TÍTULO “Implementación de Seguridad y Control de acceso mediante Endian Firewall en un Entorno de Virtualización”

Integrante 1 (Miguel Ángel Beltrán Silva)
e-mail: mabeltransil@unadvirtual.edu.co
Integrante 2 (Jesus Alfredo Chaves Rivera)
e-mail: jachavesr@unadvirtual.edu.co
Integrante 3 (Deisy Johana Sanabria González)
e-mail: djsanabria@unadvirtual.edu.co
Integrante 4 (Julián Eduardo Carrillo Bastos)
e-mail: jecarrilloba@unadvirtual.edu.co

RESUMEN: *La segmentación de redes mediante el firewall Endian Community Edition en entornos virtualizados constituye una estrategia versátil y eficaz para la administración segura en laboratorios y escenarios corporativos. Este artículo describe una experiencia guiada de implementación multinivel sobre Oracle VirtualBox, detallando la configuración de zonas LAN (verde), DMZ (naranja) y WAN (roja), así como la integración de autenticación, proxy HTTP y reglas NAT. Se incluyen resultados de pruebas funcionales y análisis crítico del control de tráfico y acceso entre zonas. Los hallazgos evidencian que la virtualización permite simular entornos reales de seguridad, optimizando el aprendizaje aplicado y la robustez de la infraestructura TI en sectores académico y empresarial.*

PALABRAS CLAVE: autenticación, Endian, firewall, GNU/Linux, proxy, segmentación de red, VirtualBox.

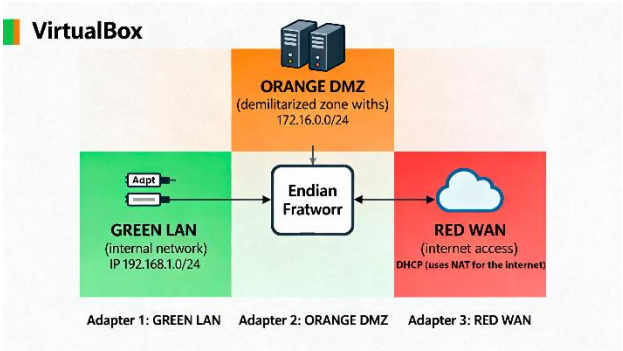
1 INTRODUCCIÓN

La seguridad y administración efectiva en redes virtualizadas son fundamentos esenciales en la formación de administradores de sistemas y en ambientes corporativos modernos. Esta investigación práctica utiliza GNU/Linux Endian y máquinas Ubuntu en VirtualBox, abordando la segmentación en zonas, el control del tráfico mediante reglas NAT y proxy, y la monitorización de resultados concretos para fortalecer la formación aplicada y la adopción de mejores prácticas en el campo de la ciberseguridad.

2 DISEÑO DE LA TOPOLOGÍA Y CONFIGURACIÓN DE ZONAS

El diseño de la topología y la configuración de zonas es el pilar fundamental para garantizar un entorno seguro, eficiente y flexible en redes virtualizadas. Al planificar y estructurar cuidadosamente la distribución de las zonas LAN, DMZ y WAN sobre una plataforma como VirtualBox, se optimiza la segmentación del tráfico, el control de accesos y la respuesta ante incidentes. Esta organización estratégica no solo facilita la administración de recursos y servicios, sino que también permite la aplicación precisa de políticas de seguridad, maximizando la resiliencia de la infraestructura y elevando los estándares profesionales en la gestión de sistemas GNU/Linux.

Figura 1. Topología de red virtual con Endian Firewall en VirtualBox: Segmentación en zonas GREEN LAN, ORANGE DMZ y RED WAN



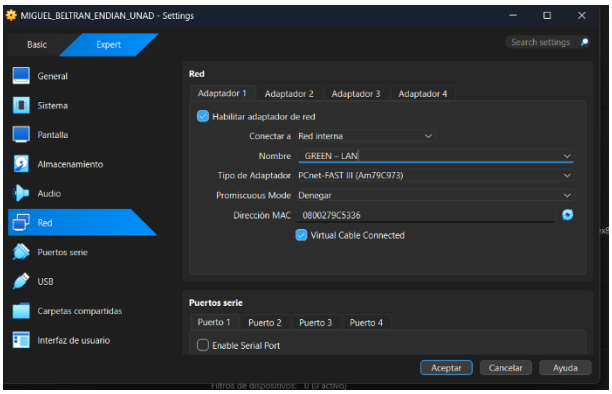
Fuente: Autoría Propia

2.1 DEFINICIÓN DE ZONAS: VERDE, NARANJA Y ROJA

La segmentación de la red mediante la definición de zonas diferenciadas permite una administración granular de los flujos y riesgos de la infraestructura virtualizada. Cada segmento cumple un rol esencial y está dotado de controles específicos para satisfacer los requerimientos de seguridad y disponibilidad.

