Arquitectura de Seguridad Perimetral GNU/Linux Basada en la Virtualización de Endian Firewall para la Delimitación de Redes

Jeisson Jair Angel Cogollo
e-mail: jjangelc@unadvirtual.edu.co
Luisa Fernanda Ocampo Cardenas
e-mail: lfocampoc@unad.edu.co
María Camila Quijano Caranton
e-mail: mcquijanoc@unad.edu.co

RESUMEN: *Este artículo presenta la implementación del firewall Endian en un entorno virtualizado como una estrategia efectiva para la segmentación de redes en sistemas GNU/Linux. Se describe la configuración de las zonas de red (LAN, WAN y DMZ) dentro del entorno virtualizado utilizando VirtualBox. Se detallan los procesos de configuración de reglas NAT para permitir la comunicación controlada entre las diferentes zonas y hacia Internet. Adicionalmente, se explora la implementación de reglas de acceso para gestionar el tráfico entre las zonas, incluyendo la habilitación de servicios específicos como HTTP y FTP para la zona DMZ y la denegación del protocolo ICMP. Finalmente, se aborda la implementación de un proxy HTTP no transparente con políticas de autenticación y listas negras para controlar el acceso a Internet desde la red LAN. Los resultados demuestran la viabilidad y eficacia de Endian Firewall en un entorno virtualizado para establecer una arquitectura de seguridad perimetral robusta en plataformas GNU/Linux*

PALABRAS CLAVE: Endian Firewall, Virtualización, Segmentación de Red, GNU/Linux, Seguridad Perimetral.

1. INTRODUCCIÓN

Ante la creciente complejidad de las redes y las ciber amenazas, la seguridad perimetral robusta, facilitada por la segmentación de redes en zonas aisladas, es crucial para mitigar riesgos. Los firewalls open source GNU/Linux, como Endian Firewall (EFW), proveen una solución eficaz. Este artículo examina la implementación de EFW virtualizado con VirtualBox para segmentar redes GNU/Linux en zonas LAN, WAN y DMZ, permitiendo un control de tráfico detallado mediante la configuración de interfaces virtuales, reglas NAT para comunicación controlada hacia/desde Internet, y reglas de acceso entre zonas. Además, se presenta la implementación de un proxy HTTP no transparente con autenticación y listas negras para gestionar el acceso web interno. El objetivo es demostrar la efectividad de EFW virtualizado como una solución práctica y adaptable para la segmentación y protección de redes GNU/Linux.

2. DESARROLLO DE ACTIVIDADES

Instalación y configuración de la distribución GNU/Linux Endian (EFW), así mismo seleccionar una de las siguientes cinco (5) temáticas y darle solución bajo esta distribución.

En este caso se realizaron las temáticas 1, 3 y 5 donde se explicará el paso a paso de la configuración de la máquina virtual y la configuración correspondiente en endian para cada tema.

2.1 INSTALACIÓN Y CONFIGURACIÓN DE LA DISTRIBUCIÓN GNU/LINUX ENDIAN (EFW)

Para llevar a cabo la implementación del firewall de código abierto Endian, se optó por realizar el proceso dentro de un entorno controlado utilizando VirtualBox, se descarga de la imagen ISO de Endian Firewall Community Edition desde su sitio oficial, las cuales se abordarán desde la temática 1

2.2 DESARROLLO DE LAS TEMÁTICAS

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

Implementación de GNU/Linux Endian con las zonas verde, roja y naranja, así: Zona verde: Red interna (LAN), es una red que conecta dispositivos en un área como un hogar, una oficina o un edificio. Zona roja: Acceso a internet (WAN), puede abarcar grandes áreas geográficas, puede estar separada por largas distancias, y Zona naranja: Servidores (DMZ), se ubica estratégicamente entre la red interna y la red externa, esto permite que los servicios públicos sean accesibles desde internet, sin poner en riesgo la seguridad la red interna. Por ende, se mostrará paso a paso la instalación de cada una las redes con el proceso a través de las imágenes.

Como primera medida se realiza la descarga de Endian en la página principal. Como se muestra en la figura 1.

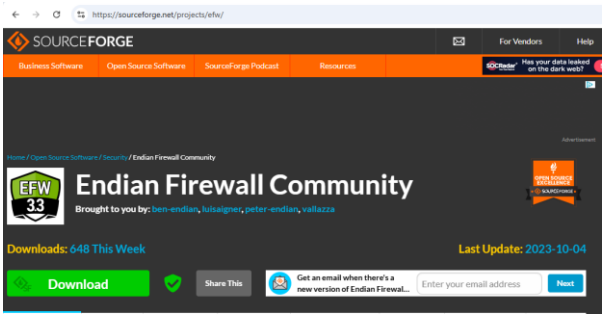

figura 1 Descarga Endian
Fuente: https://sourceforge.net/projects/efw/-2025

Una vez descargado se crea una nueva máquina, se configura se busca la descarga de Endian y se añade el disco. Como se muestra en la figura 2.

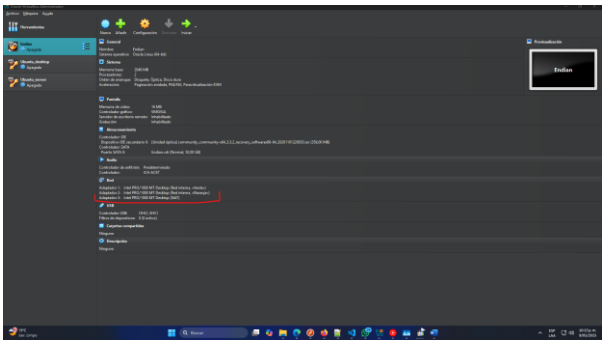

figura 2 Vista de las máquinas virtuales
Fuente: Elaboración Propia – 2025.

Crear la segmentación para las redes tanto verde como naranja, ya que es requisito para poder iniciar con la configuración, a continuación, se realiza una tabla en la cual se relacionan los rangos y las IP´s. Como se muestra en la figura 3.

Color	Segmentación	Rango IPS	Dirección red	Broadcast
Verde	192.168.10.0/24	192.168.10.1 192.168.10.254	192.168.10.0	192.168.10.255
Naranja	NAT	Virtualizada por DHCP	10.0.2.0 aproximado	10.0.2.255 aproximada
Roja	192.168.20.0/24	192.168.20.1 192.168.20.254	192.168.20.0	192.168.20.255

figura 3 Segmentación Inicial
Fuente: Elaboración Propia – 2025.

