IMPLEMENTACIÓN DE SEGURIDAD PERIMETRAL EN GNU/LINUX MEDIANTE ENDIAN FIREWALL COMMUNITY

Ingrid Johana Angulo Fajardo
e-mail: ijangulof@unadvirtual.edu.co
Héctor Darío Rodríguez Horta
e-mail: hdrodriguezh@unadvirtual.edu.co
Cristian David Rey Salgado
e-mail: cdreys@ unadvirtual.edu.co
Juan Camilo Suárez Campos
e-mail: jcsuarezca@ unadvirtual.edu.co
Fabio Andrés Sánchez Quintana
e-mail: fasanchezq@ unadvirtual.edu.co

RESUMEN: *En el presente artículo se describe el proceso de implementación de seguridad perimetral en entornos GNU/Linux utilizando la distribución Endian Firewall [1][8] como plataforma principal. Durante el desarrollo de la actividad se realizó la configuración de las zonas de red verde, roja y naranja, permitiendo organizar la red interna, la red externa y la zona destinada a servidores. Además, se realizó la configuración NAT, políticas de acceso y servicios HTTP y FTP [2][3], para controlar el tráfico entre las diferentes zonas de red. También se configuró un proxy HTTP con autenticación de usuarios y restricciones de navegación mediante listas negras. Las pruebas realizadas permitieron verificar el correcto funcionamiento de los servicios y la configuración establecida, evidenciando la importancia de aplicar mecanismos de protección en infraestructuras basadas en GNU/Linux para mejorar la administración y seguridad de la red.*

PALABRAS CLAVE: Endian Firewall, GNU/Linux, NAT, seguridad perimetral.

ABSTRACT: *This article describes the process of implementing perimeter security in GNU/Linux environments using the Endian Firewall distribution as the main platform. During the development of the activity, the configuration of the green, red, and orange network zones was carried out, allowing the organization of the internal network, external network, and the server zone. In addition, NAT configuration, access policies, and HTTP and FTP services were implemented to control traffic between the different network zones. An HTTP proxy with user authentication and browsing restrictions through blacklists was also configured. The tests carried out verified the correct functioning of the services and the established configuration, demonstrating the importance of applying protection mechanisms in GNU/Linux-based infrastructures to improve network management and security.*

KEYWORDS: Endian Firewall, GNU/Linux, NAT, Perimeter Security.

1 INTRODUCCIÓN

La seguridad en redes GNU/Linux es importante para proteger la información [1][2] y controlar el acceso entre las diferentes zonas de una red. En la actualidad, las organizaciones requieren herramientas que permitan administrar el tráfico de manera segura y reducir posibles vulnerabilidades.

En esta actividad se busca implementar GNU/Linux Endian como firewall principal [8] en un entorno virtualizado, configurando las zonas LAN, WAN y DMZ. Además, se realizaron configuraciones de NAT, reglas de acceso, servicios HTTP y FTP, y un proxy HTTP con autenticación de usuarios.

El objetivo de este artículo es presentar el desarrollo de las temáticas propuestas y los resultados obtenidos durante la implementación de los mecanismos de seguridad en GNU/Linux.

2 OBJETIVOS

2.1 OBJETIVO GENERAL

Implementar mecanismos de seguridad perimetral en un entorno GNU/Linux mediante Endian Firewall Community, aplicando segmentación de red, reglas NAT, control de tráfico y servicios proxy para fortalecer la administración y protección de la infraestructura de red.

2.2 OBJETIVOS ESPECÍFICOS

Configurar las zonas LAN, WAN y DMZ en un entorno virtualizado utilizando VirtualBox y Endian Firewall.

Implementar reglas de acceso y traducción de direcciones NAT para controlar el tráfico entre las diferentes zonas de red.

Configurar servicios HTTP, FTP y proxy autenticado para fortalecer la seguridad y administración de la red.

3 ENTORNO DE TRABAJO

3.1 ESTRUCTURA GENERAL DE LA RED

Para el desarrollo de la actividad se utilizó un entorno virtualizado mediante VirtualBox [1], donde se implementó GNU/Linux Endian como firewall principal para la administración y seguridad de la red. La infraestructura fue

configurada con tres zonas principales: red interna (LAN), acceso a Internet (WAN) y zona desmilitarizada (DMZ).

Adicionalmente, se empleó Ubuntu Server para la configuración de servicios web y FTP dentro de la zona DMZ. Las configuraciones realizadas permitieron implementar reglas NAT, control de tráfico, acceso entre zonas y políticas de seguridad mediante proxy HTTP con autenticación de usuarios.

Todas las pruebas y configuraciones fueron ejecutadas desde consola, permitiendo verificar el correcto funcionamiento de los servicios y las reglas de seguridad implementadas.

4 METODOLOGÍA

Para el desarrollo de la presente práctica se trabajó en un entorno virtualizado utilizando Oracle VirtualBox, lo que permitió simular una infraestructura de red similar a la utilizada en ambientes reales. Inicialmente se creó la máquina virtual de Endian Firewall Community, la cual funcionó como firewall principal para administrar y proteger el tráfico de la red.

Posteriormente, se configuraron las diferentes zonas de red: GREEN para la red interna LAN, ORANGE para la DMZ y RED para la conexión WAN. Organización que permitió la comunicación entre los dispositivos y aplicar políticas de seguridad específicas para cada zona.

Después de la configuración inicial, se implementaron reglas NAT y reglas de acceso con el fin de controlar el tráfico entrante y saliente. También se instalaron servicios HTTP y FTP en un servidor Ubuntu ubicado en la DMZ, permitiendo validar el acceso seguro a los servicios publicados.

Para finalizar, se configuró un proxy HTTP con autenticación de usuarios y filtrado de páginas web mediante Squid en Endian Firewall. Para comprobar el correcto funcionamiento de toda la infraestructura, se realizaron pruebas utilizando herramientas como ping, curl, telnet e iptables, verificando la conectividad, las restricciones de acceso y el funcionamiento de las políticas de seguridad implementadas.

5 TEMÁTICA 1: IMPLEMENTACIÓN DE GNU/LINUX ENDIAN

La implementación de Endian Firewall permitió establecer una arquitectura básica de seguridad perimetral en un entorno virtualizado.

5.1 CONFIGURACIÓN DEL ENTORNO VIRTUAL

Para la implementación del firewall se utilizó Oracle VirtualBox como entorno de virtualización, donde se creó una máquina virtual denominada “Endian_Ingrid_Angulo” con sistema operativo Linux de 64 bits, se le asignaron 2048 MB de memoria RAM, un procesador y un disco duro virtual de 20 GB en formato VDI con almacenamiento dinámico. Esta configuración permitió disponer de un entorno adecuado para realizar la instalación y administración del firewall Endian Firewall Community Edition.

Posteriormente, se configuraron tres adaptadores de red para representar las diferentes zonas de la arquitectura de seguridad implementada. El primer adaptador fue configurado en modo red interna para la zona GREEN (LAN), el segundo adaptador se configuró para la zona ORANGE (DMZ) y el tercer adaptador se estableció en modo NAT para representar la zona RED/WAN y permitir la salida a Internet. Esta segmentación permitió simular un entorno de red seguro dentro del laboratorio virtual.

Figura 1. Configuración de adaptadores de red en Oracle VirtualBox

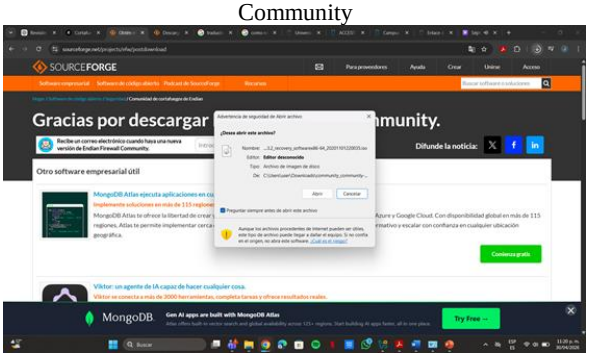
Fuente: Autoría Propia.

