GNU/LINUX SEGURO: IMPLEMENTACIÓN Y MANTENIMIENTO DE LA SEGURIDAD

Jhan Camilo Carabali Aguado
e-mail: jccarabaliag@unadvirtual.edu.co
Maira Alejandra Leyton Torres
e-mail: maleytont@unadvirtual.edu.co

RESUMEN: *La seguridad en sistemas GNU/Linux es fundamental para proteger la integridad, confidencialidad y disponibilidad de la información. Implementarla adecuadamente requiere una combinación de buenas prácticas, herramientas especializadas y configuraciones del sistema operativo.*

PALABRAS CLAVE: Autenticación, control de acceso, Firewall, permisos de archivos.

1 INTRODUCCIÓN

Este trabajo consiste en configurar interfaces de usuario y escritorio a través de tareas administrativas con los servicios esenciales dándole un óptimo nivel de seguridad al sistema operativo GNU Linux [1]. A lo siguiente se elige la temática 1: Configuración de la instancia para GNU/Linux Endian en VirtualBox (tarjetas de red) e instalación efectiva del mismo y la temática 2: Configuración NAT. También tiene como fin reconocer las principales características de desarrollo y funcionamiento del sistema operativo Open Source Linux, evaluando y desarrollando de forma detallada cada uno de los conceptos principales del cual este se encuentra compuesto, identificando cada uno de los procesos de desarrollo en base a sus sistemas de funcionamiento en un entorno de trabajo, también , se pretende implementar procesos de asociación e interacción con la máquina virtual, por medio de la identificación de procesos y características de conexión; Por otra parte, este trabajo pretende implementar una red virtualizada por medio del uso de VirtualBox, permitiendo simular por medio de este un entorno de red corporativo diferencias no en tres procesos.

2 INSTALACION ENDIAN

2.1 CARACTERÍSTICAS GENERALES

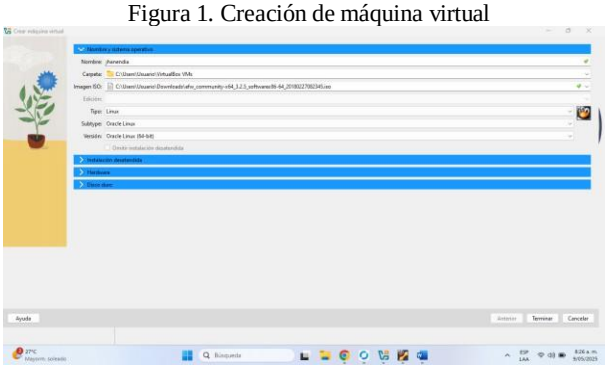
En primer lugar, se descarga la distribución de Endian UTM desde su sitio oficial [5] y se instala en plataformas como VirtualBox o en hardware físico. Es compatible con arquitecturas x86.

Se utiliza el programa Oracle VM VirtualBox para la creación de una máquina virtual con las siguientes configuraciones: [3].

- Tipo: Linux
- Versión: Oracle Linux (64 bit)
- Unidad óptica virtual: ISO

2.2 INSTALACION

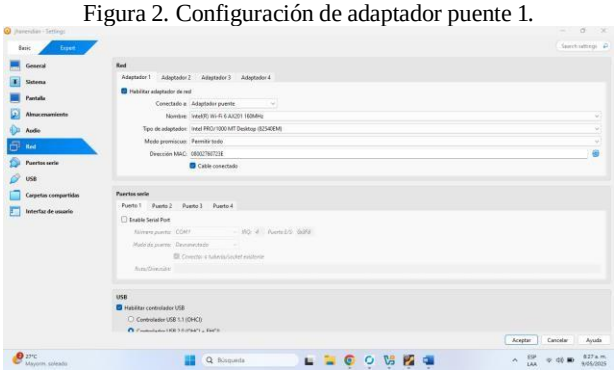
Figura 1. Creación de máquina virtual



Fuente: Autoría propia

La figura 1 muestra la creación de una nueva máquina virtual y el montaje de la ISO en dicha máquina.

