IMPLEMENTACIÓN DE SEGURIDAD PERIMETRAL EN SISTEMAS GNU/LINUX MEDIANTE INFRAESTRUCTURA DMX Y DISTRIBUCION ENDIAN

Yefferson Mena Mena
Ymenamena@unadvirtual.edu.co
Edgar Santiago Vergara Mayorga
esvergarama@unadvirtual.edu.co
Jhonathan Avila Yate
Javilay@unadvirtual.edu.co

RESUMEN: *Este artículo presenta un enfoque técnico y estructurado para la implementación de medidas de seguridad perimetral en sistemas operativos GNU/Linux, utilizando la distribución Endian como firewall principal. Se aborda la configuración de una red segmentada mediante zonas LAN, WAN y DMZ, así como la aplicación de reglas de acceso, servicios permitidos y políticas de autenticación por proxy HTTP. Cada etapa de configuración fue desarrollada bajo un entorno de red simulado con herramientas de virtualización, garantizando así la integridad y protección de datos críticos alojados en servidores web internos. La metodología incluye configuración de red, control de tráfico y establecimiento de filtros de contenido para la navegación. Se valida cada configuración a través de pruebas funcionales en consola, evidenciando la correcta implementación de políticas de seguridad.*

PALABRAS CLAVE: DMZ, ENDIAN, GNU/LINUX, VIRTUALBOX

1 INTRODUCCIÓN

La creciente demanda de entornos seguros para servicios web, bases de datos y plataformas digitales ha impulsado la adopción de configuraciones perimetrales robustas en redes empresariales. En este contexto, los sistemas basados en GNU/Linux ofrecen un conjunto de herramientas y distribuciones especializadas para la gestión de seguridad. Una de las arquitecturas más efectivas es la segmentación de la red en zonas diferenciadas (LAN, WAN y DMZ), controladas por un firewall. Este documento expone el proceso de implementación de dichas medidas utilizando la distribución Endian, configurada en un entorno de virtualización, con el propósito de mitigar riesgos de acceso no autorizado, garantizar la disponibilidad de servicios y preservar la integridad de la infraestructura.

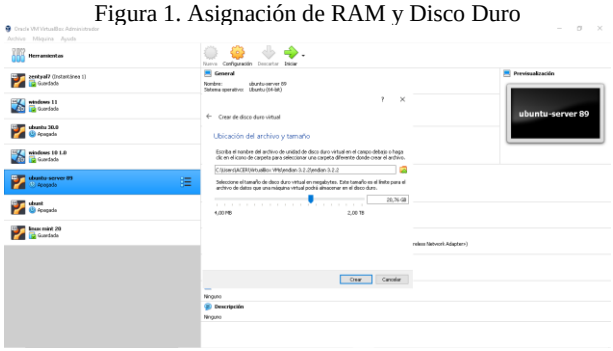
2 TEMATICA 1 - CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX (TARJETAS DE RED) E INSTALACIÓN EFECTIVA DEL MISMO.

2.1 Implementación de GNU/Linux Endian con las zonas verde, roja y naranja, así: Zona verde: Red interna (LAN), Zona roja: Acceso a internet (WAN) y Zona naranja: Servidores (DMZ).

Se crea una nueva máquina virtual para la instalación de Endian.

Realizamos la configuración de la memoria RAM y disco, el resto de configuración es estándar.

Figura 1. Asignación de RAM y Disco Duro

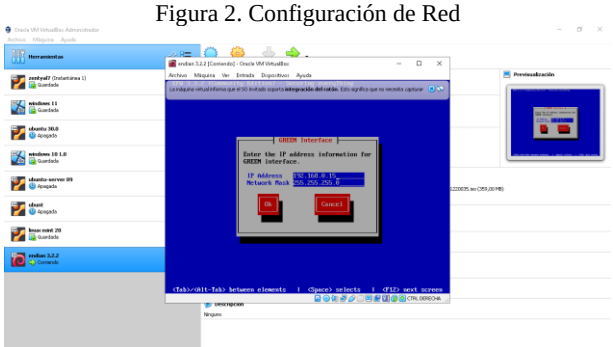


Fuente: Autoría Propia

Se inicializó la máquina para la instalación de ENDIAN.