Zona Verde (LAN): Este segmento representa el núcleo seguro de la organización. Es la red donde residen los usuarios finales, estaciones de trabajo y sistemas administrativos críticos. En la LAN, se implementan políticas de acceso restringidas y medidas de protección avanzada, como autenticación robusta y filtrado de tráfico saliente. El diseño persigue proteger la confidencialidad de la información y garantizar la integridad de los recursos internos, permitiendo únicamente las conexiones necesarias hacia el exterior a través del firewall y los servicios autorizados. Esta zona es monitoreada constantemente para detectar comportamientos anómalos y prevenir brechas de seguridad que pudieran comprometer los activos misionales de la entidad.

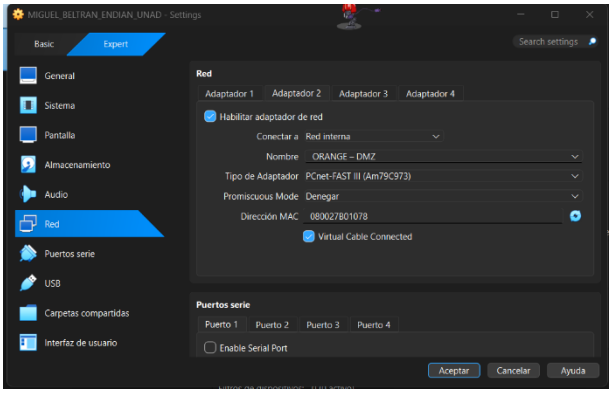
Figura 2. Configuración del adaptador de red para la Zona Verde (LAN) en Oracle VM VirtualBox



Fuente: Autoría Propia

Zona Naranja (DMZ): Esta área se encuentra deliberadamente separada tanto de la LAN interna como del acceso directo a Internet. Está reservada para los servidores cuyos contenidos deben ser accesibles desde el exterior, como páginas web institucionales, servidores de correo o aplicaciones públicas. La DMZ actúa como una zona tampón: cualquier intento de ataque proveniente de la WAN impactará primero en este entorno controlado, minimizando la exposición del resto de la red. Además, se aplican controles de tráfico cruzado y se limitan las comunicaciones desde la DMZ hacia la LAN, protegiendo los recursos internos incluso si un servidor público llegara a ser vulnerado.

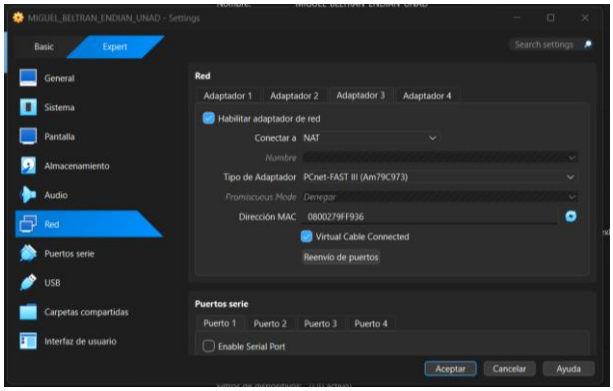
Figura 3. Configuración del adaptador de red para la Zona Naranja (DMZ) en Oracle VM VirtualBox



Fuente: Autoría Propia

Zona Roja (WAN): Funcionando como punto de frontera con el mundo exterior, la WAN es la interfaz que conecta la infraestructura local con Internet. Aquí se gestionan tanto el tráfico de salida legítimo de los usuarios, como las conexiones entrantes autorizadas hacia los servicios ubicados en la DMZ. Todos los flujos pasan primero por políticas de seguridad que incluyen reglas de firewall, NAT y registros de auditoría. Así se mitigan ataques externos y se preserva la disponibilidad y estabilidad de los servicios esenciales de la organización.

