“Implementando Seguridad Perimetral en GNU/Linux: Despliegue de Endian Firewall y Protección de Servicios en Zona DMZ”

Julián Sarmiento Cubillos
jsarmientocu@unadvirtual.edu.co
Edwar Esteven Rodríguez Bernate
eerodriguezbe@unadvirtual.edu.co

RESUMEN: *La presente actividad grupal consistió en implementar una solución de seguridad perimetral utilizando Endian Firewall Community Edition como elemento central de protección entre la red interna (LAN), la zona desmilitarizada (DMZ) y la red externa (WAN). El objetivo principal fue garantizar la seguridad e integridad de los servicios web y FTP alojados en un servidor GNU/Linux ubicado en la DMZ. Cada integrante del grupo seleccionó y desarrolló de forma individual una temática. En este caso, se ejecutaron la Temática 1 (instalación y configuración inicial de Endian Firewall con las tres zonas de red) y la Temática 3 (permitir servicios HTTP y FTP desde la zona DMZ y denegar ICMP). Todas las configuraciones se realizaron desde consola y se verificaron mediante pruebas de conectividad (HTTP, FTP e ICMP). Los resultados demostraron un control efectivo del tráfico inter-zona, cumpliendo con los requisitos de seguridad perimetral solicitados.*

PALABRAS CLAVE: seguridad perimetral, DMZ, Endian Firewall, GNU/Linux, firewall UTM, zona verde, zona naranja, ICMP, HTTP, FTP

1 INTRODUCCIÓN

La seguridad perimetral representa uno de los pilares fundamentales en la protección de infraestructuras de red modernas. En entornos donde coexisten servidores con bases de datos y aplicaciones web, es indispensable contar con un firewall que permita segmentar y controlar el tráfico entre la red interna (LAN), la zona desmilitarizada (DMZ) y la red externa (WAN).

La presente actividad académica tuvo como propósito implementar una solución de seguridad perimetral mediante la distribución Endian Firewall Community Edition, actuando como gateway UTM entre las tres zonas de red. A través del trabajo colaborativo, cada integrante configuró y administró los servicios desde consola, aplicando conceptos de direccionamiento IP, reglas de firewall y buenas prácticas de seguridad en entornos GNU/Linux.

Este artículo presenta el desarrollo individual de Julian Sarmiento Cubillos, quien ejecutó la Temática 1 (instalación y configuración inicial de Endian Firewall) y la Temática 3 (permitir servicios de la zona DMZ y denegar ICMP), detallando cada paso, configuración y evidencia obtenida.

2 TEMATICA 1

Instalación y configuración inicial de Endian Firewall con las tres zonas de red (Green, Orange y Red).

Desarrolla: Edwar Esteven Rodriguez Bernate

Durante la Etapa 7 se realizó la instalación y configuración inicial de Endian Firewall Community Edition 3.3.2 en una máquina virtual de Oracle VirtualBox, con el propósito de establecer una arquitectura de seguridad perimetral basada en la segmentación de redes. Para ello, se configuraron tres adaptadores de red que permitieron la creación de las tres zonas principales: la Zona GREEN (LAN) en el Adaptador 1 conectada a la red interna “Verde” con dirección IP 192.168.10.1/24; la Zona ORANGE (DMZ) en el Adaptador 2 conectada a la red interna “Naranja” con dirección IP 192.168.20.1/24 destinada al alojamiento de servicios públicos; y la Zona RED (WAN) en el Adaptador 3 configurada en modo NAT para permitir el acceso controlado a Internet. Se completó el asistente de configuración de red (Network Configuration Wizard), habilitando DHCP en la zona Green y verificando la correcta interconexión entre las zonas, sentando así las bases para la implementación posterior de reglas de firewall y el despliegue seguro de servicios en la zona DMZ.

