Arquitectura de Seguridad en Redes Virtualizadas con GNU/Linux Endian: Segmentación LAN-WAN-DMZ, Reglas de Firewall y Proxy Autenticado

Santiago Jimenez Diaz
sjimenezdia@campusvirtual.edu.co
Ismael Antonio Albutria Cuellar
iaalbutriac@unadvirtual.edu.co
Carlos Eduardo Trujillo Cortes
Cetrujilloc@unadvirtual.edu.co

RESUMEN: *Este artículo presenta la implementación de un entorno de red virtualizado utilizando GNU/Linux Endian como cortafuegos principal. Se configuraron las zonas de red LAN, WAN y DMZ en VirtualBox, estableciendo reglas específicas de NAT, políticas de acceso y segmentación de tráfico. Además, se permitió y restringió el acceso entre zonas según protocolos definidos, incluyendo HTTP y FTP. También se implementó un proxy HTTP no transparente con autenticación de usuarios y políticas de restricción basadas en listas negras. Se verificaron las configuraciones mediante pruebas funcionales desde terminales y navegadores, garantizando el cumplimiento de los objetivos de seguridad, control de tráfico y filtrado de contenido en redes virtualizadas. La experiencia demuestra la eficacia del uso de Endian para segmentación, administración de servicios y políticas de control de acceso en entornos simulados de seguridad de red.*

PALABRAS CLAVE: Cortafuegos, DMZ, GNU/Linux Endian, Virtualización

1 INTRODUCCIÓN

En la actualidad, la implementación de infraestructuras de red seguras y segmentadas es un pilar fundamental para garantizar la integridad, disponibilidad y confidencialidad de los datos dentro de una organización. Ante la creciente demanda de soluciones accesibles y efectivas, el uso de software libre como GNU/Linux Endian se convierte en una alternativa poderosa para la creación de firewalls robustos, configurables y altamente funcionales. Por lo tanto, se propone la implementación de un entorno virtualizado con GNU/Linux Endian como firewall perimetral, gracias a su capacidad de segmentar redes en zonas LAN, WAN y DMZ, facilitando políticas de seguridad adaptadas.

Este artículo presenta una arquitectura de red virtualizada basada en VirtualBox, donde se configura e implementa el cortafuegos Endian con las zonas clásicas de red: verde (LAN), roja (WAN) y naranja (DMZ). A partir de esta estructura, se establecen reglas de traducción de direcciones (NAT), políticas de acceso entre zonas, servicios restringidos y habilitados, y un proxy HTTP con autenticación para controlar el tráfico hacia Internet.

La investigación no solo se enfoca en la configuración técnica, sino también en la validación de reglas y servicios mediante pruebas funcionales. Esto permite una comprensión clara del funcionamiento de un entorno seguro, orientado a la administración eficiente de redes en escenarios reales o simulados.

2 MARCO TEÓRICO

2.1 VIRTUALIZACIÓN DE REDES

La virtualización de redes es una técnica que permite la creación de redes lógicas independientes sobre una misma infraestructura física, permitiendo a los administradores definir topologías de red, servicios y políticas sin cambiar físicamente la red subyacente. Esta tecnología es ampliamente utilizada en entornos de laboratorio, centros de datos y pruebas de seguridad, ya que facilita el despliegue de múltiples escenarios sin necesidad de hardware adicional (Mogul et al., 2020).

Al implementar soluciones como VirtualBox, se pueden crear máquinas virtuales que simulan distintos roles en una red, como servidores, cortafuegos o estaciones de trabajo, permitiendo controlar con precisión la comunicación entre ellas, emulando escenarios de producción de forma controlada y segura (Oracle, 2023).

En este trabajo, se utilizó VirtualBox como plataforma de virtualización debido a su capacidad de emular múltiples interfaces de red y su compatibilidad con entornos GNU/Linux como Endian Firewall.

2.2 SEGURIDAD EN REDES: LAN, WAN Y DMZ

La seguridad en redes es un conjunto de medidas diseñadas para proteger la integridad, confidencialidad y disponibilidad de los sistemas y datos de una organización. Un enfoque común es segmentar la red en diferentes zonas de seguridad, como LAN (Local Area Network), WAN (Wide Area Network) y DMZ (Demilitarized Zone).

- La zona LAN corresponde a la red interna, donde residen los dispositivos de los usuarios.
- La zona WAN representa la conexión hacia internet, usualmente considerada una red no confiable.
- La DMZ se utiliza para alojar servidores públicos, como web o FTP, que deben ser accesibles desde internet, pero sin comprometer la LAN.

