IMPLEMENTACIÓN DE SEGURIDAD PERIMETRAL CON GNU/LINUX ENDIAN EN ENTORNOS VIRTUALES

Jhon Alexander Ramírez Perdomo
e-mail: jaramirezperd@unadvirtual.edu.co
Eder Favian Bohórquez Puentes
e-mail: efbohorquezp@unadvirtual.edu.co
Darío Arles Sogamoso Castillo
e-mail: dasogamosoc@unadvirtual.edu.co
Deyninson Johany Rodríguez Melo
e-mail: djrodriguezmel@unadvirtual.edu.co
Oscar Mauricio Urueña Vidal
e-mail: omuruenav@unadvirtual.edu.co

RESUMEN: *La seguridad perimetral se ha convertido en un componente esencial para la protección de redes empresariales que integran servicios internos (LAN) y externos (WAN). Este artículo detalla la implementación de la distribución Endian Linux (EFW) en VirtualBox, centrándose en la correcta configuración de las tarjetas de red para establecer la zona verde (LAN), roja (WAN) y naranja (DMZ). Esta segmentación permite controlar y proteger el tráfico de red, garantizando la integridad de los servidores y bases de datos alojados en la zona desmilitarizada. Los procesos de instalación, configuración inicial y validación de acceso a través del panel de administración se describen paso a paso como parte de una estrategia de seguridad integral.*

PALABRAS CLAVE: Configuración de firewall, Distribución GNU/Linux Endian, Infraestructura segura, Redes LAN y WAN.

1 INTRODUCCIÓN

La protección de los activos digitales en una organización requiere la implementación de mecanismos robustos de seguridad perimetral. En este sentido, GNU/Linux Endian Firewall (EFW) se presenta como una solución de código abierto altamente funcional para segmentar y proteger redes mediante zonas diferenciadas: verde (LAN), roja (WAN) y naranja (DMZ).

La correcta configuración de estas zonas permite establecer políticas de acceso controlado entre usuarios, servidores y servicios expuestos al exterior, garantizando así la integridad de los datos y la estabilidad de los sistemas críticos. Este artículo desarrolla la primera fase de la implementación, correspondiente a la creación de una instancia virtual de Endian en VirtualBox, la asignación estratégica de interfaces de red y la instalación efectiva del sistema. Lo anterior constituye la base para integrar servicios adicionales de seguridad en etapas posteriores.

Además, se destaca la utilidad de este enfoque para entornos académicos y corporativos donde se requiere simular escenarios reales de ciberseguridad. La virtualización facilita pruebas controladas y ajustes sin comprometer infraestructuras productivas.

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

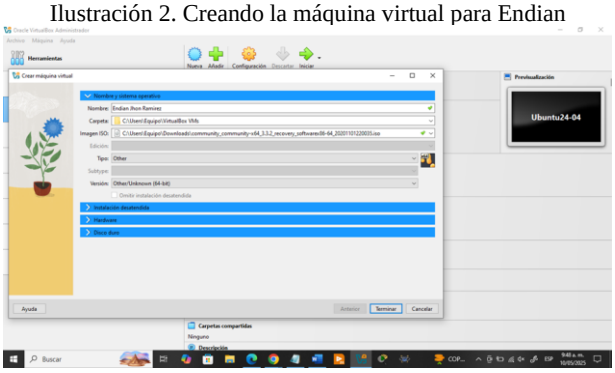
En el contexto actual de redes seguras y segmentadas, la implementación de firewalls de nivel empresarial se vuelve una necesidad crítica para la protección de sistemas y servicios. GNU/Linux Endian, una solución de código abierto para seguridad perimetral, permite la creación de entornos controlados mediante zonas de red como la LAN (verde), WAN (roja) y DMZ (naranja).

Esta primera temática aborda la configuración de una instancia de Endian en VirtualBox, enfocándose en la correcta asignación de tarjetas de red virtuales y en el proceso de instalación del sistema, sentando así las bases para una administración eficiente del tráfico de red y una política de seguridad estructurada. A continuación, se presentan los pasos detallados para llevar a cabo la Temática 1:

Ilustración 1. Descarga de Endian Firewall Community ISO

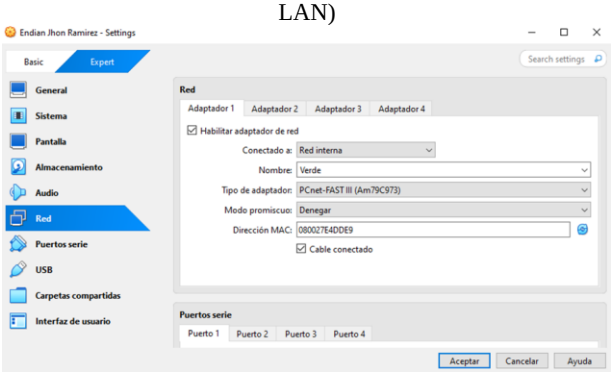
Fuente: Autoría Propia

Ilustración 2. Creando la máquina virtual para Endian



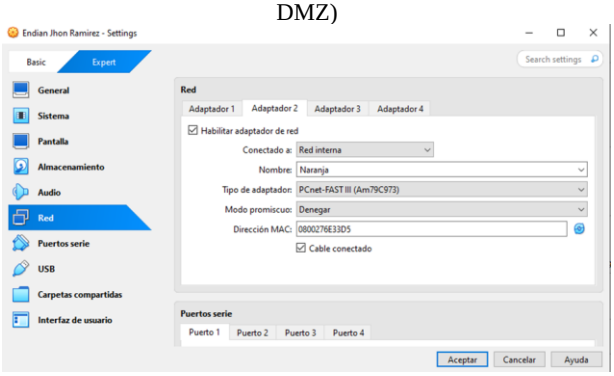
Fuente: Autoría Propia

Ilustración 3. Configuración de la zona verde (Red interna - LAN)