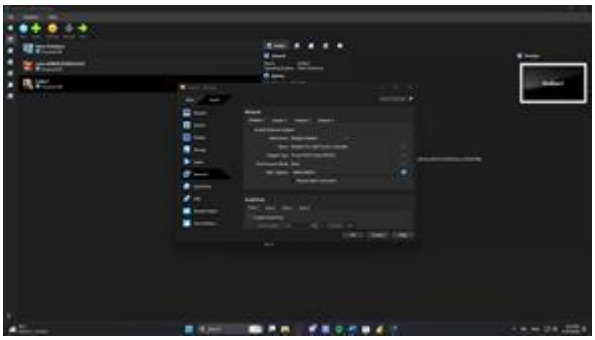
Las direcciones a tener en cuenta respecto a las zonas serán

Tabla 1
zonas a implementar

Zona	IP del firewall	Red
GREEN	192.168.10.1/24	Red interna LAN
ORANGE	192.168.20.1/24	Zona DMZ
RED	DHCP (NAT)	Conexión a Internet

Fuente: Autoría propia

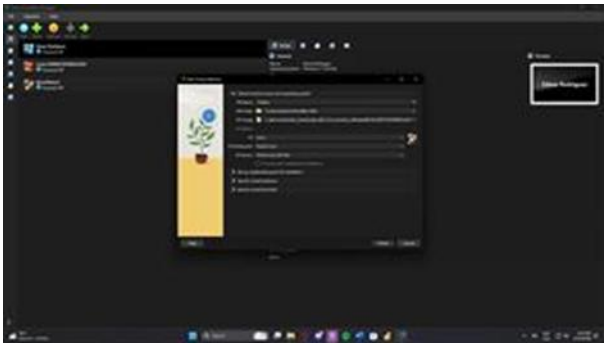
Figura 1.
Configuración del adaptador 1 de Endian



Fuente: Autoría propia

Configuración del Adaptador 1 en Oracle VirtualBox, conectado a la red interna denominada "Verde", correspondiente a la Zona GREEN (LAN). En esta pantalla se observa la asignación del tipo de adaptador y la habilitación del cable virtual para la conexión de la zona interna.

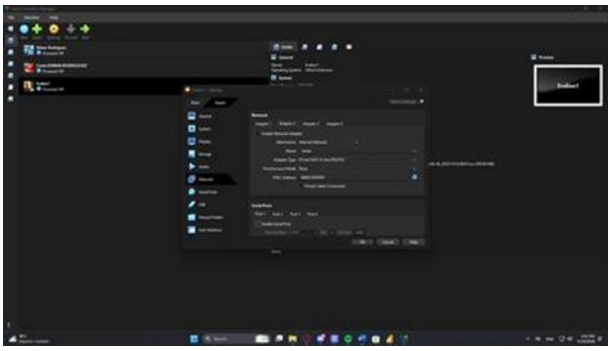
Figura 2.
instalación del ISO Image



Fuente: Autoría propia

Pantalla de inicio de la instalación del archivo ISO de Endian Firewall Community Edition 3.3.2 en la máquina virtual de Oracle VirtualBox.

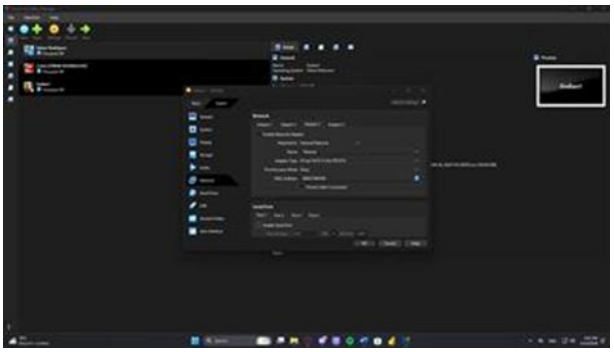
Figura 3.
Adaptador 1 conectado a la red interna 'Verde' (Zona LAN)



Fuente: Autoría propia

Detalle de la configuración final del Adaptador 1 asignado a la red interna "Verde", estableciendo la Zona GREEN (LAN). Esta configuración es fundamental para definir la red interna y permitir la comunicación segura con el firewall.

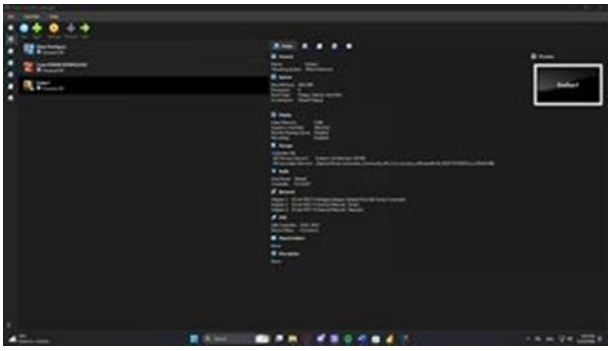
Figura 4.
Configuración del adaptador 3 Naranja



Fuente: Autoría propia

Configuración del Adaptador 3 en modo NAT, destinado a la Zona RED (WAN). Esta interfaz permite la conexión controlada del firewall hacia Internet, simulando el acceso a la red externa.