Figura 4. Configuración del adaptador de red en modo NAT para la Zona Roja (WAN) en Oracle VM VirtualBox

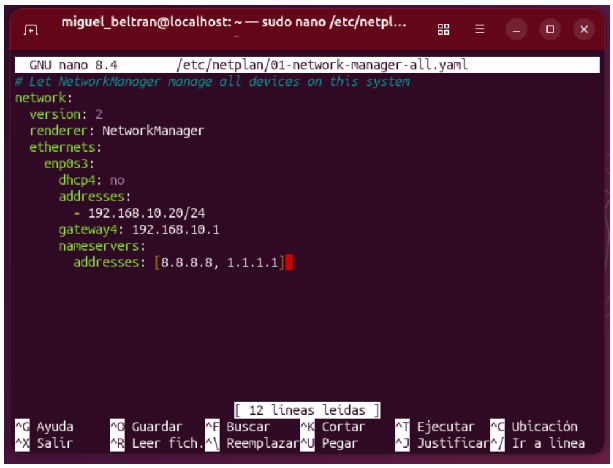


Fuente: Autoría Propia

2.2 CONFIGURACIÓN DE ADAPTADORES Y ASIGNACIÓN DE IPS

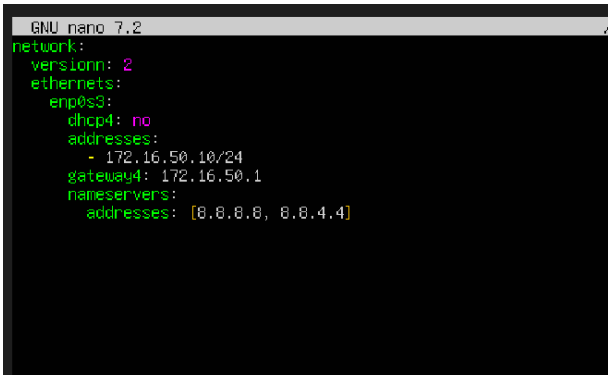
Cada zona se implementa como un adaptador de red virtual diferente en VirtualBox. La Zona Verde y la DMZ utilizan “Red Interna” con rangos de IP 192.168.10.0/24 y 172.16.50.0/24 respectivamente, mientras la WAN utiliza NAT para simular acceso a Internet. La configuración manual de direcciones IP en cada máquina es esencial para garantizar el enrutamiento correcto y la segmentación.

Figura 5. Configuración de la dirección IP estática en Ubuntu Desktop Zona Verde.



Fuente: Autoría Propia

Figura 6. Configuración de red en Ubuntu Server ubicado en la zona DMZ.



Fuente: Autoría Propia

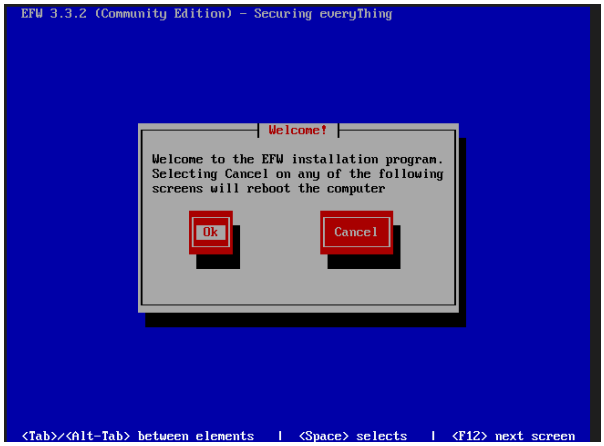
3 IMPLEMENTACIÓN Y AJUSTES DE SEGURIDAD

La implementación y ajustes de seguridad en el entorno virtualizado con Endian Firewall sobre VirtualBox requieren un enfoque metódico y profesional. Primero, se instala la solución Endian en una máquina virtual, configurando cuidadosamente los adaptadores de red para definir las zonas: GREEN (LAN), ORANGE (DMZ) y RED (WAN). Posteriormente, se asignan direcciones IP adecuadas a cada interfaz, asegurando la segmentación lógica y el aislamiento entre áreas críticas de la red. Se configuran reglas de firewall estrictas, políticas de traducción de direcciones (NAT), y, cuando es necesario, servicios de proxy autenticado. Estos parámetros permiten controlar y monitorear el tráfico, proteger los servicios expuestos en la DMZ y garantizar que el acceso a Internet desde la LAN cumpla con los requisitos de seguridad y trazabilidad que demanda una infraestructura moderna y robusta.