Esta segmentación mejora el control del tráfico y la protección de los recursos internos, al permitir reglas de acceso personalizadas según el origen y destino del tráfico (Stallings, 2021).

2.3 FIREWALLS Y NAT

Los firewalls son dispositivos o programas que filtran el tráfico de red según políticas definidas, actuando como una barrera entre diferentes zonas de confianza. Los firewalls modernos permiten reglas detalladas basadas en direcciones IP, puertos, protocolos y comportamientos (Zwicky et al., 2000).

Por su parte, el Network Address Translation (NAT) es una técnica que permite a varios dispositivos de una red interna acceder a internet usando una sola dirección IP pública. NAT oculta la estructura interna de la red, mejorando la seguridad y facilitando la administración del direccionamiento IP (Perkins, 2018). El uso conjunto de firewalls y NAT es fundamental en redes como las que se implementan con GNU/Linux Endian.

En la solución propuesta, se configuraron reglas NAT en Endian para permitir la salida controlada de paquetes desde la LAN hacia la WAN, reforzando el aislamiento de servicios sensibles en la DMZ.

2.4 SERVICIOS PROXY Y AUTENTICACIÓN

Un proxy es un servidor que actúa como intermediario entre los clientes de una red y los recursos externos, como páginas web. Existen diferentes tipos de proxies, pero uno de los más utilizados es el proxy HTTP, el cual puede ser configurado para filtrar contenidos, restringir el acceso a ciertos sitios y registrar las actividades de los usuarios.

La incorporación de políticas de autenticación permite que solo usuarios registrados accedan a internet, aplicando distintos permisos según su perfil. Estas políticas son esenciales en entornos educativos o empresariales, donde es necesario monitorear y controlar el uso de internet (Squid Proxy, 2022).

3 METODOLOGÍA

La metodología empleada en este proyecto se basa en un enfoque experimental y práctico para la implementación de un entorno virtualizado con la distribución Endian Firewall Community, orientado a la segmentación de redes mediante zonas LAN, DMZ y WAN, y la gestión del tráfico entre ellas con reglas de seguridad. Para ello, se utilizaron herramientas de virtualización, sistemas operativos basados en GNU/Linux, y configuraciones de red específicas, documentadas paso a paso.

Se eligió esta distribución debido a su interfaz gráfica amigable, su licencia libre y su arquitectura de seguridad basada en zonas diferenciadas.

3.1 INFRAESTRUCTURA VIRTUAL

Se utilizó Oracle VM VirtualBox como plataforma de virtualización, en la cual se crearon tres máquinas virtuales (VM):

- **Endian Firewall** (con tres interfaces de red)
- **Ubuntu Desktop** (representando la red interna LAN)
- **Ubuntu Server** (ubicado en la zona desmilitarizada - DMZ)

Cada VM fue configurada con los recursos necesarios (CPU, RAM, disco) y con adaptadores de red asignados según la zona correspondiente:

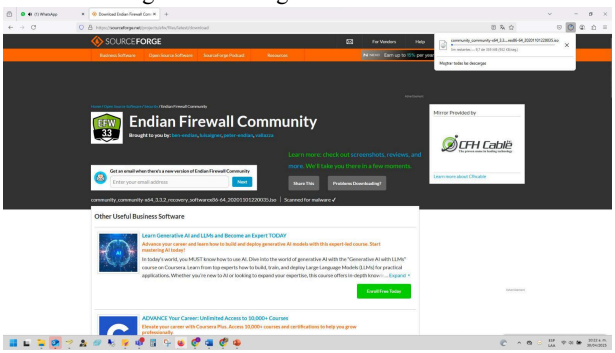
- eth0 (LAN/Verde): 192.168.1.1/24
- eth1 (DMZ/Naranja): 10.0.0.1/24
- eth2 (WAN/Roja): asignación dinámica por DHCP

Estas direcciones fueron definidas con el objetivo de simular una infraestructura empresarial estándar, donde la LAN y la DMZ están en subredes distintas, gestionadas desde el firewall.

