLAS INTER-ZONA: LAN → DMZ (HTTP Y FTP)

La Desde el panel Firewall → Inter-Zone Traffic se crearon las reglas que permiten el tráfico desde la Zona Verde hacia la Zona Naranja. La regla 6 permite TCP/80 (HTTP) con el comentario "LAN a DMZ HTTP" y la regla 7 permite TCP/21 (FTP) con el comentario "LAN a DMZ FTP".

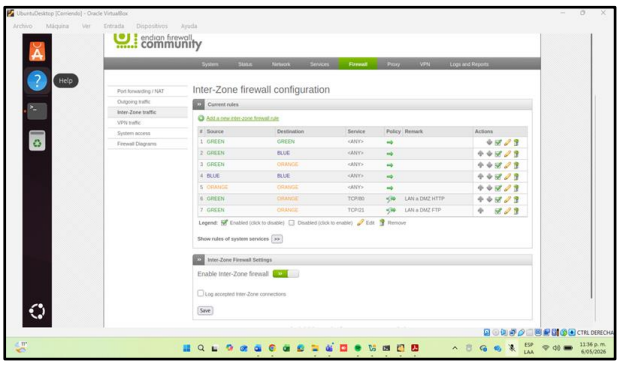
Figura 41.
Configuración regla 1: LAN → DMZ HTTP (TCP/80) en Endian Firewall.



Fuente: Autoría Propia.

Desde el panel de administración web de Endian Firewall, se creó la regla de acceso que permite el tráfico HTTP desde la zona Verde (LAN) hacia la zona Naranja (DMZ)

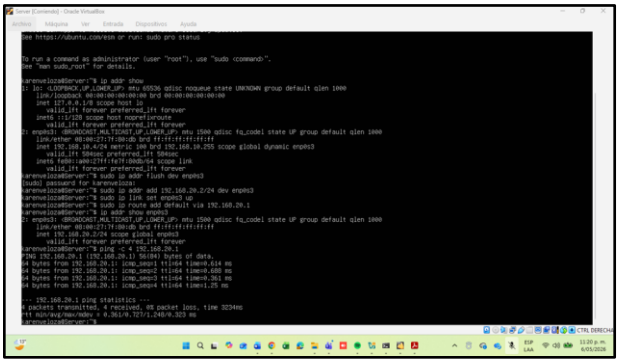
Figura 42.
Configuración regla 2: LAN → DMZ FTP (TCP/21) en Endian Firewall.



Fuente: Autoría Propia.

Se creó la segunda regla de acceso para permitir el tráfico FTP desde la zona Verde (LAN) hacia la zona Naranja (DMZ).

Figura 43.
Verificación de reglas Inter-Zona activas — reglas HTTP y FTP desde LAN a DMZ.



Fuente: Autoría Propia.

En el Ubuntu Server se realizó el proceso de configuración de la dirección IP correspondiente a la zona Naranja (DMZ)

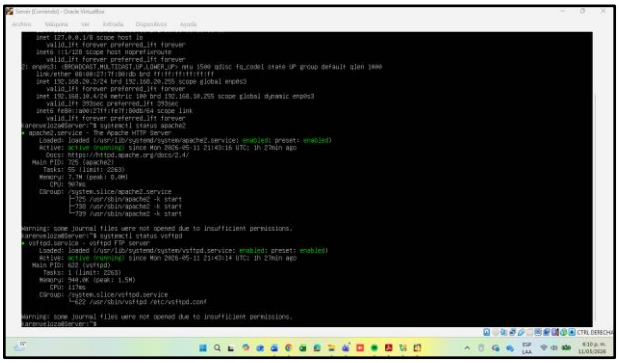
5.4 CONFIGURACIÓN DEL SERVIDOR EN LA DMZ

El Ubuntu Server fue Configurado con IP estática en la zona DMZ mediante los siguientes comandos:

```
sudo ip addr flush dev enp0s3
sudo ip addr add 192.168.20.2/24 dev enp0s3
sudo ip link set enp0s3 up
sudo ip route add default via 192.168.20.1
```

Se instalaron los servicios Apache2 (HTTP, puerto 80) y vsftpd (FTP, puerto 21) para disponer de los servidores que recibirán las conexiones de prueba desde las diferentes zonas. La verificación de escucha de servicios se realizó con el comando netstat -tlnp.[1]