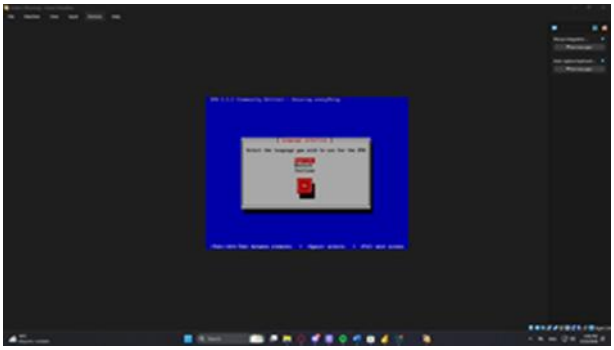
Figura 5.
Configuración del adaptador 3 Naranja



Fuente: Autoría propia

Pantalla inicial de carga y arranque del sistema Endian Firewall Community Edition 3.3.2, una vez completado el proceso de instalación del archivo ISO en la máquina virtual. Esta imagen muestra el momento en que el sistema operativo del firewall inicia por primera vez, confirmando que la instalación se realizó de manera exitosa y que el equipo está listo para continuar con la configuración de las zonas de red y los servicios.

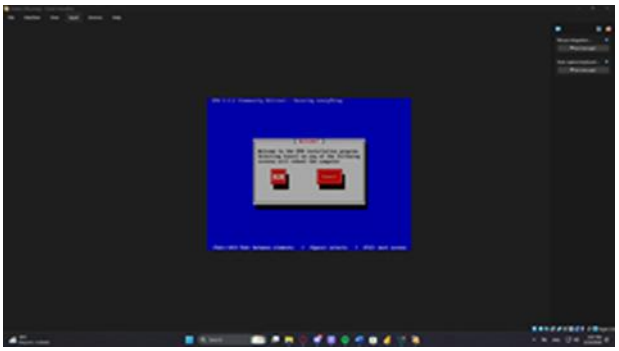
Figura 6.
Configuración de lenguaje del Endian



Fuente: Autoría propia

Pantalla del asistente de instalación inicial donde se selecciona el idioma del sistema. En este caso se eligió inglés para continuar con el proceso de configuración.

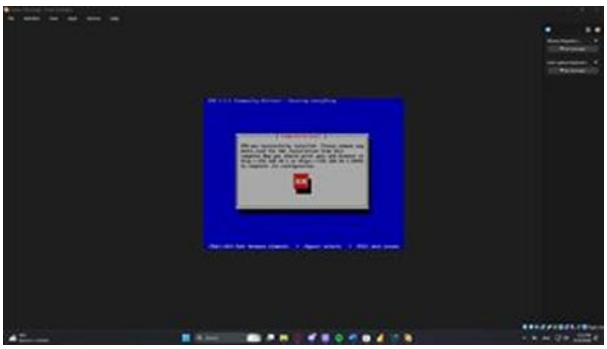
Figura 7.
Configuración del Edian



Fuente: Autoría propia

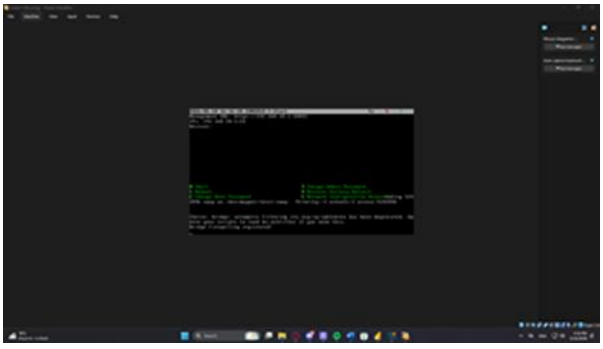
Pantalla principal del asistente de configuración inicial de Endian Firewall, donde se definen los parámetros básicos del sistema antes de proceder con la configuración de las zonas de red.