3.2 INSTALACIÓN Y CONFIGURACIÓN DE ENDIAN

La instalación de Endian Firewall 3.3.2 se realizó siguiendo el asistente de instalación gráfico. Se definieron los parámetros regionales, credenciales administrativas y se configuraron las zonas de red:

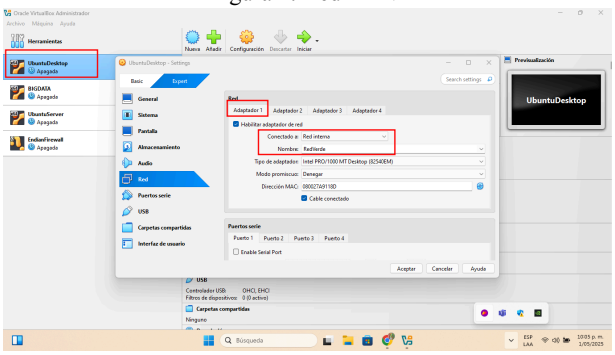
Figura 1: descarga de endian Firewall



Fuente: Autoría Propia

- **Zona Verde (LAN)**: para clientes internos

Figura 2: Red LAN

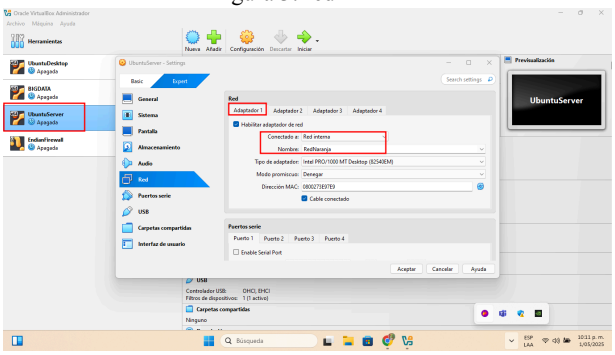


Fuente: Autoría Propia

En la Figura 2 se configura el adaptador 1 en ubuntu Desktop para dejarlo conectado a red interna (Red verde)

- **Zona Naranja (DMZ):** para servidores públicos

Figura 3: red DMZ

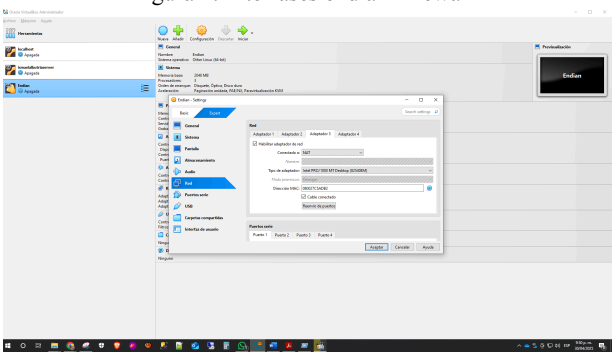


Fuente: Autoría Propia

En la figura 3 se configura el adaptador 1 en ubuntu Server para dejarlo conectado a red interna (Red Naranja)

- **Zona Roja (WAN):** con conexión simulada a Internet mediante NAT

Figura 4: Interfases endian Firewall



Fuente: Autoría Propia

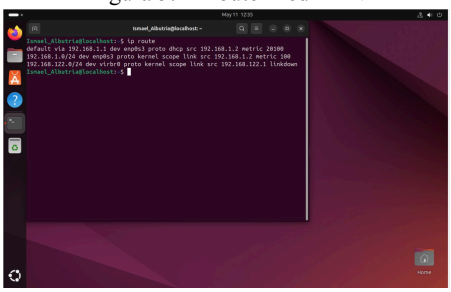
En la figura 4 se configura el adaptador 3 en Endian Firewall para dejarlo conectado a red Nat

Después de la instalación, se accedió a la interfaz web de administración a través de la IP 192.168.1.1 desde Ubuntu Desktop.

3.3 CONFIGURACIÓN DE LOS CLIENTES

- **Ubuntu Desktop (Zona Verde)** fue configurado con una IP estática en la subred 192.168.1.0/24.

Figura 5: IP route Red LAN

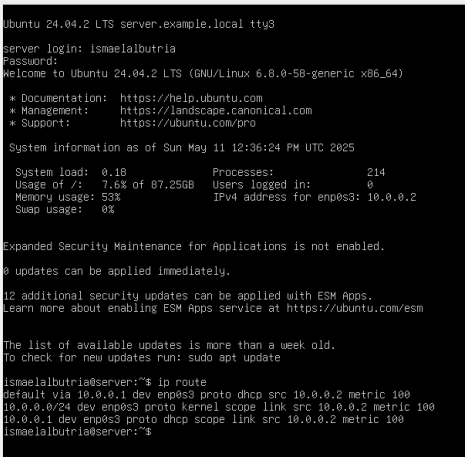


Fuente: Autoría Propia

En la Figura 5 se evidencia la IP estatica 192.168.1.1

- **Ubuntu Server (Zona Naranja)** recibió configuración en la subred 10.0.0.0/24 y se le instaló un servidor web Apache y un servidor FTP para simular servicios públicos.