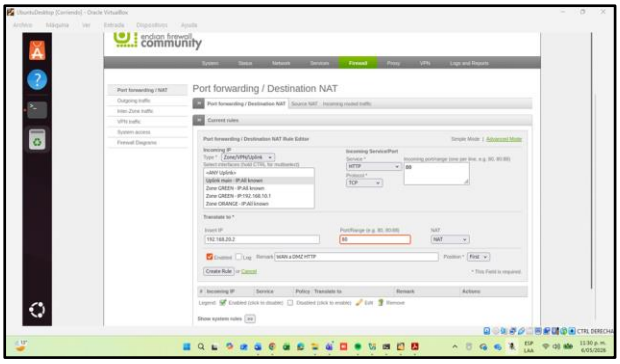
Figura 44.
Configuración de IP estática en Ubuntu Server — zona Naranja (DMZ).



Fuente: Autoría Propia.

Configuración de red de la máquina y los servicios de servidor web (Apache) y servidor FTP (vsftpd) están activos y ejecutándose correctamente.

Figura 45.
Instalación y estado de Apache2 y vsftpd en el servidor DMZ.



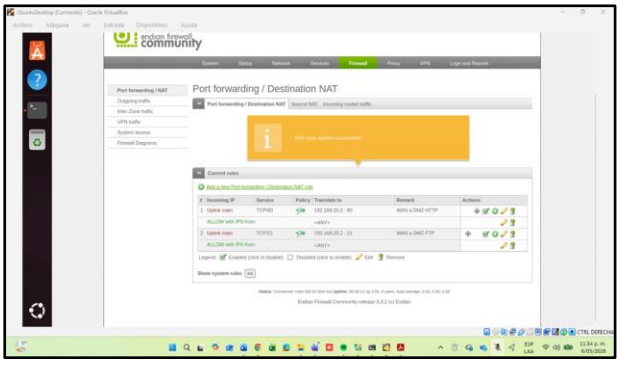
Fuente: Autoría Propia.

Tráfico del puerto HTTP (80) hacia la dirección IP interna 192.168.20.2

5.5 REGLAS WAN → DMZ (PORT FORWARDING/NAT)

Para permitir el acceso desde Internet hacia los servicios de la DMZ se Configuraron reglas en Firewall → Port Forwarding / NAT. La regla 1 redirige TCP/80 (HTTP) desde el Uplink main (WAN) hacia 192.168.20.2:80 con política "ALLOW with IPS". La regla 2 redirige TCP/21 (FTP) desde WAN hacia 192.168.20.2:21, también con política "ALLOW with IPS". [12]

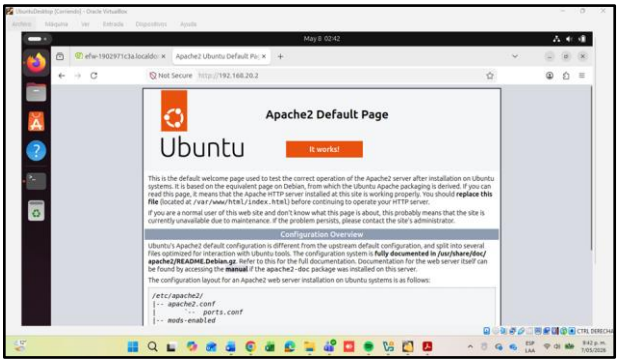
Figura 46.
Configuración regla 3: WAN → DMZ HTTP en Port Forwarding / NAT.



Fuente: Autoría Propia.

Reglas de Port Forwarding aplicadas exitosamente para HTTP y FTP.

Figura 47.
HTTP desde LAN hacia DMZ — página Apache2.



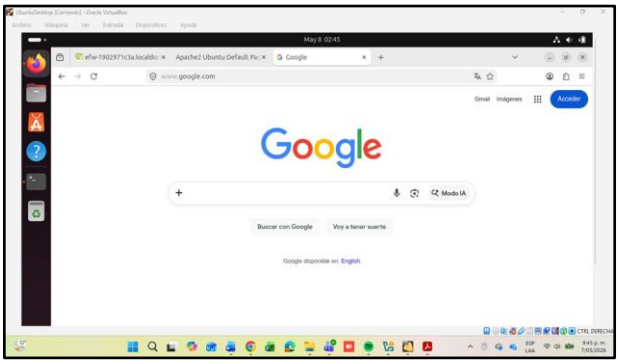
Fuente: Autoría Propia.

