# Implementación de un Laboratorio Virtual para la Simulación de Arquitectura de Seguridad Empresarial: Caso de Uso con Endian Firewall en Entorno VirtualBox.

Alexander Rodriguez Leiva
e-mail: al80rod361@unadvirtual.edu.co
Carlos Andres Guevara Ordoñez
e-mail: caguevarao@unadvirtual.edu.co
Edicson Andres Sativa Avendaño
e-mail: easativaa@unadvirtual.edu.co
Luis Carlos Castañeda Suarez
e-mail: lccastanedas@unadvirtual.edu.co
Sebastian Soto Tintinago
e-mail: ssotot@unadvirtual.edu.co

**RESUMEN:** *La formación en ciberseguridad y administración de redes requiere entornos controlados que permitan validar configuraciones de seguridad perimetral sin comprometer infraestructuras productivas. Este artículo presenta el diseño e implementación de un laboratorio virtual basado en Endian Firewall Community y VirtualBox para simular una arquitectura de red segmentada en zonas LAN, DMZ y WAN. Sobre este entorno se desarrollaron cinco temáticas: configuración de interfaces y zonas de seguridad, reglas NAT, habilitación controlada de servicios en la DMZ, políticas de acceso inter-zona y proxy HTTP no transparente con autenticación y filtrado de contenido. La validación se realizó mediante pruebas de conectividad, revisión de reglas, verificación de servicios y análisis de registros. Los resultados evidencian que el laboratorio permite reproducir escenarios funcionales de seguridad perimetral, constituyéndose en una alternativa de bajo costo y basada en software libre para fortalecer competencias prácticas en redes y ciberseguridad.*

**PALABRAS CLAVE**: Endian Firewall, laboratorio virtual, seguridad de redes, firewall perimetral, NAT, DMZ, proxy HTTP, VirtualBox, educación en ciberseguridad, simulación de redes empresariales.

## 1 INTRODUCCIÓN

La enseñanza de la seguridad perimetral exige escenarios de práctica que permitan configurar, probar y auditar controles de red sin afectar entornos reales de producción. En este contexto, los laboratorios virtuales representan una alternativa eficiente para la formación técnica, ya que facilitan la simulación de arquitecturas empresariales mediante herramientas de virtualización y plataformas de seguridad de código abierto.

El presente trabajo documenta la implementación de un laboratorio virtual orientado a la simulación de una arquitectura de red segmentada en tres zonas de seguridad: LAN, DMZ y WAN, utilizando Endian Firewall Community como plataforma central de control. Sobre esta infraestructura se desarrollaron cinco temáticas relacionadas con configuración de interfaces, traducción de direcciones de red, publicación controlada de servicios, reglas de acceso inter-zona y despliegue de un proxy autenticado con filtrado de contenido.

El objetivo general del artículo es documentar el diseño, implementación y validación funcional de un laboratorio virtual de seguridad perimetral, con el fin de demostrar la viabilidad de Endian Firewall como herramienta académica para la enseñanza de conceptos de segmentación, filtrado y control de tráfico. De manera específica, se buscó configurar la arquitectura de red, validar el uso de reglas NAT, exponer servicios en la DMZ bajo criterios de seguridad, establecer políticas de comunicación entre zonas y controlar la navegación web mediante autenticación y listas de restricción.

La relevancia de este trabajo radica en que ofrece una metodología reproducible, de bajo costo y apoyada en software libre, adecuada para procesos de formación en administración de redes y ciberseguridad. Además, las pruebas realizadas permiten evidenciar el comportamiento del sistema ante diferentes escenarios de conectividad y control de acceso, fortaleciendo la dimensión práctica del aprendizaje

.

## 2 TRABAJOS RELACIONADOS

La implementación de laboratorios virtuales para la enseñanza de ciberseguridad ha demostrado mejorar significativamente la adquisición de competencias prácticas en estudiantes, al proporcionar entornos seguros para experimentar con herramientas profesionales como Nmap y Nessus sin riesgos operativos [7]. Plataformas de virtualización como VirtualBox facilitan el despliegue de topologías de red complejas sobre hardware convencional, reduciendo barreras de costo y accesibilidad en contextos académicos [12].

En cuanto a soluciones de seguridad perimetral de código abierto, proyectos como OPNsense [8] y pfSense [9] han sido ampliamente documentados y comparados en términos de rendimiento y características de gestión [13]. No obstante, Endian Firewall Community representa una alternativa menos explorada en la literatura educativa, a pesar de ofrecer funcionalidades UTM integradas (firewall, proxy, filtrado de contenido, VPN) en una distribución Linux unificada [3] [4]. Si bien existen guías técnicas para la instalación de Endian [14], se identifica una brecha en trabajos que documenten de forma integral su aplicación pedagógica: desde la configuración de zonas de seguridad (LAN/DMZ/WAN) hasta la validación empírica de políticas de tráfico y control de navegación. Este

artículo contribuye a cerrar dicha brecha mediante un caso de uso reproducible, con evidencia funcional de cada etapa de implementación.

# 3 METODOLOGÌA Y ARQUITECTURA DEL SISTEMA

## 3.1 ENFOQUE METODOLÓGICO

La investigación desarrollada corresponde a un estudio aplicado con enfoque práctico y validación funcional, orientado al diseño e implementación de un laboratorio virtual para la simulación de una arquitectura de seguridad perimetral. El método de trabajo consistió en un estudio de caso experimental, en el cual se configuró un escenario controlado y posteriormente se verificó el comportamiento de cada uno de sus componentes mediante pruebas técnicas y análisis de resultados.

El procedimiento se estructuró en cinco fases:

1. Diseño de la topología de red y definición del direccionamiento IP.
2. Despliegue de las máquinas virtuales y configuración de interfaces.
3. Implementación progresiva de las cinco temáticas planteadas en la guía.
4. Ejecución de pruebas de validación funcional desde consola y navegador.
5. Registro de evidencias, análisis de resultados y consolidación de la documentación técnica.