Figura 6: IP route Red DMZ



Fuente: Autoría Propia

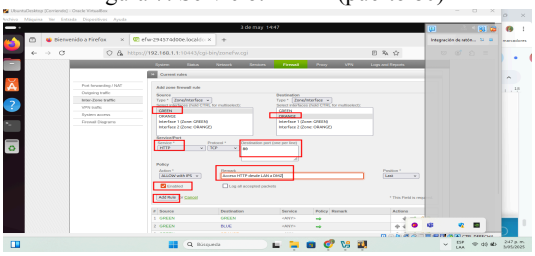
En la Figura 6 se evidencia la IP estatica 10.0.0.1

3.4 REGLAS DE ACCESO Y SEGURIDAD

A través del módulo de Firewall de Endian, se definieron reglas de comunicación entre zonas:

- Se permitió tráfico **HTTP (puerto 80) y FTP (puerto 21)** desde la Zona Verde hacia la DMZ.

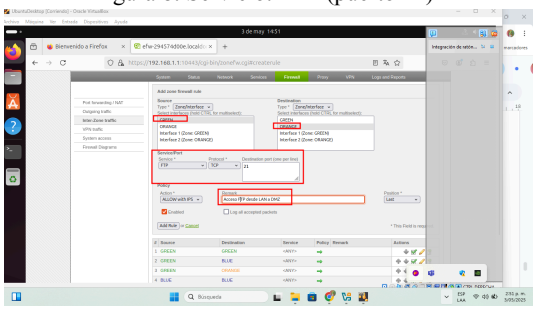
Figura 7: Servicio: HTTP (puerto 80)



Fuente: Autoría Propia

En la figura 7 se evidencia reglas de comunicación entre zona verde a naranja por medio del servicio HTTP

figura 8: Servicio: FTP (puerto 21)

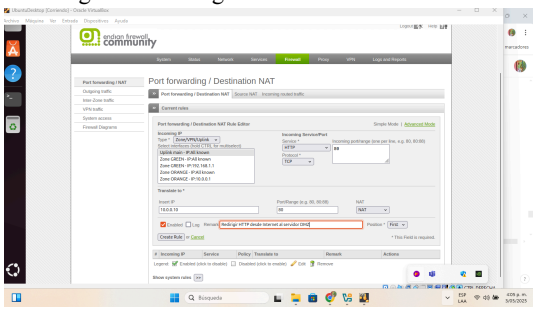


Fuente: Autoría Propia

En la figura 8 se evidencia reglas de comunicación entre zona verde a naranja por medio del servicio FTP

- Se habilitó el **port forwarding** para permitir el acceso externo desde la WAN hacia un servidor en la DMZ.

Figura 9: Redirigir a: IP interna en la DMZ



Fuente: Autoría Propia

En la figura 9 se evidencia reglas de redireccionamiento permitiendo el acceso desde la zona roja a la zona naranja.

- Se probaron conexiones HTTP desde distintas zonas para verificar el aislamiento y control de tráfico.

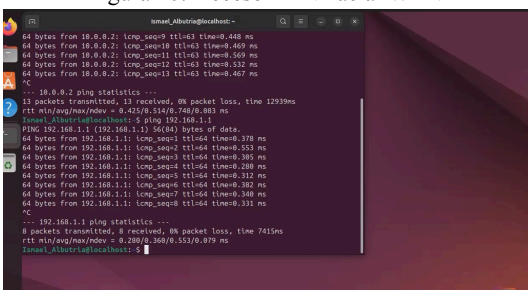
Las reglas fueron verificadas desde el módulo de tráfico interzonal de Endian, confirmando que solo los servicios autorizados estaban activos entre las zonas.

3.5 VALIDACIÓN DE CONECTIVIDAD

Se utilizaron herramientas como ip route, ping y navegadores web para validar la conectividad:

- Acceso desde Ubuntu Desktop hacia el firewall y hacia servidores en DMZ.

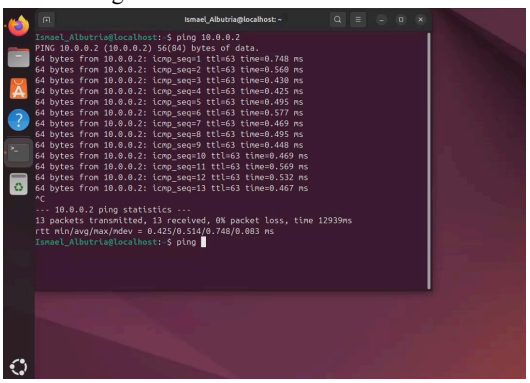
Figura 10: Acceso LAN hacia WAN



Fuente: Autoría Propia

En la figura 10 se evidencia la conectividad desde la zona verde hacia la zona roja

