“IMPLEMENTACIÓN DE SEGURIDAD EN GNU/LINUX “

Carlos Alberto Puerta Acosta
e-mail: capuertaac@unadvirtual.edu.co
Luisa Fernanda Canizales Valencia
e-mail: lfcanizalesv@unadvirtual.edu.co
Juan David Tique Robayo
e-mail: jdtiquero@unadvirtual.edu.co
Juan Pablo Lopez Reinoso
e-mail: jplopezr@unadvirtual.edu.co
Danny Alexander Mesa Barragan
e-mail: damesab@unadvirtual.edu.co

RESUMEN: *En esta actividad se desarrolló la implementación de medidas de seguridad en sistemas GNU/Linux con el propósito de fortalecer la administración de servicios esenciales desde un enfoque práctico. Inicialmente, se revisaron los contenidos del tema 101 del curso Linux Essentials del LPI, realizando ejercicios guiados y exploratorios que permitieron comprender la estructura básica del sistema y sus permisos. De manera colaborativa, se trabajó en un escenario de seguridad perimetral donde se configuró la distribución Endian Firewall (EFW) para proteger la infraestructura conformada por LAN, WAN y una zona DMZ. Cada integrante instaló y verificó los servicios del sistema mediante comandos administrativos, documentando su ejecución. La actividad permitió relacionar conceptos de seguridad, planificación de red y administración de servicios bajo GNU/Linux, fortaleciendo competencias necesarias para la protección de entornos informáticos.*

PALABRAS CLAVE: GNU/Linux, Endian Firewall, seguridad, administración de servicios.

1 INTRODUCCIÓN

En el desarrollo de esta actividad se trabajó la implementación de medidas de seguridad en sistemas GNU/Linux, con el fin de comprender cómo gestionar servicios esenciales y fortalecer el entorno operativo desde un enfoque administrativo.

2 DESARROLLO

2.1 DESARROLLO DE LA ACTIVIDAD

La actividad grupal planteó un escenario relacionado con la protección perimetral de una red que integra LAN, WAN y una zona DMZ. Para abordar este reto se definió como prioridad garantizar la integridad de los servidores que alojan bases de datos y aplicaciones web bajo plataformas GNU/Linux. Para ello se seleccionó la distribución Endian Firewall (EFW) como solución de seguridad.

Cada integrante realizó la instalación, configuración y revisión de los servicios del sistema mediante comandos administrativos, validando el estado de los procesos. Todas las ejecuciones se documentaron con fecha y hora para asegurar la evidencia técnica. Este procedimiento permitió comprender de manera práctica cómo opera un firewall y cómo se gestionan sus módulos internos desde la consola.

2.2 PLANIFICACIÓN

En la implementación se definió una arquitectura funcional compuesta por GNU/Linux para la LAN, un firewall Endian encargado de gestionar el tráfico de la red, y un servidor GNU/Linux en la DMZ. La planificación también incluyó la asignación de direccionamientos IP coherentes que permitieran garantizar la comunicación entre cada segmento de la red. Este direccionamiento debía mantenerse uniforme entre los integrantes del grupo para facilitar la consolidación del trabajo final.

3 RESULTADOS

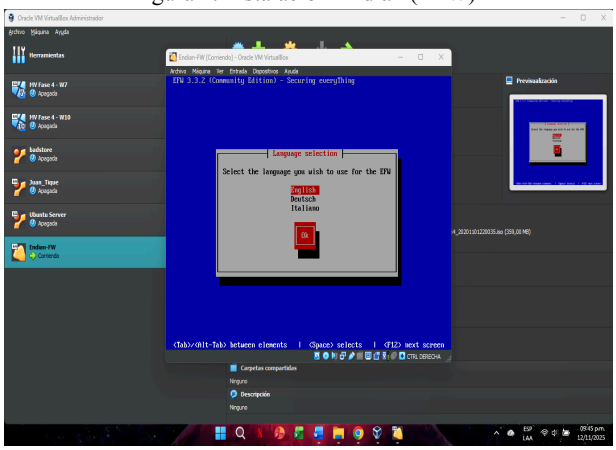
El desarrollo permitió comprender los fundamentos de seguridad en redes, así como la importancia de aplicar buenas prácticas en la gestión de servicios. El uso de herramientas como Endian Firewall facilitó el aprendizaje sobre políticas de acceso, monitoreo del tráfico y administración de servicios. Además, la revisión del material Linux Essentials fortaleció la comprensión de los elementos básicos necesarios para operar entornos GNU/Linux con mayores niveles de seguridad.