Figura 8.
Configuración del Exitosa



Fuente: Autoría propia

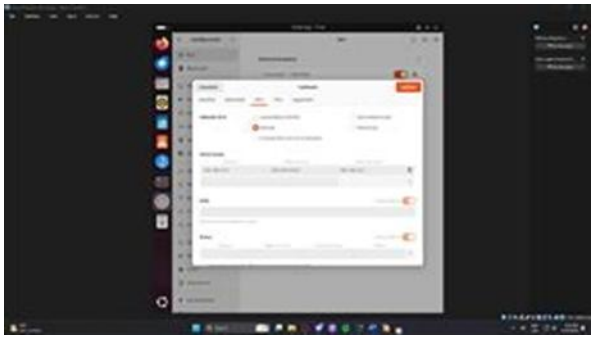
Figura 9.
Se visualiza inicio exitoso



Fuente: Autoría propia

Pantalla que muestra el arranque exitoso del sistema Endian Firewall una vez finalizada la fase de instalación y configuración inicial

Figura 10.
Se realiza configuración en la maquina



Fuente: Autoría propia

Verificación de los parámetros de configuración aplicados en la máquina virtual de Endian Firewall durante el proceso de ajuste de red y definición de zonas.

Figura 11.
Se realiza configuración en la maquina

Fuente: Autoría propia

Verificación de los parámetros de configuración aplicados en la máquina virtual de Endian Firewall durante el proceso de ajuste de red y definición de zonas.

Figura 12.
Verificación en la máquina funcionando

Fuente: Autoría propia

Acceso al panel de administración (dashboard) de Endian Firewall a través del navegador web, utilizando la dirección URL https://192.168.10.1:10443 desde la máquina Desktop.

Figura 13.
Se visualiza configuración exitosa

Confirmación visual en el dashboard de Endian Firewall que indica que la configuración de las zonas de red y los servicios básicos se ha realizado de forma exitosa.

Con la Temática 1 se logró instalar y configurar Endian Firewall Community Edition 3.3.2, creando las tres zonas de red (Green, Orange y Red) con sus respectivas direcciones IP. Los resultados obtenidos validaron una correcta segmentación de la red, cumpliendo con los requisitos base de la arquitectura perimetral. Esta práctica fortaleció las competencias en instalación y configuración inicial de firewalls UTM en entornos GNU/Linux.

3 TEMATICA 3

Permitir servicios de la Zona DMZ para la red.

Desarrolla: Julián Sarmiento Cubillos

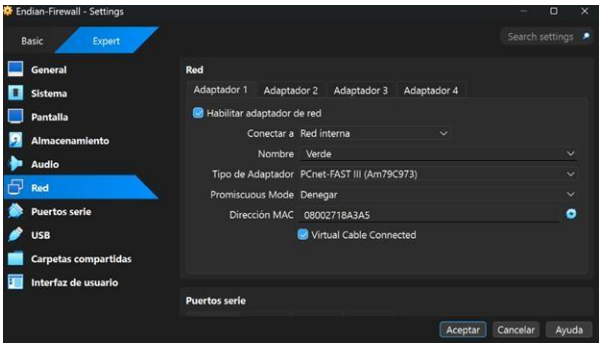
En el presente trabajo se ejecutaron la Temática 1 y la Temática 3 de la Etapa 7. Para la Temática 1 se instaló Endian Firewall Community Edition 3.3.2 en una máquina virtual de Oracle VirtualBox, configurando tres adaptadores de red para crear las tres zonas de seguridad: Adaptador 1 en la red interna "Verde" (Zona GREEN – LAN), Adaptador 2 en la red interna "Naranja" (Zona ORANGE – DMZ) y Adaptador 3 en modo NAT (Zona RED – WAN). Posteriormente se completó el asistente de configuración asignando las direcciones IP 192.168.10.1/24 para la Zona GREEN y 192.168.20.1/24 para la Zona ORANGE. Para la Temática 3 se configuraron tres reglas de firewall en la sección Inter-Zone traffic: permitir HTTP (puerto 80) desde la Zona Orange hacia Orange, permitir FTP (puerto 21) desde la Zona Orange hacia Orange y denegar ICMP (ping) desde Any hacia Any con acción Reject. Todas las reglas fueron habilitadas y aplicadas correctamente. Finalmente se realizaron las pruebas de funcionalidad: se verificó el acceso exitoso al sitio WordPress alojado en el servidor de la Zona DMZ mediante HTTP, se estableció una conexión FTP exitosa mediante FileZilla y se confirmó el bloqueo total de ICMP al obtener 100% de pérdida de paquetes en el ping desde la Zona Verde hacia el servidor.