Se inicia con la configuración de la red verde, la cual será la interna (LAN). Se debe ingresar por la opción Expert y desde allí seleccionar el Adaptador 1, opción Red Inter y allí se escribe el nombre de la red, los demás campos de dejan por defecto, se debe tener presente la MAC. Como se muestra en la figura 4.

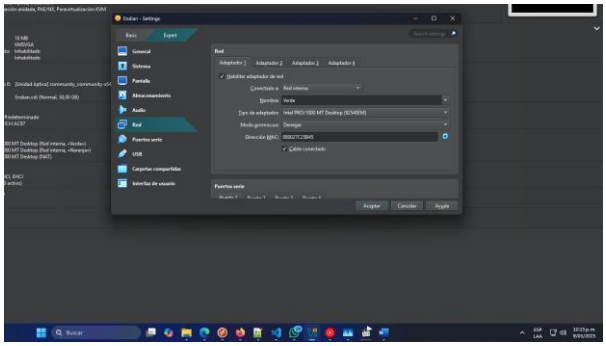

figura 4 Configuración red verde.
Fuente: Elaboración Propia – 2025.

Luego se configura la red naranja la cual será la interna (DMZ), debemos ingresar por la opción Expert y desde allí seleccionar el Adaptador 2, opción Red Interna y allí se escribe el nombre de la red, los demás campos se dejan por defecto, se debe tener presente la MAC. Como se muestra en la figura 5.

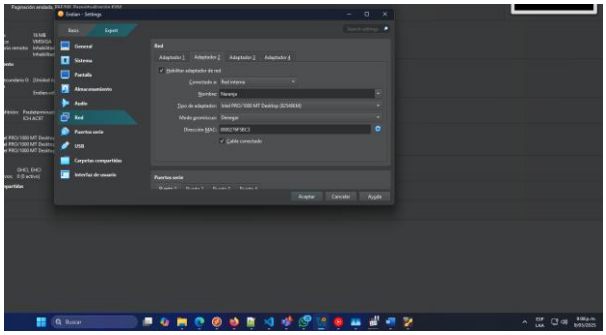

figura 5 Configuración red naranja
Fuente: Elaboración Propia – 2025.

Es siguiente paso es la configuración de la red ROJA (NAT), simplemente se habilita el adaptador 3, eligiendo la opción NAT, y los demás campos se dejan por defecto, obteniendo, acceso a Internet (WAN). Como se muestra en la figura 6.

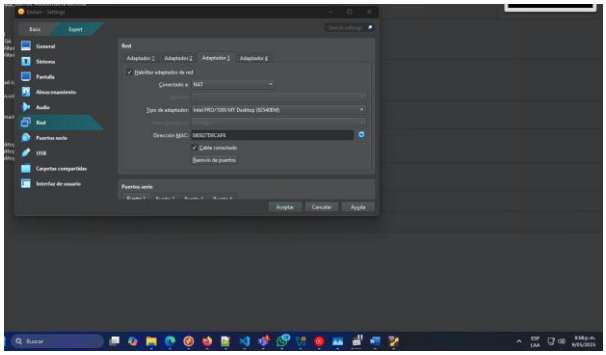

figura 6 Configuración Adaptador 3 NAT
Fuente: Elaboración Propia – 2025.

Se evidencia la creación de las redes solicitadas en la maquina Endian Firewall, esto es necesario para los pasos siguientes, se señalan las redes creadas. Como se muestra en la figura 7.

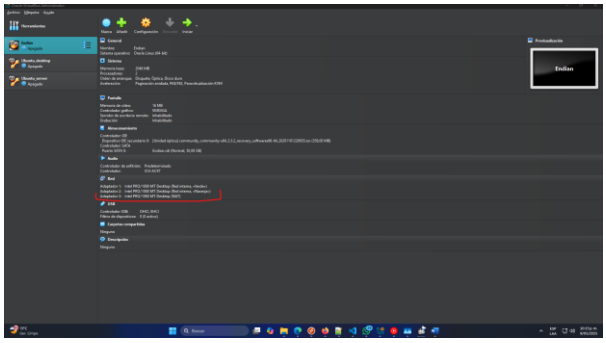

figura 7 Vista de redes creadas en Endian
Fuente: Elaboración Propia – 2025.

Se crean las máquinas adicionales a Endian, se crea la maquina Ubuntu_Desktop la cual se conectará a la Red de la zona Verde (LAN) y se crea la maquina Ubuntu_Server la cual se conectará a la Red de la zona Naranja (DMZ). Como se muestra en la figura 8.

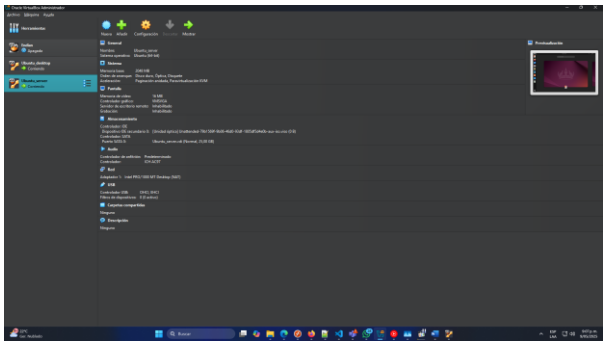

figura 8 Máquinas instaladas Endian Ubuntu_desktop y Ubuntu_server.
Fuente: Elaboración Propia – 2025.

Se realiza la configuración inicial de la maquina desktop creada, esto es aconsejable realizarlo antes de instalar un sistema operativo en la máquina, como se observa por medio de la opción Red, seleccionar la opción verde, estas opciones ya se precargan con la creación de las redes en la maquina principal Endian. Como se muestra en la figura 9.

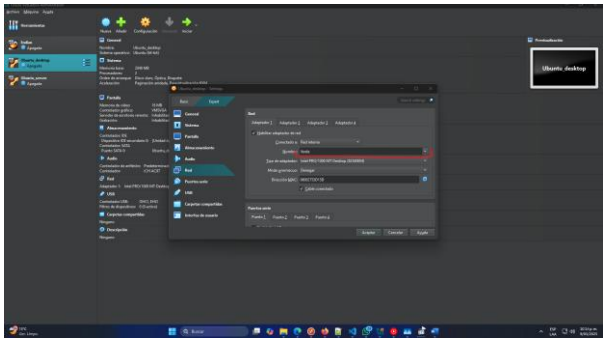

figura 9 Máquinas instaladas Endian Ubuntu_desktop y Ubuntu_server.
Fuente: Elaboración Propia – 2025.