5.2 INSTALACIÓN DE ENDIAN FIREWALL

La instalación se realizó mediante la descarga de la imagen ISO oficial desde el repositorio de Endian Community. Posteriormente, la imagen fue montada en la unidad óptica virtual de VirtualBox para iniciar el proceso de instalación del sistema.

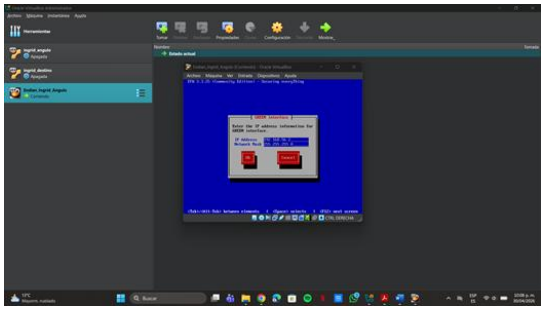
Durante la instalación se ejecutó el asistente de configuración, permitiendo la instalación de paquetes necesarios y la configuración inicial de las interfaces de red. La interfaz GREEN fue configurada con la dirección IP 192.168.56.2, mientras que la interfaz ORANGE fue configurada con la dirección IP 192.168.57.1 y la interfaz RED fue configurada mediante DHCP para permitir conectividad hacia Internet.

Figura 2. Descarga de la imagen ISO de Endian Firewall Community



Fuente: Autoría Propia.

Figura 3. Proceso de instalación y configuración de la interfaz GREEN



Fuente: Autoría Propia.

Figura 4. Montaje de la imagen ISO en VirtualBox

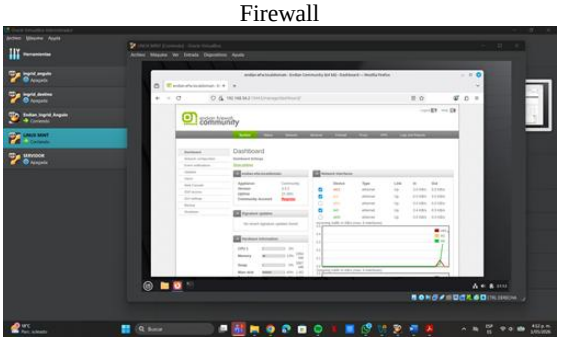
Fuente: Autoría Propia.

5.3 VERIFICACIÓN Y PRUEBAS DE CONECTIVIDAD

Una vez finalizada la instalación, se verificó el funcionamiento del sistema mediante consola y acceso web a la interfaz de administración de Endian Firewall. Para validar la conectividad de la zona GREEN se utilizó una máquina virtual Linux Mint configurada dentro de la red interna.

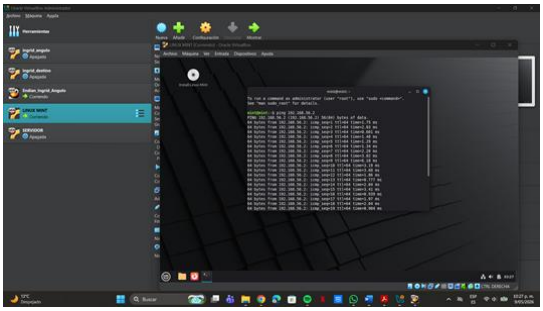
Las pruebas realizadas mediante el comando ping permitieron comprobar la comunicación entre Linux Mint y la interfaz GREEN del firewall. Adicionalmente, se verificó el acceso a la consola web de administración y la conectividad WAN mediante pruebas hacia direcciones externas, confirmando el correcto funcionamiento de las interfaces configuradas y de la segmentación de red implementada.

Figura 5. Verificación de conectividad y acceso web de Endian Firewall



Fuente: Autoría Propia.

Figura 6. Prueba de conectividad hacia la interfaz GREEN de Endian



Fuente: Autoría Propia.

6 TEMÁTICA 2: CONFIGURACIÓN NAT

Pantalla de Source NAT en la interfaz de administración de Endian Firewall, donde se configuraron las reglas de traducción de direcciones de red para el tráfico saliente. Se crearon dos reglas: la primera para el segmento 192.168.56.0/24 (zona verde) y la segunda para el segmento 192.168.57.0/24 (zona naranja), ambas con destino 'Uplink main' y NAT automático, lo que permite que todo el tráfico saliente de ambas zonas sea traducido a la IP pública del firewall.

Figura 7. Creación de reglas SNAT para los segmentos verde y naranja

Fuente: Autoría Propia

Configuración del Destination NAT / Port Forwarding en Endian Firewall. Se definieron tres reglas de reenvío de puertos desde la zona RED (WAN) hacia el servidor 192.168.57.2 en la DMZ: HTTPS (443), HTTP (80) y FTP (21).

Figura 8. Creación de reglas DNAT para publicación de servicios

Fuente: Autoría Propia

Salida del comando 'iptables -t nat -L -n -v' ejecutado directamente en la consola del firewall. Muestra la configuración NAT activa a nivel de kernel Linux con dos cadenas relevantes:

PORTFW: reglas de reenvío de puertos DNAT hacia 192.168.57.2 en puertos 443, 80 y 21.

SOURCENAT: enmascaramiento de los segmentos 192.168.56.0/24 y 192.168.57.0/24 hacia 10.22.221.29.

Figura 9. Ejecución de iptables -t nat -L -n -v – Verificación completa del NAT

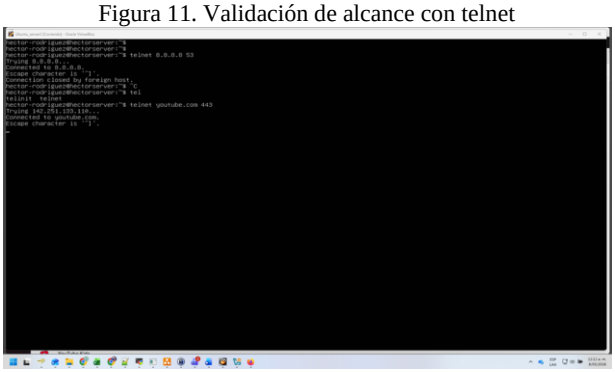
Fuente: Autoría Propia

Los resultados de la ejecución de comandos curl y telnet desde ambas zonas confirman la correcta implementación del NAT. Esto se evidencia en los resultados obtenidos de 200 OK y conexión establecida a puerto solicitado respectivamente, comprobando así la configuración SNAT.

Figura 10. Validación de alcance con curl

Fuente: Autoría Propia

Figura 11. Validación de alcance con telnet

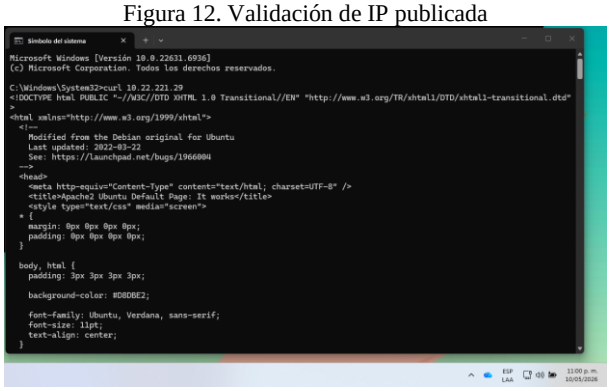


Fuente: Autoría Propia

Se evidencia una prueba práctica ejecutada desde un cliente desde una red WAN simulada donde por medio del comando curl desde la máquina física, se logra tener alcance al servicio HTTP publicado en el servidor Ubuntu. El resultado muestra respuesta la dirección 10.22.221.29, confirmando que el DNAT está funcionando correctamente.

Lo anterior permitió comprobar que el tráfico efectivamente se traduce desde la IP pública configurada hacia el servidor de la DMZ.

Figura 12. Validación de IP publicada



Fuente: Autoría Propia

El Source NAT (SNAT/Masquerade) configurado para los segmentos 192.168.56.0/24 y 192.168.57.0/24 permitió el acceso a Internet desde las zonas LAN y DMZ utilizando una única IP pública, optimizando el uso del direccionamiento y ocultando la topología interna de la red ante el exterior.