Desde el navegador Firefox del Ubuntu Desktop ubicado en la zona Verde (LAN - 192.168.10.3), se accedió exitosamente a la dirección http://192.168.20.2

5.6 PRUEBAS DE CONECTIVIDAD

Se prueba conectividad http desde LAN hacia DMZ:

Figura 48.
HTTP desde LAN hacia WAN — acceso a Google desde la red interna.

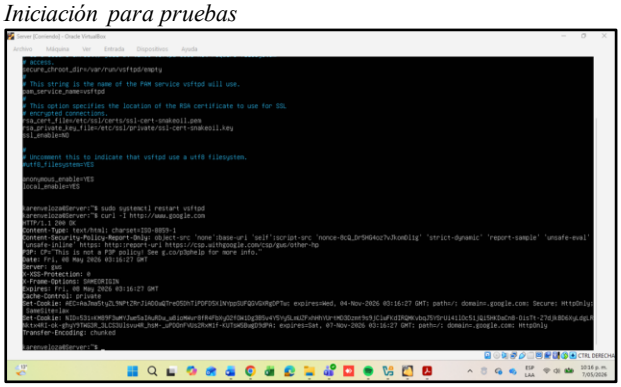


Fuente: Autoría Propia.

Desde el navegador Firefox de Ubuntu Desktop en la zona Verde (LAN), se accedió exitosamente a http://www.google.com, cargando completamente la página de Google

Se prepara entorno para pruebas:

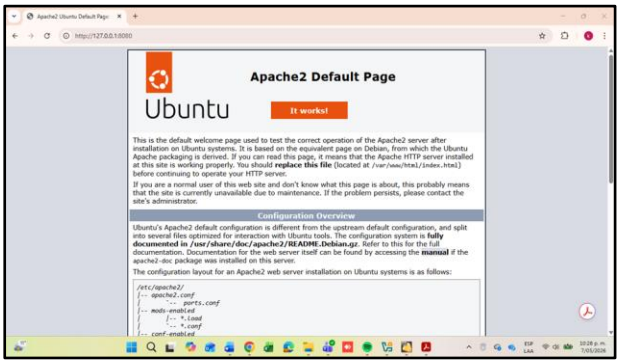
Figura 49.
Iniciación para pruebas



Fuente: Autoría Propia.

Desde la terminal de Ubuntu Server ubicado en la zona Naranja, se ejecutó el comando curl -I http://www.google.com obteniendo respuesta HTTP/1.1 200 OK.

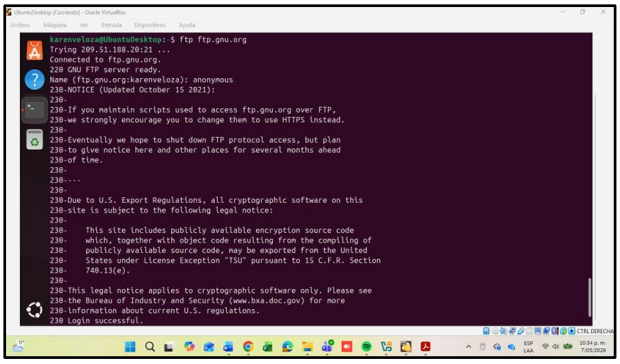
Figura 50.
HTTP desde DMZ hacia WAN



Fuente: Autoría Propia.

Desde el navegador de Windows, se accedió exitosamente a http://127.0.0.1:8080.

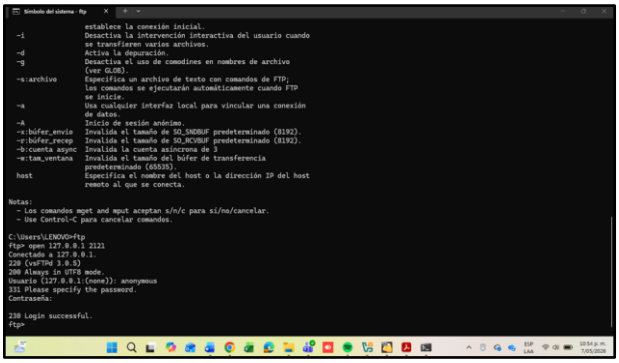
Figura 51.
HTTP desde WAN hacia DMZ



Fuente: Autoría Propia.