4 DESARROLLO DE TEMÁTICAS

A continuación, se presenta el desarrollo de cada una de las temáticas realizada por cada integrante del grupo, evidenciado la funcionalidad de lo requerido para la actividad.

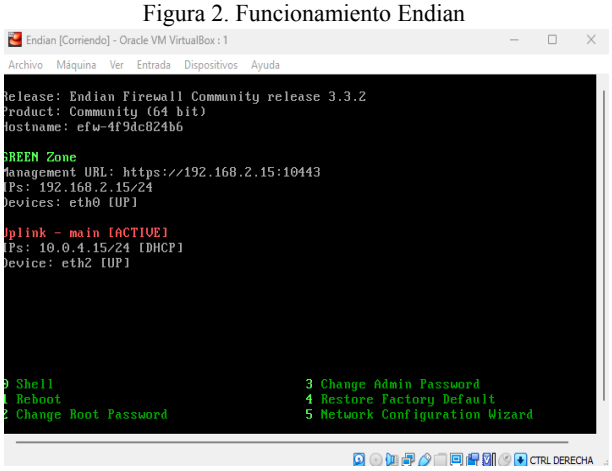
Adaptador 1: Red interna, Redverde (LAN), Adaptador 2: Red Interna, Rednaranja (DMZ), Adaptador 3: NAT, Zona Roja (WAN).

Figura 1. Instalación Endian (EFW)