Figura 11: Acceso LAN hacia DMZ

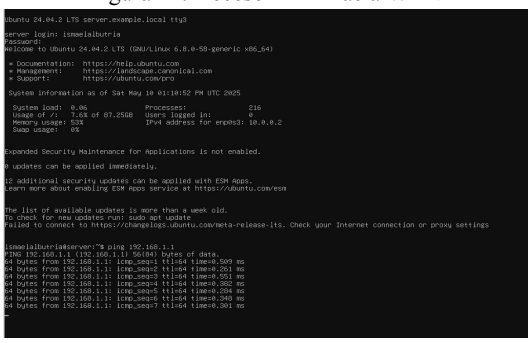


Fuente: Autoría Propia

En la figura 11 se evidencia la conectividad desde la zona verde hacia la zona naranja

- Acceso desde DMZ hacia Internet.

Figura 12: Acceso DMZ hacia WAN

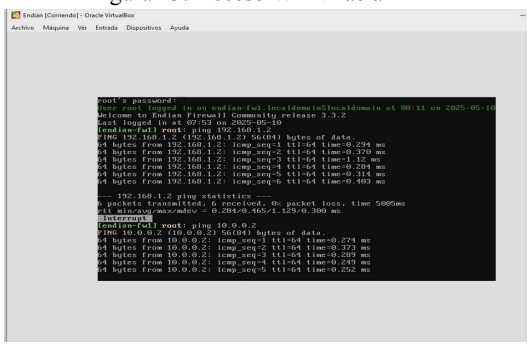


Fuente: Autoría Propia

En la figura 12 se evidencia la conectividad desde la zona naranja hacia la zona roja

- Acceso desde la red WAN simulada hacia servicios en DMZ mediante redirección de puertos.

Figura 13: Acceso WAN hacia DMZ



Fuente: Autoría Propia

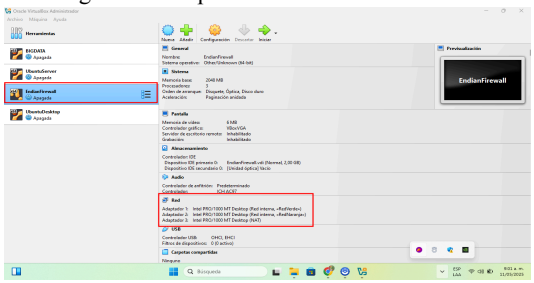
En la figura 13 se evidencia la conectividad desde la zona roja hacia la zona naranja

3.6 EVIDENCIAS DOCUMENTADAS

Se seleccionaron las capturas de pantalla más claras y representativas de cada etapa del proceso, incluyendo:

- Creación de adaptadores de red en VirtualBox

figura 14: adaptadores en Endian Firewall

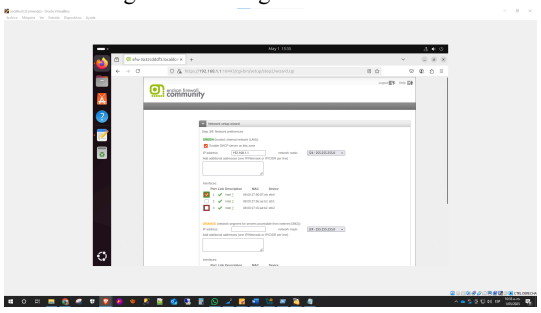


Fuente: Autoría Propia

En la figura 14 se evidencia los tres adaptadores en endian firewall

- Asignación de IPs y roles a cada interfaz

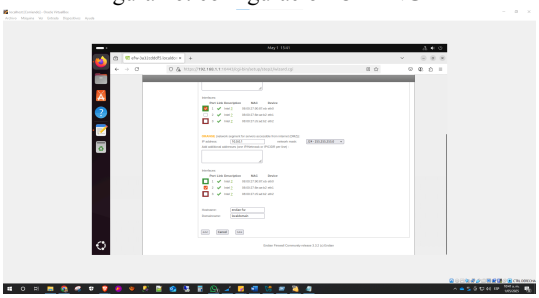
Figura 15: configuración GREEN



Fuente: Autoría Propia

En la figura 15 se evidencia la configuración de la zona Verde desde la interfaz de endian web