Se ejecuta el cliente FTP para conectarse al servidor público ftp.gnu.org, donde se observa una autenticación exitosa con acceso anónimo.

Figura 52.
FTP desde LAN hacia WAN - conexión exitosa a ftp.gnu.org.



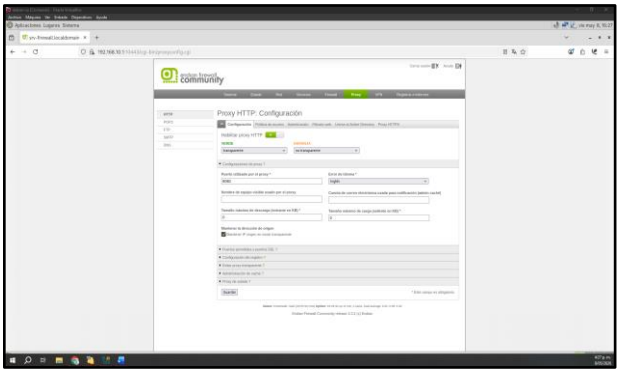
Fuente: Autoría Propia.

Desde el símbolo del sistema Windows, se ejecuta el comando ftp seguido de open 127.0.0.1 2121, siendo redirigido por la regla de Port Forwarding, obteniendo la respuesta 230 Login successful.

6. PROXY HTTP

Se entiende que desde el menú de configuración de Endian accediendo mediante la ip 192.168.10.1 desde un navegador, se encuentra la opción proxy, con la cual se configura lo solicitado en la temática 5. Véase Figura x.

Figura 53.
FTP desde WAN hacia DMZ — conexión al servidor vsftpd vía Port Forwarding,



Fuente: Autoría Propia.

Dentro de la configuración del Proxy, primero se activa el proxy y se asegura de dejar la red verde en no transparente. [10]

Figura 54.
Configuración del proxy HTTP

Fuente: Autoría Propia.

Primero, se configura el perfil de filtrado web, para bloquear el acceso a las páginas web solicitadas por guía. Las cuales son:

- www.youtube.com
- www.hotmail.com
- http://c.www.elnuevodia.com.co/

De esta manera, en la sección del proxy HTTP en su submenú, hay una opción llamada filtrado web.

Figura 55.
Configuración del filtrado web por proxy HTTP.

Fuente: Autoría Propia.

En esta parte se configura las páginas web a las que el proxy debe bloquear. Ahora, a continuación, se configuró la política de acceso, para esto en primera instancia se creó un usuario y a continuación un grupo al cual el usuario creado fue asignado.

Una vez creado el grupo, se creará la política de acceso, la cual se le asignará tanto el grupo creado como el perfil del filtrado web creado.

Figura 56.
Configuración de la política de acceso

Fuente: Autoría Propia.

Como se ve en la figura, se creó la política de acceso en base al grupo creado "UNAD" que tiene el usuario "kevin" y se asignó todos los agentes de usuario. Une vez hecho eso, se seleccionó como política de acceso "permitir acceso" y el filtro de perfil, el perfil "UNAD" que hace referencia al perfil creado desde el filtro web.

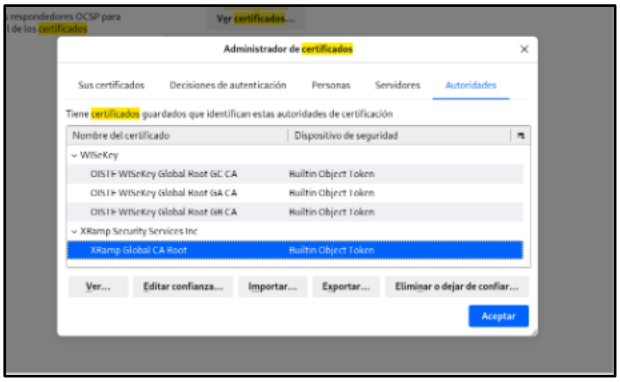
Para continuar con la configuración. Se habilita el Proxy HTTPS, ya que si no está habilitada las páginas https no podrán ser bloqueadas por el proxy. Se habilita desde "proxy HTTPS" ubicada en el submenú del proxy HTTP. Se habilitó aplicando la configuración de "decypt and scan" en "https operation mode" como se ve en la siguiente figura:

Figura 57.
Configuración proxy HTTPS

Fuente: Autoría Propia.