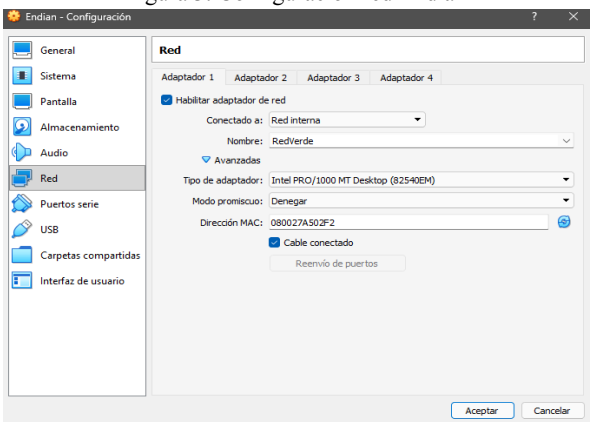
Fuente: Autoría Propia

Figura 2. Funcionamiento Endian



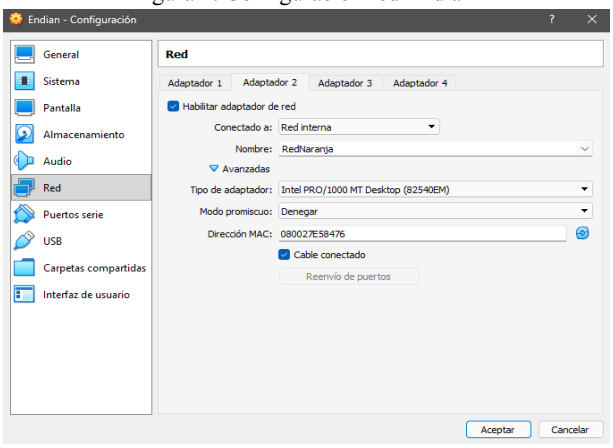
Fuente: Autoría Propia

Figura 3. Configuración red Endian



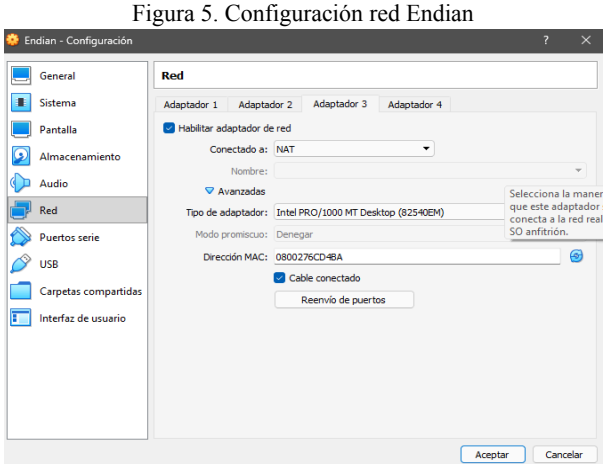
Fuente: Autoría Propia

Figura 4. Configuración red Endian



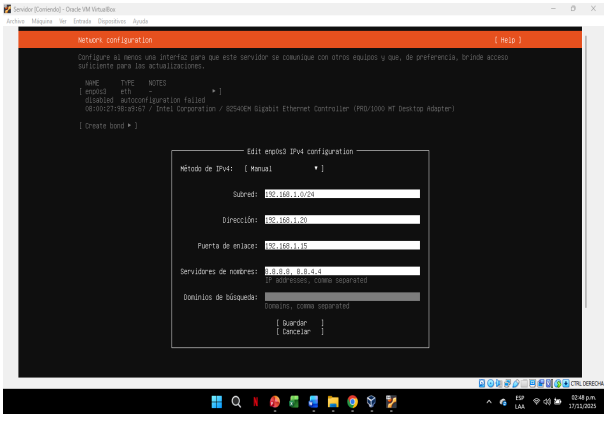
Fuente: Autoría Propia

Figura 5. Configuración red Endian



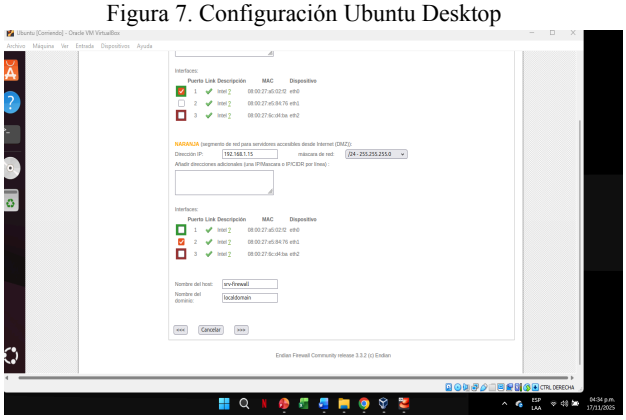
Fuente: Autoría Propia

Figura 6. Configuración Ubuntu Server



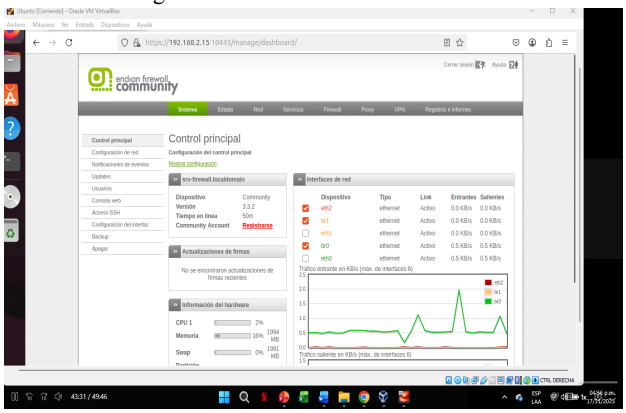
Fuente: Autoría Propia

Figura 7. Configuración Ubuntu Desktop



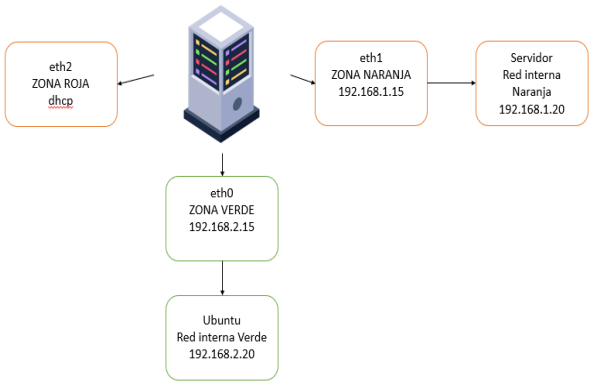
Fuente: Autoría Propia

Figura 8. Funcionamiento de Zonas



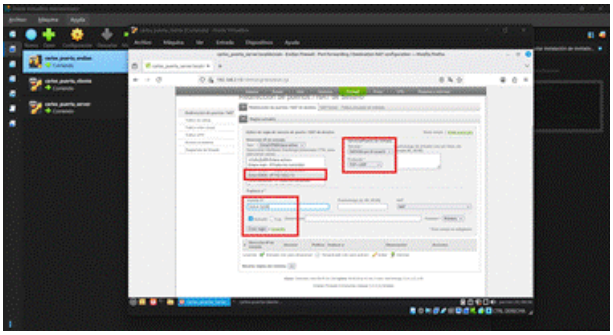
Fuente: Autoría Propia

Figura 9. Diagrama de configuración de zonas.