Como se observa en la Fig. 2, configuramos la IP y la máscara de red a lo cual dejamos como se encuentra.

Figura 2. Configuración de Red

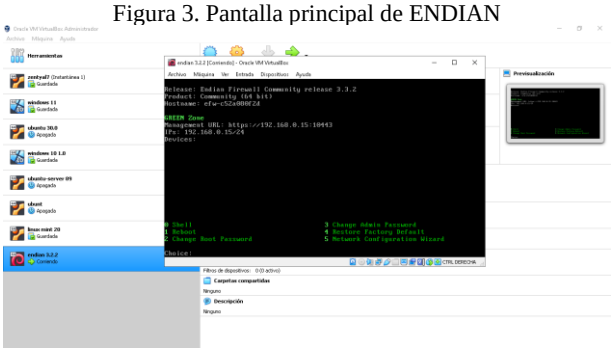


Fuente: Autoría Propia

Al finalizar la instalación, se puede observar que el ingreso a la plataforma de ENDIAN es por medio de la dirección http://192.168.0.15:10443

Como se observa en la Fig. 3, la instalación fue correcta.

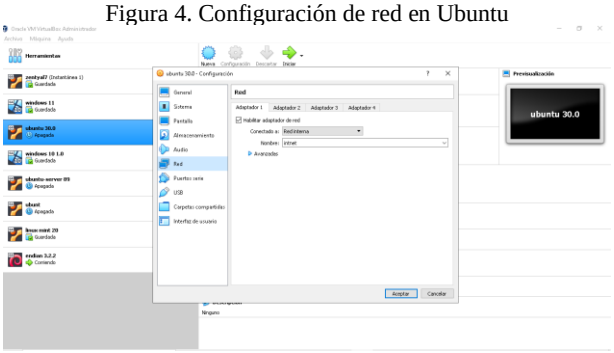
Figura 3. Pantalla principal de ENDIAN



Fuente: Autoría Propia

Se verifica la configuración de la red de la máquina virtual Ubuntu, el cual se debe encontrar en red interna.

Figura 4. Configuración de red en Ubuntu

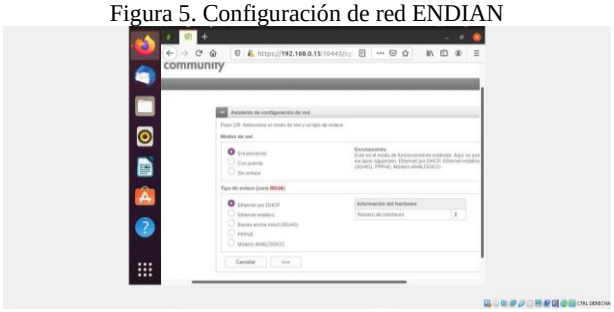


Fuente: Autoría Propia

Se ingresa a la plataforma de ENDIAN con la dirección ya antes mencionada se configuran parámetros básicos, como hora, fecha, usuario y contraseña.

Como se observa en la Fig. 5, se escoge el modo de red Enrutamiento y tipo de enlace DHCP

Figura 5. Configuración de red ENDIAN



Fuente: Autoría Propia

Se escoge la zona de red naranja para DMZ

Figura 6. Configuración de Zona DMZ

Fuente: Autoría Propia

Para habilitar el acceso a los servicios HTTP (puerto 80) y FTP (puerto 21) desde la zona DMZ (naranja), se accede al módulo de configuración de proxy en Endian Firewall, se activa el servicio HTTP y autorizamos explícitamente el tráfico a través de los puertos 80 y 21 para la interfaz correspondiente a la zona naranja.