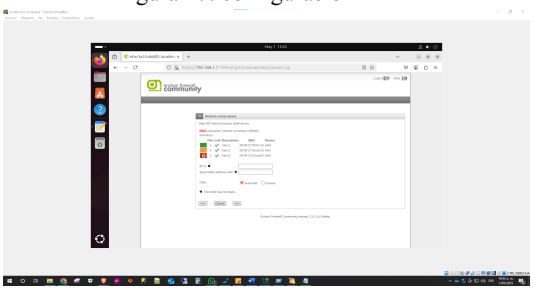
Figura 16: configuración ORANGE



Fuente: Autoría Propia

En la figura 16 se evidencia la configuración de la zona Naranja desde la interfaz de endian web

figura 17: configuración RED

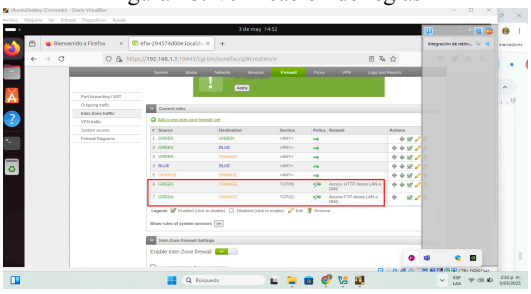


Fuente: Autoría Propia

En la figura 17 se evidencia la configuración de la zona Roja desde la interfaz de endian web

- Configuración del firewall y creación de reglas

Figura 18: Verificación de reglas

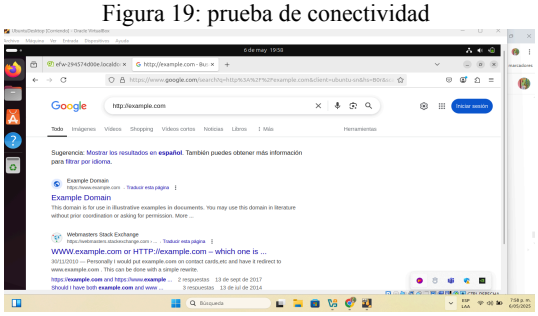


Fuente: Autoría Propia

En la figura 18 se evidencia la configuración de las diferentes reglas desde la interfaz de endian web

- Pruebas de conectividad y navegación

Figura 19: prueba de conectividad



Fuente: Autoría Propia

En la figura 19 se evidencia la conectividad desde un navegador web desde ubuntu desktop al servicio HTTP lo que evidencia el correcto funcionamiento de las reglas.

4 RESULTADOS Y PRUEBAS

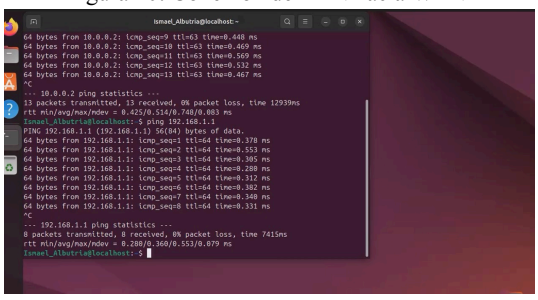
Una vez implementada la infraestructura virtual y configuradas las reglas de seguridad, se realizaron diversas pruebas para validar la comunicación entre zonas, la funcionalidad del firewall y las políticas de restricción a través del proxy HTTP. Las evidencias fueron documentadas a través de capturas de pantalla y comandos ejecutados desde terminales o navegadores.

4.1 PRUEBAS DE CONEXIÓN ENTRE ZONAS

Se validó la conectividad entre las zonas Verde (LAN), Naranja (DMZ) y Roja (WAN) mediante comandos ping, ftp y navegación web. Los resultados fueron los siguientes:

- Desde LAN (Ubuntu Desktop) hacia la WAN: Se logró acceder a sitios web públicos como example.com mediante navegador, demostrando que la configuración NAT de salida estaba activa.

Figura 20: Conexión de LAN hacia WAN

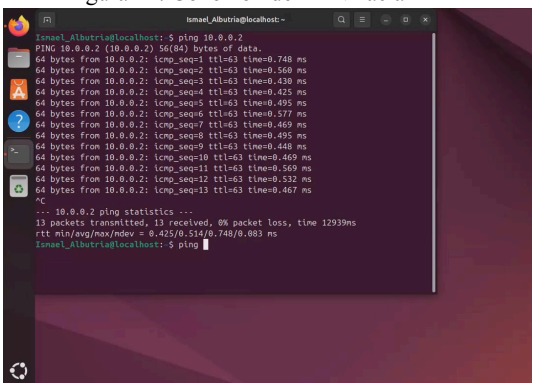


Fuente: Autoría Propia

Como se observa en la figura 20, el acceso al sitio web externo fue exitoso. Esto confirma que las reglas de salida desde la zona Verde hacia la Roja funcionan adecuadamente.

- Desde LAN hacia DMZ: Se pudo acceder al servidor web ubicado en la zona Naranja mediante el protocolo HTTP (puerto 80), lo que confirmó que las reglas de tráfico entre zonas fueron correctamente establecidas.