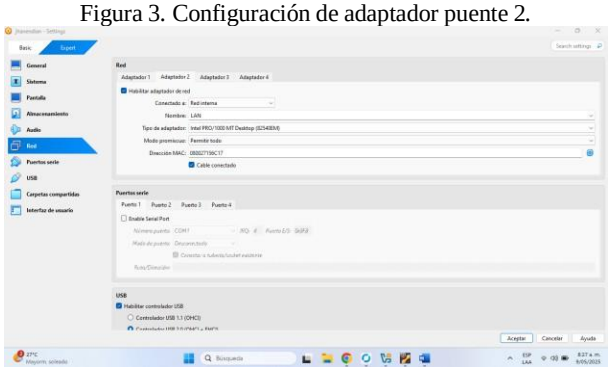
Figura 2. Configuración de adaptador puente 1.



Fuente: Autoría propia

Como se muestra en la figura 2 se hace la respectiva configuración en el adaptador 1 de red como adaptador puente (RED) [4].

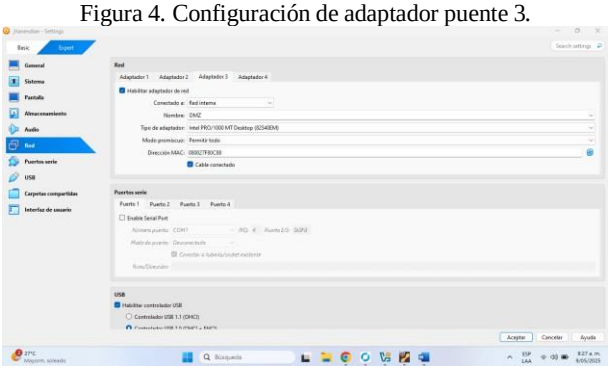
Figura 3. Configuración de adaptador puente 2.



Fuente: Autoría propia

Como se muestra en la figura 3 se configuró el adaptador 2 como red interna LAN (GREEN).

Figura 4. Configuración de adaptador puente 3.



Fuente: Autoría propia

Como se muestra en la figura 4 se configuró el adaptador 3 como red interna DMZ (ORANGE).

Figura 5. Se inició la máquina virtual de Endian.

Fuente: Autoría propia

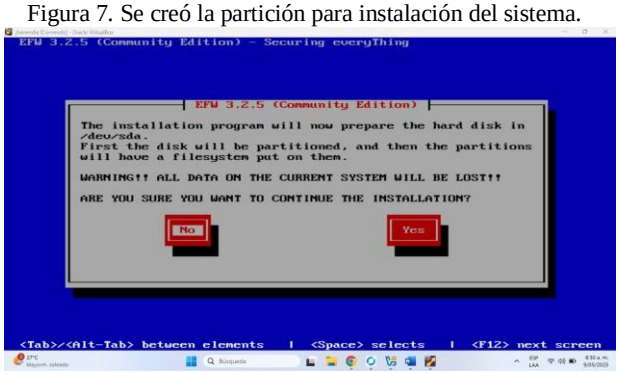
Como se muestra en la figura 5 se inició la máquina virtual de Endian.

Figura 6. Selección de idioma.

Fuente: Autoría propia

Como se muestra en la figura 6 se escogió el idioma de inglés.

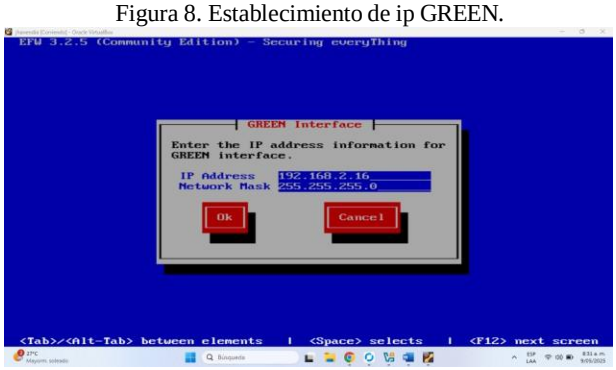
Figura 7. Se creó la partición para instalación del sistema.