Este enfoque permitió no solo implementar la solución propuesta, sino también comprobar su funcionamiento en condiciones controladas, garantizando trazabilidad en cada una de las configuraciones realizadas

## 3.2 ARQUITECTURA DE RED SIMULADA

**Tabla 1** *Componentes*

| Componente | Sistema Operativo | Interfaces de red | Dirección IP / Configuración |
|---|---|---|---|
| Firewall | Endian Firewall 3.3.2 x64 | ETH0 (LAN/Verde), ETH1 (DMZ/Naranja), ETH2 (WAN/Roja) | ETH0: 192.168.2.15/27, ETH1: 192.168.1.15/27, ETH2: DHCP (WAN simulada) |
| Servidor Web (DMZ) | Ubuntu Server 20.04.6 x64 | 1 interfaz (conectada a DMZ) | 192.168.1.20/27 |
| Cliente (LAN) | Linux Mint 22.3 x64 | 1 interfaz (conectada a LAN) | 192.168.2.20/27 |
| Hypervisor | VirtualBox 7.x | Adaptadores internos + NAT | Redes internas: LAN_Int, DMZ_Int; WAN: modo NAT |

Fuente: Autoría propia

- **Zonas de Seguridad:**

🔴 Zona Roja (WAN): Simula Internet (acceso mediante NAT del hypervisor).
🟢 Zona Verde (LAN): Red interna de usuarios finales (192.168.2.0/27).
🟠 Zona Naranja (DMZ): Red de servidores públicos (192.168.1.0/27).

## 3.3 HERRAMIENTAS Y REQUISITOS

- Software: VirtualBox, Endian Firewall ISO, imágenes Ubuntu Server y Linux Mint.
- Hardware mínimo recomendado: 4 GB RAM, 2 núcleos CPU, 50 GB almacenamiento.
- Servicios para desplegar en Ubuntu Server: Apache2 (HTTP), vsftpd (FTP).

# 4 DESARROLLO DEL CASO DE USO: IMPLEMENTACIÓN POR TEMATICAS

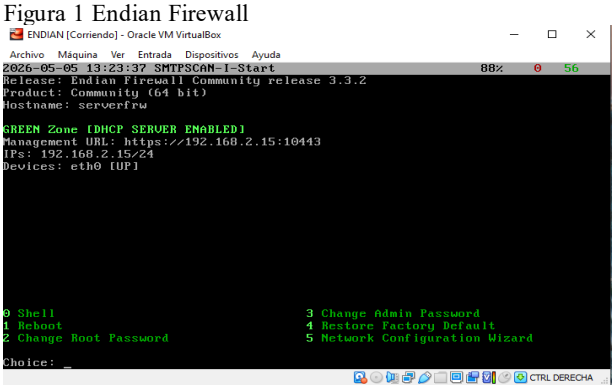
## 4.1 TEMÁTICA 1: CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX (TARJETAS DE RED) E INSTALACIÓN EFECTIVA DEL MISMO

Para la instalación de Endian Firewall, se requiere el uso de VirtualBox como herramienta de virtualización para la creación de la máquina virtual. Asimismo, es necesario contar con la imagen ISO de Endian, la cual se descarga desde el sitio oficial y se monta en la máquina.

Una vez configurada, se inicia el proceso de instalación del sistema operativo. Durante este proceso, se selecciona el idioma y se continúa con la detección de los discos disponibles. Posteriormente, se confirma la instalación y se da inicio al proceso de división de discos.

Finalizada la partición, se procede con la configuración de la interfaz de red verde según los parámetros establecidos. Con esto, se completa la instalación del sistema, quedando Endian Firewall listo para su uso.

Figura 1 Endian Firewall



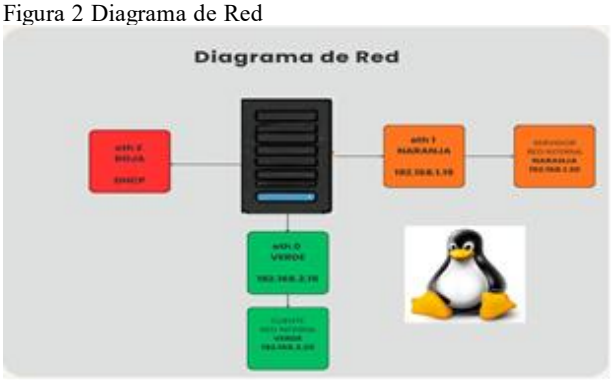

Fuente: Autoría Propia

Configuración de la instancia para GNU/Linux Endian en Virtualbox (tarjetas de red) e instalación efectiva del mismo.

Producto esperado: 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).

Diagrama de red: Se evidencia la configuración de los tres adaptadores correspondientes a las zonas roja, verde y naranja:

Figura 2 Diagrama de Red




Fuente: Autoría Propia

Para el desarrollo de esta temática, inicialmente se realiza la creación de una máquina virtual de Endian Firewall en VirtualBox, a la cual se le configuran tres adaptadores de red.

El **primer adaptador** se establece en modo **red interna**, asignándole la denominación de **red verde (LAN)**, destinada a la conexión del cliente.

El **segundo adaptador** también se configura en modo **red interna**, denominado **red naranja (DMZ)**, orientado a la conexión del servidor.

Finalmente, el **tercer adaptador** se configura en modo **NAT**, correspondiente a la **red roja (WAN)**, que proporciona la salida y conexión a Internet.

Figura 3. Adaptadores de Red

Fuente: Autoría Propia

Se accede a la interfaz gráfica de Endian Firewall a través de la dirección IP 192.168.2.15, donde se verifica que la red verde se encuentra correctamente configurada. A continuación, se procede con la configuración de la red naranja**,** asignándole la dirección IP 192.168.1.15. Para ello, se selecciona el segundo adaptador de red y se realiza la asignación correspondiente del nombre de host.

Figura 4. Configuración Red Naranja

Fuente: Autoría Propia

Posteriormente, se evidencia la correcta configuración de los tres segmentos de red, reflejados como activos y en línea dentro del entorno de Endian Firewall. Cada uno de los adaptadores cumple su función específica: la red verde permite la comunicación del cliente, la red naranja permite los servicios del servidor, y la red roja garantiza la conectividad hacia Internet.