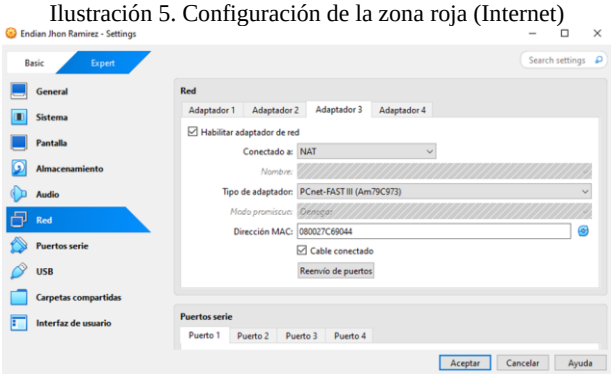
Fuente: Autoría Propia

Ilustración 4. Configuración de la zona naranja (servidores - DMZ)



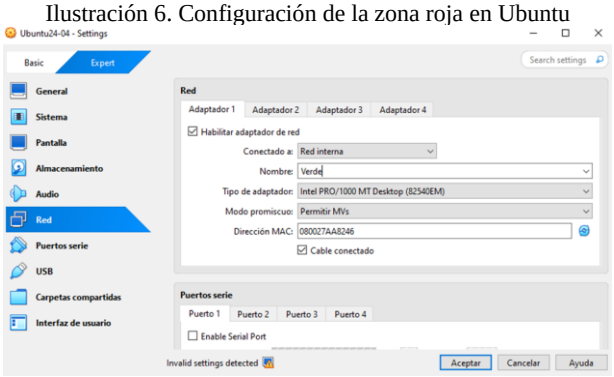
Fuente: Autoría Propia

Ilustración 5. Configuración de la zona roja (Internet)



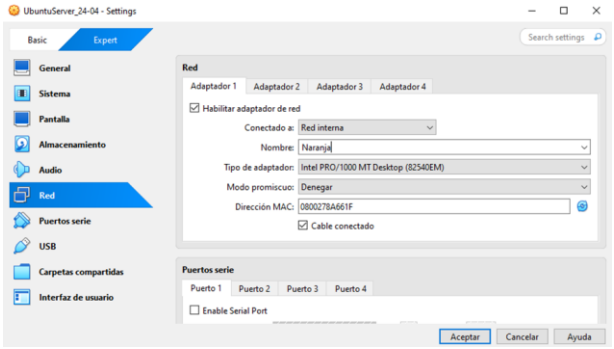
Fuente: Autoría Propia

Ilustración 6. Configuración de la zona roja en Ubuntu



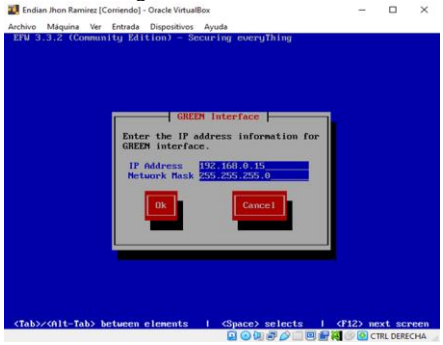
Fuente: Autoría Propia

Ilustración 7. Configuración de la zona verde en el Ubuntu server



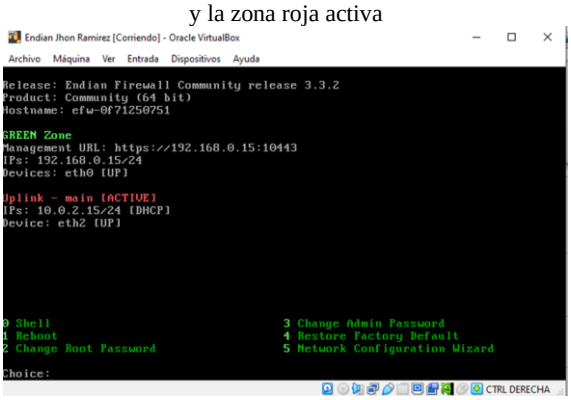
Fuente: Autoría Propia

Ilustración 8. Asignación de la dirección IP a Endian



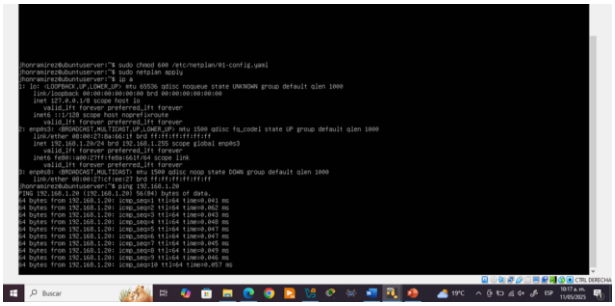
Fuente: Autoría Propia

Ilustración 9. Interfaz de Edian, donde se aprecia la zona verde y la zona roja activa