Fuente: Autoría propia

La figura 7 muestra la creación de particiones para la instalación del sistema. [5].

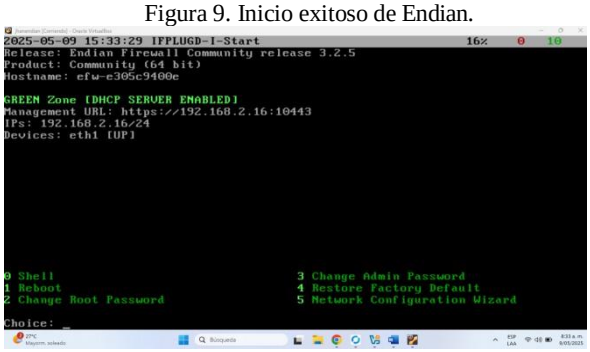
Figura 8. Establecimiento de ip GREEN.



Fuente: Autoría propia

La figura 8 establece la IP y la máscara de (GREEN).

Figura 9. Inicio exitoso de Endian.



Fuente: Autoría propia

La figura 11 muestra se inició Endian, donde nos muestra la ip de (GREEN) [5].

3 DESARROLLO TEMATICAS

3.1 TEMATICA 1: 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).

Figura 10. Descarga de archivo Endian en el navegador.

Fuente: Autoría propia

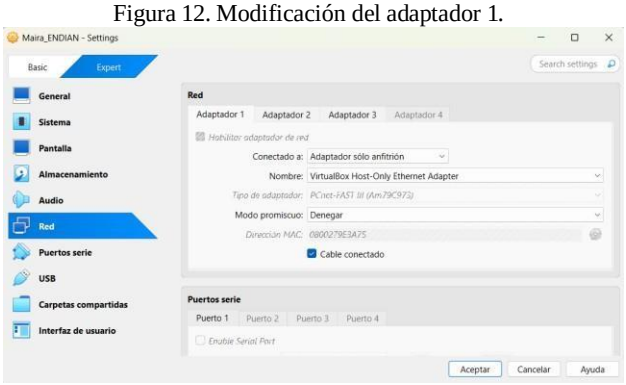
En la figura 10, evidenciamos que se realizó la descarga de Endian en la página oficial.

Figura 11. Instalamos la máquina virtual ENDIAN en VirtualBox.

Fuente: Autoría propia

En la figura 11, se creó la máquina virtual Endian y se observa toda la información general de la maquina

Figura 12. Modificación del adaptador 1.



Fuente: Autoría propia

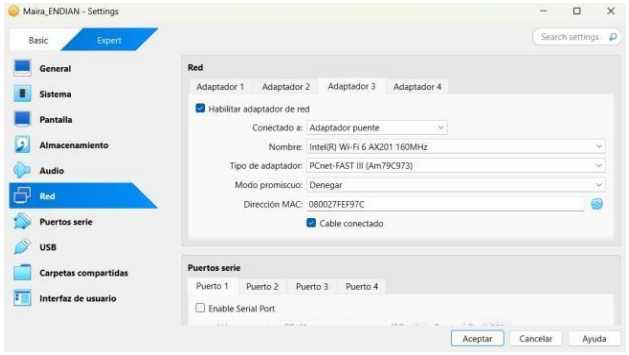
La figura 12 presenta la configuración del adaptador 1 en modo solo anfitrión.

Figura 13. Modificación del adaptador 2

Fuente: Autoría propia

La figura 13 ilustra la configuración del adaptador 2 en modo red interna (NARANJA).