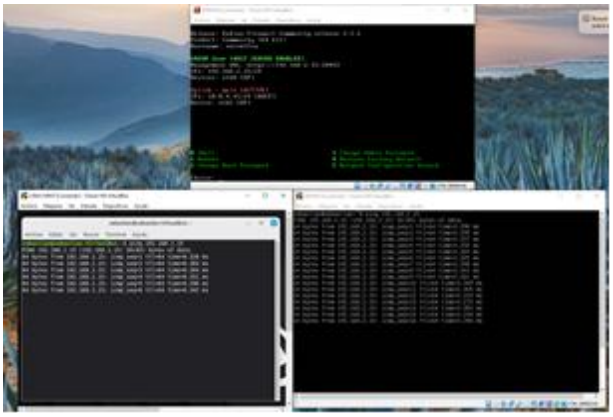
De esta manera, se valida la adecuada segmentación de la red y el funcionamiento de los tres entornos, asegurando la comunicación controlada entre ellos y el cumplimiento de los principios de seguridad.

Figura 5. Operatividad de Red Activa


Fuente: Autoría Propia

Una vez finalizada la configuración de los adaptadores de red, se realizan pruebas de conectividad entre Endian Firewall, el servidor y el cliente, con el fin de verificar la comunicación entre los diferentes segmentos. Para ello, se ejecutan pruebas de ping hacia las direcciones IP 192.168.1.15 y 192.168.2.15, confirmando la respuesta satisfactoria. Asimismo, se valida la correcta salida a Internet, evidenciando el adecuado funcionamiento de la red configurada.

Figura 6. Pruebas de Conectividad



Fuente: Autoría Propia

## 4.2 TEMÁTICA 2: CONFIGURACIÓN DE NAT (NETWORK ADDRESS TRANSLATION)

Inicialmente se verificó que Endian Firewall reconociera correctamente las tres interfaces de red y que cada una se encontrara asociada a su zona correspondiente. Una vez validado el direccionamiento IP, se procedió a configurar las reglas NAT requeridas para permitir la traducción de direcciones desde las redes privadas hacia la interfaz roja, que representa el acceso a la WAN.

Figura 7. Verificación interfaces en Endian

Fuente: Autoría Propia

La primera configuración correspondió a la regla NAT para la zona verde, cuyo objetivo fue permitir que el cliente de la LAN, con dirección 192.168.2.20, pudiera establecer comunicación hacia la red externa usando la interfaz WAN del firewall.

Figura 8. Configuración NAT desde LAN a WAN

Fuente: Autoría Propia

Posteriormente se creó la regla NAT para la zona naranja, permitiendo que el servidor de la DMZ, con dirección 192.168.1.20, también pudiera salir a Internet mediante la misma interfaz roja.

Figura 9. Configuración NAT desde DMZ a Internet

Fuente: Autoría Propia

De acuerdo con la guía de aprendizaje, después de la creación de las reglas fue necesario verificar su existencia dentro del apartado de reenvío de puertos o NAT. Esta validación se complementó con pruebas de conectividad realizadas desde consola, en cumplimiento de la exigencia institucional de evidenciar los procedimientos técnicos sin depender de interfaces gráficas, salvo en la conexión remota de equipos.

Figura 10. Verificaciones de conectividad

Fuente: Autoría Propia

El procedimiento aplicado para la configuración de la Temática 2 se desarrolló en la siguiente secuencia:

- Verificación de la topología de red y del direccionamiento definido para las zonas verde, naranja y roja.
- Comprobación desde consola del estado de red mediante comandos como date, ip a e ip route, con el fin de dejar evidencia de fecha, hora e interfaces activas.
- Configuración de la regla NAT de salida desde la LAN hacia la WAN.
- Configuración de la regla NAT de salida desde la DMZ hacia la WAN.
- Aplicación de los cambios en Endian Firewall y revisión del apartado NAT para validar la creación de las reglas.
- Ejecución de pruebas de conectividad desde el cliente de la red verde y desde el servidor ubicado en la red naranja.

- Registro documental mediante capturas de pantalla y salidas por consola como soporte de la implementación.

Este procedimiento permitió cumplir con el producto esperado de la guía, en la que se exige demostrar la comunicación LAN-WAN y DMZ-Internet a través de reglas NAT correctamente configuradas.

Las pruebas realizadas mostraron que el cliente de la red verde pudo establecer comunicación con la WAN una vez aplicada la regla NAT correspondiente. De forma similar, el servidor ubicado en la zona naranja logró salida hacia la red externa, confirmando el funcionamiento correcto de la segunda regla de traducción.

La revisión del módulo NAT permitió comprobar que ambas reglas quedaron registradas en el firewall, lo cual constituye la evidencia solicitada por la actividad. En términos funcionales, la práctica confirmó que Endian Firewall puede administrar la salida de dos segmentos privados diferentes hacia la red externa sin perder la separación entre la LAN y la DMZ, conservando el enfoque de seguridad perimetral propuesto por la guía.

## 4.3 TEMÁTICA 3: HABILITACIÓN Y RESTRICCIÓN DE SERVICIOS EN DMZ

Para poder dar protección a la intranet, debemos contar con un entorno seguro basado en un sistema DMZ, esto garantizará la seguridad tanto en los sistemas como en las bases de datos y aplicativos.

Es importante tener una buena arquitectura de servicios que permita garantizar la estabilidad de los sistemas en las organizaciones.

Actualmente y a pesar de los avances tecnológicos podemos observar muchas brechas de seguridad que exponen conexiones, enrutadores y demás accesos a los sistemas.

A continuación, veremos la administración esencial de servicios y la aplicación de denegaciones de tráfico no autorizado.

Tecnologías usadas:

- Sistema Firewall (Máquina virtual con Endian)
- DMZ (Máquina virtual con Ubuntu Server)
- Cliente (Máquina virtual con Ubuntu Desktop)

Toda la gestión se realiza bajo la consola de comando Verificando el estado de los servicios y la denegación de tráfico.

**Instalación y configuración de los servicios en la DMZ**
Para la habilitación de los servicios requeridos, se usa la línea de comandos del servidor.
Servicio apache (HTTP) y servicio FTP (vsftpd): por medio del gestor de paquetes se realiza la instalación de los servicios. Una vez instalado se verifica el correcto funcionamiento.