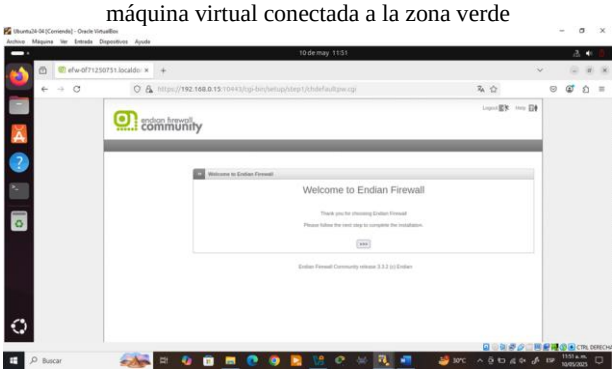
Fuente: Autoría Propia

Ilustración 10. Verificación de conexión desde el servidor hacia la zona verde



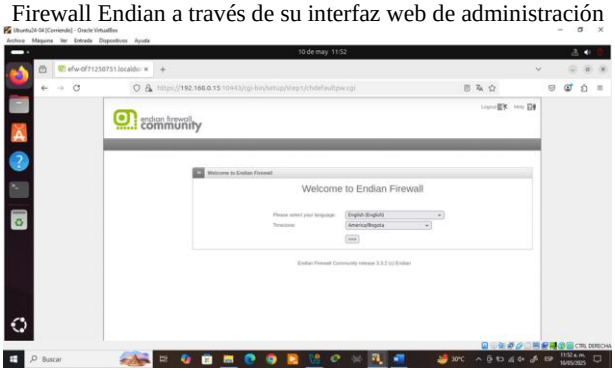
Fuente: Autoría Propia

Ilustración 11. Acceso al panel web de Endian desde una máquina virtual conectada a la zona verde



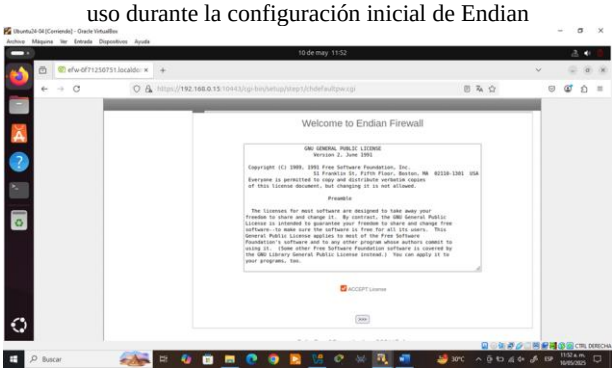
Fuente: Autoría Propia

Ilustración 12. Configuración avanzada de los parámetros del Firewall Endian a través de su interfaz web de administración



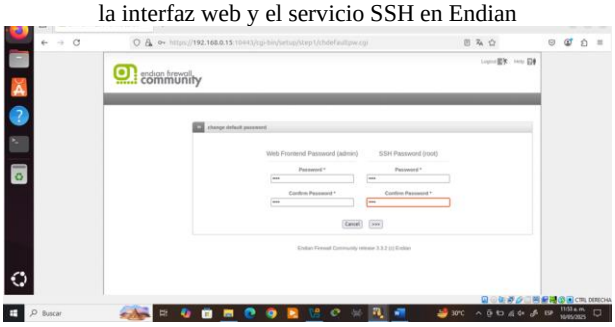
Fuente: Autoría Propia

Ilustración 13. Aceptación de los términos y condiciones de uso durante la configuración inicial de Endian



Fuente: Autoría Propia

Ilustración 14. Establecimiento de credenciales de acceso para la interfaz web y el servicio SSH en Endian

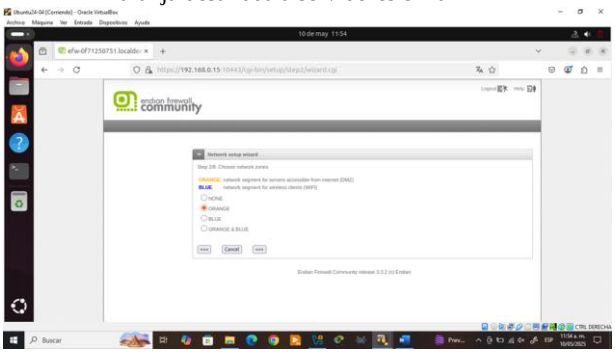


Fuente: Autoría Propia

Ilustración 15. Definición de los parámetros de red para la zona roja, correspondiente al acceso WAN

Fuente: Autoría Propia

Ilustración 16. Asignación de parámetros de red para la zona naranja destinada a servidores en la DMZ

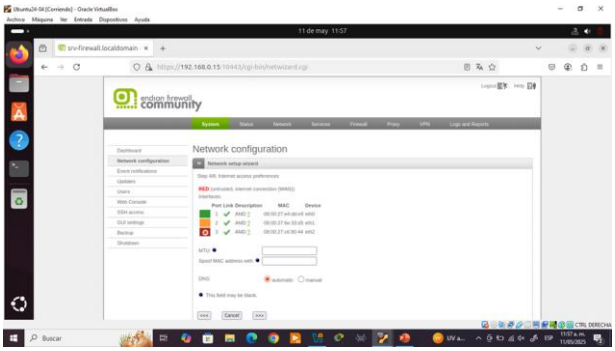


Fuente: Autoría Propia

Ilustración 17. Establecimiento de parámetros de red para la zona verde correspondiente a la red interna (LAN) y la zona naranja correspondiente a la red del servidor