Configuración de redes en VirtualBox (Endian):

Se configuraron tres adaptadores de red en la máquina virtual Endian Firewall:

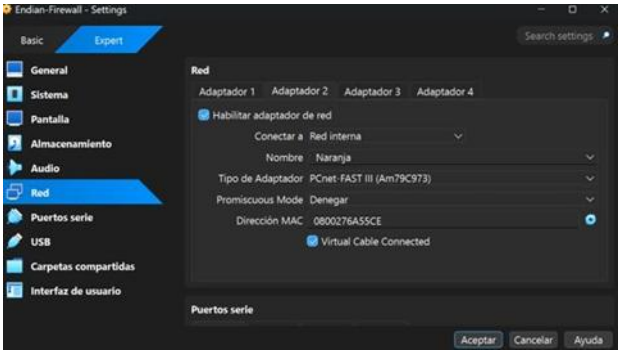
- Adaptador 1: Red interna "Verde" (Zona LAN)
- Adaptador 2: Red interna "Naranja" (Zona DMZ)
- Adaptador 3: Modo NAT (Zona WAN) Esto permite la correcta segmentación de las tres zonas requeridas.

Figura 14.
Adaptador 1 conectado a la red interna 'Verde' (Zona Lan)



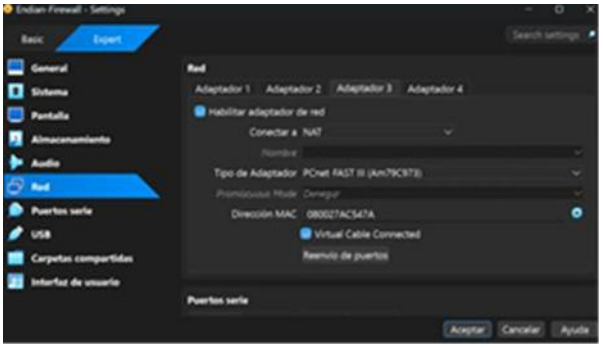
Fuente: Autoría propia

Figura 15.
Adaptador 2 conectado a la red interna ‘Naranja’ (Zona DMZ)



Fuente: Autoría propia

Figura 16.
Adaptador 3 en modo NAT (Zona WAN)

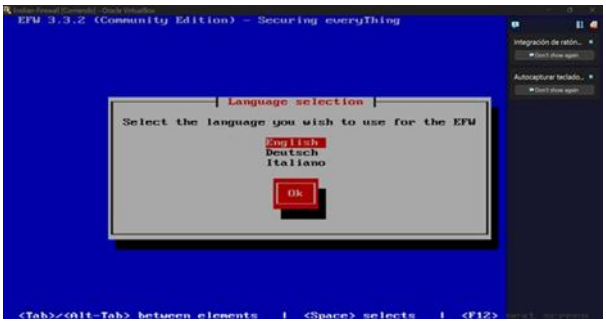


Fuente: Autoría propia

Instalación de Endian Firewall

Proceso de instalación de Endian Firewall Community Edition 3.3.2. Se seleccionó el idioma inglés y se completó el asistente de instalación inicial.

Figura 17.
Pantalla de selección de idioma y asistente de instalación



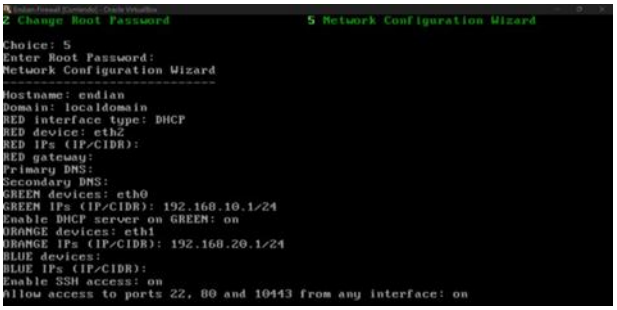
Fuente: Autoría propia

Configuración inicial de zonas

Configuración de las zonas de red en el asistente de Endian:

- Zona Green (LAN): 192.168.10.1/24
- Zona Orange (DMZ): 192.168.20.1/24 Resumen final del Network Configuration Wizard (Temática 1 completada).