Se realiza la configuración sobre la maquina Server la cual se encarga de conectarse a la red Naranja (DMZ), esto se aconseja realizar antes de instalar el sistema operativo, la opción se selecciona desde red. Como se muestra en la figura 10.

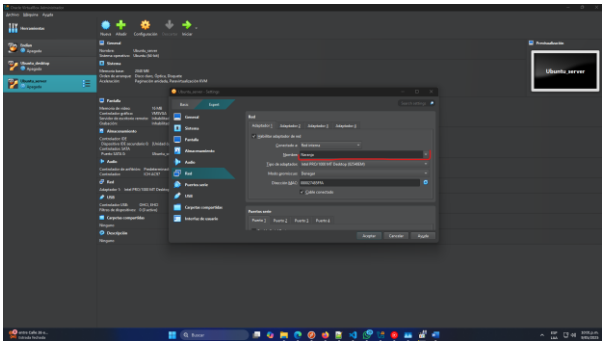

figura 10 Configuración Ubuntu_server con red interna Naranja
Fuente: Elaboración Propia – 2025.

A continuación, se inicia con la instalación del sistema operativo Endian, se debe descargar el sistema operativo en .iso desde la web oficial (https://www.endian.com/en/community/) en el botón “Download Now”, con ello ya se tiene el sistema operativo y simplemente es seleccionarlo en la maquina e iniciarla para que pueda tener comienzo a la configuración del sistema operativo. Como se muestra en la figura 11.

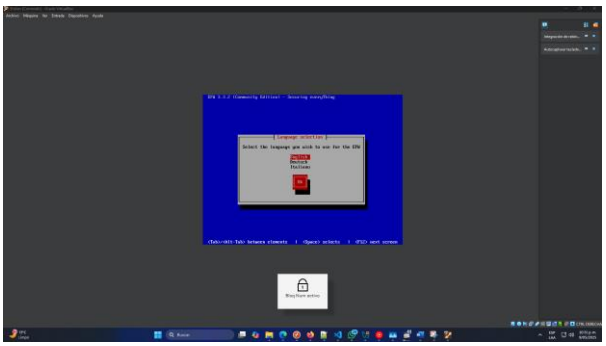

figura 11 Instalación Endian
Fuente: Elaboración Propia – 2025.

Se selecciona la opción Ok para continuar con la instalación del sistema operativo. Como se muestra en la figura 12 y 13.

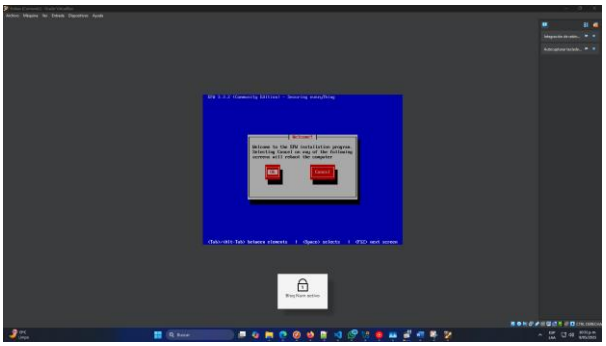

figura 12 Instalación Endian 2
Fuente: Elaboración Propia – 2025.

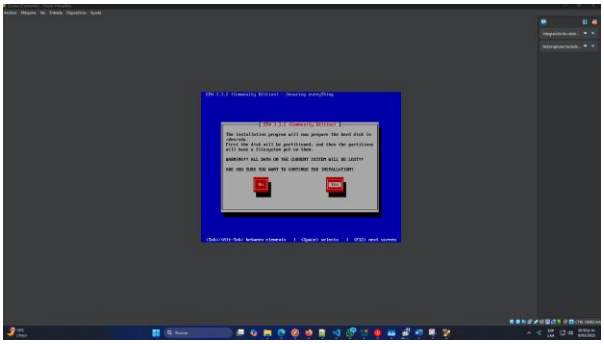

figura 13 Instalación Endian 3
Fuente: Elaboración Propia – 2025.

Luego de las configuraciones iniciales, el sistema operativo solicita la configuración de la zona GREEN (Verde), en la cual se agrega la IP add Addresses para que extraiga la segmentación de IP´s, la cual se describe al inicio de la actividad. Al igual que la máscara. Como se muestra en la figura 14.

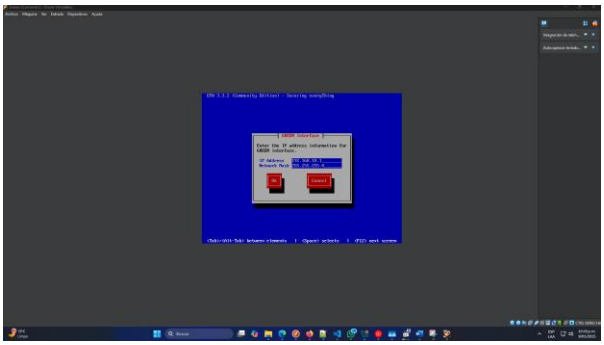

figura 14 Instalación Endian sobre interfaz verde
Fuente: Elaboración Propia – 2025

Una vez configurado el sistema operativo se reinicia luego indica que la zona GREEN ya se encuentra activa y la IP de la misma, adicional como la Red ROJA se deja como (NAT), el mismo sistema operativo se encarga de tomarla ya que es dinámica (WAN). Como se muestra en la figura 15.

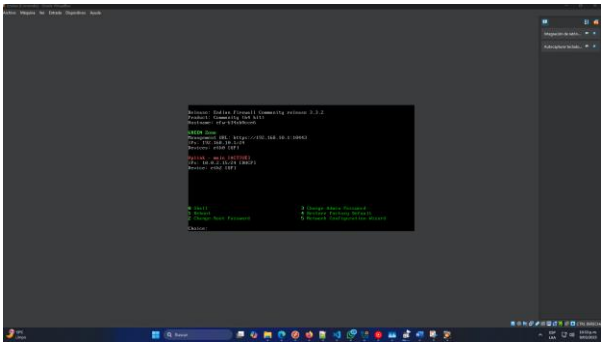

figura 15 Zona verde activa
Fuente: Elaboración Propia – 2025

Se valida acceso mediante la opción 0 Shell, en la cual se ingresa con comando login y la contraseña es la que tiene por defecto el sistema operativo “Endian”. Como se muestra en la figura 16.