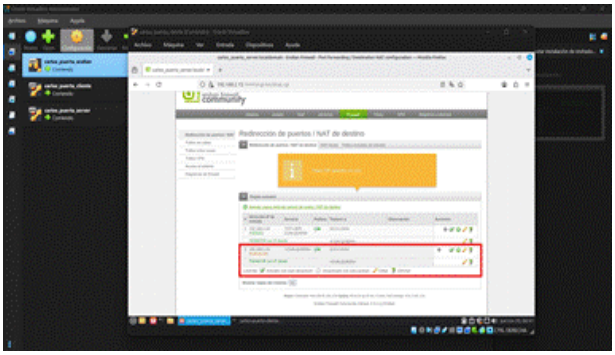
Fuente: Autoría Propia

Figura 10. Configuración de la primera regla en endian (temática 2)



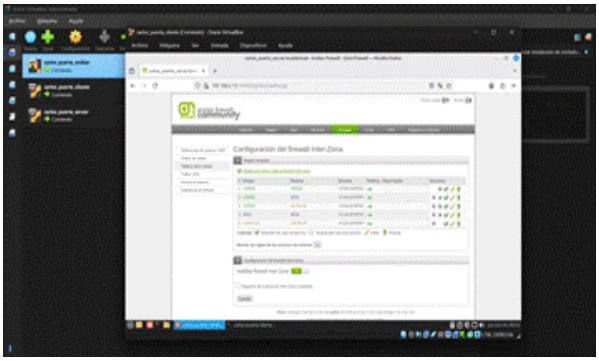
Fuente: Autoría Propia

Figura 11. Configuración de la segunda regla en endian (temática 2)



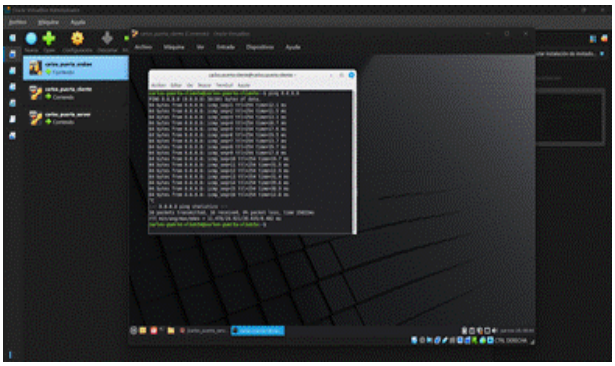
Fuente: Autoría Propia

Figura 12. Tráfico entre zonas en endian (temática 2)



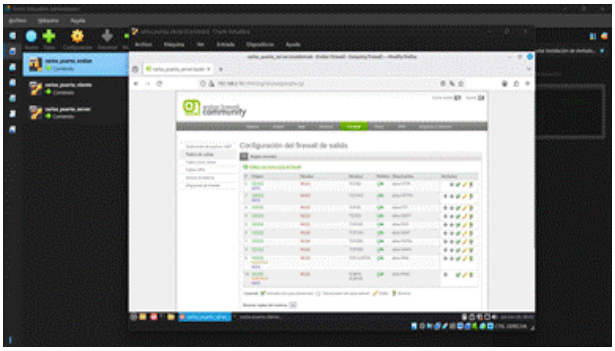
Fuente: Autoría Propia

Figura 13. Prueba de conexión DNS de Google (temática 2)



Fuente: Autoría Propia

Figura 14. Tráfico de salidas en endian (temática 2)