Para que funcione correctamente el proxy HTTPS, se debe instalar el certificado generado desde el servicio de ENDIAN e instalar en el navegador como se indica en la siguiente figura:

Figura 58.
Configuración de certificados de autoridades permitidas.



Fuente: Autoría Propia.

- Al descargarlo, se importa al navegador buscando certificados.
- Ahora, al buscar una de las páginas aparecerá se ha denegado el acceso.

Figura 59.
Pagina bloqueada por Endian.

Fuente: Autoría Propia.

7. CONCLUSIONES

Endian Firewall Community demostró ser una solución funcional y accesible para implementar seguridad perimetral en entornos virtualizados, sin necesidad de hardware dedicado, lo que la hace viable tanto en contextos académicos como en organizaciones de pequeña escala. Su modelo de segmentación por zonas (VERDE, NARANJA, ROJA) permite estructurar arquitecturas de red con claridad, y la correcta asignación de interfaces (eth0→WAN, eth1→LAN, eth2→DMZ) resulta el factor más crítico antes de cualquier configuración de reglas. La implementación de NAT con Source MASQUERADE sobre esta arquitectura permitió verificar en la práctica que una distribución GNU/Linux especializada ofrece las herramientas suficientes para gestionar de forma centralizada el tráfico entre zonas. En cuanto a las reglas de firewall, las pruebas confirmaron que el orden de procesamiento es determinante: las reglas de denegación deben definirse antes que las de permisión para que el sistema las evalúe correctamente. Esto también permitió validar el principio de mínimo privilegio, logrando que un mismo origen de tráfico pueda tener servicios habilitados y otros bloqueados simultáneamente, como HTTP permitido e ICMP denegado desde la DMZ. Las verificaciones realizadas desde navegador, consola y herramientas de red confirmaron que las políticas de filtrado inter-zona funcionaron según lo configurado. Finalmente, la funcionalidad de proxy integrada en Endian agrega una capa adicional de control sobre el acceso a contenidos, aunque su efectividad sobre tráfico HTTPS depende de configuraciones de inspección SSL que requieren autorización explícita del cliente.

8. REFERENCIAS

[1] Stallings, W. (2017). Cryptography and network security: Principles and practice (7.ª ed.). Pearson. https://www.pearson.com/en-us/subject-catalog/p/cryptography-and-network-security-principles-and-practice/P200000003477

[2] Tanenbaum, A. S., y Wetherall, D. J. (2011). Computer networks (5.ª ed.). Prentice Hall. https://www.pearson.com/en-us/subject-catalog/p/computer-networks/P200000003188

[3] Endian S.r.l. (2016). Endian UTM appliance 3.2: Reference manual. http://docs.endian.com/3.2/utm/index.html

[4] Srisuresh, P., y Egevang, K. (2001). Traditional IP network address translator (Traditional NAT) (RFC 3022). IETF. https://www.rfc-editor.org/rfc/rfc3022

[5] Oracle. (2020). VirtualBox user manual. https://www.virtualbox.org/manual/

[6] Linux Professional Institute. (2022). LPIC-1 Exam 101: Tema 101 – Determinar y configurar los ajustes de hardware. https://learning.lpi.org/es/learning materials/101-500/101/101.1/

[7] Canonical. (2023). Ubuntu desktop guide 20.04 LTS. https://help.ubuntu.com/

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

[9] Cibersafety. (2025, julio). Guía definitiva sobre la DMZ: cómo implementarla en redes corporativas y mejorar la seguridad perimetral.

[10] Guzmán Arévalo, D. (2017). OVI Unidad I: Nivelación [Material educativo]. Repositorio UNAD. http://hdl.handle.net/10596/10570

[11] Endian S.r.l. (s.f.). Free open source firewall for home networks. https://www.endian.com/en/community/

[12] Carrigan, T. (s.f.). Introduction to Linux firewalld zones and rules. Red Hat. https://www.redhat.com/en/blog/firewalld-zones-and-rules