Figura 7. Habilitación servicios http

Fuente: Autoría Propia

Para denegar el protocolo ICMP (Puerto 80) se crea una nueva regla en el firewall de protocolo ICM y servicio establecido por el usuario donde deniegue los accesos a puerto 8 y 30.

Figura 8. Denegación de protocolo ICMP

Fuente: Autoría Propia

La configuración de puertos y servicios específicos en un firewall constituye una práctica recomendada por los estándares de seguridad actuales. La restricción de protocolos como ICMP reduce significativamente la superficie de ataque al limitar la capacidad de reconocimiento por parte de actores

maliciosos [9]. La implementación de estas medidas en Endian sigue los lineamientos descritos en la documentación oficial del sistema [3][4].

3 TEMATICA 2 – CONFIGURACION NAT

Configurar la regla de NAT (Network Address Translation / Traducción de Direcciones de Red), demostrando el establecimiento de la comunicación desde la LAN hacia la WAN (Red simulada de Internet).

En la interfaz web de Endian se configura lo siguiente: en menú > Firewall > Source NAT, añadimos una nueva regla, tal como se observa en la Fig. 9 con dichas especificaciones.

Figura 9. Configuración de la regla NAT

Fuente: Autoría Propia

Se configura los parámetros de salida, esto es importante para permitir las conexiones necesarias.

Figura 10. Ajustes firewall de salida

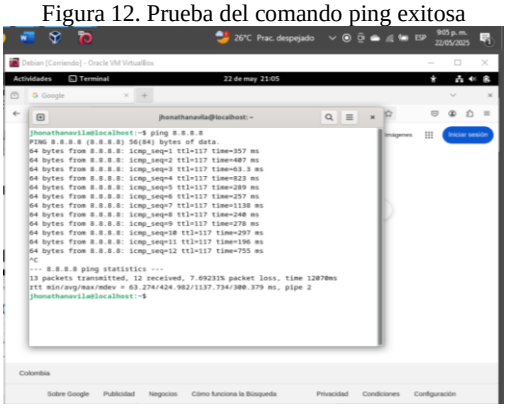
Fuente: Autoría Propia

Con las configuraciones aplicadas el equipo conectado a la LAN debe de tener conexión a internet, como se observa en la Fig. 11 y Fig. 12, la conexión es exitosa.

Figura 11. Verificación de funcionamiento de la regla NAT

Fuente: Autoría Propia

Figura 12. Prueba del comando ping exitosa



Fuente: Autoría Propia

Configurar la regla de NAT, demostrando el establecimiento de la comunicación de la Zona DMZ hacia la Internet. Verificar en el reenvió de puertos / NAT, la creación de las reglas.

Se agrega nuevamente una regla Source NAT, la fuente en este caso es la zona DMZ y el destino es la WAN (Zona Roja), se puede apreciar la configuración en la Fig. 13.

Figura 13. Configuración NAT para DMZ

Fuente: Autoría Propia

Se asigna una nueva configuración de zona de salidas para permitir las conexiones, como se puede apreciar en la Fig. 14, desde la zona naranja se permiten conexiones de todo tipo a la zona roja.

Figura 14. Configuración de trafico de salida

Fuente: Autoría Propia

Se realiza las pruebas de funcionamiento, desde una conexión en DMZ debe de tener conexión a internet, como se observa en la Fig. 15 y Fig. 16, las pruebas son exitosas.

Figura 15. Verificación de conexión a internet

Fuente: Autoría Propia

Figura 16. Prueba de ping a DNS Google

Fuente: Autoría Propia

La implementación de NAT en entornos de red segmentada es fundamental para mantener la separación lógica entre zonas sin comprometer la conectividad necesaria. Esta tecnología no solo permite la traducción de direcciones, sino que también añade una capa adicional de seguridad al ocultar la estructura interna de la red [11]. La configuración realizada sigue las especificaciones técnicas documentadas por la Internet Engineering Task Force para la implementación de servicios de red [6].