3.1 INSTALACIÓN DE ENDIAN Y ASIGNACIÓN DE INTERFAZ

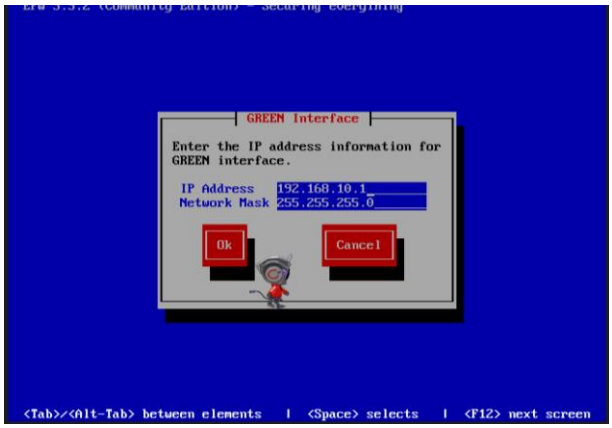
La instalación de Endian inicia con la selección minuciosa del idioma y el proceso de particionamiento del disco, asegurando una base adecuada para el sistema. Seguidamente, se realiza la asignación precisa de cada adaptador de red a las interfaces GREEN, ORANGE y RED, lo que permite segmentar eficazmente el tráfico y garantizar el aislamiento entre zonas. Una vez culminada la instalación, toda la gestión y administración se lleva a cabo de forma segura a través de una interfaz web protegida, facilitando el control centralizado y avanzado de las políticas de seguridad y servicios en la infraestructura virtual.

Figura 7. Pantalla de bienvenida al instalador de Endian Firewall.



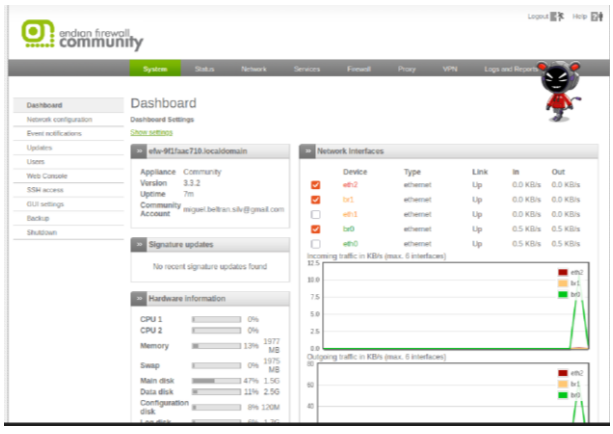
Fuente: Autoría Propia

Figura 8. Asignación de dirección IP para la interfaz GREEN durante la instalación de Endian Firewall



Fuente: Autoría Propia

Figura 9. Acceso inicial al panel de administración de Endian Firewall Community

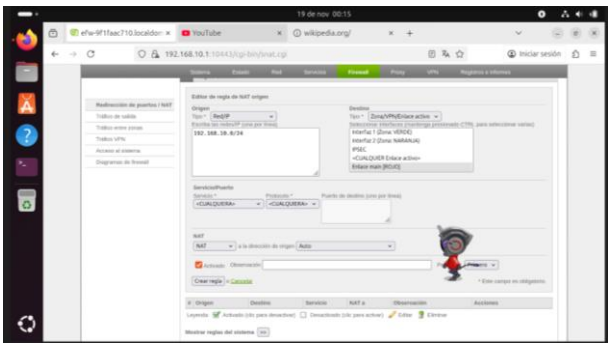


Fuente: Autoría Propia

3.2 NORMATIVA DE REGLAS NAT Y PROXY

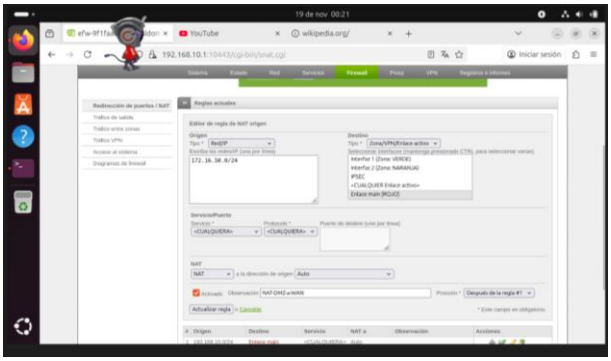
Tras la configuración básica, se implementan reglas NAT que habilitan la comunicación saliente desde la LAN y la DMZ hacia la red externa, pero restringen el acceso entrante, excepto para servicios explícitamente autorizados, como HTTP o FTP en la DMZ. El proxy HTTP no transparente obliga la autenticación de usuarios y permite la aplicación de políticas de filtrado a través de listas negras, restringiendo dominios y servicios según requerimientos institucionales o empresariales.