El Destination NAT (DNAT) habilitó la publicación controlada de servicios web (HTTP/HTTPS) y FTP del servidor en la DMZ sin exponer directamente su IP privada, manteniendo el principio de mínima exposición que caracteriza una arquitectura de seguridad perimetral bien diseñada.

La verificación mediante iptables confirmó la coherencia entre la configuración gráfica de Endian y las reglas efectivamente aplicadas en el kernel de Linux, validando que no existen brechas entre la política definida y su implementación real.

Las pruebas de conectividad (telnet y curl) desde ambas zonas demostraron que el NAT opera correctamente en los dos sentidos: tráfico saliente desde las redes internas hacia Internet (SNAT) y tráfico entrante desde Internet hacia los servicios publicados en la DMZ (DNAT).

La combinación de NAT con las reglas del Outgoing Firewall garantiza que solo los servicios y protocolos explícitamente autorizados (HTTP, HTTPS, DNS, FTP, Traceroute) puedan atravesar el perímetro, rechazando cualquier otro intento de comunicación no contemplado en la política de seguridad.

7 TEMÁTICA 3: IMPLEMENTACIÓN DE SERVICIOS EN LA DMZ

La seguridad en redes corporativas es un tema central en la administración de sistemas operativos. La creación de una zona DMZ (Demilitarized Zone) [1][2] responde a la necesidad de exponer servicios públicos —como páginas web o servidores FTP— sin comprometer la integridad de la red interna. En este proyecto, se configuró un servidor Ubuntu en la DMZ y se aplicaron reglas en el firewall Endian para permitir únicamente los servicios esenciales (HTTP y FTP), bloqueando protocolos inseguros como ICMP.

La práctica se fundamenta en estándares internacionales de ciberseguridad como NIST SP 800-41, que recomiendan segmentar las redes y aplicar políticas de control de tráfico. Además, se alinea con regulaciones como GDPR y PCI-DSS [10], que exigen medidas de protección para datos sensibles y servicios expuestos a Internet.

El desarrollo de la Temática 3 dependió directamente de la Temática 1, realizada por la compañera Ingrid Angulo, donde se configuró el firewall Endian en VirtualBox con tres zonas:

- VERDE (LAN): 192.168.56.0/24, clientes Linux Mint.
- NARANJA (DMZ): 192.168.57.0/24, servidores Ubuntu.
- ROJA (WAN): acceso a Internet vía NAT.

Este diseño garantizó la segmentación de red, condición indispensable para aplicar reglas de seguridad inter-zona. La DMZ se convirtió en el espacio controlado donde se desplegaron los servicios públicos, mientras que la LAN permaneció protegida de accesos externos.

7.1 OBJETIVOS DEL PROYECTO

- Permitir tráfico HTTP (puerto 80) y FTP (puerto 21) desde el servidor Ubuntu en la DMZ.
- Denegar el protocolo ICMP (Echo Request y Echo Reply) para evitar reconocimiento mediante ping.
- Verificar la correcta aplicación de reglas y evidenciar el tráfico generado en los logs del sistema.

Estos objetivos buscan equilibrar funcionalidad y seguridad: se habilitan servicios necesarios para la operación, pero se bloquean protocolos que podrían ser usados en ataques de reconocimiento o denegación de servicio.

7.2 DESARROLLO TÉCNICO

7.2.1 CONFIGURACIÓN DEL SERVIDOR UBUNTU (DMZ)

Se asignó una IP estática (192.168.57.10) con gateway 192.168.57.1, correspondiente al firewall Endian. La configuración se realizó mediante Netplan, validando la conectividad con comandos como ip a e ip route.

Posteriormente, se instalaron y verificaron los servicios:
Apache (HTTP): activo y escuchando en el puerto 80. Validado con curl -I http://localhost.

vsftpd (FTP): instalado desde repositorios oficiales, habilitado al arranque y operativo en el puerto 21.

Estos servicios representan los más comunes en entornos corporativos, y su exposición controlada en la DMZ es una práctica estándar.

Figura 13. Configuración Ubuntu

Fuente: Autoría Propia

La imagen muestra la configuración de red de la máquina virtual en Oracle VirtualBox. Se trata del servidor Ubuntu, que forma parte de la zona DMZ definida en el proyecto. En la pestaña de red se observa que el Adaptador 1 está habilitado y conectado a una red interna llamada DMZ, con el tipo de adaptador Intel PRO/1000 MT Desktop (82540EM).

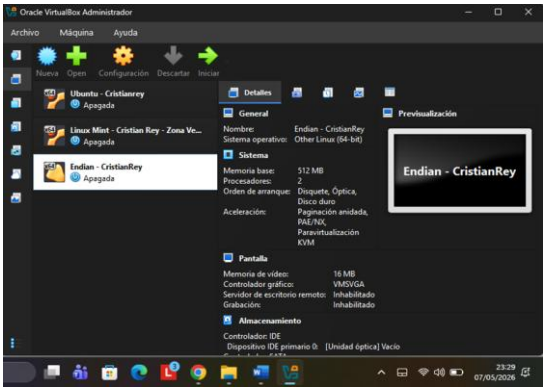
7.3 CONFIGURACIÓN EN ENDIAN FIREWALL

En el módulo Inter-Zone Traffic se definieron reglas para:

- Permitir tráfico HTTP y FTP desde la DMZ hacia la WAN.
- Bloquear ICMP, comprobado mediante pruebas de ping fallidas desde clientes en la LAN.

La administración se realizó desde la consola web de Endian (https://192.168.56.2:10443 (192.168.56.2 in Bing)), lo que permitió un control centralizado y seguro de las políticas.

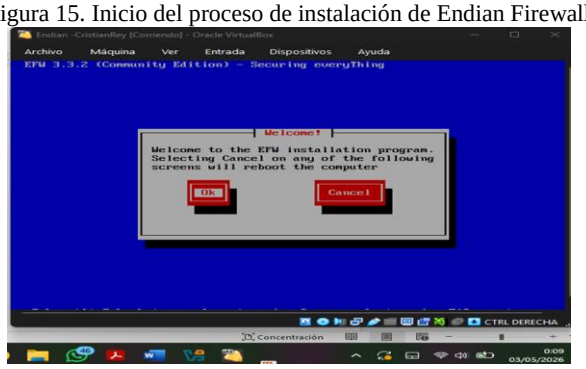
Figura 14. Administración de máquinas virtuales en Oracle VirtualBox



Fuente: Autoría Propia

En esta captura se identifica que se está gestionando las máquinas virtuales dentro de Oracle VirtualBox. Se pueden ver tres entornos creados: Ubuntu - Cristianrey, Linux Mint - Zona Verde, y Endian - CristianRey, todos apagados en ese momento. La ventana de detalles muestra la configuración de la máquina Endian, que es el firewall central del proyecto.

Figura 15. Inicio del proceso de instalación de Endian Firewall



Fuente: Autoría Propia

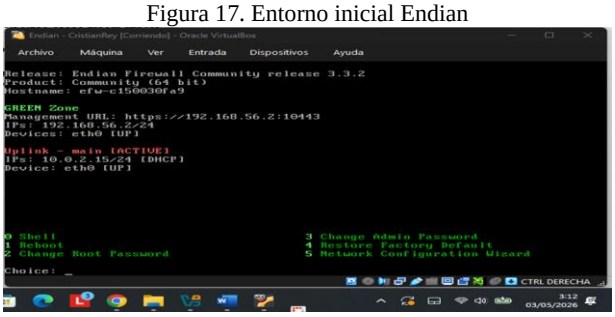
En esta imagen se evidencia el proceso de instalación del Endian Firewall Community Edition dentro de la máquina virtual en Oracle VirtualBox. Se aprecia la pantalla de bienvenida del asistente de instalación, donde se confirma que el sistema está iniciando la configuración del firewall.