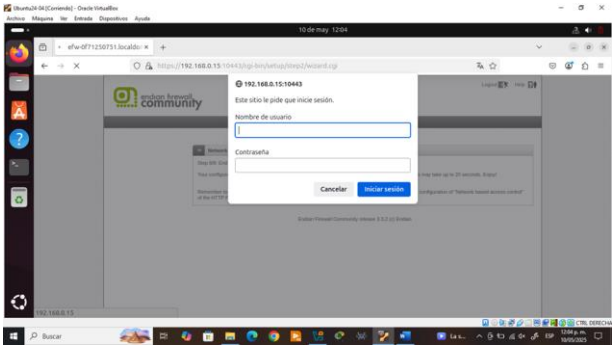
Fuente: Autoría Propia

Ilustración 18. Verificación de las configuraciones realizadas en cada una de las zonas



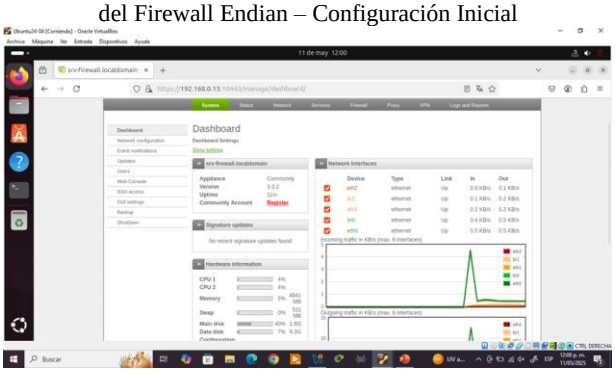
Fuente: Autoría Propia

Ilustración 19. Finalización del asistente de configuración e inicio de sesión en Endian con credenciales administrativas



Fuente: Autoría Propia

Ilustración 20. Acceso a la Consola de Administración Central del Firewall Endian – Configuración Inicial



Fuente: Autoría Propia

3. TEMÁTICA 2: CONFIGURACIÓN NAT

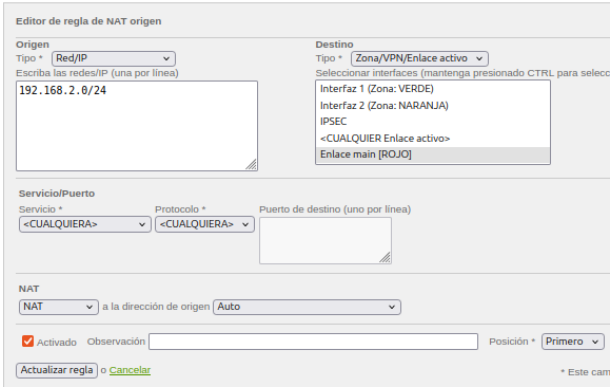
La configuración de NAT (Network Address Translation) es esencial para permitir la comunicación entre redes privadas (LAN) y redes públicas (WAN/Internet), así como para gestionar el acceso de zonas específicas como la DMZ.

3.1 CONFIGURACIÓN DE LA REGLA NAT PARA LA LAN

El primer paso consistió en acceder al menú 'Firewall' del dispositivo de red, desde donde se gestionan las reglas de NAT. En la pestaña “NAT Fuente”, se agregó una nueva regla para permitir el acceso a Internet desde la red LAN (zona verde). Esta configuración habilita que todos los dispositivos dentro del rango de la red local puedan comunicarse hacia el exterior, es decir, hacia la red WAN.

Tras guardar y aplicar los cambios, se verificó exitosamente la navegación a Internet desde una máquina cliente ubicada en la zona verde, confirmando la correcta aplicación de la regla NAT. Este paso es fundamental para garantizar que los equipos internos accedan a recursos en línea sin exponer directamente sus direcciones IP reales. Además, esta técnica contribuye a fortalecer la seguridad al limitar las rutas de acceso no autorizadas desde el exterior.

Ilustración 21. Configuración de la regla NAT para la LAN



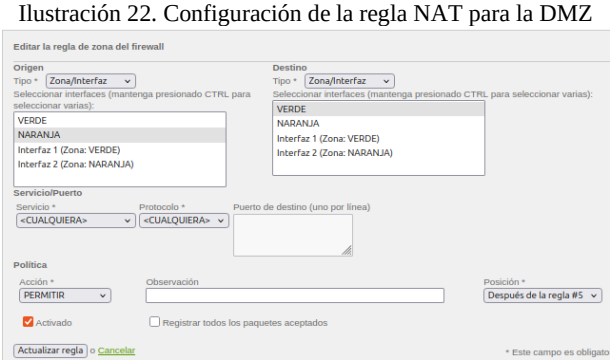
Fuente: Autoría Propia

3.2 CONFIGURACIÓN DE LA REGLA NAT PARA LA DMZ

Posteriormente, se procedió a configurar el acceso de la zona DMZ (zona naranja) hacia Internet. Para ello, se creó una nueva regla de firewall interzonas, estableciendo la DMZ como origen y la roja verde como destino. Esta regla permite que los servidores ubicados en la DMZ tengan salida controlada hacia la red pública, manteniendo la segmentación y seguridad de la infraestructura.

La verificación demostró que el servidor en la DMZ pudo establecer conexión con la red verde y, a través de esta, acceder a Internet.

Ilustración 22. Configuración de la regla NAT para la DMZ



Fuente: Autoría Propia

Nota. Se evidencia la creación y aplicación de la regla, así como la conectividad de la DMZ hacia la red verde e Internet.