4 TEMATICA 3 – PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

Permitir los servicios HTTP (Puerto 80) y FTP (Puerto 21) desde el servidor Web bajo Ubuntu Server.

Denegar el protocolo ICMP (Puerto 8 y puerto 30) para no permitir hacer ping en la red. Probar a través de una consola o terminal la no respuesta del comando ping hacia una IP de la red. Verificar en el tráfico de salida, la creación de las reglas.

Asignamos tarjetas de red: Configuración > Red, esta configuración se evidencia en la Fig. 17.

Adaptador 1: Red interna "red_verde"
Adaptador 2: Adaptador puente "red_roja"
Adaptador 3: Red interna "red_naranja"

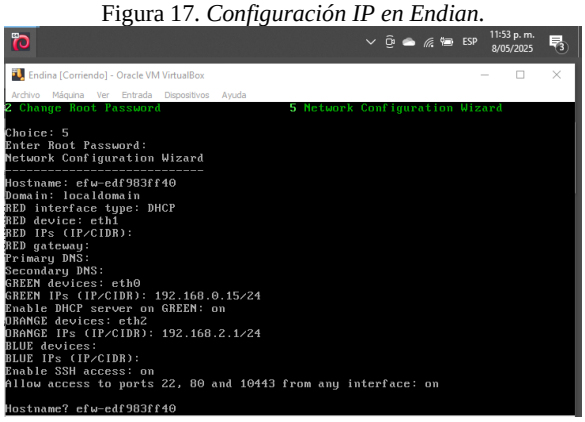
Luego de esto se configura las IP en Endian, esto se puede realizar de manera grafica o en consola, la distribución IP se realiza acorde a lo descrito en la Tabla 1:

Tabla 1.

ZONA	DISPOSITIVO	IP EJEMPLO	NOTA
ROJA (WAN)	ENDIAN (ETH1)	DHCP	ASIGNADA POR ROUTER
VERDE (LAN)	ENDIAN (ETH0)	192.168.0.15	YA CONFIGURADA
NARANJA (DMZ)	ENDIAN (ETH2)	192.168.2.1	POR CONFIGURAR (PARA CONECTAR DEBIAN).
NARANJA (DMZ)	SERVIDOR DEBIAN	192.168.2.10	IP ESTÁTICA, GATEWAY: 192.168.2.1.

Fuente: Autoría Propia

Figura 17. *Configuración IP en Endian.*



Fuente: Autoría Propia

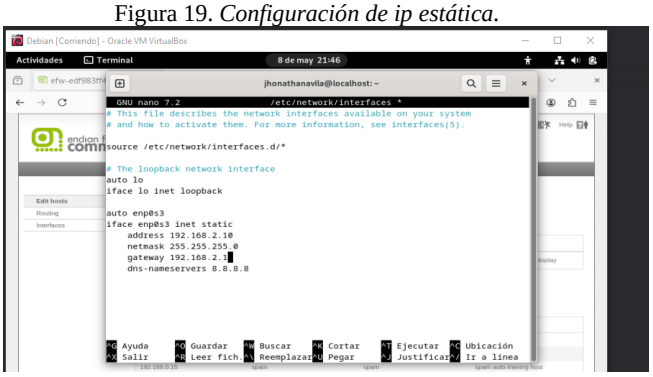
En Debian se asigna a red interna > red_naranja