Figura 16. Configuración de la interfaz GREEN en Endian Firewall

Fuente: Autoría Propia

En esta imagen se aprecia la configuración de la interfaz GREEN del firewall Endian dentro de la máquina virtual en Oracle VirtualBox. Aquí se define la dirección IP y la máscara de red que corresponden a la zona interna o confiable de la arquitectura.

Figura 17. Entorno inicial Endian



Fuente: Autoría Propia

7.4 CONFIGURACIÓN LINUX MINT EN LA ZONA VERDE (LAN)

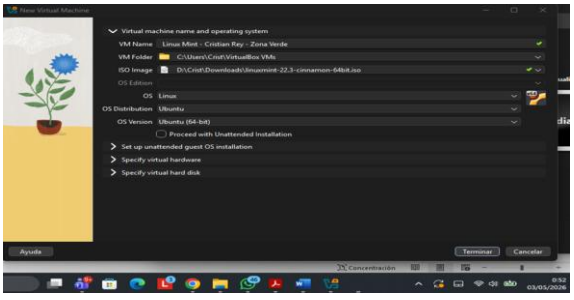
La máquina virtual Linux Mint fue creada con el propósito de actuar como cliente dentro de la red interna (zona VERDE), siguiendo la arquitectura definida en la Temática 1. Esta configuración es fundamental porque permite validar la segmentación de red y comprobar la correcta aplicación de las reglas de firewall en Endian.

7.4.1 PARÁMETROS PRINCIPALES

- Tipo de red: Red interna.
- Nombre de la red: VERDE_LAN.
- Dirección IP: Asignada automáticamente mediante el servicio DHCP habilitado en el firewall Endian.
- Puerta de enlace: 192.168.56.2 (interfaz GREEN del firewall).

De esta manera, Linux Mint no requiere configuración manual de IP, lo que facilita la administración de clientes en la LAN y asegura que todos los equipos se integren de forma homogénea.

Figura 18. Creación de máquina virtual Linux Mint en VirtualBox

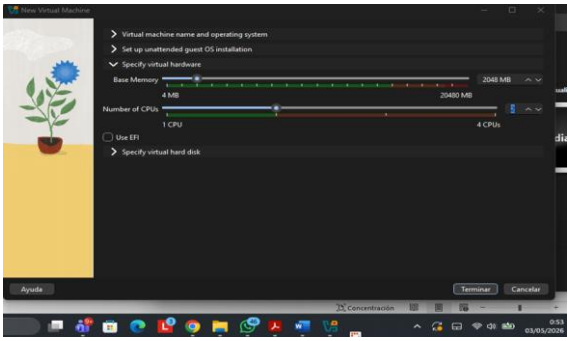


Fuente: Autoría Propia

Se observa una nueva máquina virtual en Oracle VirtualBox para instalar Linux Mint, que será el cliente dentro de la zona VERDE (LAN). Se observa el asistente de

configuración y se asigna el nombre Linux Mint - Cristian Rey - Zona Verde, se define la carpeta de destino y se selecciona la ISO de instalación desde el disco.

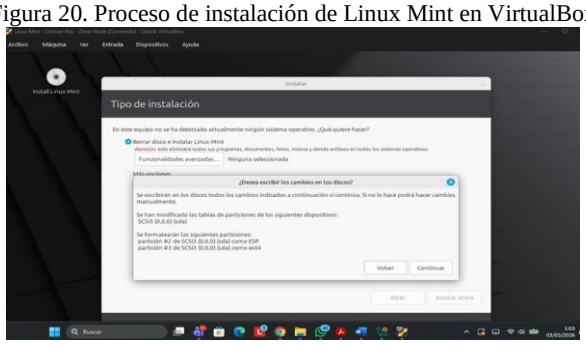
Figura 19. Asignación de recursos de hardware para Linux Mint



Fuente: Autoría Propia

En esta imagen se realiza la configuración de hardware de la máquina virtual Linux Mint.

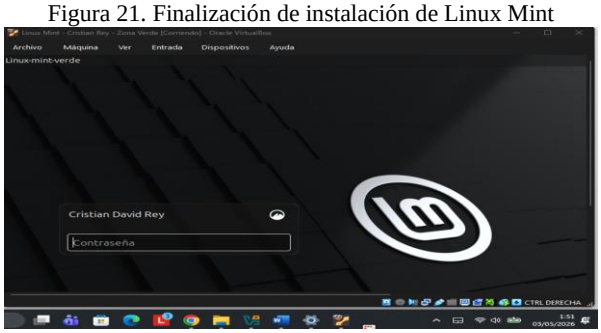
Figura 20. Proceso de instalación de Linux Mint en VirtualBox



Fuente: Autoría Propia

En esta imagen se evidencia el proceso de instalación de Linux Mint dentro de la máquina virtual en Oracle VirtualBox. Se muestra la pantalla donde se debe elegir el tipo de instalación y confirmar los cambios en el disco, lo que implica borrar el contenido previo y crear nuevas particiones para el sistema.

Figura 21. Finalización de instalación de Linux Mint

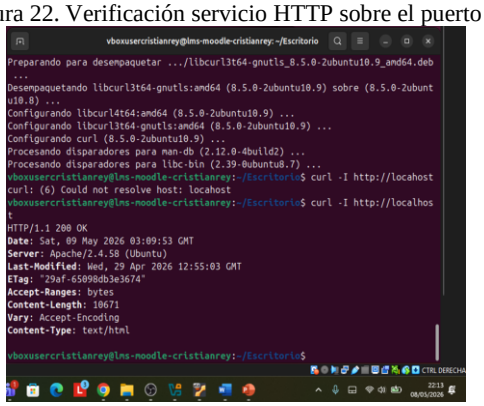


Fuente: Autoría Propia

7.5 VERIFICACIÓN PRÁCTICA

Se utilizaron herramientas como curl, telnet y nc para validar la conectividad de los servicios. Además, se revisaron los logs (journalctl, /var/log/ufw.log) para confirmar la aplicación de las reglas y detectar intentos de acceso bloqueados.

Figura 22. Verificación servicio HTTP sobre el puerto 80



Fuente: Autoría Propia

Para este paso se está verificando el funcionamiento del servidor Apache en la máquina Ubuntu dentro de la zona DMZ. En la terminal se ven los mensajes de instalación de librerías necesarias y luego ejecutó comando curl para comprobar la respuesta del servidor web.

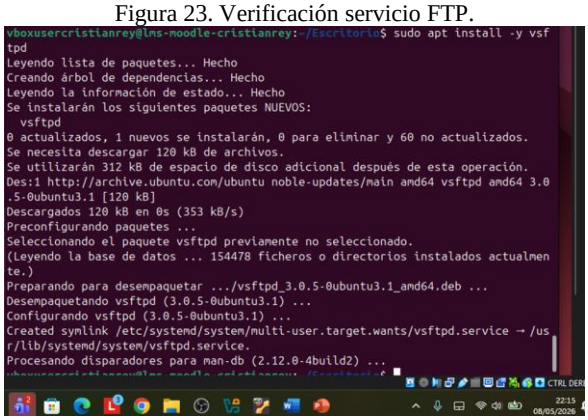
7.5.1 RESULTADOS OBTENIDOS

La implementación permitió:

- Exponer servicios web y FTP de manera controlada desde la DMZ.
- Garantizar la disponibilidad de recursos sin comprometer la red interna.
- Bloquear ICMP, reforzando la protección contra intentos de reconocimiento y ataques básicos.

Este resultado demuestra que la combinación de segmentación de red + reglas de firewall es una estrategia efectiva para balancear accesibilidad y seguridad.

Figura 23. Verificación servicio FTP.



Fuente: Autoría Propia.

Se evidencia la configuración del servicio FTP en el servidor Ubuntu. Se ejecutó el comando para instalar vsftpd y el sistema descargó los paquetes necesarios desde los repositorios oficiales. Al finalizar, el servicio quedó habilitado y listo para iniciar automáticamente con el sistema. Este paso es fundamental porque permite ofrecer un servicio de transferencia de archivos en la DMZ, controlado por las reglas del firewall Endian, garantizando disponibilidad y seguridad en el acceso.