Figura 11. Instalación de servicios en la DMZ

Fuente: Autoría Propia

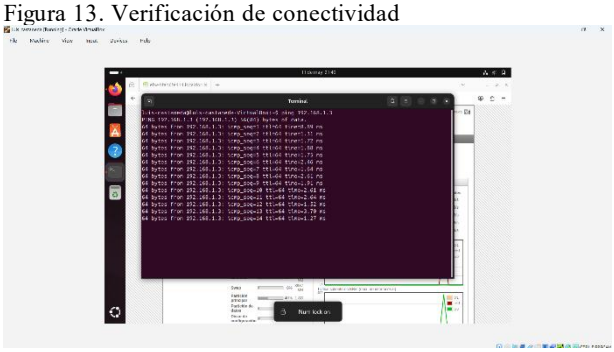
Para validar la implementación usamos los comandos de control status, start, stop para garantizar la implementación.

Tras asegura que los servicios se encuentran operativos en el servidor de la DMZ, verificamos los puertos 80 y 21. Por medio de la terminal y la línea de comandos nos aseguramos de que apache responda por el puerto 80 y el servicio FTP por el 21.
Figura 12. Verificación de puertos 80 (Apache) y 21 (FTP)

Fuente: Autoría Propia

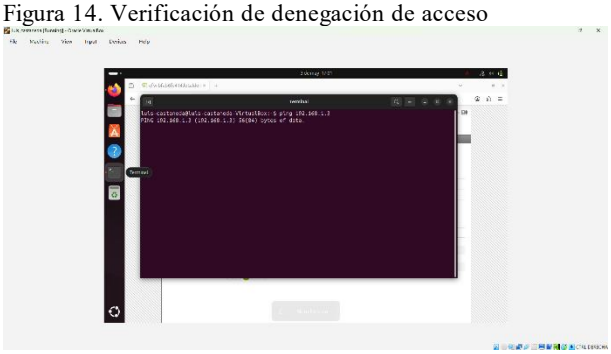
Para poder verificar la conectividad, vamos a realizar unta traza desde una terminal externa hacia la IP de red que apunta a la DMZ, esto por medio de un ping esperando una respuesta que confirma la ejecución y seguido se aplica la regla de bloqueo y el mismo ping no devolverá respuesta confirmado la aplicación efectiva de la regla.

Figura 13. Verificación de conectividad



Fuente: Autoría Propia

Figura 14. Verificación de denegación de acceso



Fuente: Autoría Propia

Es importante no menospreciar la segmentación de zonas ya que esto permite un control de los servicios, exponiendo solo lo necesario externamente.

Prácticas como la desactivación ICMP son esenciales para ocultar topologías de red.

## 4.4 TEMÁTICA 4: REGLAS DE ACCESO INTER-ZONA

Para contextualizar la importancia en la seguridad perimetral debemos conocer la segmentación de las redes que se vino desarrollando en las temáticas anteriores mediante la escogencia de zonas de confianza como se identificaron en el esquema de la fase 1 (Verde, Naranja y Roja) con el uso de nuestro simulador de dispositivos VB en un entorno controlado se dará solución a 4 literales los cuales permitirán comprobar la comunicación Inter Zonas.

Problemática 1 Segmentación y Comunicación Segura Inter-Zona (Verde a Naranja): este primer desafío consistía en establecer un canal de comunicación controlado entre la Zona Verde (LAN) y la zona Naranja (DMZ) como se infiere inicialmente el firewall de Endian restringe el tráfico entre segmento nos solicita que se con protocolos HTTP Y FTP.

Solución Técnica:
Para el caso del protocolo HTTP lo que se busca es que se busca facilitar que la red LAN acceda a los servidores por lo que debemos configurar la regla en el puerto 80 bajo el protocolo HTTP con la acción de permitir y dando prioridad sobre las demás reglas que cuenta el Firewall de ENDIAN por default:

Figura 15. Creación regla con Protocolo HTTP


Fuente: Autoría Propia

Resultado obtenido: al ejecutar en la terminal de Mint el comando que nos permite validar la conexión con el servidor (192.168.1.20) debemos recibir una confirmación con el mensaje “HTTP/1.1 200 OK” lo que indica que el Firewall de endian permitió el tráfico desde la zona verde a la Naranja por medio del puerto 80 y que el servidor de Ubuntu respondió correctamente así:

Figura 16. Validación Regla Protocolo HTTP

```
andres@andres-VirtualBox:~$ hostname -I
192.168.2.17
andres@andres-VirtualBox:~$ arp -a
_gateway (192.168.2.15) en 08:00:27:92:64:08 [ether] en enp0s3
andres@andres-VirtualBox:~$ curl -I http://192.168.1.20
HTTP/1.1 200 OK
Date: Mon, 11 May 2026 00:43:53 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Sun, 10 May 2026 01:49:34 GMT
ETag: "2aa6-6516cd787ffad"
Accept-Ranges: bytes
Content-Length: 10918
Vary: Accept-Encoding
Content-Type: text/html
```

Fuente: Autoría Propia

Para el caso del protocolo FTP se busca permitir el protocolo desde la zona Verde a la zona Naranja a través del puerto 21 con la misma acción de permitir y dando una segunda prioridad a la regla inicialmente creada:

Figura 17. Creación regla con Protocolo FTP


Fuente: Autoría Propia

Resultado Obtenido: en la terminal de Mint al ejecutar el comando telnet 192.168.1.20 21 nos debe arrojar que estamos conectados a través del puerto 21 y este puerto debe responder con la confirmación que el puerto está abierto y escuchando, identificando el servidor con el apartado vsTFPd 3.0.2 lo que nos confirmara que el servicio se encuentra activo y es accesible desde la zona verde:

Figura 18. Validación Regla con Protocolo FTP

```
andres@andres-VirtualBox:~$ telnet 192.168.1.20 21
Trying 192.168.1.20...
Connected to 192.168.1.20.
Escape character is '^]'.
220 (vsFTPd 3.0.5)
421 Timeout.
Connection closed by foreign host.
```

Fuente: Autoría Propia

A continuación, se expone la tabla de conectividad sobre las pruebas solicitadas:

**Tabla 2.** Resultado Pruebas de Conectividad

| Origen | Destino | Protocolo | Puerto | Estado |
|---|---|---|---|---|
| Zona Verde (Mint) | Zona Naranja (Ubuntu) | HTTP | 80 | EXITOSO |
| Zona Verde (Mint) | Zona Naranja (Ubuntu) | FTP | 21 | EXITOSO |