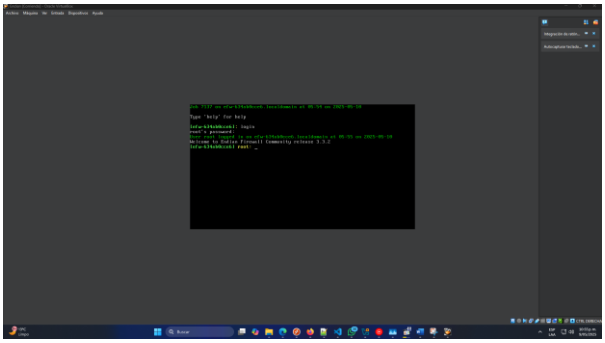

figura 16 Validar acceso a super usuario “root”
Fuente: Elaboración Propia – 2025

Se inicia la configuración de la red naranja ya que Endian al inicio de la instalación solo permite configurar la red GREEN, estos pasos se realizarán por medio de consola, para ello se usa la opción 5, como se muestra en la figura 17.

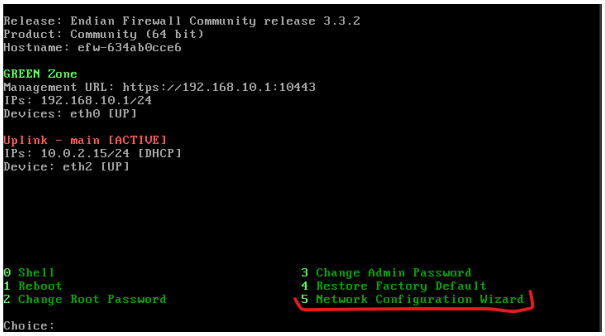

figura 17 Configuración de Red Naranja desde Endian 1
Fuente: Elaboración Propia – 2025

Al inicio la consola solicita la contraseña para el entorno Web la cual se configura, en este paso se aumenta la seguridad de Endian ajustando la clave por defecto “endian” por una más segura. Como se observa en la figura 18.

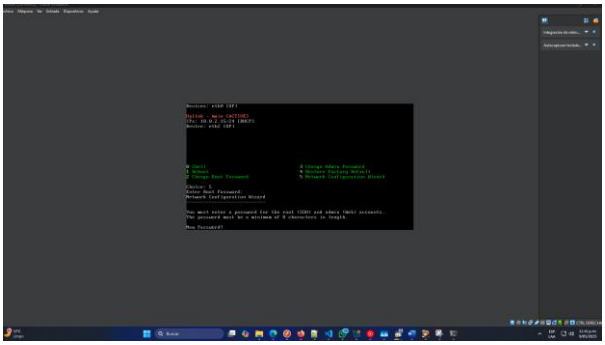

figura 18 Configuración de Red Naranja desde Endian 2
Fuente: Elaboración Propia – 2025

Solicita la configuración de las salidas de interfaz de la red, se ajusta la salida de la red Roja la cual está configurada como NAT, acá es muy importante configurar los DNS de salida, ya que en la configuración inicial solo solicitó IP y mascara, acá se puede configurar los DNS globales, para los cuales se configura los DNS de Google. Como se observa en la figura 19.

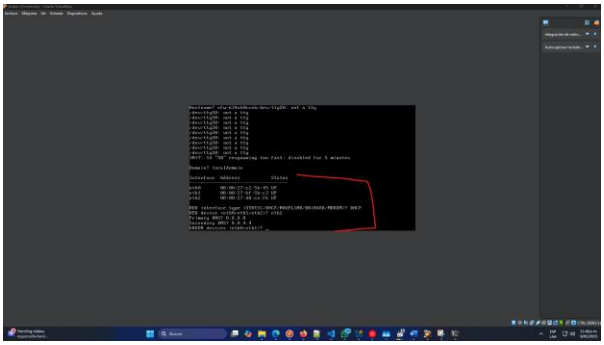

figura 19 Configuración de Red Naranja desde Endian 3
Fuente: Elaboración Propia – 2025

A continuación, se solicita configuraciones adicionales de la red GREEN los cuales no se solicitaron en la instalación, acá se puede definir sobre la red Verde, si se desea habilitar DHCP, opcional, para el ejercicio no se usa, como se observa también solicita si se quiere configurar la zona Naranja, la cual es la que se debe configurar. Como se muestra en la figura 20.

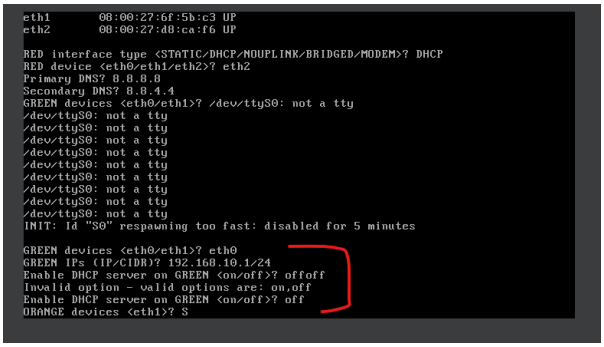

figura 20 Configuración de Red Naranja desde Endian 4
Fuente: Elaboración Propia – 2025

Se validan datos adicionales como SSH “https”, y si se dá acceso a los puertos 22, 80 y 10443, los cuales son protocolos de red. Como se muestra en la figura 21.

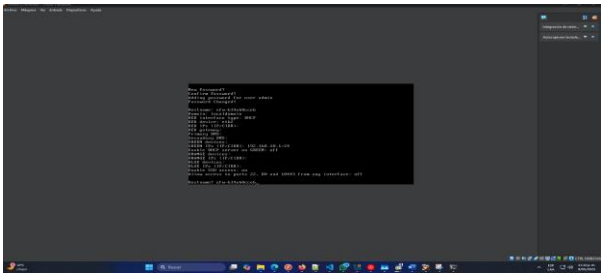

figura 21 Configuración de Red Naranja desde Endian 5
Fuente: Elaboración Propia – 2025

Una vez configuradas las IP´s, según la segmentación informada al inicio de la actividad, se validan los datos ajustados, allí se pueden ver los DNS domains, y la IP asignada a la red Naranja, y si se está seguro se escribe “yes”. Como se observa en la figura 22.