Ilustración 23. Conexión hacia la zona verde

```
servidor@servidor:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=118 time=10.2 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=11.3 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=118 time=11.5 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2052ms
rtt min/avg/max/mdev = 10.221/11.017/11.528/0.570 ms
servidor@servidor:~$ ping 192.168.2.15
PING 192.168.2.15 (192.168.2.15) 56(84) bytes of data.
64 bytes from 192.168.2.15: icmp_seq=1 ttl=64 time=0.987 ms
64 bytes from 192.168.2.15: icmp_seq=2 ttl=64 time=1.19 ms
^C
--- 192.168.2.15 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1006ms
rtt min/avg/max/mdev = 0.987/1.090/1.194/0.103 ms
servidor@servidor:~$ ping 192.168.2.20
PING 192.168.2.20 (192.168.2.20) 56(84) bytes of data.
64 bytes from 192.168.2.20: icmp_seq=1 ttl=63 time=0.664 ms
64 bytes from 192.168.2.20: icmp_seq=2 ttl=63 time=1.85 ms
64 bytes from 192.168.2.20: icmp_seq=3 ttl=63 time=1.96 ms
^C
--- 192.168.2.20 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2059ms
rtt min/avg/max/mdev = 0.664/1.490/1.959/0.586 ms
servidor@servidor:~$ _
```

Fuente: Autoría Propia

La correcta implementación de las reglas NAT fue validada mediante pruebas de conectividad desde los diferentes segmentos de red.

3.3 VERIFICACIÓN DE LOS RESULTADOS

- La red LAN (verde) accede a Internet sin restricciones, gracias a la regla NAT configurada.
- La zona DMZ (naranja) puede comunicarse con la red verde y, a través de esta, acceder a Internet, manteniendo la separación lógica y la seguridad entre zonas.
- El monitoreo de las reglas y el tráfico confirma que las políticas de acceso cumplen con los objetivos de la segmentación y la traducción de direcciones, fundamentales para el funcionamiento y la protección de la red interna.

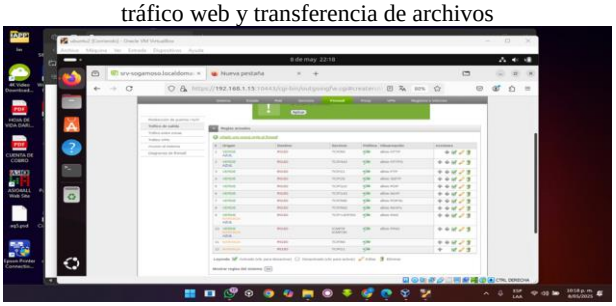
Estos resultados demuestran la importancia de una configuración adecuada de NAT y reglas de firewall para garantizar la conectividad y seguridad en entornos de red segmentados.

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

Durante esta fase, se habilitó el acceso controlado desde la zona DMZ hacia la red externa y ciertos servicios internos específicos, manteniendo la seguridad de la red LAN. Se configuraron reglas de firewall en Endian para permitir los servicios HTTP (puerto 80) y FTP (puerto 21) desde un servidor web ubicado en la DMZ bajo Ubuntu Server. Estas reglas se añadieron manualmente en el cortafuegos de Endian, asegurando la publicación de servicios hacia el exterior sin comprometer la red interna.

Adicionalmente, se establecieron filtros para restringir el tráfico entrante solo a las direcciones IP autorizadas, mitigando riesgos de acceso no deseado. Esta estrategia permite ofrecer servicios públicos de forma segura, manteniendo un control riguroso sobre el flujo de datos entre zonas.

Ilustración 24. Permitir servicios HTTP (puerto 80) y FTP (puerto 21) a través de la configuración de reglas para permitir tráfico web y transferencia de archivos



Fuente: Autoría Propia

Ilustración 25. Adición manual de los puertos específicos en las reglas del cortafuegos en Endian

Fuente: Autoría Propia

Como medida complementaria de seguridad, se configuró una regla para denegar el protocolo ICMP (puertos 8 y 30**)**. Esta práctica es común para prevenir escaneos de red, ya que herramientas como ping o traceroute utiliza ICMP para identificar la presencia de dispositivos activos. Al bloquear este protocolo desde y hacia la DMZ, se minimiza la exposición de los servicios ante amenazas externas y se evita la recopilación de información útil para un posible atacante. Adicionalmente, se implementó una regla de seguridad para denegar el protocolo ICMP (puertos 8 y 30), lo que impide realizar pings a través de la red, aumentando la protección contra escaneos y ataques de red.

Ilustración 26. Loqueo del protocolo ICMP (puertos 8 y 30) como una prueba de política para denegar el ping mediante ICMP como medida de seguridad

Fuente: Autoría Propia

Este enfoque sigue el principio de mínimo privilegio, otorgando únicamente el acceso necesario para el correcto funcionamiento de los servicios, y defensa en profundidad, donde múltiples capas de seguridad como firewall, reglas de acceso, y monitoreo trabajan en conjunto para proteger el entorno. Además, se realizaron pruebas de verificación de conectividad desde clientes ubicados en diferentes zonas de red, confirmando que:

- Los servicios HTTP y FTP respondían desde la red externa.
- No era posible realizar pings al servidor de la DMZ desde la WAN ni desde la LAN.
- Los servicios internos permanecían inaccesibles desde la zona DMZ.