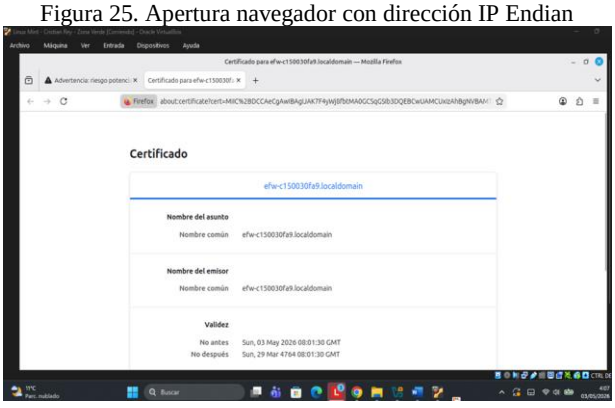
Figura 24: Verificación conexión con Endian

Fuente: Autoría Propia.

La imagen corresponde a una sesión en la terminal de Linux Mint ejecutado en Oracle VirtualBox, en la cual se realiza una prueba de conectividad mediante el comando ping hacia la dirección IP 192.168.56.2.

El resultado evidencia la transmisión de cuatro paquetes ICMP, todos recibidos exitosamente, con un 0% de pérdida de paquetes y tiempos de respuesta mínimos (1.36 ms) y máximos (5.10 ms). El promedio de latencia registrado fue de 3.324 ms, lo que confirma una comunicación estable entre la máquina virtual y el dispositivo de destino.

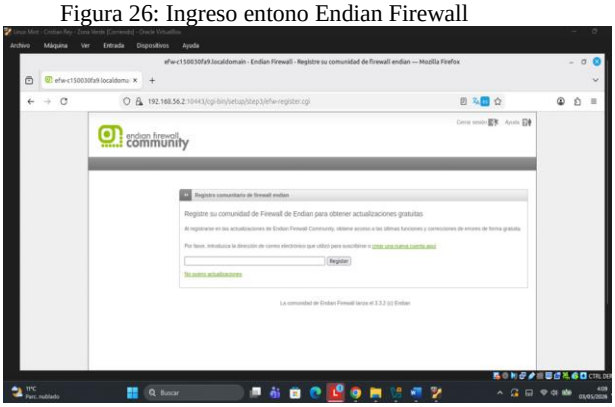
Figura 25. Apertura navegador con dirección IP Endian



Fuente: Autoría Propia.

La imagen muestra la visualización de un certificado digital en Mozilla Firefox dentro de Linux Mint ejecutado en VirtualBox, correspondiente al dominio efw-c15003fa9.localdomain. El certificado presenta coincidencia entre el nombre del asunto y el emisor, con una validez que inicia el 3 de mayo de 2026 y se extiende hasta el 29 de marzo del año 4764. La interfaz advierte un posible riesgo de seguridad, lo que evidencia que se trata de un certificado autofirmado o no confiable para el navegador. Este registro constituye evidencia técnica de la configuración de servicios en un entorno virtualizado y su impacto en la gestión de seguridad informática.

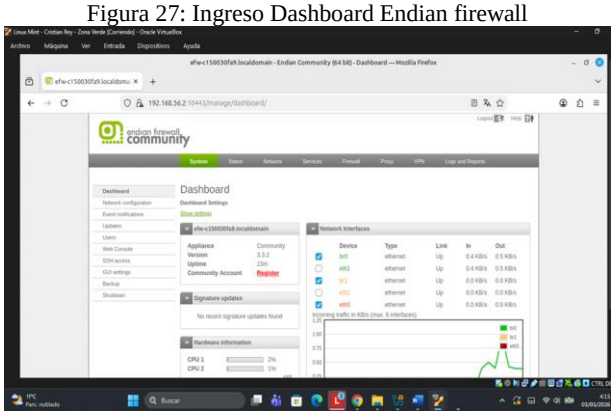
Figura 26: Ingreso entono Endian Firewall



Fuente: Autoría Propia.

En la imagen se muestra el entorno donde se está realizando la configuración inicial del firewall Endian desde una máquina virtual en VirtualBox, accediendo a su interfaz web mediante el navegador Firefox. En este paso, se realiza el registro en la comunidad de Endian Firewall para habilitar actualizaciones gratuitas y acceso a mejoras del sistema. Este proceso hace parte de la puesta en marcha y aseguramiento del correcto funcionamiento del firewall en el entorno de red.

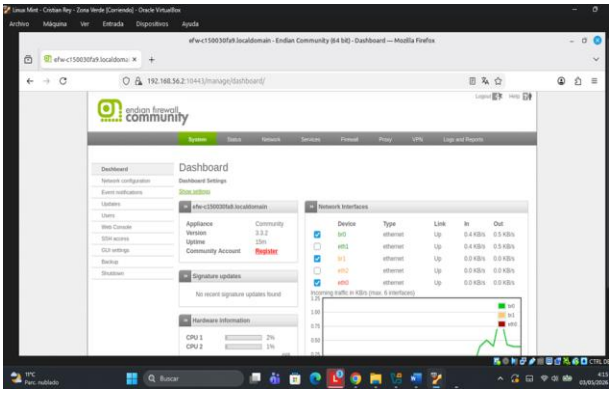
Figura 27: Ingreso Dashboard Endian firewall



Fuente: Autoría Propia.

En la imagen se evidencia el panel principal del dashboard de Endian Firewall Community, desde donde se monitorea el estado del sistema y las interfaces de red. Este panel permite verificar el funcionamiento del firewall y el tráfico de la red en tiempo real.

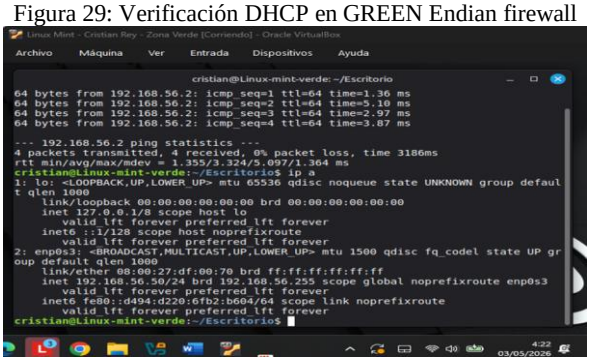
Figura 28: Verificación DHCP en GREEN Endian firewall



Fuente: Autoría Propia.

En la imagen se evidencia la configuración del servicio DHCP en Endian Firewall, activándolo en la interfaz GREEN para asignar direcciones IP de forma automática. Esta configuración permite gestionar la red interna de manera eficiente y controlada.

Figura 29: Verificación DHCP en GREEN Endian firewall



Fuente: Autoría Propia.

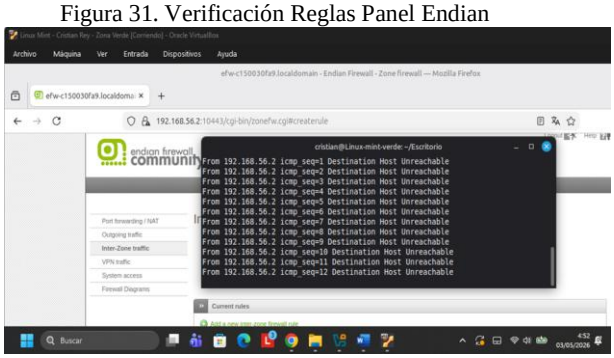
Se valida la conectividad de red desde la terminal de Linux Mint, comprobando la comunicación con el firewall mediante comandos ping y ip a. Los resultados confirman que la interfaz de red está activa y correctamente configurada dentro del entorno virtual.

Figura 30. Configuración Reglas Panel Endian

Fuente: Autoría Propia.

En este paso se está gestionando las reglas del firewall en Endian, configurando el tráfico permitido entre las diferentes zonas de red como GREEN, BLUE y ORANGE. Estas reglas permiten controlar el acceso y asegurar la comunicación entre los segmentos de la red de forma segura.

Figura 31. Verificación Reglas Panel Endian



Fuente: Autoría Propia.