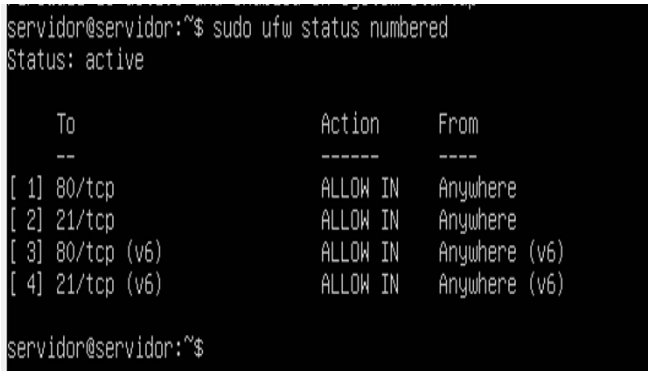


Fuente: Autoría Propia

Figura 15. Reglas de Firewall para permitir los servicios HTTP y FTP (Temática 3)

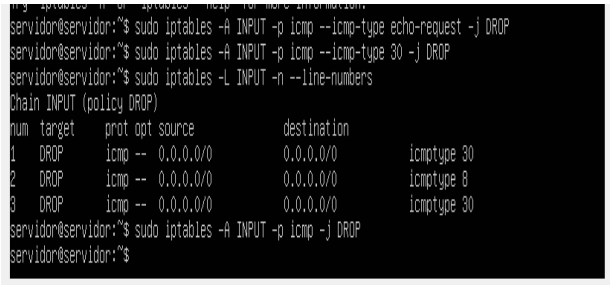
Fuente: Autoría Propia

Figura 16. Evidencia de la activación de las reglas creadas en Ubuntu Server (Temática 3)



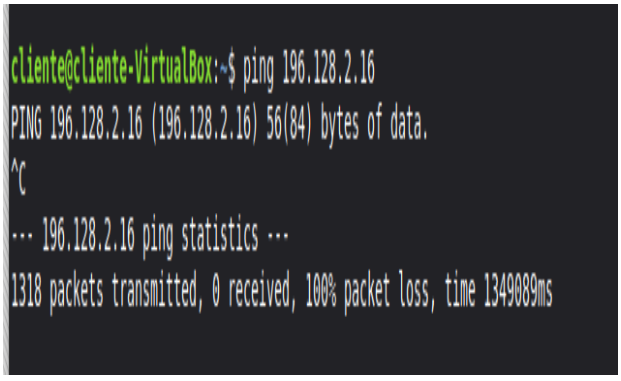
Fuente: Autoría Propia

Figura 17. Denegar protocolo ICMP (Puerto 8 y 30) (Temática 3)



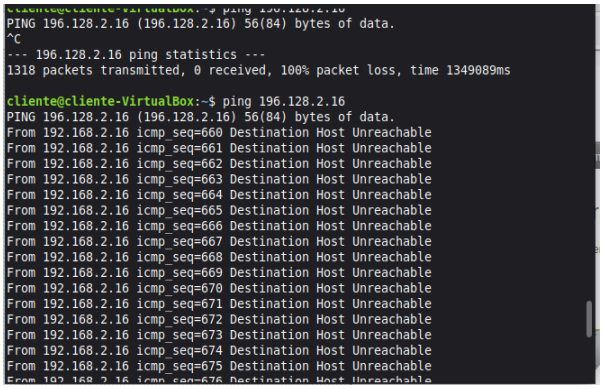
Fuente: Autoría Propia

Figura 18. Ejecución del ping desde la terminal. (Temática 3)



Fuente: Autoría Propia

Figura 19. Ejecución del ping desde la terminal nuevamente. (Temática 3)



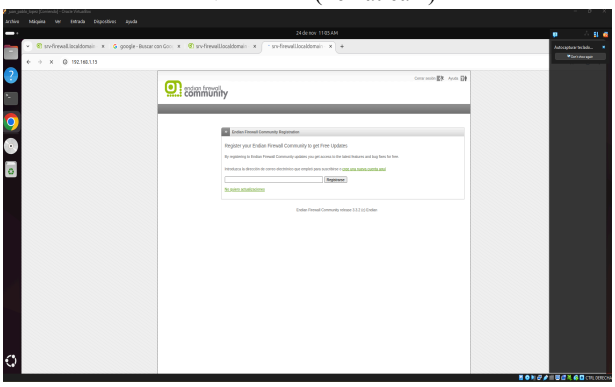
Fuente: Autoría Propia

Figura 20. Reglas de Firewall para permitir los servicios HTTP y FTP (Temática 4)