Figura 14. Modificación del adaptador 3

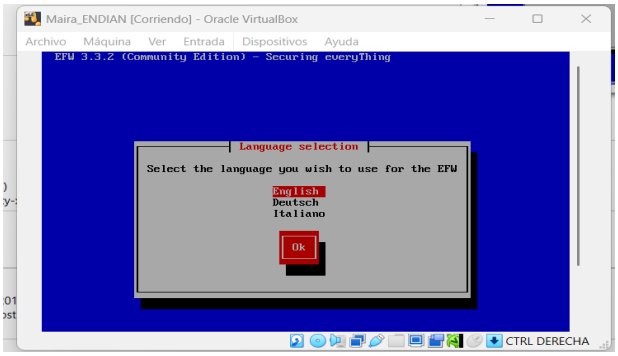


Fuente: Autoría propia

La figura 14 muestra la configuración del adaptador 3 en modo adaptador puente.

.

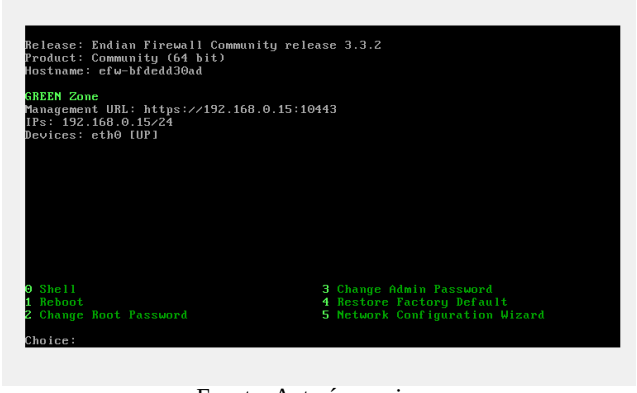
Figura 15. Inicio de la máquina virtual y configuración



Fuente: Autoría propia

La figura 15 evidencia el inicio de la máquina virtual y la configuración correspondiente.

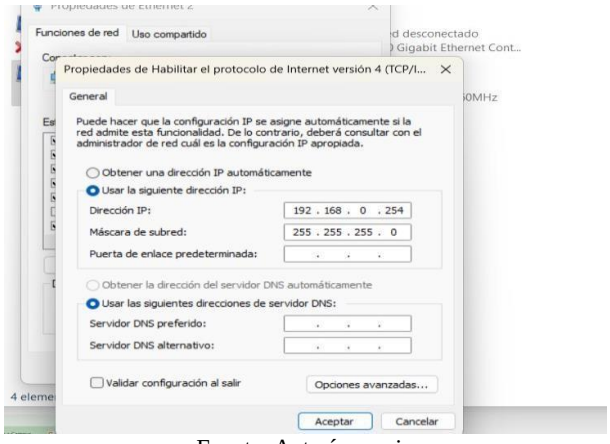
Figura 16. Acceso a la interfaz de Endian



Fuente: Autoría propia

La figura 16 muestra el acceso a la interfaz de Endian en la máquina virtual.[5]

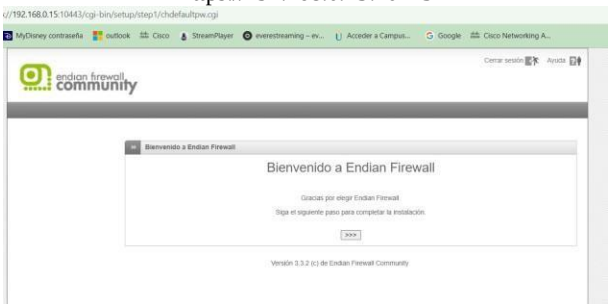
Figura 17. Modificación del host en el panel de control de Windows



Fuente: Autoría propia

La figura 17 presenta la configuración de red en Windows, estableciendo una IP estática.