Figura 21: Conexión de LAN hacia DMZ

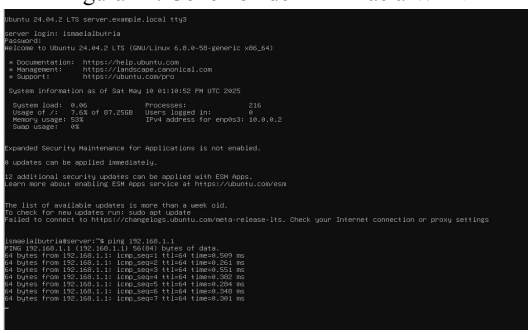


Fuente: Autoría Propia

En la figura 21 se evidencia la conectividad desde la terminal de ubuntu desktop hacia ubuntu server

- Desde DMZ hacia WAN: El servidor ubicado en la zona naranja tuvo salida a internet, verificada mediante ping y pruebas desde consola.

Figura 22: Conexión de DMZ hacia WAN

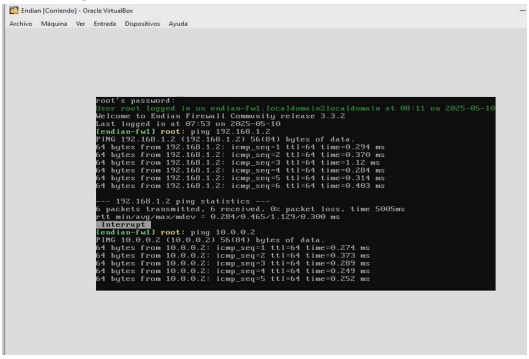


Fuente: Autoría Propia

En la figura 22 se evidencia la conectividad desde la terminal de ubuntu server hacia endian firewall

- Desde WAN hacia DMZ: Se implementó un redireccionamiento de puertos desde la IP pública simulada hacia el servidor web en DMZ, permitiendo el acceso a servicios HTTP y FTP desde la red externa.

Figura 23: Conexión de WAN hacia DMZ



Fuente: Autoría Propia

En la figura 23 se evidencia la conectividad desde la terminal de endian firewall hacia ubuntu server.

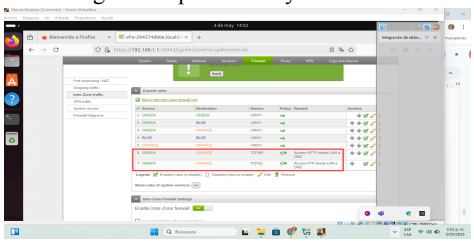
Estas pruebas aseguraron que cada zona se comunica sólo en función de las reglas explícitamente definidas, reforzando el principio de mínima exposición.

4.2 VERIFICACIÓN DEL TRÁFICO Y REGLAS APLICADAS

Se utilizaron las funciones integradas de Endian para monitorear el tráfico interzonal y validar que:

- Solo los puertos habilitados (80 y 21) se encontraban activos entre zonas.

Figura 24: puertos 80 y 21 activos

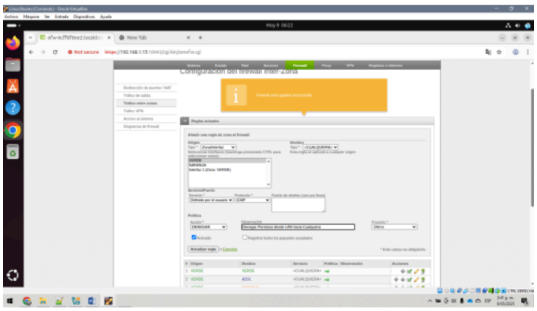


Fuente: Autoría Propia

En la figura 24 se evidencia la creación de las reglas desde la zona verde hacia la naranja utilizando los servicios HTTP y FTP

- El protocolo ICMP fue bloqueado desde DMZ y LAN, como parte de la política de denegación de ping.

Figura 25: Bloquear el tráfico ICMP



Fuente: Autoría Propia

En la figura 25 se evidencia el bloqueo del protocolo ICMP desde la zona naranja hacia la zona verde.

Las capturas de tráfico en la interfaz gráfica confirmaron que las reglas definidas fueron respetadas y aplicadas correctamente, cumpliendo así con los objetivos de seguridad y segmentación planteados en la metodología.

5 DISCUSIÓN

La implementación de un entorno de red segmentado utilizando GNU/Linux Endian en un entorno virtualizado permitió comprobar la efectividad de los principios de seguridad perimetral aplicados a redes modernas. A través de la separación lógica en zonas Verde (LAN), Roja (WAN) y Naranja (DMZ), se logró un control granular del tráfico y una gestión clara de los servicios expuestos.