Figura 18. *configuración de red en Debian.*

Fuente: Autoría Propia

Se configura en Debian IP estática con sudo nano /etc/network/interfaces

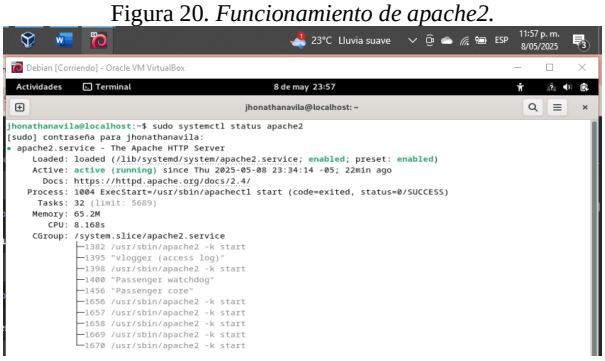
Figura 19. *Configuración de ip estática.*



Fuente: Autoría Propia

Se configuran los servicios en Debian, los cuales son el Apache2 y servicio FTP

Figura 20. *Funcionamiento de apache2.*



Fuente: Autoría Propia

Figura 21. *Funcionamiento de FTP (vsftpd).*

Fuente: Autoría Propia

Ahora se configura las reglas en Endian Firewall:

Permitir HTTP (puerto 80) desde DMZ:
En "Firewall" > "Traffic Policies"
Agregamos una nueva regla:
Source: Green (LAN)
Destination: Orange (DMZ)
Service: HTTP
Action: Accept
Log: Enabled

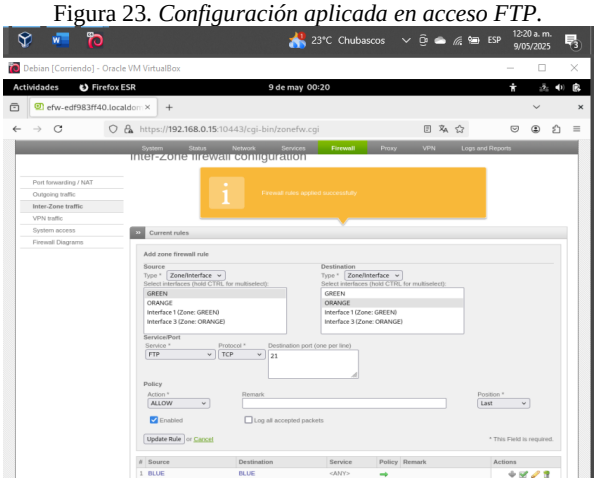
Figura 22. *Configuración aplicada en Firewall*

Fuente: Autoría Propia

Permitir FTP (puerto 21) desde DMZ:

Otra nueva regla:
Source: Green (LAN)
Destination: Orange (DMZ)
Service: FTP
Action: Accept
Log: Enabled

Figura 23. *Configuración aplicada en acceso FTP.*



Fuente: Autoría Propia

Denegar ICMP (ping):

Protocol: ICMP
Action: Drop
Source: Any
Destination: Any
Log: Enabled

Figura 24. *Configuración aplicada en denegación ICMP.*

.

Fuente: Autoría Propia

Ahora se realizará la prueba de funcionamiento, desde la consola de Endian se ejecuta el comando curl http://192.168.2.10

Figura 25. *Ejecución del comando Curl.*

.

Fuente: Autoría Propia

Se ejecuta el comando ftp 192.168.2.10 para verificar el acceso al FTP

Figura 26. *Ejecución del comando ftp.*

.

Fuente: Autoría Propia

Se realiza la prueba de ping con el comando ping 192.168.2.1, debe de rechazar la conexión

Figura 27. *Ejecución del comando ping.*

.

Fuente: Autoría Propia

La configuración de servicios web y FTP en servidores Debian requiere una implementación cuidadosa para garantizar tanto la disponibilidad como la seguridad. De

acuerdo con la documentación oficial [2], la correcta configuración de los archivos de interfaz de red es esencial para establecer conectividad estable en entornos virtualizados. Adicionalmente, estudios recientes destacan la importancia de verificar la funcionalidad de los servicios a través de pruebas sistemáticas de conectividad desde diferentes segmentos de red [7].