Fuente: Autoría Propia

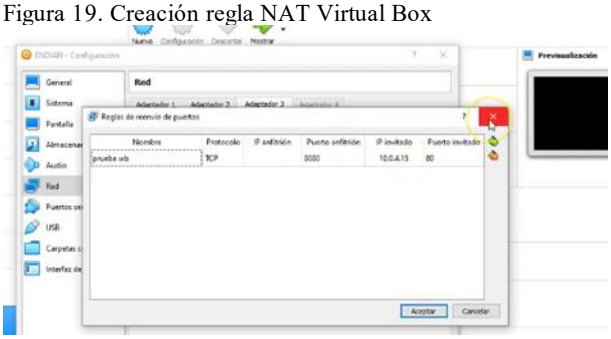
Problemática 2 Publicación de Servicios internos mediante Redirección de puertos (DNAT): La segunda problemática radico en permitir que usuarios de la zona Roja (WAN/Internet) accedan al servidor web de la DMZ sin exponer la Ip privada del servidor ni compromete la seguridad de la red LAN.

Solución Técnica:

Para este caso se empleó una regla de traducción de Direcciones (DNAT) o port forwarding configurando que el firewall escuchara las peticiones del puerto 8080 de la interfaz roja y lo redirigiera internamente al puerto 80 de la zona naranja asi:

Como primera medida en el Virtual Box Nat se mapeo el puerto 8080 del PC real (Windows) al puerto 80 de la Ip roja accediendo al Virtual Box de la maquina Endian en opciones RED Reenvió de Puertos en esta opción se define la regla indicada y se crea con los parámetros necesarios para establecer la comunicación así:

Figura 19. Creación regla NAT Virtual Box



Fuente: Autoría Propia

Como segunda instancia se debe hacer la apertura del Firewall para permitir el tráfico TCP entrante en las opciones de la interfaz WEB Firewall, Redirección de puerto / Nat destino y crear regla con los parámetros que indiquen ingreso de Zona Roja y redirección a Zona Naranja (192.168.1.20).

Figura 20. Creación regla NAT Firewall

Fuente: Autoría Propia

Por último, hacemos la apertura del firewall para permitir el tráfico TCP entrante así:

Figura 21. Creación Regla tráfico TCP entrante

Fuente: Autoría Propia

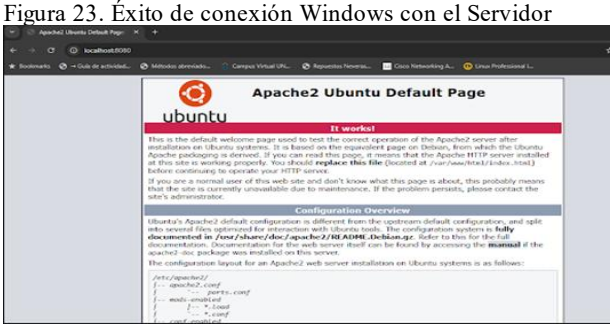
Resultado Obtenido: En la terminal de Windows (CMD) indicada con el comando netstat -an | findstr 8080 debe aparecer LISTENING significa que VirtualBox ya abrió la puerta en Windows:

Figura 22. Comunicación Windows (CMD)


Fuente: Autoría Propia

Como segunda medida vamos a comprobar la conexión solicitada accediendo desde el navegador a la url 127.0.0.1:8080 arrojándonos la página del servidor de Apache con el mensaje ¡It Works! Lo que corrobora la conexión entre las zonas solicitadas.

Figura 23. Éxito de conexión Windows con el Servidor




Fuente: Autoría Propia

Problemática 3 Filtrado de paquetes y Gestión de estado de Conexión: en este apartado debemos verificar el tráfico inter-zona y la creación de las reglas ya elaboradas dado que el Firewall actúa como mecanismo de control

Tráfico Zona Verde a Zona Naranja.

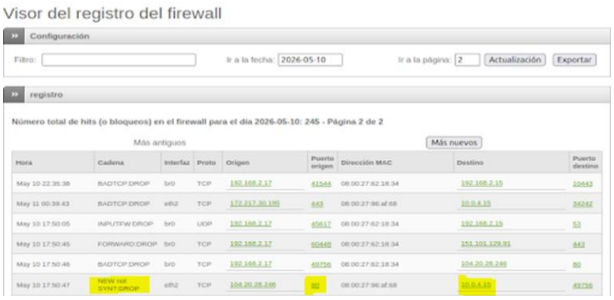
Figura 24. Regla de tráfico Zona verde a Naranja


Fuente: Autoría Propia

Trafico Zona Roja a Naranja (configurada en la literal anterior figura 21)

Para verificar el tráfico real del firewall debemos acceder a la interfaz WEB en la opción Registros y Firewall donde podemos verificar los registros en tiempo real que se detectaron y bloquearon de paquetes con etiquetas como BADTCP:DROP y NEW not SYN.

Figura 25. Registros del Firewall Endian




Fuente: Autoría Propia

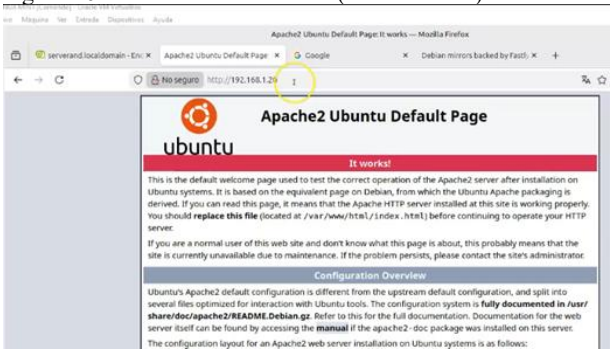
La anterior confirmación demuestra que la protección del firewall no es solo a nivel de puerto sino a nivel de protocolo profundo.

Problemática 4 validación sistemática de control de acceso: en esta parte del proceso debemos verificar las reglas que configuramos al Firewall mediante la ejecución de pruebas cruzadas entre las distintas zonas (Verde, Roja, Naranja) y validar los resultados.