Figura 10. Configuración de la regla NAT para permitir la comunicación desde la red LAN hacia la zona WAN en Endian Firewall



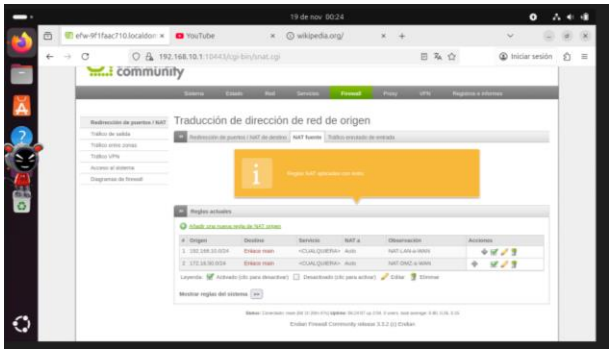
Fuente: Autoría Propia

Figura 11. Actualización de regla NAT para permitir la comunicación desde la zona DMZ hacia la WAN.



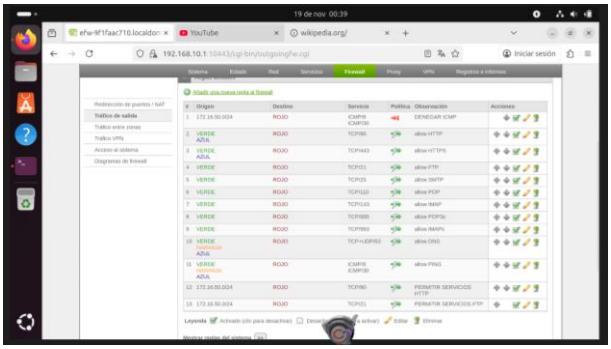
Fuente: Autoría Propia

Figura 11. Aplicación de reglas NAT en Endian para la comunicación desde LAN y DMZ hacia la red WAN



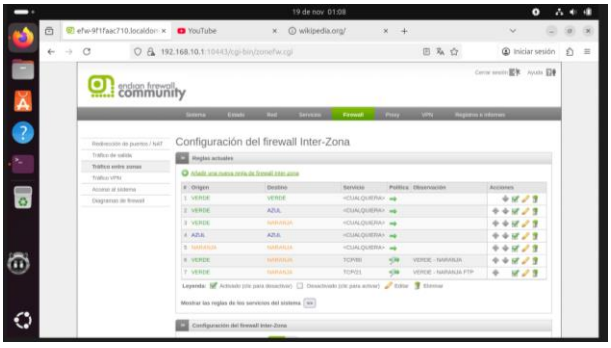
Fuente: Autoría Propia

Figura 12. Políticas que regulan servicios como HTTP, HTTPS, FTP, SMTP, ICMP, necesarios para la comunicación entre las zonas Verde, Roja y Naranja.



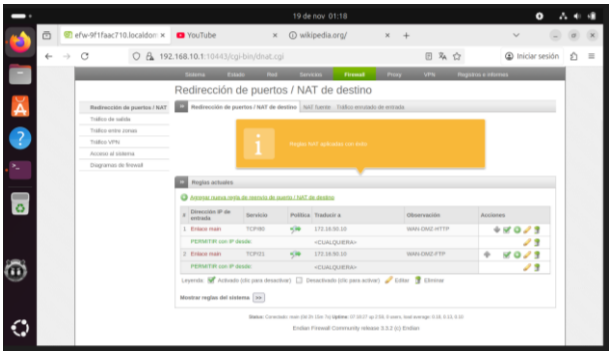
Fuente: Autoría Propia

Figura 12. Reglas Inter-Zona aplicadas en Endian Firewall



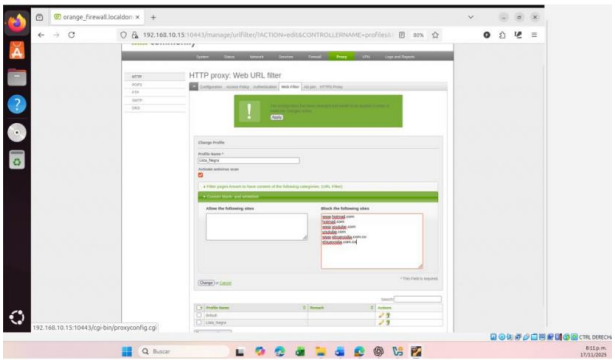
Fuente: Autoría Propia

Figura 13. Visualización y administración de reglas de redirección de puertos NAT en Endian Firewall