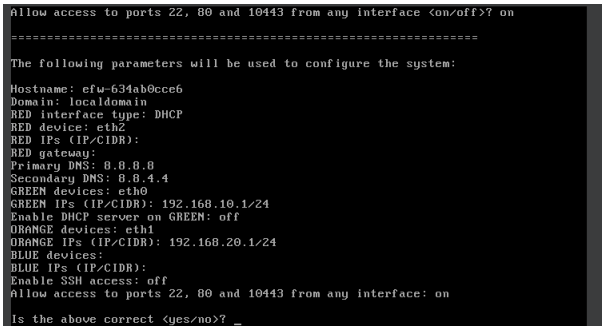

figura 22 Configuración de Red Naranja desde Endian 6
Fuente: Elaboración Propia – 2025

Luego se realiza la instalación del sistema operativo de Ubuntu_server, esto se realiza igual que con cualquier sistema operativo, por medio de la iso oficial del entorno, para ello se puede realizar mediante: ”https://ubuntu.com/download/server”, se aconseja descargar la versión LTS que es la más estable y de largo soporte, luego se monta la iso en el sistema operativo y se inicia, esta versión es solo de consola, luego de iniciar solicita usuario y contraseña los cuales se indica al crear la máquina virtual, se evidencia que se puede acceder con usuario y contraseñas definidas.

Al inicio se valida si el servidor tiene una IP ya configurada ya que se debe asignar una en el segmento que se usa para la red Naranja (DMZ), como es un nuevo sistema operativo no tiene configurada su ipV4. Se configura la red del segmento, para ello se usa el editor “nano” que provee Linux, por medio de él se edita el archivo “00-installer-config. yaml”, y se agrega las líneas de la red y la IP que manejará.

Luego de guardar cambios usamos el comando “sudo netaplan apply”, por medio de este se aplican los cambios, es normal que puedan aparecer warnings, para el ejemplo no se ocupa, si aparecen Errores si se deben validar, como se aplica la IP que se requiere.

Luego se instala y configura Ubuntu-desktop, Una vez instalado el sistema operativo, procedemos a iniciar con las configuraciones de la red por medio de línea de comandos, se tiene la interfaz inicial para acceder por medio de administrador, adicional genera un error normal ya que está configurado por la red verde, pero hay una IP valida dentro del segmento. Se inicia la configuración del a IP *por* medio de consola, esto lo realzamos como en el server por medio del “00-installer-config. yaml” como se evidencia a continuación, se ingresa la IP del segmento de la red verde. Luego se confirman los cambios con el comando “sudo netplan apply”, por medio de este se aplican los cambios, los WARNING no impiden continuar con la prueba, si aparecen errores si se deben validar. Una vez configuradas las redes, se realizan las pruebas de conexión, quedando optimo el proceso de LAN, WAN y DMZ.

2.2.2 TEMÁTICA 3: PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED.

Para la implementación de los servicios en la zona DMZ, se empleó la distribución Endian Firewall dentro de un entorno virtualizado utilizando VirtualBox. La configuración se realizó de la siguiente manera: se habilitaron tres interfaces de red para

la máquina virtual Endian, correspondientes a las zonas Verde (LAN), Naranja (DMZ) y Roja (WAN).

Dentro de la consola de administración de Endian, se accedió a la sección de Firewall > Reglas de Entrada para crear reglas específicas que permitieran el tráfico a través de los puertos 80 (HTTP) y 21 (FTP) dirigidos al servidor Ubuntu ubicado en la DMZ. Estas reglas se configuraron especificando la interfaz de entrada como la zona Verde, la de destino como la zona Naranja y se definieron los respectivos puertos de servicio, como se muestran en la figura 23, 24, 25 y 26

Posteriormente, se configuró una regla adicional para denegar el protocolo ICMP (puertos 8 y 30), con el fin de bloquear solicitudes de ping desde la LAN hacia la DMZ, y viceversa. Esto se logró mediante la creación de reglas de tipo "bloquear" entre ambas zonas, como se muestra en la figura 29, 30 y 31

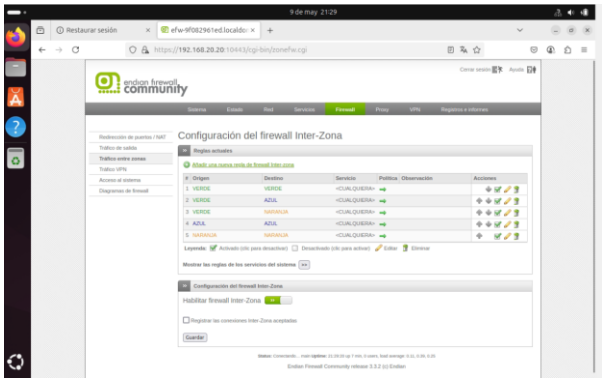

figura 23 Firewall Endian
Fuente: Elaboración Propia – 2025.

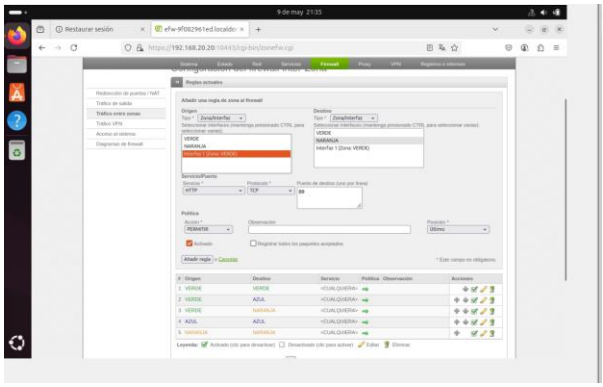

figura 24 creación regla http puerto 80
Fuente: Elaboración Propia – 2025.

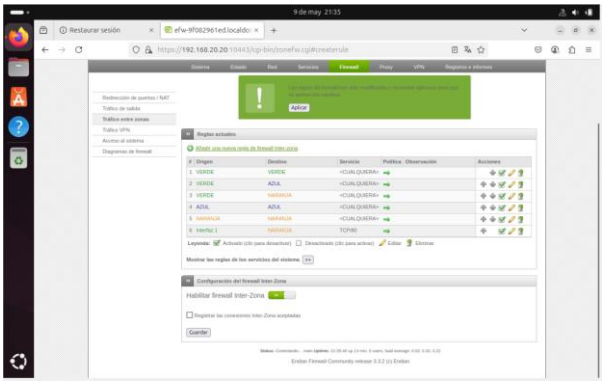

figura 25 Aplicación regla http puerto 80
Fuente: Elaboración Propia – 2025.