El objetivo de este paso es verificar que la implementación de las reglas tenga una efectividad dirigida en un orden indicado en la problemática por lo cual se analizan las ejecuciones así:

Análisis de conectividad LAN-DMZ: al existir una regla que permite el tráfico en el puerto 80 el firewall crea una entrada en su tabla de estados y permite que los paquetes del servidor regresen a Mint sin necesidad de retorno.

Figura 26. Prueba 1 LAN a DMZ (Mint-Ubuntu)




Fuente: Autoría Propia

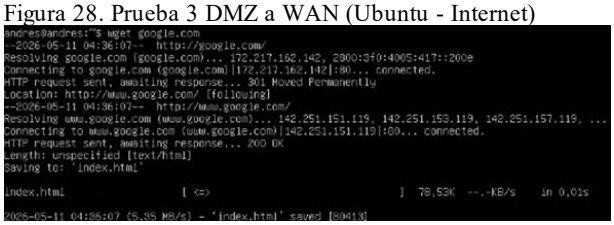
Análisis de tráfico LAN-WAN: se implementó el NAT para traducir las direcciones IP privadas de la LAN a la IP publica y permitir la salida a internet lo que confirma que el enrutamiento y la resolución DNS están operativos.

Figura 27. Prueba 2 LAN a WAN (Mint-Endian)

Fuente: Autoría Propia

Análisis de restricción DMZ-WAN: En este caso es una medida de seguridad puesto que el servidor UBUNTU se vería en riesgo al denegar la acción en caso de un ataque el paquete llegaría, pero sería descartado al no coincidir con las políticas definidas.

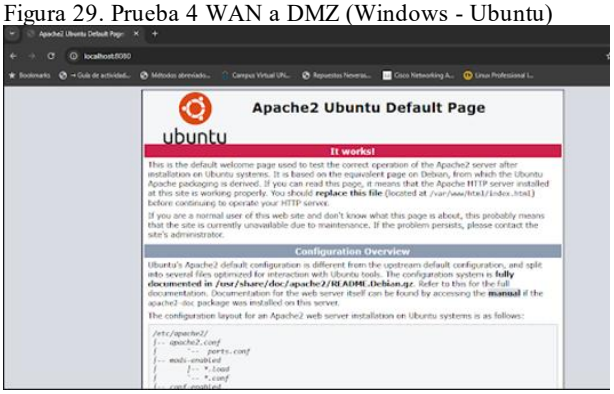
Figura 28. Prueba 3 DMZ a WAN (Ubuntu - Internet)




Fuente: Autoría Propia

Análisis de WAN-DMZ: mediante la destination NAT el firewall recibe los paquetes en el puerto 8080 desde la zona roja y modifica la IP destino a 192.168.1.20:80 el éxito demuestra que la conexión entre usuario externo funciona y protege la IP real del servidor Ubuntu.

Figura 29. Prueba 4 WAN a DMZ (Windows - Ubuntu)




Fuente: Autoría Propia

Análisis Gestión FTP de LAN-WAN a través del servidor el FTP: esta prueba corresponde a un protocolo que usa el puerto 21 el éxito en la conexión se debe a que ENDIAN rastreo la

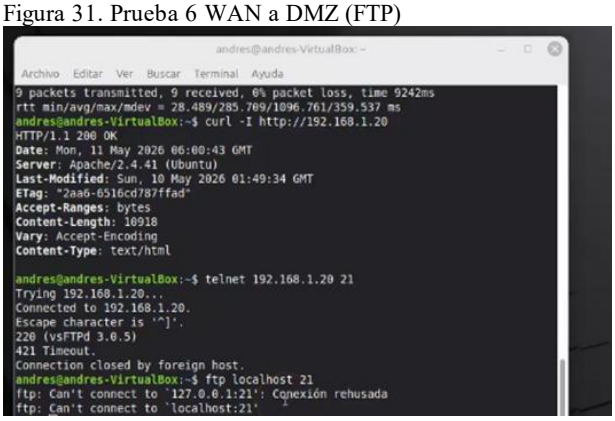
conexión de datos y permite la conexión de Mint en la dirección FTP publica (ftp.debian.org)

Figura 30. Prueba 5 LAN a WAN (Mint - Internet)


Fuente: Autoría Propia

Análisis gestión FTP de WAN a DMZ: en este caso no existe una regla de puertos DNAT para el servicio FTP el firewall descarta el paquete por defecto.

Figura 31. Prueba 6 WAN a DMZ (FTP)




Fuente: Autoría Propia

Resultados Obtenidos:

**Tabla 3.** Resultados pruebas de conectividad Inter-Zona

| Directiva de Tráfico | Servicio | Resultado |
|---|---|---|
| LAN (Verde) → DMZ (Naranja) | HTTP (80) | EXITOSO |
| LAN (Verde) → WAN (Roja) | HTTP/S (80/443) | EXITOSO |
| DMZ (Naranja) → WAN (Roja) | HTTP (80) | DENEGADO |
| WAN (Roja) → DMZ (Naranja) | HTTP (8080) | EXITOSO |
| LAN (Verde) → WAN (Roja) | FTP (21) | EXITOSO |
| WAN (Roja) → DMZ (Naranja) | FTP (21) | BLOQUEADO |

Fuente: Autoría Propia

Por último, debemos confirmar que en esta fase el uso de las IP estáticas facilito la creación de las políticas minimizando los casos de filtrado de paquetes en su ejecución.

## 4.5 TEMÁTICA 5: PROXY HTTP CON AUTENTICACIÓN Y POLÍTICAS DE CONTENIDO

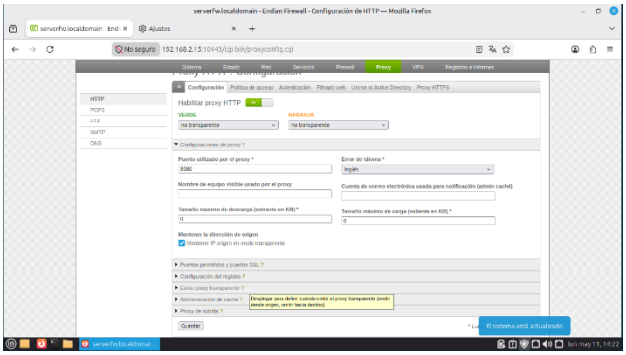
- **Objetivo y alcance.**

El propósito de esta temática fue desplegar y validar un servidor proxy HTTP no transparente en la zona LAN (Zona Verde), con el fin de controlar el acceso a Internet mediante autenticación de usuarios y filtrado de contenido basado en listas negras. La implementación se realizó sobre el módulo de proxy integrado en Endian Firewall Community 3.3.2, el cual utiliza Squid como motor de procesamiento subyacente.