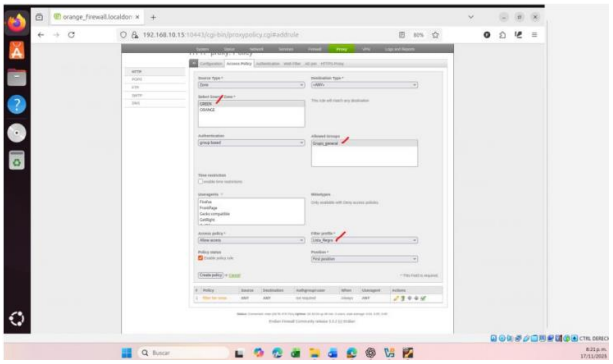
Fuente: Autoría Propia

Figura 14. Creación y gestión de perfil de lista negra en el proxy HTTP para filtrado de URL web



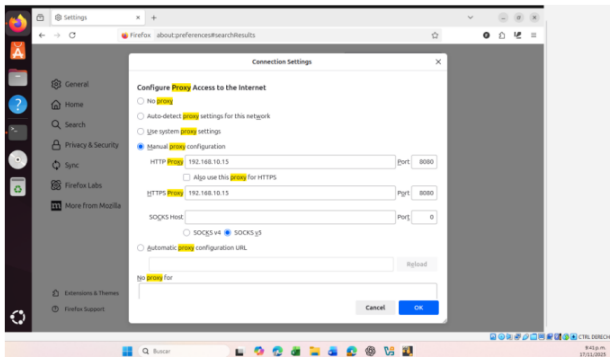
Fuente: Autoría Propia

Figura 15. Configuración de política de acceso y filtrado en el proxy HTTP de Endian Firewall



Fuente: Autoría Propia

Figura 16. Configuración manual de proxy de red en Ubuntu para acceso HTTP

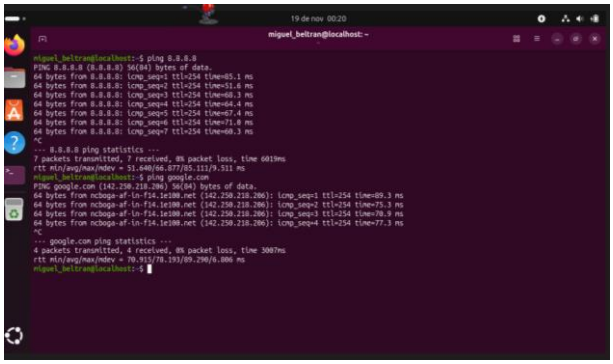


Fuente: Autoría Propia

4 RESULTADOS DE LAS PRUEBAS FUNCIONALES Y VALIDACIÓN DE POLÍTICAS

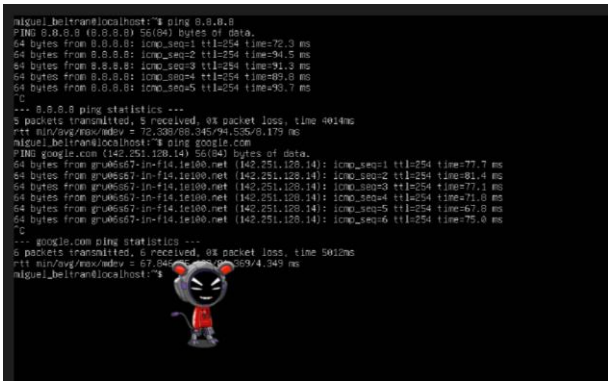
Los resultados de las pruebas funcionales y la validación de políticas evidenciaron la correcta segmentación y gestión de los flujos de red, verificando que las reglas y controles implementados con Endian Firewall cumplen los objetivos de seguridad establecidos. Las pruebas de conectividad confirmaron el aislamiento entre zonas y el acceso seguro a los servicios permitidos, mientras que los mecanismos de bloqueo demostraron ser efectivos en la restricción de tráfico no autorizado. De este modo, se validó la eficacia de la configuración y se reforzó la confianza en la operatividad y robustez de la solución desplegada.