Uno de los aspectos más relevantes fue la correcta aplicación de reglas de firewall interzonales, las cuales demostraron que es posible permitir o denegar tráfico entre redes según protocolos específicos, como HTTP y FTP, garantizando la mínima exposición de los recursos internos. Además, se evidenció que el uso de NAT permite que los clientes internos accedan a internet sin necesidad de direcciones públicas, sin comprometer la estructura de red interna.

Durante las pruebas, se enfrentaron desafíos relacionados con la configuración de adaptadores en VirtualBox y la correcta asignación de direcciones IP estáticas dentro de cada zona. No obstante, dichas dificultades fueron superadas mediante el análisis sistemático de rutas, diagnósticos con comandos de red (ip route, ping, ftp) y la reconfiguración de interfaces a nivel del sistema.

En términos pedagógicos, este ejercicio evidenció el valor de utilizar entornos virtuales para el aprendizaje de conceptos avanzados de seguridad informática. La posibilidad de replicar infraestructuras reales en un entorno controlado permite que los estudiantes no solo comprendan los fundamentos teóricos, sino que también desarrollen competencias prácticas aplicables en entornos corporativos.

6 CONCLUSIONES

La implementación de una arquitectura de red virtualizada utilizando GNU/Linux Endian permitió demostrar de manera práctica los principios fundamentales de la seguridad perimetral en redes informáticas. Mediante la segmentación lógica en zonas LAN, WAN y DMZ, se garantizó el aislamiento de servicios y el control del tráfico entre zonas con base en políticas personalizadas de firewall.

El uso de reglas de acceso interzonales, junto con la traducción de direcciones (NAT), evidenció la capacidad de Endian para gestionar tanto el acceso interno como externo de manera segura. Las pruebas de conectividad, navegación HTTP y uso de servicios FTP confirmaron la funcionalidad esperada y la correcta aplicación de las políticas configuradas.

Finalmente, este ejercicio práctico permitió consolidar conocimientos sobre redes, firewalls, NAT, servicios de proxy y virtualización, al tiempo que fortaleció las competencias técnicas necesarias para el diseño y despliegue de infraestructuras seguras en escenarios reales.

Como trabajo futuro, se sugiere automatizar la gestión de reglas mediante scripts o integrar soluciones de monitoreo que alerten sobre intentos de acceso no autorizados entre zonas.

7 REFERENCIAS

[1] Linux Professional Institute, LPI LPIC-1 Exam 101, Tema 102: Comandos GNU y Unix, 2022. [En línea]. Disponible en: https://learning.lpi.org/es/learning-materials/101-500/102/

[2] Canonical, Guía del Ubuntu Desktop 20.04 LTS, Ubuntu Help, 2023. [En línea]. Disponible en: https://help.ubuntu.com/20.04/ubuntu-help/index.html

[3] Debian, El manual del administrador de Debian 12.5.0, Proyecto Debian, 2023. [En línea]. Disponible en: https://www.debian.org/releases/stable/amd64/index.es.html

[4] Oracle Corporation, Manual del usuario VirtualBox, 2020. [En línea]. Disponible en: https://www.virtualbox.org/manual/

[5] Endian SRL, Endian UTM 3.2 - Manual de referencia, 2016. [En línea]. Disponible en: http://docs.endian.com/3.2/utm/index.html

[6] ACM SIGCOMM. Mogul, L., Ricci, R., Hibler, M., Lepreau, J., y Sharafuddin, E. "Virtualization support for network experiments", ACM SIGCOMM Comput. Commun. Rev., vol. 50, no. 4, pp. 67–74, Oct. 2020.

[7] ACM. Mogul, J. C., McKeown, N., y Shenker, S. "Virtualizing network functions in the cloud", Commun. ACM, vol. 63, no. 4, pp. 56–63, Abr. 2020.

[8] Oracle, VirtualBox User Manual, 2023. [En línea]. Disponible en: https://www.virtualbox.org/manual/

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

[10] Pearson. Stallings, W. Network Security Essentials: Applications and Standards, 6.ª ed. Pearson, 2021.

[11] O'Reilly Media. Zwicky, E. D., Cooper, S., y Chapman, D. B. Building Internet Firewalls, 2.ª ed. O'Reilly Media, 2000.

[12] Wiley. Perkins, C. IP Addressing and Subnetting Including IPv6. Wiley, 2018.

[13] Squid Proxy, Squid Proxy Documentation, 2022. [En línea]. Disponible en: http://www.squid-cache.org/Doc/

.