Estos resultados demuestran que la segmentación de redes y el control granular del tráfico es una estrategia efectiva para proteger los activos digitales sin afectar la disponibilidad de los servicios expuestos al público.

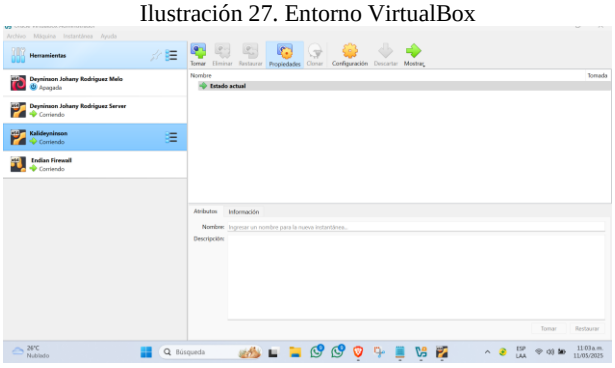
5. TEMÁTICA 4: REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO

La gestión de reglas de acceso Inter zonas es crucial para controlar el tráfico entre redes segmentadas en un entorno GNU/Linux, asegurando la seguridad perimetral. Esta actividad implementó reglas en Endian Firewall (EFW) para permitir tráfico HTTP (puerto 80) y FTP (puerto 21) entre las zonas Verde (LAN, 192.168.0.1/24) y Naranja (DMZ, 192.168.10.1/24), utilizando comandos en consola. Las pruebas verifican la efectividad de las configuraciones, protegiendo los servicios críticos alojados en la DMZ. Estas reglas también facilitan un entorno seguro para el intercambio de datos entre usuarios internos y servidores expuestos. Además, su correcta aplicación permite minimizar vulnerabilidades al definir explícitamente qué tipos de tráfico están autorizados.

5.1 CONFIGURACIÓN DEL ENTORNO

El entorno virtual se preparó en VirtualBox con las siguientes máquinas:

Ilustración 27. Entorno VirtualBox

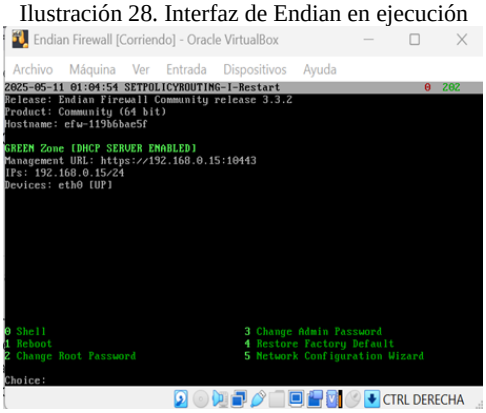


Fuente: Autoría Propia

Endian Firewall (EFW) fue configurado con tres interfaces de red y estas son:

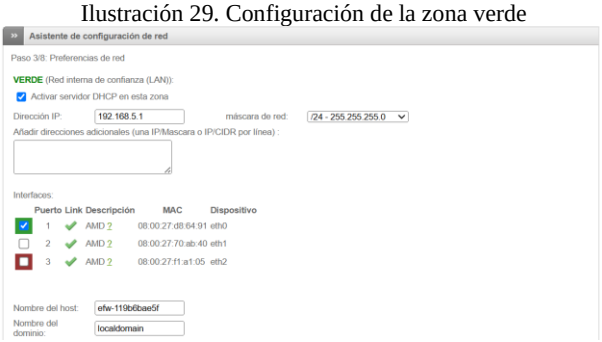
- Zona Verde (LAN): IP 192.168.5.1/24, interfaz eth1.
- Zona Roja (WAN): IP 192.168.0.1/24, interfaz eth0.
- Zona Naranja (DMZ): IP 192.168.10.1/24, interfaz eth2.

Ilustración 28. Interfaz de Endian en ejecución



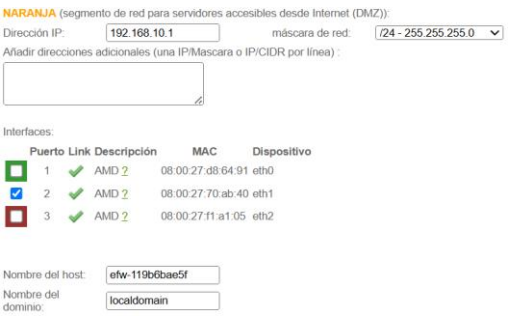
Fuente: Autoría Propia

Ilustración 29. Configuración de la zona verde



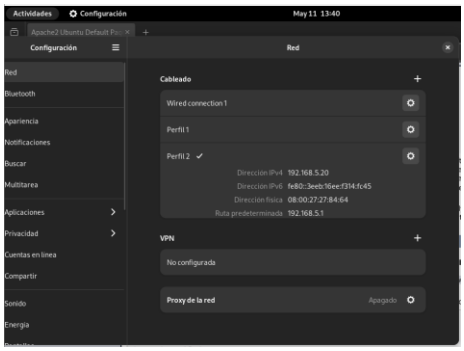
Fuente: Autoría Propia

Ilustración 30. Configuración de la zona naranja



Fuente: Autoría Propia

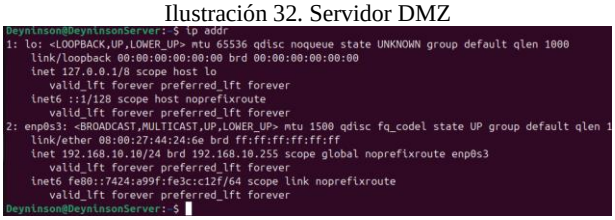
Ilustración 31. LAN cliente



Fuente: Autoría Propia

Servidor DMZ: Máquina Ubuntu Server con IP 192.168.10.10, alojando servicios HTTP (Apache) y FTP (vsftpd), conectada a la zona Naranja.