Verificamos con ping 192.168.57.10 el cual debe fallar, es decir, sin respuestas. En este momento se verifica la conectividad entre redes mientras se ajustan las reglas del firewall en Endian, ejecutando pruebas de ping desde la terminal. El mensaje Destination Host Unreachable lo que indica que el tráfico está siendo bloqueado, lo que confirma que las políticas de seguridad están aplicándose correctamente.

Figura 32. Verificación Reglas Panel Endian

Fuente: Autoría Propia.

Ejecutamos ping 192.168.56.2 y verificamos que si se obtienen respuestas. En este paso se verifica nuevamente la conectividad de red desde la terminal de Linux Mint, ejecutando un comando ping hacia el firewall. Las respuestas exitosas confirman que la comunicación se ha restablecido correctamente y que las reglas configuradas están funcionando como se esperaba.

7.6 LA PRÁCTICA EVIDENCIÓ QUE:

- La DMZ es un componente esencial en arquitecturas seguras, ya que permite publicar servicios sin abrir la LAN a riesgos externos.
- La correcta configuración de reglas de firewall es determinante para garantizar que solo los protocolos necesarios estén habilitados.
- El bloqueo de ICMP, aunque pueda parecer una restricción menor, es clave para evitar ataques de

reconocimiento que suelen ser la primera fase de intrusiones más complejas.

- La dependencia de la Temática 1 muestra la importancia del trabajo colaborativo: la configuración inicial del firewall fue la base para el éxito de la Temática 3.

En conclusión, este ejercicio no solo cumplió con los objetivos técnicos, sino que también fortaleció competencias en administración de sistemas Linux, gestión de firewalls y aplicación de estándares de ciberseguridad.

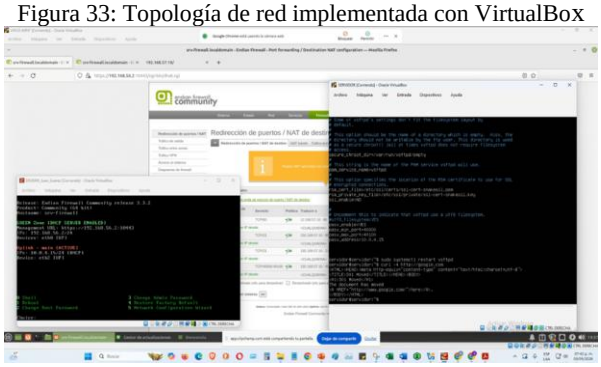
8 TEMÁTICA 4: REGLAS DE ACCESO Y CONTROL DE TRÁFICO

La seguridad perimetral en entornos virtualizados constituye una habilidad esencial para cualquier profesional de infraestructura tecnológica. En esta actividad se buscó aplicar conceptos de segmentación de redes y control de tráfico mediante herramientas de código abierto. Para ello, se utilizó GNU/Linux como sistema base y Endian Firewall Community (EFW) como solución de firewall. El objetivo principal fue diseñar e implementar una arquitectura que separara de manera segura las zonas LAN, DMZ y WAN, permitiendo únicamente el tránsito autorizado de datos. Esta experiencia simuló un escenario realista, lo que facilitó la comprensión práctica de los principios de defensa por profundidad y aislamiento de servicios críticos.

8.1 IMPLEMENTACIÓN DEL ENTORNO Y CONFIGURACIÓN DE REGLAS

En esta práctica se implementó un entorno de seguridad perimetral virtualizado utilizando GNU/Linux y Endian Firewall Community (EFW). Se empleó Oracle VirtualBox para crear tres máquinas virtuales que representan el firewall perimetral, un servidor en la zona DMZ y un cliente en la LAN. Se configuró cuidadosamente la topología de red, asignando cada interfaz a la zona correspondiente (LAN, DMZ y WAN) y ajustando las direcciones IP para garantizar conectividad estable. Posteriormente, se definieron reglas de acceso en la consola de Endian que permiten únicamente el tráfico legítimo de los servicios HTTP y FTP entre la LAN y la DMZ, limitando puertos, direcciones origen y destino. También se extendieron las políticas para controlar el acceso desde la WAN hacia la DMZ. Las pruebas de conectividad se realizaron con comandos como ping, curl y ftp, confirmando el correcto aislamiento de las zonas.

Figura 33: Topología de red implementada con VirtualBox

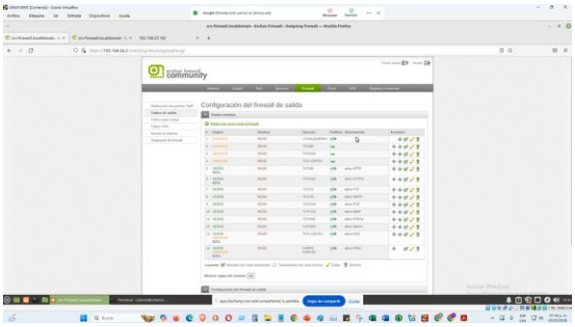


Fuente: Autoría Propia.

8.2 SEGMENTACIÓN DE REDES Y GESTIÓN DE REGISTROS

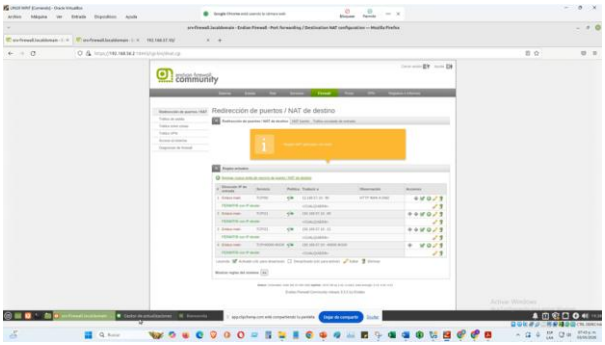
La segmentación de redes resultó fundamental para lograr que cada zona opere de forma independiente y segura. Al separar la LAN, la DMZ y la WAN mediante reglas de firewall, se evitó que una posible falla en un segmento comprometa a los demás, cumpliendo así el principio de seguridad perimetral de aislar los recursos críticos. Además, la administración de los registros (logs) del firewall permitió depurar errores de configuración, como puertos incorrectos o direcciones IP mal asignadas. Esta experiencia práctica reforzó competencias en administración de sistemas GNU/Linux y en el manejo de herramientas de firewall, mostrando cómo la teoría se traduce directamente en escenarios reales.

Figura 34: Configuración de reglas de acceso en la consola de Endian Firewall



Fuente: Autoría Propia.

Figura 35: Prueba de conectividad HTTP desde el navegador en la zona LAN



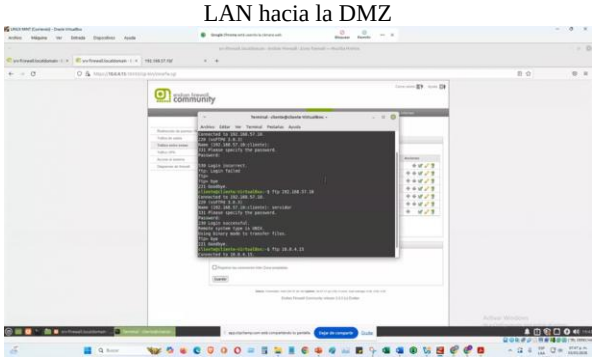
Fuente: Autoría Propia.