#	Origen	Destino	Servicio	Política	Observación	Acciones
1	<CUALQUIERA>	NARANJA	TCP/80			
2	VERDE	NARANJA	TCP/21			
3	VERDE	NARANJA	TCP/80			
4	VERDE	VERDE	<CUALQUIERA>			

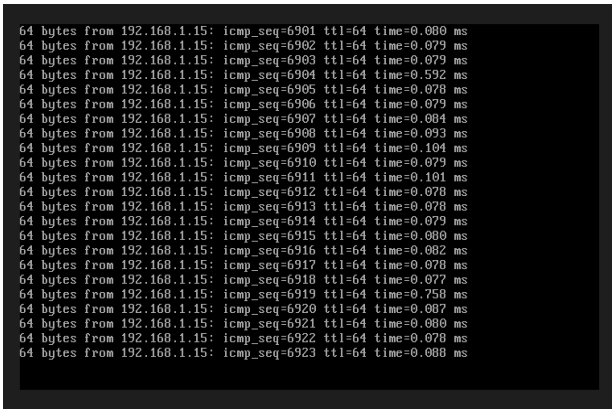
Fuente: Autoría Propia

Figura 21. Pruebas con navegador y cliente FTP: HTTP desde LAN → DMZ (Temática 4)



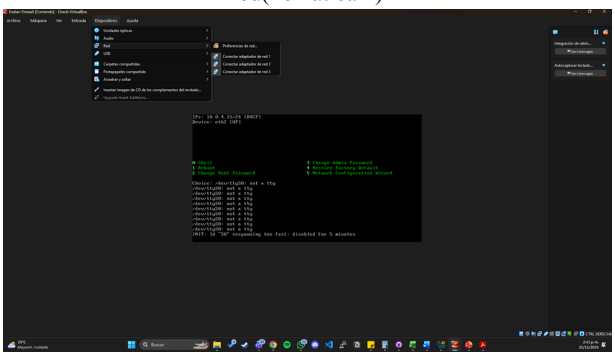
Fuente: Autoría Propia

Figura 22. Ejecución del ping desde la terminal (Temática 4)



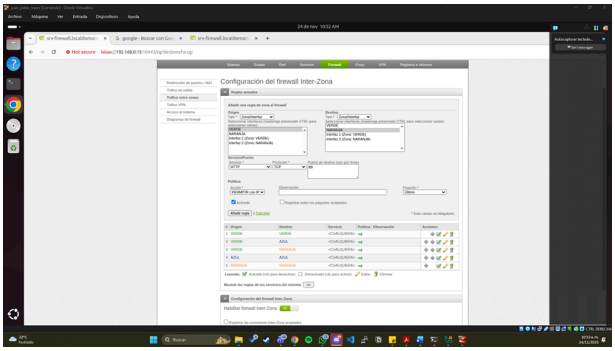
Fuente: Autoría Propia

Figura 23. 3 Interfaces/Adaptadores de RED, Green, Orange, Red(Temática 4)



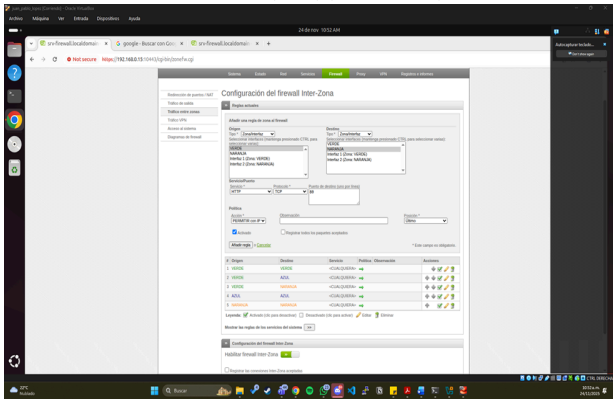
Fuente: Autoría Propia

Figura 24. Configuración de Reglas Firewall GREEN → ORANGE (HTTP)(Temática 4)



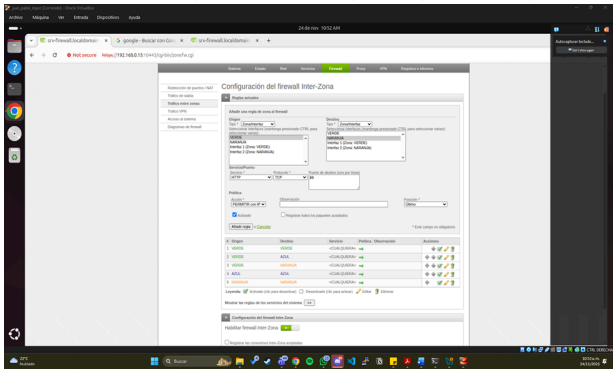
Fuente: Autoría Propia

Figura 25. Configuración de Reglas Firewall. GREEN → ORANGE (FTP)(Temática 4)