- **Configuración del Proxy en ENDIAN Firewall.**

El proceso de configuración se ejecutó mediante la interfaz de administración web del firewall. Primero, se habilitó el servicio proxy en modo no transparente, lo que obliga a los clientes a declarar explícitamente la dirección IP y el puerto del proxy en sus navegadores. Posteriormente, se crearon cuentas de usuario y grupos locales en el sistema de autenticación integrado. Se definió una política de acceso vinculando el grupo de usuarios al perfil de filtrado configurado. En dicho perfil, se cargó una lista negra con los dominios www.hotmail.com, www.youtube.com y www.elnuevodia.com.co. Finalmente, se aplicó la política a la interfaz de la zona Verde y se reinició el servicio para asegurar la carga de las nuevas reglas.

Figura 32. Configuración del proxy http no transparente en ENDIAN.



Fuente: Autoría Propia

- **Validación experimental y resultados obtenidos.**

Una vez finalizada la configuración, se procedió a la validación funcional desde la estación cliente (Linux Mint 22.3, IP 192.168.2.20). Los resultados obtenidos tras la ejecución de las pruebas se resumen a continuación:

• El proxy operó correctamente para los usuarios de la LAN, interceptando y gestionando las solicitudes HTTP.

• La lista negra de dominios fue aplicada de forma efectiva, bloqueando el acceso a las URLs especificadas.

• Se crearon y gestionaron exitosamente usuarios y grupos locales en el backend de autenticación (Squid).

• La política de acceso quedó vinculada al usuario definido, actuando como mecanismo de control granular.

• La configuración del proxy en el navegador del equipo cliente se completó sin errores de sintaxis o conectividad

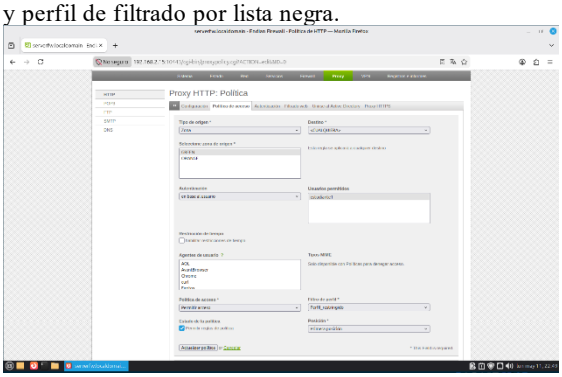
• El sistema solicitó autenticación al primer intento de navegación, validando el flujo de credenciales.

• El filtro de contenido respondió correctamente ante los dominios de la lista negra, redirigiendo a la página de denegación nativa del sistema.

• La conectividad SSH al firewall permitió auditar el estado del servicio y revisar los registros del sistema, confirmando la ejecución estable del proceso Squid.

Para formalizar la evidencia técnica, la Tabla 1 presenta la matriz de validación con los indicadores medidos durante la prueba.

Figura 33. Vinculación de política de acceso, grupo de usuarios y perfil de filtrado por lista negra.



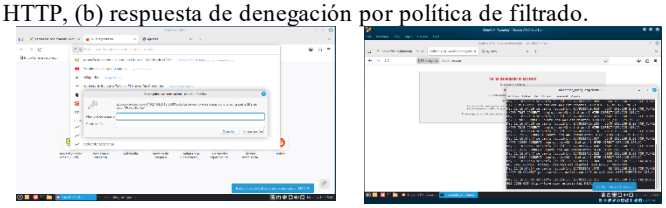

Fuente: Autoría Propia

Tabla 4. Matriz de validación del Proxy HTTP y políticas de autenticación.

| **Prueba realizada** | **Resultado esperado** | **Estado** | **Evidencia técnica** |
|---|---|---|---|
| Configuración proxy en navegador | Solicitud de credenciales (HTTP 407) | OK | Prompt de autenticación nativo del navegador |
| Navegación sin credenciales | Denegación de acceso | OK | Mensaje "Proxy Authentication Required" |
| Acceso a dominio permitido (ej. google.com) | Carga completa (HTTP 200) | OK | Página renderizada, log Squid: TCP_HIT/200 |
| Acceso a dominio en lista negra (youtube.com) | Bloqueo (HTTP 403) | OK | Página de bloqueo Endian, log: DENIED |
| Estado del servicio Squid (vía SSH) | active (running) | OK | Comando systemctl status squid (o equivalente EFW) |
| Revisión de logs de acceso | Registro de IPs, usuarios y códigos HTTP | OK | Archivo /var/log/squid/access.log poblado |

Fuente: Autoría Propia

Figura34. Validación en cliente: (a) solicitud de autenticación HTTP, (b) respuesta de denegación por política de filtrado.



Fuente: Autoría Propia

- **Auditoria y evidencia mediante línea de comandos.**

Para complementar la validación desde la interfaz gráfica, se estableció una conexión SSH hacia el firewall y se ejecutaron comandos de diagnóstico. El estado del servicio se verificó mediante "date && /etc/init.d/squid status", confirmando su ejecución continua y sin errores críticos. Adicionalmente, se inspeccionó el archivo de registros de acceso, donde se observaron entradas que correlacionan la dirección IP del cliente (192.168.2.20), el nombre de usuario autenticado, la URL solicitada y el código de respuesta HTTP. Esta trazabilidad garantiza que el proxy no solo filtra contenido, sino que también cumple con los requisitos de auditoría y cumplimiento normativo en entornos controlados.

Los resultados confirman que la implementación cumple con los objetivos planteados, demostrando la viabilidad de ENDIAN Firewall como plataforma integral para el control de navegación, autenticación de usuarios y filtrado de contenido en redes LAN corporativas.

Figura35. Validación en cliente: (a) Estado del servicio SQUID runnig, (b) Navegación en dominio no bloqueado.