8.3 VALIDACIÓN DE SERVICIOS

Se validó el funcionamiento de los servicios HTTP y FTP desde diferentes puntos de la red, comprobando que tanto desde el cliente en la LAN como desde un navegador web se accedía correctamente a los recursos de la DMZ, mientras que el tráfico no autorizado era bloqueado. El uso de comandos básicos de GNU/Linux permitió verificar el estado de los servicios y ajustar procesos cuando fue necesario. Esta actividad demostró que un firewall no es una “caja negra” sino una herramienta que

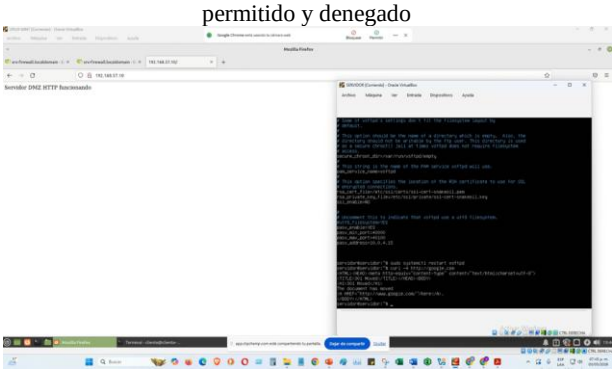
exige diseño, prueba continua y ajuste. Se consolidaron habilidades para definir políticas de acceso precisas, controlar el tráfico entre zonas y proteger infraestructuras virtualizadas, fortaleciendo así la formación en seguridad informática y redes basadas en Linux.

Figura 36: Prueba de conectividad FTP desde cliente en la LAN hacia la DMZ



Fuente: Autoría Propia.

Figura 37: Registro de logs (firewall) mostrando tráfico permitido y denegado



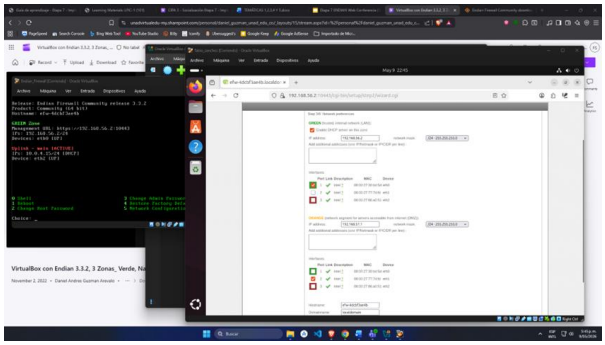
Fuente: Autoría Propia.

9 TEMÁTICA 5: IMPLEMENTACIÓN DEL PROXY HTTP

En esta práctica de la temática 5 se implementó un proxy HTTP no transparente con autenticación de usuarios utilizando el Endian Firewall Community que venimos trabajando y el servicio Squid [9] con el objetivo principal de controlar y monitorear el acceso a Internet desde la red LAN mediante autenticación de usuarios, políticas de acceso y filtrado de contenido web.

Inicialmente, se verificó la correcta configuración de las zonas de red GREEN y ORANGE dentro de Endian Firewall, asegurando la conectividad entre las máquinas virtuales y el acceso a Internet.

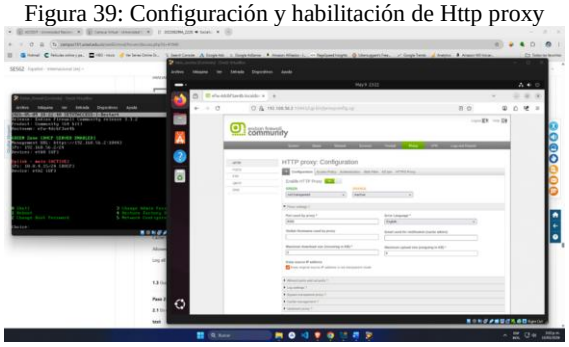
Figura 38: Configuración redes GREEN y ORANGE



Fuente: Autoría Propia.

Posteriormente, se habilitó el servicio HTTP Proxy en modo no transparente sobre la zona GREEN, utilizando el puerto 8080 para las conexiones de los clientes internos.

Figura 39: Configuración y habilitación de Http proxy



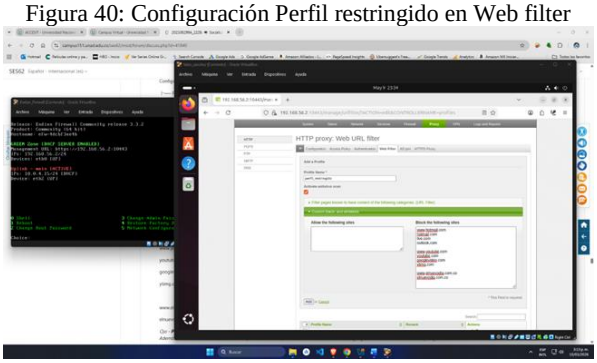
Fuente: Autoría Propia.

Luego, se creó un perfil de filtrado web denominado “perfil_restringido”, en el cual se agregaron dominios bloqueados como:

- hotmail.com
- youtube.com
- elnuevodia.com.co

Esta configuración permitió restringir el acceso a determinados sitios web desde la red LAN.

Figura 40: Configuración Perfil restringido en Web filter



Fuente: Autoría Propia.

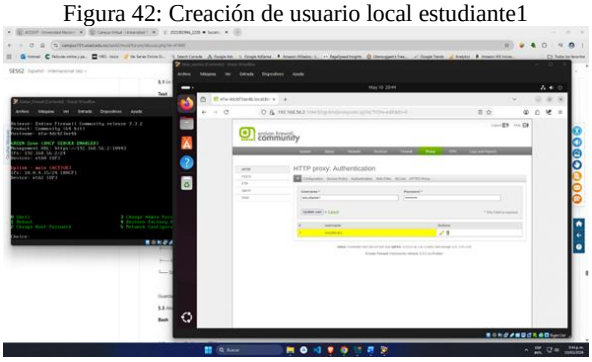
Después de configurar el web filter, se configuró el módulo de autenticación utilizando el método Local Authentication (NCSA). Se definió el "Authentication Realm" denominado "Proxy Seguro UNAD", permitiendo que los usuarios deban autenticarse antes de acceder a Internet a través del proxy.

Figura 41: Pantalla de Authentication del proxy

Fuente: Autoría Propia.

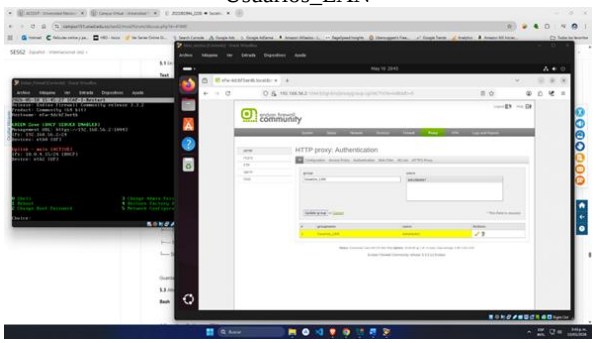
Posteriormente, se creó un usuario local dentro de Endian Firewall para utilizar el proxy autenticado, y el usuario fue asociado luego al crear un grupo de usuarios llamado Usuarios_LAN.

Figura 42: Creación de usuario local estudiante1



Fuente: Autoría Propia.

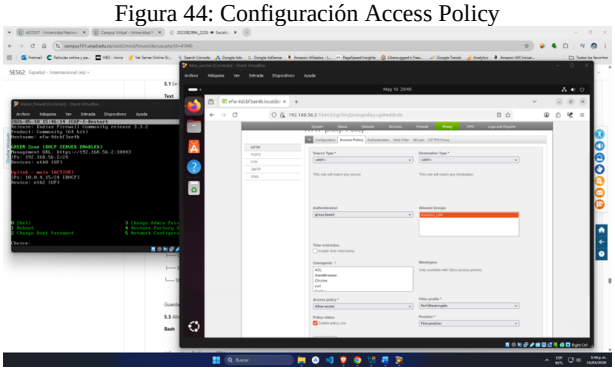
Figura 43: Creación de Grupo de usuarios local Usuarios_LAN



Fuente: Autoría Propia.

A continuación, se configuró una política de acceso dentro del módulo "Access Policy", seleccionando autenticación basada en usuario y asociando el perfil de filtrado creado anteriormente. Esta política permitió aplicar las restricciones web únicamente a los usuarios autenticados.