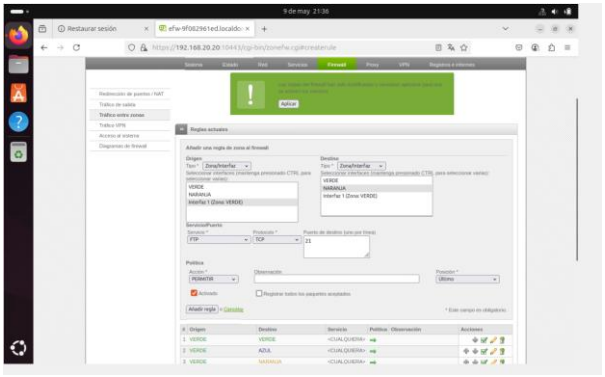

figura 26 creación regla firewall FTP puerto 21
Fuente: Elaboración Propia – 2025.

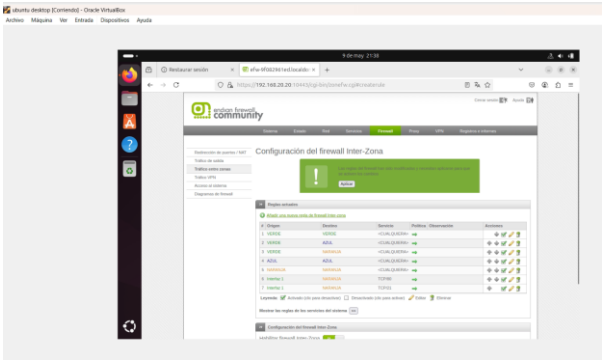

figura 27 Aplicación regla FTP puerto 21
Fuente: Elaboración Propia – 2025.

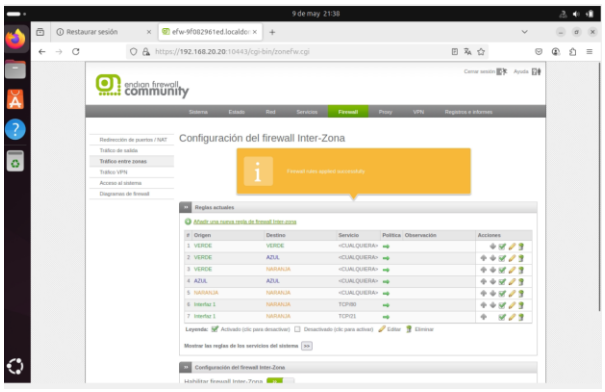

figura 28 Aplicación reglas en el firewall.
Fuente: Elaboración Propia – 2025.

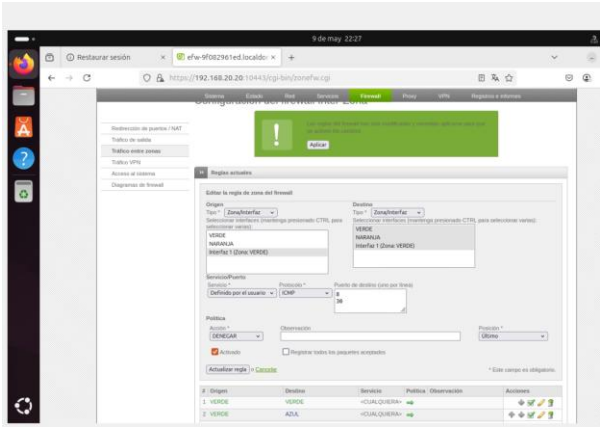

figura 29 creación reglas en el firewall de denegación protocolo ICMP puerto 8 y 30.
Fuente: Elaboración Propia – 2025.

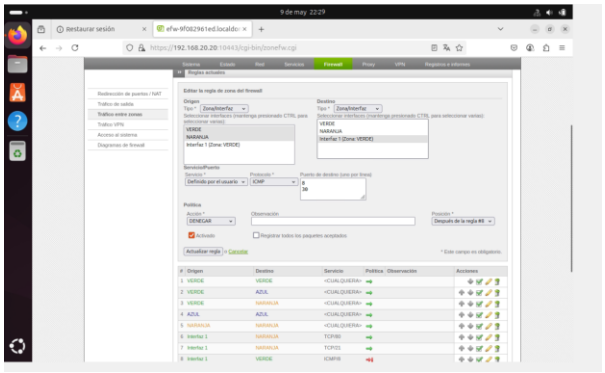

figura 30 denegación servicio zona naranja hacia zona verde ICMP.
Fuente: Elaboración Propia – 2025.

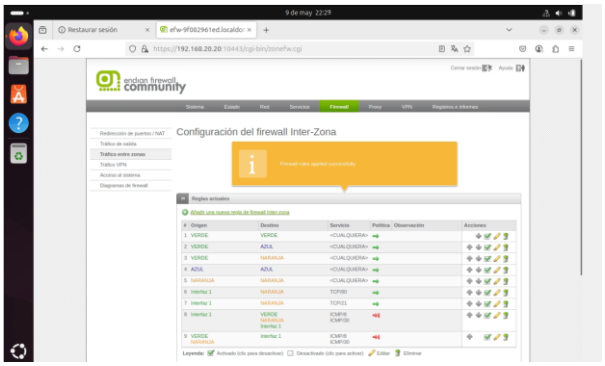

figura 31 Reglas solicitadas aplicadas en el firewall.
Fuente: Elaboración Propia – 2025.

2.2.3 TEMÁTICA 5: IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE) CON POLÍTICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET.

Este artículo técnico explica la implementación y configuración de un proxy HTTP no transparente en Endian Firewall sobre GNU/Linux como se muestra en las figuras 32, 33 y 34, centrándose en la definición de políticas para controlar el acceso a internet. El documento describe la creación de perfiles de navegación y la elaboración de listas negras para bloquear sitios web específicos como www.hotmail.com, www.youtube.com, y www.elnuevodia.com.co, como se muestra en la figura 35 Además, detalla la configuración de la autenticación de usuarios, abarcando la creación de usuarios y grupos, el diseño de políticas de acceso personalizadas y su conexión con los perfiles de navegación como se muestra en la figura 36.