Ilustración 32. Servidor DMZ



Fuente: Autoría Propia

Este esquema asegura la segmentación lógica de la red, permitiendo pruebas controladas entre zonas.

5.2 CONFIGURACIÓN DE LAS REGLAS DE ACCESO

Las reglas de acceso interzonal se implementan directamente en la consola de Endian Firewall utilizando el comando iptables, que gestiona las políticas de filtrado de paquetes en el núcleo de Linux. A continuación, se presentan los comandos ejecutados para permitir el tráfico específico:

Permitir tráfico HTTP desde LAN a DMZ: La salida muestra que las reglas están activas y que el tráfico HTTP y FTP está siendo permitido, mientras que el resto del tráfico no autorizado es manejado por la política predeterminada del sistema.

Estas configuraciones garantizan que solo los servicios necesarios estén expuestos, limitando así la superficie de ataque. También se incorporaron reglas explícitas de denegación para reforzar el aislamiento entre zonas cuando no se requiere comunicación. Esta estructura modular permite ajustar fácilmente las políticas según los requerimientos del entorno.

Ilustración 33. Reglas de tráfico

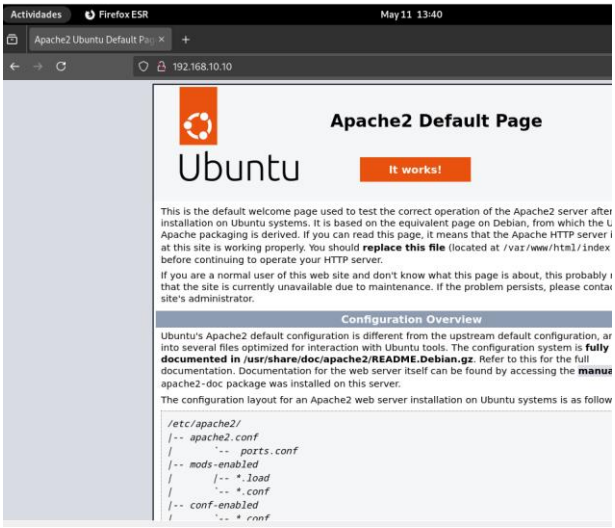
Fuente: Autoría Propia

5.3 VERIFICACIÓN DE CONECTIVIDAD

Se realizaron pruebas desde el cliente en la zona Verde para validar el funcionamiento de las reglas:

- Prueba de acceso HTTP: Desde el cliente LAN (192.168.5.20), se ejecutó: El resultado confirma que el servicio HTTP en el servidor DMZ es accesible desde la LAN.
- Prueba de acceso FTP: Desde el mismo cliente, se intentó una conexión FTP (ftp 192.168.10.10): El resultado indica que el servidor FTP ubicado en la zona DMZ respondió correctamente a la solicitud desde la LAN, validando que la regla configurada en el firewall permite el tráfico en el puerto 21. La transferencia de archivos de prueba también se realizó sin inconvenientes, confirmando la operatividad del servicio.

Ilustración 34. Prueba del servidor DMZ



Fuente: Autoría Propia

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

En la implementación de un proxy HTTP no transparente con políticas de autenticación para navegación en Internet, el concepto de endianness cobra relevancia en aspectos de bajo nivel relacionados con la interoperabilidad entre arquitecturas de hardware y el correcto manejo de datos en los protocolos de red.

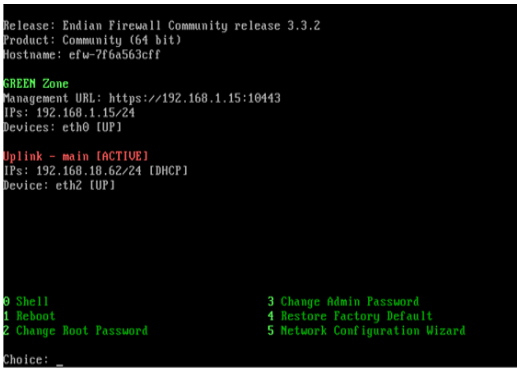
Aunque no interviene directamente en la configuración funcional del proxy, comprender el orden de los bytes en memoria resulta fundamental al interactuar con estructuras binarias, funciones de red que requieren conversión entre el orden del host y el orden de red (big-endian), o al compilar software de red en entornos heterogéneos. Ignorar esta característica puede derivar en errores sutiles en la autenticación o en la transmisión de datos, particularmente en sistemas distribuidos o multiplataforma.

Por tanto, el conocimiento del endianness contribuye a una implementación más robusta, portable y segura del sistema proxy.

6.1 INSTALACIÓN DE ENDIAN

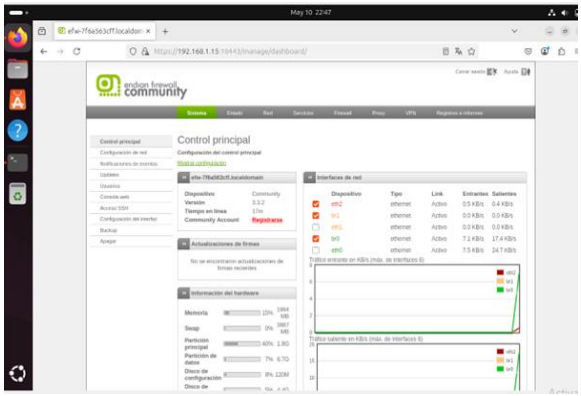
Este paso consistió en realizar la instalación del Endian en Virtual Box con las configuraciones Red Interna y Red Externa, se mostrará como evidencia el funcionamiento de endian y el funcionamiento en linux.