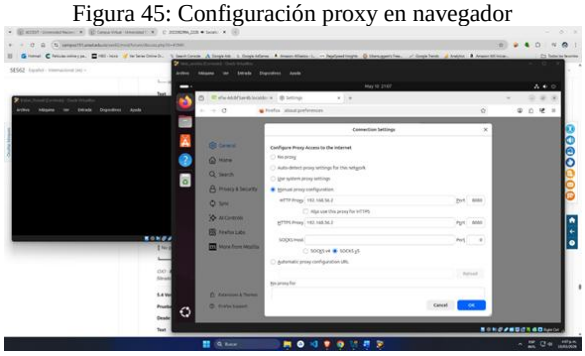
Figura 44: Configuración Access Policy



Fuente: Autoría Propia.

Posteriormente, desde nuestro cliente Ubuntu-LAN se configuró manualmente el proxy en el navegador Firefox utilizando la dirección IP del firewall y el puerto 8080. Esta configuración fue necesaria debido a que el proxy implementado era no transparente.

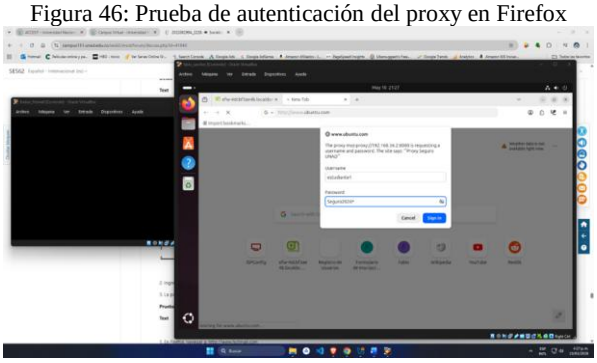
Figura 45: Configuración proxy en navegador



Fuente: Autoría Propia.

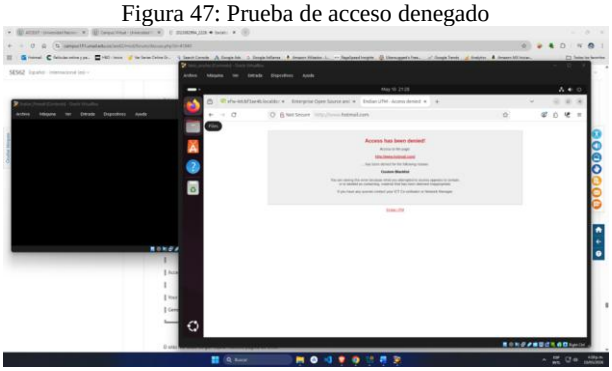
Finalmente, se realizaron pruebas de funcionamiento para verificar el comportamiento del proxy evidenciando que, al intentar acceder a sitios permitidos, el navegador solicitó autenticación mediante usuario y contraseña. Después de autenticarse correctamente, fue posible navegar normalmente. Sin embargo, al intentar acceder a dominios incluidos en la lista negra, el proxy mostró mensajes de acceso denegado, confirmando el correcto funcionamiento del filtrado web

Figura 46: Prueba de autenticación del proxy en Firefox



Fuente: Autoría Propia.

Figura 47: Prueba de acceso denegado



Fuente: Autoría Propia.

10 DISCUSIÓN

La implementación realizada permitió comprender la importancia de la seguridad perimetral en entornos GNU/Linux y cómo la segmentación de redes ayuda a proteger la infraestructura frente a accesos no autorizados. El uso de Endian Firewall facilitó la administración centralizada de las reglas de seguridad, permitiendo controlar el tráfico entre las diferentes zonas de la red de manera organizada.

Durante el desarrollo de la práctica se evidenció que la configuración de servicios en la DMZ representa una estrategia importante para publicar recursos sin comprometer directamente la red interna. Asimismo, las reglas NAT y las políticas de acceso ayudaron a limitar únicamente el tráfico permitido, fortaleciendo la protección de la infraestructura virtualizada.

Sin embargo, durante el desarrollo se presentaron algunas dificultades relacionadas con la configuración inicial de las interfaces de red y la validación de conectividad entre las máquinas virtuales. En algunos casos fue necesario ajustar reglas del firewall y parámetros de red para lograr una comunicación correcta entre las zonas.

En general, la práctica permitió fortalecer conocimientos relacionados con administración de sistemas GNU/Linux, segmentación de redes y configuración de mecanismos de seguridad perimetral, además de evidenciar la importancia de aplicar políticas de control de tráfico en entornos de red.

11 CONCLUSIONES

El ejercicio práctico de seguridad perimetral en un entorno de virtualización en GNU/Linux y Endian Firewall puso de manifiesto los mecanismos de segmentación y protección que debe tener una infraestructura de red. Durante el desarrollo de la actividad, la segmentación por zonas local (LAN), desmilitarizada (DMZ) [1][8] y de acceso a Internet (WAN) permitió aportar un control más específico del tráfico, mientras que las reglas construidas para los servicios HTTP (Hypertext Transfer Protocol) y FTP (File Transfer Protocol) validaron que solo el tráfico autorizado pudiera cruzar entre las distintas redes.

Por otro lado, la integración de NAT (Network Address Translation), las políticas de acceso y el proxy HTTP con autenticación de usuarios permitió incorporar un nivel adicional de seguridad, pero también poder controlar adecuadamente la navegación y los permisos de los usuarios. Las pruebas habilitaron la correcta configuración de los servicios bajo las políticas definidas, lo cual mostró la importancia de estas técnicas para proteger la información y el manejo de redes Linux.

La implementación de herramientas basadas en GNU/Linux permitió fortalecer conocimientos relacionados con la administración de sistemas, configuración de servicios y aplicación de mecanismos de seguridad en entornos virtualizados.

En conjunto, la práctica permitió aplicar los conceptos de seguridad perimetral, segmentación de red y administración de servicios en un entorno virtualizado basado en GNU/Linux. Además de la configuración técnica, la actividad permitió comprender la importancia de aplicar políticas de seguridad adecuadas para proteger la infraestructura de red.

Este ejercicio práctico permitió fortalecer las bases teóricas, pero también el hecho de adquirir un nivel significativo en el manejo de firewalls, de control del tráfico y de segmentación de redes en escenarios reales de ciberseguridad.

La práctica también permitió implementar un proxy HTTP no transparente con autenticación [9] utilizando Endian Firewall Community y Squid. Además, se configuraron políticas de acceso y filtrado web para restringir sitios específicos, comprobando el funcionamiento correcto de la autenticación y el control de navegación en la red LAN.

12 REFERENCIAS

[1] Belmar, A. (2025). Seguridad GNU/Linux: Curso práctico. Ediciones de la U. [En línea]. Disponible en: https://www.perlego.com/es/book/5163054/seguridad-gnulinux-curso-prctico-pdf

[2] Canonical (2023). Help Ubuntu. Ubuntu. [En línea]. Disponible en: https://help.ubuntu.com/

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

[4] Documentation about the netfilter/iptables project. (s/f). Netfilter.org. [En línea]. Disponible en: https://www.netfilter.org/documentation/

[5] Endian. (s.f.). *Endian Firewall Community*. Endian. [En línea]. Disponible en: https://www.endian.com/community/

[6] Ferrer, J., & Fernández-Sanguino, J. (s.f.). El sistema operativo GNU/Linux y sus herramientas libres en el mundo de la seguridad: estudio del estado del arte [En línea]. Disponible en: https://www.ibiblio.org/pub/Linux/docs/LuCaS/Presentaciones/200103hispalinux/ferrer/pdf/seguridad-y-sw-libre_v1.0.pdf

[7] Granados Navarro, B. M., Silva Maldonado, C. F., Garavito Feliciano, D. A., Rodríguez Martín, J. A., & Reyes Hernández, J. S. (2025). Diseño e Implementación de Seguridad Perimetral Basada en Zonas Mediante Endian Firewall en Entornos Gnu/Linux [Diplomado de profundización, Universidad Nacional Abierta y a Distancia UNAD]. Repositorio Institucional UNAD. [En línea]. Disponible en: https://repository.unad.edu.co/handle/10596/77418

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

[9] Squid Project. (s.f.). *Squid Proxy Wiki*. Squid Cache [En línea]. Disponible en: https://wiki.squid-cache.org/

[10] The Linux Foundation. (2024). Linux Documentation Project [En línea]. Disponible en: https://www.kernel.org/doc/