Se realizan pruebas de navegación sin las políticas aplicadas con el fin de garantizar el correcto funcionamiento del proxy no transparente como se observa en las figuras 37,38 y 39.

Finalmente, se exponen las pruebas efectuadas desde una LAN para comprobar la eficacia del bloqueo de los sitios restringidos, evidenciando la capacidad del proxy no transparente para ejercer un control detallado sobre la navegación web de los usuarios como se muestra en la figura 40.

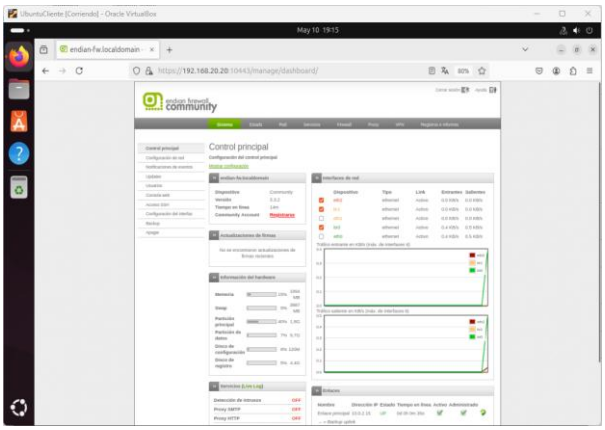

figura 32 Ingresar al administrador del endian
Fuente: Elaboración Propia – 2025.

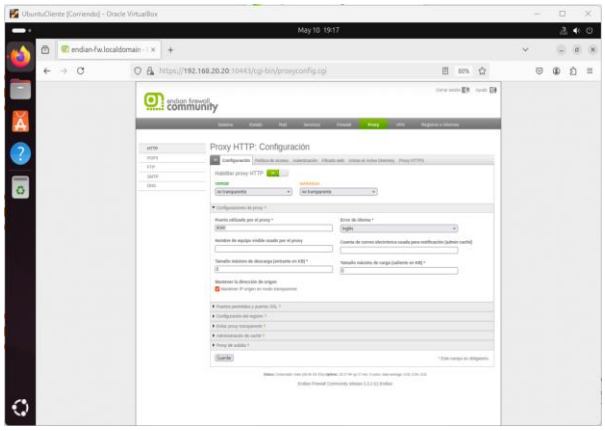

figura 33 la configuración del proxy no transparente
Fuente: Elaboración Propia – 2025

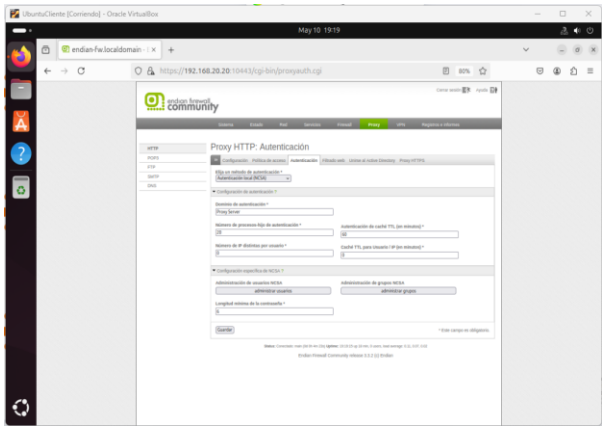

figura 34 la configuración del proxy no transparente
Fuente: Elaboración Propia – 2025

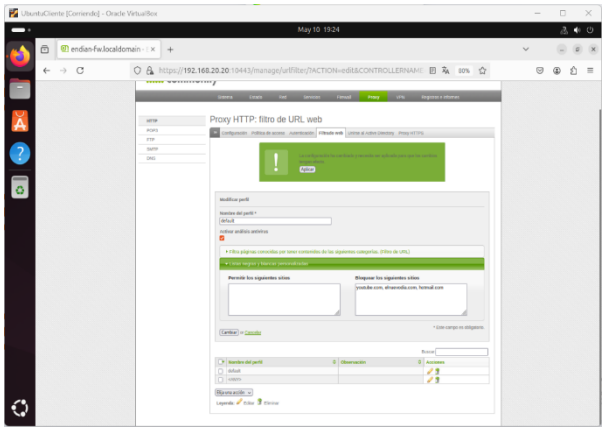

figura 35 lista de filtrado web
Fuente: Elaboración Propia – 2025

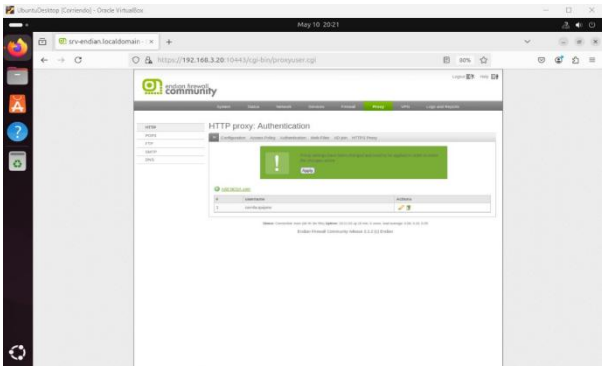

figura 36 Agregar usuario
Fuente: Elaboración Propia – 2025

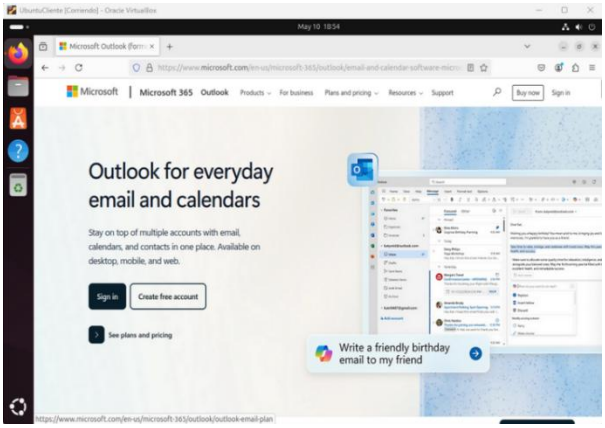

figura 37 Accesos a los sitios Hotmail, youtube y el nuevodia
Fuente: Elaboración Propia – 2025.