5 TEMATICA 5 - Reglas de acceso para permitir o denegar el tráfico.

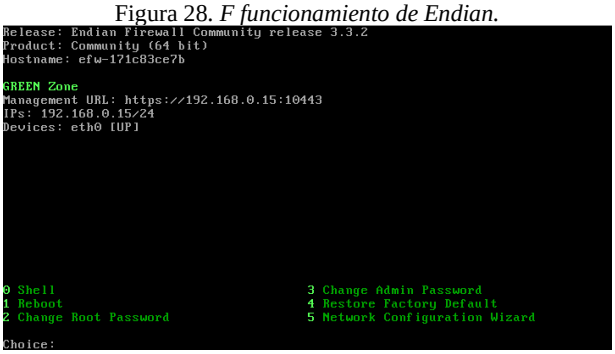
Comunicar la zona Verde con la zona Naranja con el protocolo HTTP y FTP con sus respectivos puertos.

Comunicar la zona Internet con la zona DMZ.

Verificar en el tráfico Inter - Zona, la creación de las reglas. Probar desde un navegador Web, las siguientes directivas:

El ingreso del servicio HTTP desde la LAN hacia la zona DMZ. El ingreso del servicio HTTP desde la LAN hacia la WAN.

Figura 28. *F funcionamiento de Endian.*

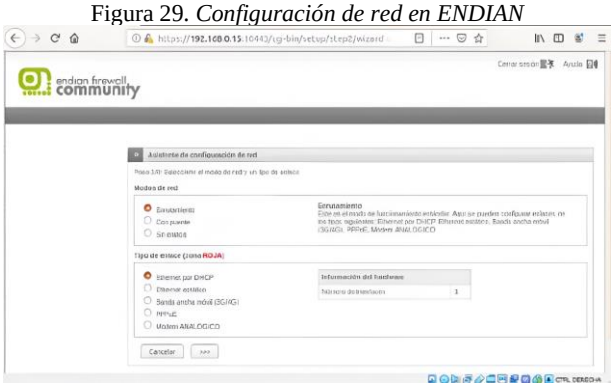


.

Fuente: Autoría Propia

Se selecciona el modo de enrutamiento en DHCP

Figura 29. *Configuración de red en ENDIAN*

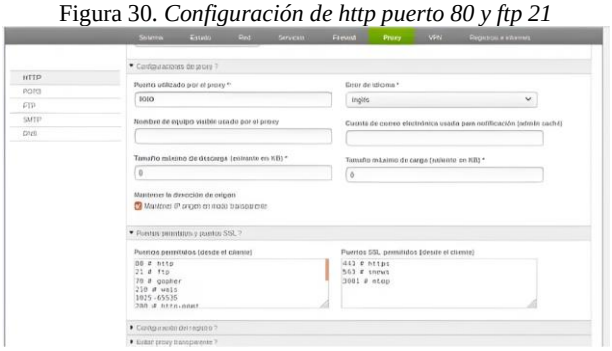


.

Fuente: Autoría Propia

Luego se procede a permitir los servicios http puerto 80 y ftp puerto 21 vamos a la opción proxy y habilitamos la configuración http y luego damos en el puerto 80 y 21

Figura 30. *Configuración de http puerto 80 y ftp 21*



.

Fuente: Autoría Propia

Luego buscamos que el enlace este activo y buscamos nuestra respectiva WAN y seleccionamos para el servicio FTP

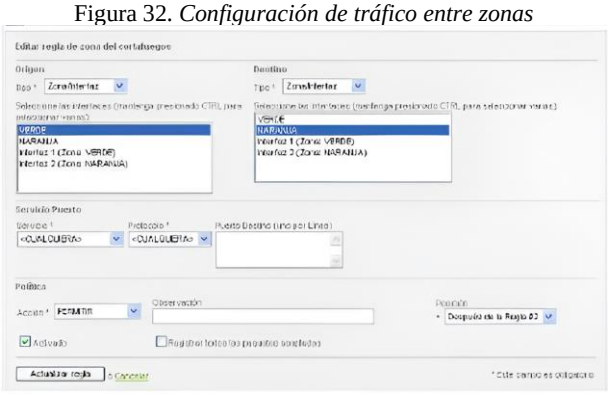
Figura 31. *Imagen en la que se el servicio FTP*

.