Ilustración 35. Instalación Endian



Fuente: Autoría Propia

Ilustración 36. Dashboard Endian en Linux



Fuente: Autoría Propia

6.2 AUTENTICACIÓN DE USUARIO

Este paso consiste en configurar el filtrado web con el usuario para empezar con los bloqueos de las páginas youtube, mi nuevo día y Hotmail (Outlook).

Ilustración 37. Autenticación Usuario y lista negra de páginas

Fuente: Autoría Propia

Se habilitó la autenticación mediante proxy HTTP no transparente, lo que requiere que los usuarios introduzcan credenciales antes de acceder a Internet. Esta medida permite aplicar políticas personalizadas según el perfil del usuario autenticado. Además, se definieron listas de control de acceso (ACL) para restringir contenidos no permitidos conforme a las políticas de navegación establecidas.

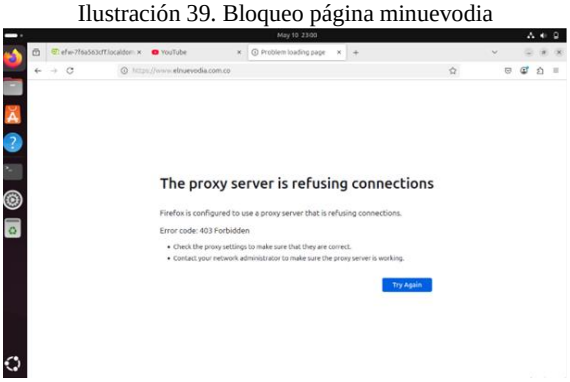
6.3 VERIFICACIÓN DE WEB LAN

Una vez realizado, realizamos las respectivas verificaciones de las páginas webs que están en lista negra.

Ilustración 38. Página Youtube Bloqueada

Fuente: Autoría Propia

Ilustración 39. Bloqueo página minuevodia



Fuente: Autoría Propia

Ilustración 40. Página Hotmail bloqueada

Fuente: Autoría Propia

7. CONCLUSIONES

La implementación de GNU/Linux Endian en un entorno virtualizado permitió comprender de manera práctica cómo se estructuran y gestionan las zonas de seguridad en una arquitectura de red. A través de la correcta configuración de las interfaces de red en VirtualBox y la asignación de roles específicos a cada zona (verde como LAN, roja como WAN y naranja como DMZ), se logró simular un escenario real de firewall y control de tráfico.

Asimismo, el uso de la interfaz web de Endian facilitó la administración de las políticas de red, mostrando la importancia de contar con herramientas visuales para la gestión de la seguridad perimetral. Se destacó la relevancia de una configuración precisa durante el proceso de instalación, como la asignación de contraseñas, el direccionamiento IP y la aceptación de términos, para garantizar la estabilidad y protección del sistema.

Finalmente, esta experiencia práctica refuerza el valor de los firewalls de tipo UTM (Gestión Unificada de Amenazas) en infraestructuras de red actuales, donde la segmentación por zonas contribuye significativamente a mejorar la seguridad, disponibilidad y control del entorno.

Además, la implementación del proxy HTTP no transparente con autenticación evidenció cómo es posible aplicar políticas diferenciadas de acceso a Internet según el perfil del usuario, reforzando el control de navegación y reduciendo riesgos asociados al uso inadecuado de los recursos web. Esta funcionalidad resulta clave en entornos corporativos o educativos, donde es necesario supervisar y restringir el acceso a ciertos contenidos sin comprometer la experiencia del usuario autorizado.

8. REFERENCIAS

[1] D. Comer, Internetworking with TCP/IP: Principles, Protocols, and Architecture, 6th ed., Pearson, pp. 143–160, 2014.

[2] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, y T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1: Message Syntax and Routing", Internet Engineering Task Force (IETF), RFC 7230, pp. 1–84, Jun. 2014.

[3] B. Hubert, "The Definitive Guide to Squid: The Web Proxy Cache", O'Reilly Media, 1st ed., pp. 23–57, 2005.

[4] A. Tanenbaum y D. Wetherall, Computer Networks, 5th ed., Pearson, pp. 368–375, 2011.

[5] G. Lyon, Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning, Insecure.Com LLC, pp. 102–120, 2009.

[6] J. Love, Linux System Programming, 2nd ed., O'Reilly Media, pp. 54–60, 2013.

[7] B. Albahari y J. Albahari, C# 9.0 in a Nutshell, 7th ed., O'Reilly Media, pp. 476–480, 2021. [Incluye detalles sobre endianness en sistemas].

[8] M. Tim Jones, "Anatomy of Linux Networking", IBM DeveloperWorks, pp. 1–12, Aug. 2006. [En línea]. Disponible: https://developer.ibm.com/articles/l-linux-networking/

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

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

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

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

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

[14] 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

[15] Cervelión, Á. J. (2023). Instalación de Nagios Core 4.4 en Ubuntu 22.04. [Objeto_virtual_de_información_OVI]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/54230