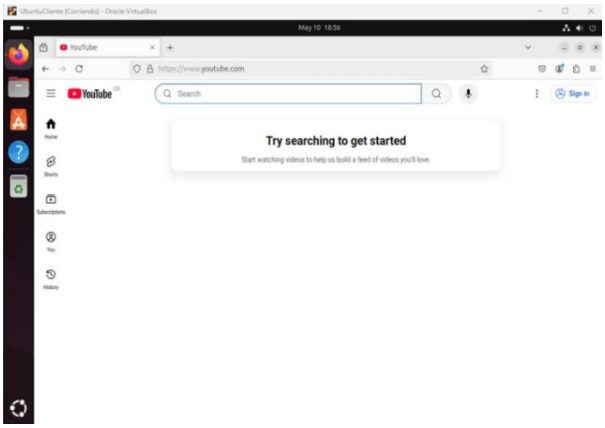

figura 38 Accesos a los sitios Hotmail, YouTube y el nuevodia
Fuente: Elaboración Propia – 2025

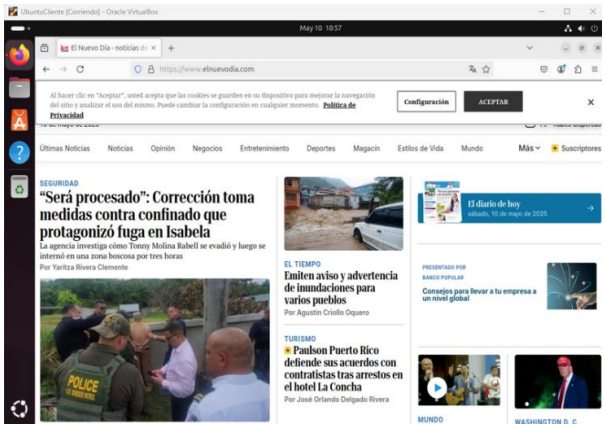

figura 39 Accesos a los sitios Hotmail, YouTube y el nuevo dia
Fuente: Elaboración Propia – 2025

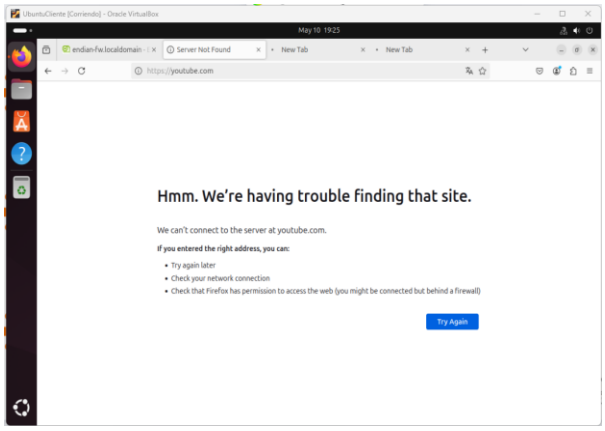

figura 40 Navegación restringida
Fuente: Elaboración Propia – 2025

3. CONCLUSIONES

Viabilidad y Eficacia de Endian Firewall Virtualizado para la Segmentación de Redes: La implementación detallada de Endian Firewall en un entorno virtualizado con VirtualBox demuestra de manera concluyente su viabilidad y eficacia como herramienta para establecer una arquitectura de seguridad perimetral robusta en plataformas GNU/Linux. La capacidad de configurar y gestionar las zonas de red (LAN, WAN y DMZ) de forma aislada, así como la aplicación de reglas NAT y reglas de acceso específicas (como las que permiten HTTP y FTP a la DMZ y deniegan ICMP), valida Endian como una solución práctica y adaptable para la segmentación de redes, un pilar fundamental en la mitigación de ciberamenazas.

Control Granular del Tráfico y la Navegación Web: El estudio pone de manifiesto la capacidad de Endian Firewall, incluso en un entorno virtualizado, para ejercer un control granular sobre el tráfico de red y la navegación web. La implementación exitosa de un proxy HTTP no transparente con políticas de autenticación, perfiles de navegación y listas negras (bloqueando sitios específicos como Hotmail, YouTube y El Nuevo Día) valida la funcionalidad de Endian para gestionar y restringir el acceso a internet desde la red interna (LAN). Esto subraya la importancia de este tipo de soluciones para aplicar políticas de seguridad y uso de recursos de red de manera efectiva.

Potencial de la Virtualización en la Implementación de Soluciones de Seguridad: La elección de VirtualBox como plataforma para la implementación de Endian Firewall resalta el potencial de la virtualización para el diseño, prueba y despliegue de arquitecturas de seguridad perimetral. Este enfoque permite una configuración flexible de múltiples interfaces de red, la simulación de diversos escenarios de tráfico y una gestión eficiente de los recursos, lo que lo convierte en un método altamente ventajoso tanto para entornos de aprendizaje y experimentación como para despliegues controlados en infraestructuras reales, facilitando la comprensión y aplicación de conceptos avanzados de seguridad de red.

4. REFERENCIAS

[1] Canonical (2023). Guía del Ubuntu desktop 20.04 LTS. Help Ubuntu.https://help.ubuntu.com/20.04/ubuntu-help/index.html.
[2] Debian (2023). El manual del administrador de Debian 12.5.0. Debian https://www.debian.org/releases/stable/amd64/index.es.html.
[3] Endian (2016), Endian UTM 3.2 Manual referencia. Endian. http://docs.endian.com/3.2/utm/index.html.
[4] Jay LaCroix. (2020). Mastering Ubuntu Server: Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting Ubuntu Server. Packt Publishing. https://research-ebsco-com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b41952.
[5] Oracle (2020), Manual de usuario VirtualBox. VirtualBox. https://www.virtualbox.org/manual/.
[6] SANS Institute (2020-2023) Understanding Network Segmentation for Improved Security https://www.sans.org/blog/understanding-network-segmentation-for-improved-security/
[7] Comunidad Endian (2024-2025) Endian Firewall Community Wiki/Forum https://community.endian.com/forum/
[8] Salomón, R. E. R. (2012). El gran libro de Debian GNU/Linux. Marcombo.
[9] Viñas, R. B., & Llinàs, F. A. (2003). Sistema operativo GNU/Linux básico. UOC.
[10] Hughes, P. (1996). GNU/Linux: Instalacion y Primeros Pasos.