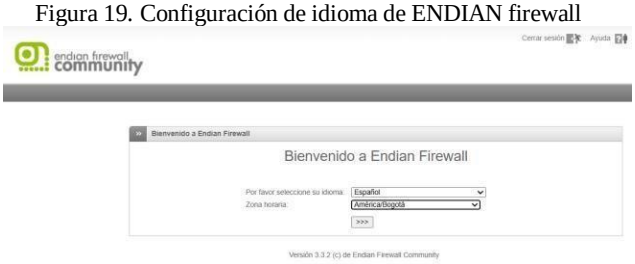
Figura 18. Acceso a Endian por medio de la URL https://192.168.0.15:10443



Fuente: Autoría propia

La figura 18 ilustra el acceso a Endian mediante la URL https://192.168.0.15:10443. [5]

Figura 19. Configuración de idioma de ENDIAN firewall



Fuente: Autoría propia

La figura 19 muestra la configuración del idioma de Endian.

Figura 20. Activación de red naranja, verde y roja

Fuente: Autoría propia

La figura 20 evidencia la activación de las redes naranja, verde y roja.

Figura 21. Verificación de estado de redes

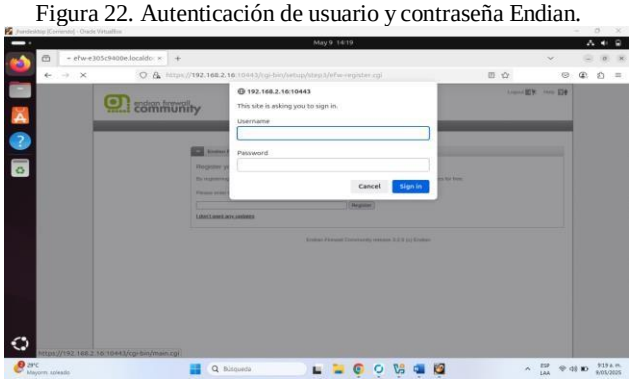
Fuente: Autoría propia

La figura 21 verifica el estado activo de las redes.

3.2 TEMÁTICA 2: CONFIGURACIÓN NAT.

Producto esperado: Configurar la regla de NAT para permitir la comunicación desde la LAN hacia la WAN y desde la Zona DMZ hacia la Internet, verificando el reenvío de puertos y la correcta creación de las reglas de NAT.

Figura 22. Autenticación de usuario y contraseña Endian.



Fuente: Autoría propia

La figura 22 muestra la autenticación de usuario y contraseña en Endian. [5].

Figura 23. Configuración de RED en modo DHCP.

Fuente: Autoría propia

La figura 23 confirma la configuración de RED en modo DHCP.

Figura 24. Confirmación de ip de GREEN y ORANGE

Fuente: Autoría propia

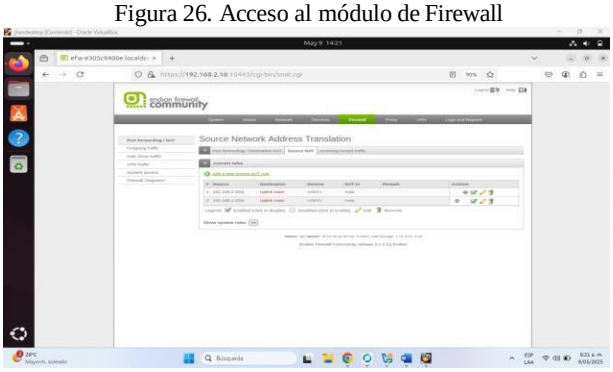
La figura 24 verifica que las IP de GREEN y ORANGE estén correctamente configuradas.

Figura 25. Confirmación de configuración de RED en DHCP.

Fuente: Autoría propia

La figura 25 confirma que WAN esté en el puerto eth0

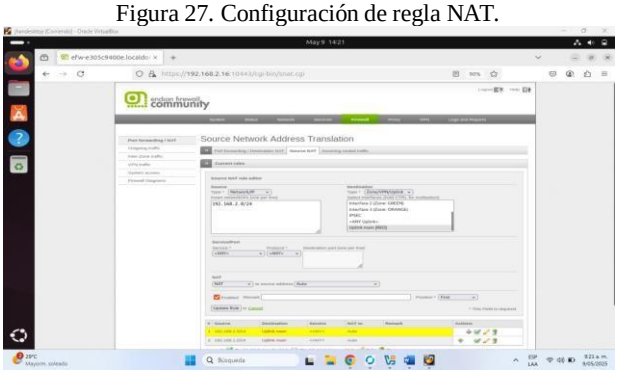
Figura 26. Acceso al módulo de Firewall



Fuente: Autoría propia

La figura 26 ilustra el acceso al módulo de Firewall – Source NAT.