Fuente: Autoría Propia

## 5 RESULTADOS Y EVALUACIÓN

- **Métricas Técnicas de Validación.**

Tabla 5. Métricas técnicas de validación

| Temática | Prueba Realizada | Resultado Esperado | Resultado Obtenido | Estado |
|---|---|---|---|---|
| T1: Instalación | Acceso a interfaz web de Endian | HTTPS en 192.168.2.15 | Acceso exitoso | OK |
| T2: NAT | ping 8.8.8.8 desde LAN/DMZ | Respuesta recibida | Respuesta <100ms | OK |
| T3: Servicios DMZ | curl http://192.168.1.20 desde LAN | Código HTTP 200 | Página apache por defecto | OK |

| | | | | |
|---|---|---|---|---|
| T3: Bloqueo ICMP | ping 192.168.1.20 desde LAN | Timeout / No respuesta | Sin respuesta (ICMP DROP) | OK |
| T4: Inter-Zona | Acceso HTTP WAN→DMZ | Puerto 80 accesible | Sitio web cargado | OK |
| T4: Inter-Zona | Acceso FTP WAN→DMZ | Conexión rechazada | Conexión timeout | OK |
| T5: Proxy | Acceso a live.com con proxy | Página de bloqueo | Mensaje "Access Denied" | OK |
| T5: Autenticación | Proxy sin credenciales | Error 407 Proxy Auth Required | Autenticación forzada | OK |

Fuente: Autoría Propia

## 6 DISCUSIÓN

La implementación realizada evidencia que un laboratorio virtual basado en Endian Firewall y VirtualBox constituye una alternativa funcional para la enseñanza de conceptos de seguridad perimetral, ya que permite integrar segmentación de red, control de acceso, traducción de direcciones, publicación restringida de servicios y filtrado de navegación en un mismo entorno de prueba. La posibilidad de documentar cada procedimiento y validar su comportamiento mediante evidencias de consola, capturas y registros fortalece el valor pedagógico del laboratorio.

Entre las principales fortalezas del enfoque propuesto se encuentra su carácter reproducible, el bajo costo de implementación y la utilización de herramientas de software libre. Estas características facilitan su adopción en escenarios académicos donde se requiere experimentar con topologías realistas sin depender de infraestructura física especializada.

No obstante, el entorno implementado presenta algunas limitaciones. Endian Firewall Community 3.3.2 corresponde a una plataforma con menor vigencia frente a soluciones más actuales, y la WAN simulada mediante NAT de VirtualBox no reproduce completamente las condiciones de una red externa real, como variaciones de latencia, tráfico hostil o escenarios avanzados de ataque. Asimismo, el proxy no transparente requiere configuración manual en los clientes, lo que reduce escalabilidad en ambientes con múltiples estaciones.

Como lección principal, el trabajo confirma que la validación progresiva de reglas y servicios es determinante para evitar errores de configuración y garantizar la coherencia entre políticas de seguridad y comportamiento real de la red. De igual forma, la combinación entre administración por consola y supervisión desde el firewall permite desarrollar competencias prácticas valiosas en monitoreo, auditoría y resolución de incidentes básicos

.

## 7 CONCLUSIONES Y TRABAJO FUTURO

La implementación del laboratorio virtual permitió simular de manera satisfactoria una arquitectura de seguridad perimetral segmentada en zonas LAN, DMZ y WAN, utilizando Endian Firewall como plataforma central de administración y control. Las pruebas desarrolladas confirmaron la operación funcional de las configuraciones asociadas con NAT, habilitación de servicios, control de tráfico inter-zona y filtrado de navegación mediante proxy autenticado.

El desarrollo de las cinco temáticas evidenció que el entorno propuesto es adecuado para fortalecer competencias prácticas en administración de redes y ciberseguridad, al integrar procedimientos de configuración, validación técnica y análisis de evidencias dentro de un escenario reproducible. En este sentido, el laboratorio representa una estrategia útil de formación basada en software libre y enfocada en la experimentación controlada.

Como trabajo futuro, se recomienda ampliar el laboratorio con herramientas de monitoreo y correlación de eventos, incorporar escenarios de ataque y defensa para ejercicios de análisis ofensivo y defensivo, y evaluar la migración hacia plataformas UTM con soporte más vigente, manteniendo la topología lógica desarrollada en este estudio

## 8 Referencias


[1] K. Scarfone y P. Mell, *Guide to Intrusion Detection,* National Institute of Standards and Technology, 2007.

[2] N. Otoum, A. A. Maqousi, M. Alauthman y A. Almomani, *Remote Labs in Cybersecurity Education: Analyzing Software Requirements and Challenges,* International Journal of Cloud Applications and Computing, 2025.

[3] Endian GmbH, *Endian Firewall Community,* endian, 2026.

[4] *Endian Firewall Community,* SOURCEFORGE, 2024.

[5] Oracle Corporation, *User Guide for Release 7.2,* VirtualBox.org, 2026.

[6] D. N. Răceanu y C. V. Marian, *Cybersecurity Virtual Labs for Pentesting Education,* IEEE, 2023.

[7] J. Son, C. Irrechukwu y P. Fitzgibbons, *Virtual Lab for Online Cyber Security Education,* Communications of the IIMA ©2012, 2012.

[8] OPNsense®, *OPNsense® is an open source, feature rich firewall and routing platform,* OPNsense®, 2026.

[9] pfSense®, *pfSense® - World's Most Trusted Open Source Firewall,* pfSense®, 2026.

[10] Wikipedia, the free encyclopedia, *DMZ (computing),* Wikipedia, the free encyclopedia, 2026.

[11] E. Dart, L. Rotman, B. Tierney, M. Hester y J. Zurawski, *The Science DMZ: A Network Design Pattern for Data-Intensive Science,* ESnet Energy Sciences Network, 2013.

[12] N. P. Sy, T. Tran, T. N. Khanh, P. L. T. Bich y T. N. Dinh, *Applying Virtualization and Cloud Computing Platform in Designing Cybersecurity Lab,* IEEE, 2023.

[13] H. J. Kiratsata, D. P. Raval, P. K. Viras, P. Lalwani, H. Patel y P. S. D., *Behaviour Analysis of Open-Source Firewalls Under Security Crisis,* IEEE, 2022.

[14] endian, *Endian UTM 6.8 Reference Manual,* endian.