Fuente: Autoría Propia

Y luego se configura el tráfico entre zonas

Figura 32. *Configuración de tráfico entre zonas*



.

Fuente: Autoría Propia

El establecimiento de reglas específicas de tráfico entre zonas es un componente crucial de cualquier arquitectura de seguridad en red. La simulación de infraestructuras de red en plataformas como VirtualBox permite validar la eficacia de las políticas de seguridad antes de su implementación en producción [10]. La configuración realizada implementa los principios de mínimo privilegio promovidos para entornos GNU/Linux [5].

6 CONCLUSIONES

La configuración de la instancia GNU/Linux Endian en un entorno de virtualización permitió establecer las bases de una arquitectura de red segmentada en zonas verde (LAN), roja (WAN) y naranja (DMZ). Esta división lógica es fundamental para la implementación de políticas de seguridad diferenciadas y facilita el control del tráfico entre redes internas y externas. La instalación y adecuación del sistema dentro de VirtualBox proporcionaron un entorno controlado y replicable, ideal para pruebas y validaciones sin comprometer entornos de producción reales.

La implementación de reglas de NAT (Network Address Translation) en Endian facilitó la interconexión efectiva entre las zonas LAN, DMZ e Internet (WAN), cumpliendo con los requisitos de direccionamiento y traducción necesarios para permitir la salida controlada del tráfico desde redes internas. Esta configuración demuestra cómo el uso de NAT no solo permite el enmascaramiento de direcciones privadas, sino también la aplicación de reglas específicas para permitir o restringir el acceso externo a servicios internos, consolidando así una primera línea de defensa en la seguridad perimetral.

La habilitación de servicios HTTP y FTP desde la zona DMZ, así como la denegación explícita del protocolo ICMP, permitió evidenciar el control granular del tráfico entre segmentos de red. Esta configuración resalta la importancia de definir de forma precisa qué servicios son accesibles y desde qué ubicaciones, minimizando la superficie de ataque. Al verificar estas reglas mediante pruebas en consola, se confirma la eficacia de las políticas de filtrado implementadas, fortaleciendo la confidencialidad y disponibilidad de los servicios web alojados en servidores de la DMZ.

La creación de reglas de acceso entre las distintas zonas de la red fue clave para validar el principio de mínimo privilegio. Las pruebas de conectividad desde y hacia la DMZ, LAN y WAN mostraron cómo una política bien definida puede restringir el tráfico no deseado, mientras mantiene disponibles los servicios esenciales. La simulación de accesos HTTP y FTP desde múltiples puntos demostró la capacidad del sistema para gestionar flujos interzonales de forma segura, fortaleciendo así la postura defensiva del entorno de red implementado.

7 REFERENCIAS

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

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

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

[4] Endian. (s.f.). *Endian Firewall Community*. https://www.endian.com/community

[5] Free Software Foundation. (2016). *Software Libre y educación: El sistema operativo GNU*. http://www.gnu.org/education/education.html

[6] Internet Engineering Task Force (IETF). (s.f.). *RFC 959 – File Transfer Protocol (FTP)*. https://www.ietf.org/rfc/rfc959.txt

[7] Jay LaCroix. (2020). *Mastering Ubuntu Server: Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting Ubuntu Server*. Packt Publishing. https://research-ebsco-com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b41952

[9] Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2020). *Guía de seguridad en redes*. https://www.mintic.gov.co

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

[11] Tanenbaum, A. S., & Wetherall, D. J. (2011). *Redes de computadoras* (5.ª ed.). Pearson.