Figura 16. Verificación de conectividad desde la máquina cliente Ubuntu Desktop hacia la WAN utilizando comandos ICMP



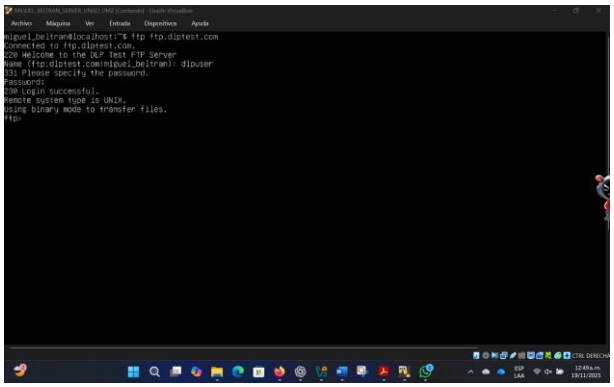
Fuente: Autoría Propia

Figura 17. Comprobación de conectividad desde el servidor ubicado en la DMZ hacia la WAN tras la aplicación de reglas NAT



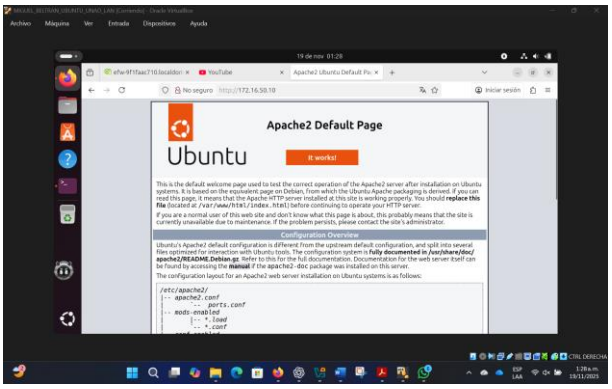
Fuente: Autoría Propia

Figura 18. Prueba de conexión FTP desde la máquina Ubuntu Server en la zona DMZ.



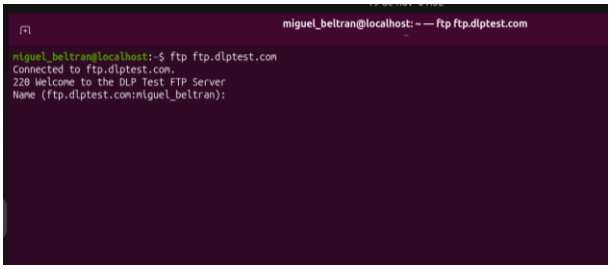
Fuente: Autoría Propia

Figura 19. Prueba validación del acceso HTTP a través de Apache2 desde distintas zonas de red en entorno virtualizado



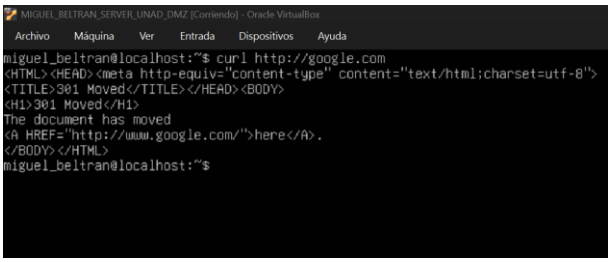
Fuente: Autoría Propia

Figura 20 Prueba de conexión al servicio FTP externo desde terminal Ubuntu en entorno virtualizado



Fuente: Autoría Propia

Figura 21 Prueba de acceso HTTP a sitio externo mediante consola en servidor Ubuntu virtualizado