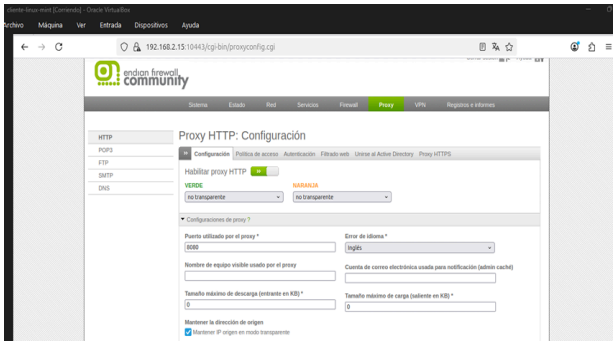
Fuente: Autoría Propia

Figura 26. Configuración de Reglas Firewall. RED (INTERNET) → ORANGE (DMZ)(Temática 4)



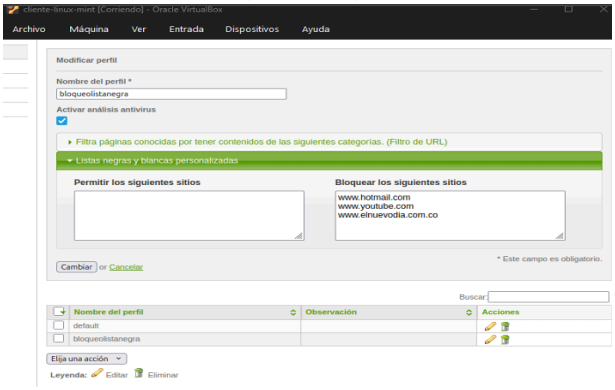
Fuente: Autoría Propia

Figura 27. Poner el proxy en modo NO transparente en la interfaz de Endian (Temática 5)



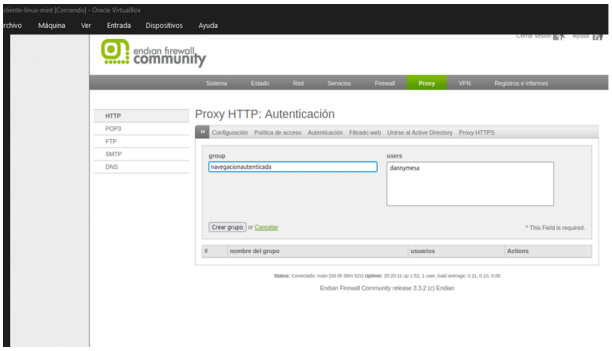
Fuente: Autoría Propia

Figura 28. Crear el perfil con lista negra y política de acceso (Temática 5)



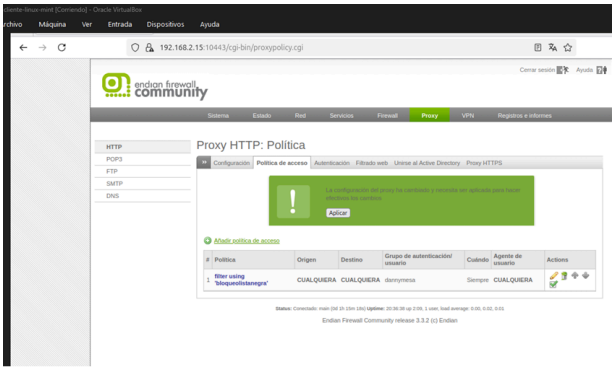
Fuente: Autoría Propia

Figura 29. Crear usuarios y grupos locales (Temática 5)