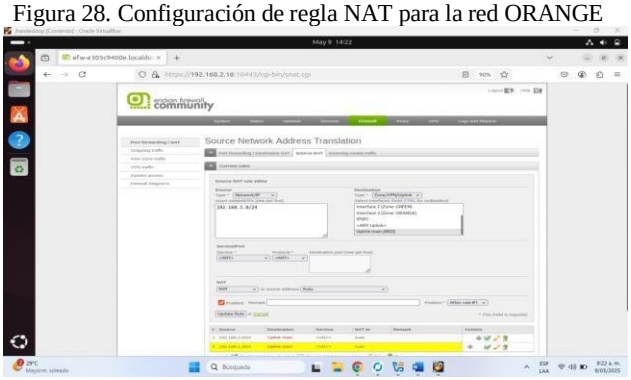
Figura 27. Configuración de regla NAT.



Fuente: Autoría propia

La figura 27 muestra la configuración de una regla de Source NAT para permitir que el tráfico de la red GREEN acceda a Internet.

Figura 28. Configuración de regla NAT para la red ORANGE



Fuente: Autoría propia

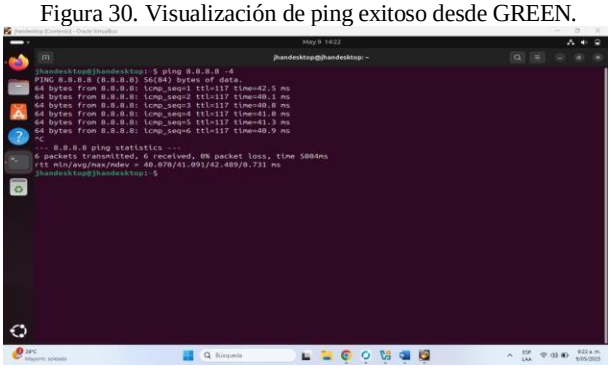
La figura 28 presenta la configuración de una regla de Source NAT para la red ORANGE.

Figura 29. Visualización de reglas creadas.

Fuente: Autoría propia

La figura 29 visualiza las reglas creadas de manera exitosa.

Figura 30. Visualización de ping exitoso desde GREEN.



Fuente: Autoría propia

La figura 30 muestra un ping exitoso desde GREEN.[2]

4 CONCLUSIONES

La implementación de GNU/Linux Endian como solución de firewall con segmentación de red en zonas verde, roja y naranja en esta actividad se representa una estrategia eficaz para fortalecer la seguridad perimetral de una infraestructura de red [5]. Esta arquitectura permite clasificar y aislar adecuadamente los distintos tipos de tráfico y dispositivos según su nivel de confianza y exposición, cumpliendo con uno de los principios fundamentales de la seguridad informática: la segmentación de redes.

También se puede decir que la implementación de GNU/Linux Endian con esta estructura zonificada no solo cumple con los objetivos técnicos de segmentar, controlar y proteger el tráfico de red, sino que también promueve una cultura de seguridad informática proactiva. Al ser una solución basada en software libre, ofrece una excelente relación costo-beneficio, brindando herramientas de nivel empresarial sin necesidad de licencias costosas, lo que la convierte en una opción ideal para entornos académicos, empresariales o institucionales que buscan proteger su infraestructura digital de forma eficiente y sostenible.

5 REFERENCIAS

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

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

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

[4] Jay LaCroix. (2020). Mastering Ubuntu Server: Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting

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