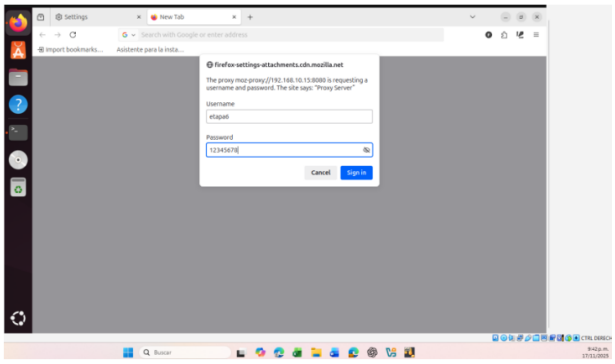


Fuente: Autoría Propia

4.1 PRUEBAS DE CONECTIVIDAD Y AUTENTICACIÓN

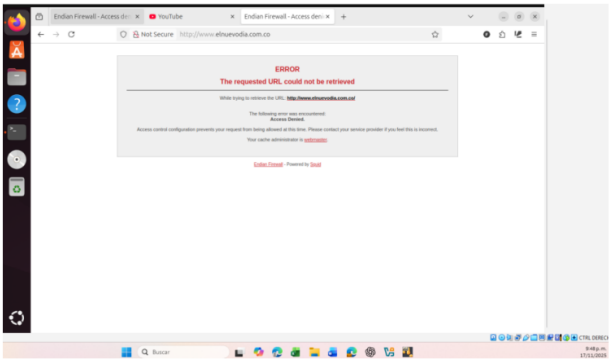
Se realizaron pruebas de conectividad desde clientes Ubuntu en la LAN y servidores en la DMZ hacia servicios internos y externos, validando la correcta operatividad del NAT, el proxy y la autenticación. Los intentos de navegación hacia dominios restringidos fueron denegados, mientras el acceso a sitios permitidos dependió de la autenticación previa y la membresía en los grupos configurados en Endian.

Figura 22 Solicitud de autenticación por proxy HTTP ante acceso web en cliente Ubuntu



Fuente: Autoría Propia

Figura 23. Bloqueo de acceso web por lista negra personalizada en proxy HTTP



Fuente: Autoría Propia

4.2 CONTROL DE TRÁFICO Y SEGMENTACIÓN EFECTIVA

Las reglas de firewall permitieron bloquear protocolos como ICMP y limitar el acceso entre zonas, exceptuando servicios específicos habilitados para transferencia de archivos o web. Se verificó que los servicios en la DMZ quedaran a la vez expuestos y protegidos por políticas estrictas, un requerimiento típico en arquitecturas empresariales modernas.

4.3 EVALUACIÓN DEL CUMPLIMIENTO Y ROBUSTEZ

Las pruebas demostraron un cumplimiento íntegro de las políticas de segmentación y acceso, sin filtraciones entre zonas no autorizadas. Esto respalda el enfoque de virtualización con Endian para proyectos académicos y simulaciones empresariales, permitiendo un control exhaustivo sin comprometer la usabilidad.

5 Conclusiones.

La implementación precisa de tarjetas de red en VirtualBox y la instalación efectiva de Endian permitieron segmentar funcionalmente el entorno en tres zonas —verde, roja y naranja—, facilitando el control granular del tráfico y la administración de servicios críticos en una infraestructura virtualizada robusta.

La creación y validación de reglas NAT aseguraron la correcta traducción de direcciones, permitiendo la comunicación fluida entre la LAN y la WAN, así como entre la zona DMZ y el acceso a Internet. Esta configuración fue fundamental para garantizar la conectividad y el direccionamiento seguro de los servicios en el entorno simulado.

La habilitación específica de servicios HTTP y FTP desde la DMZ, junto con la restricción del protocolo ICMP, demostró la capacidad de control efectivo sobre los servicios expuestos. La verificación mediante pruebas en consola confirmó la robustez de las políticas para proteger y administrar el tráfico según los requerimientos de seguridad.

El establecimiento de reglas precisas para permitir o denegar tráfico entre zonas logró una segmentación funcional eficiente. Las pruebas de navegación y acceso a servicios desde diferentes segmentos de la red confirmaron la operatividad y pertinencia de la configuración, evidenciando aislamiento, selectividad y cumplimiento de políticas diseñadas.

La implementación de un proxy HTTP no transparente con políticas de autenticación y bloqueo selectivo de sitios sentó las bases para un control avanzado sobre el acceso a recursos externos. La creación de perfiles, listas negras y usuarios representó una solución flexible y segura, alineada con las mejores prácticas de gestión de navegación corporativa y académica.

La implementación de Endian Firewall permitió construir una infraestructura segmentada en zonas Verde, Naranja y Roja, garantizando seguridad perimetral y control granular del tráfico.

Las pruebas realizadas demostraron:
Correcto funcionamiento de reglas HTTP y FTP en ambas direcciones. Funcionamiento del aislamiento de zonas DMZ. Bloqueo efectivo de ICMP. Validación funcional mediante herramientas curl, ping y ftp.

6 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. Debian. https://www.debian.org/releases/stable/amd64/index.es.html

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

[4] Kifarunix, “Install and configure Endian Firewall on VirtualBox,” kifarunix.com, May 21, 2019. [Online]. Available: https://kifarunix.com/install-and-configure-endian-firewall-on-virtualbox/. [Accessed: May 7, 2025].

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

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

[7] Endian, “Endian Firewall Community – free open source security for home users,” Endian.com. [Online]. Available: https://www.endian.com/en/community/. [Accessed: May 7, 2025].