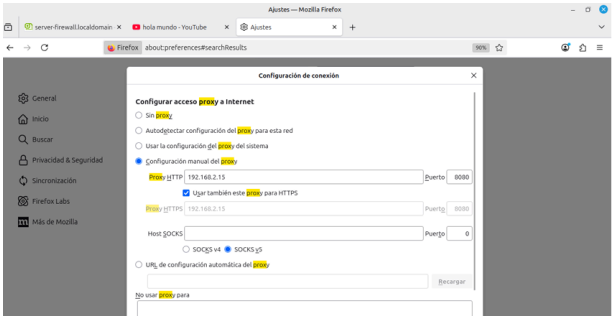
Fuente: Autoría Propia

Figura 30. Vincular perfil y autenticación (Temática 5)



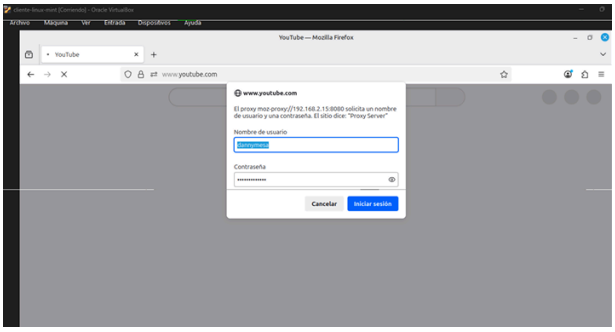
Fuente: Autoría Propia

Figura 31. Configurar los navegadores del lado del cliente (Temática 5)



Fuente: Autoría Propia

Figura 32. Pruebas desde la LAN de ingreso a los dominios (Temática 5)



Fuente: Autoría Propia

Enlace de los trabajos individuales de la actividad:
https://drive.google.com/drive/folders/1S_OGKAe9JwQ3PSbsTKzaO_zvl3-KO3M2?usp=sharing

5 CONCLUSIONES

En la temática 1 la configuración de Endian en VirtualBox me permitió comprender cómo funcionan las zonas verde, roja y naranja, y la importancia de separarlas para organizar y proteger mejor el tráfico entre la LAN, la WAN y la DMZ.

En la temática 2 la implementación de NAT dentro de un entorno de red administrado con Endian Firewall demostró ser una solución eficaz para asegurar la comunicación entre diferentes segmentos de red y permitir el acceso controlado a Internet. A través de la configuración de las zonas GREEN, ORANGE y RED, así como del establecimiento de reglas específicas de enrutamiento y traducción de direcciones, se logró una segmentación segura y un manejo eficiente del tráfico. Las pruebas de conectividad y acceso validaron el correcto funcionamiento del servicio, evidenciando que NAT no solo optimiza el uso de direcciones IPv4, sino que también fortalece la seguridad y la administración del entorno de red. Este proceso confirma la importancia del uso de firewalls dedicados y de una correcta planificación de la topología para garantizar un rendimiento estable y seguro en las redes modernas.

En la temática 3 se realizó la configuración básica de políticas de firewall en un servidor Ubuntu con el fin de controlar el tráfico de red permitido y denegado. En primer lugar, se habilitan los servicios HTTP y FTP mediante la apertura de los puertos 80 y 21, garantizando el acceso a los servicios web y de transferencia de archivos desde la red. Posteriormente, se implementaron reglas para negar el protocolo ICMP, con el objetivo de impedir la ejecución del comando ping hacia el servidor y dentro de la red.

En la temática 4 se realizó la configuración inicial del firewall Endian, enfocada en la creación y organización de las zonas de red GREEN, ORANGE y RED. Se asignaron las interfaces de red correspondientes, definiendo GREEN como la red interna segura, ORANGE como la DMZ para servicios públicos y RED como la conexión hacia Internet. Además, se establecieron parámetros básicos como dirección IP, puerta de enlace y métodos de asignación de red. Esta estructuración garantiza un control segmentado del tráfico y sienta las bases para aplicar reglas de seguridad más avanzadas en las siguientes temáticas.

La implementación de un proxy HTTP no transparente con autenticación mediante Endian Firewall permite establecer un control efectivo sobre el tráfico web en entornos organizacionales por ello es de tal importancia la temática 5. La configuración de listas negras y políticas de autenticación por usuario no solo fortalece la seguridad perimetral, sino que también garantiza trazabilidad completa de las acciones de navegación. Esta práctica consolida competencias fundamentales en la administración de servicios de seguridad en sistemas GNU/Linux, preparando al profesional para implementar soluciones de filtrado y control de acceso en infraestructuras empresariales reales.

6 REFERENCIAS

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

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

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

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

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

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

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

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