Figura 18.
Configuración-Resumen del Network Wizard



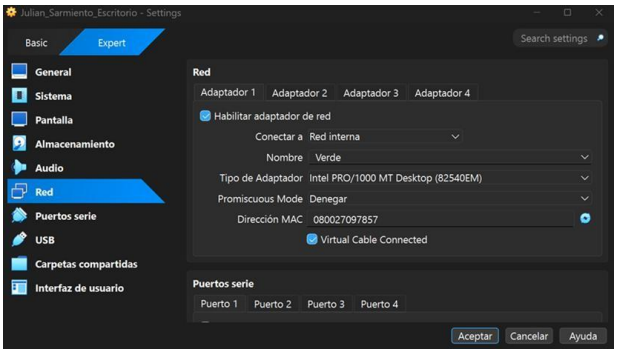
Fuente: Autoría propia

Configuración de la máquina Desktop y Server:

- Configuración del adaptador de red de la máquina Desktop en la red interna “Verde” (Zona LAN), lista para acceder al dashboard de Endian.

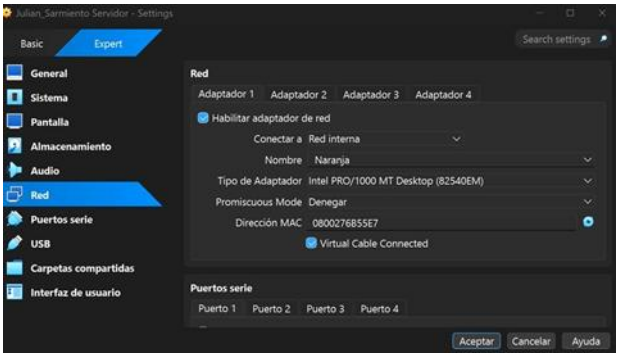
- Configuración del adaptador de red de la máquina Servidor en la red interna “Naranja” (Zona DMZ), donde se alojará el servicio web y FTP.

Figura 19.
Configuración del adaptador Verde del Desktop



Fuente: Autoría propia

Figura 20.
Configuración del adaptador Naranja del Server

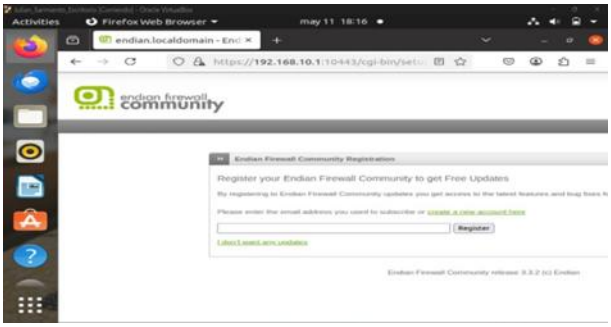


Fuente: Autoría propia

Acceso al Dashboard de Endian

Acceso al panel de administración de Endian Firewall desde la máquina Desktop mediante la URLhttps://192.168.10.1:10443

Figura 21.
Pantalla de login o dashboard principal



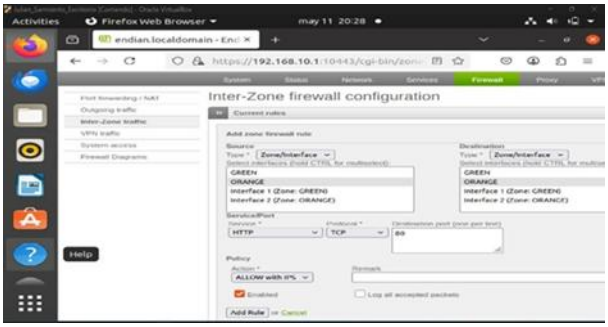
Fuente: Autoría propia

Creación de las reglas de Firewall:

Creación de las tres reglas de Inter-Zone traffic para la Temática 3:

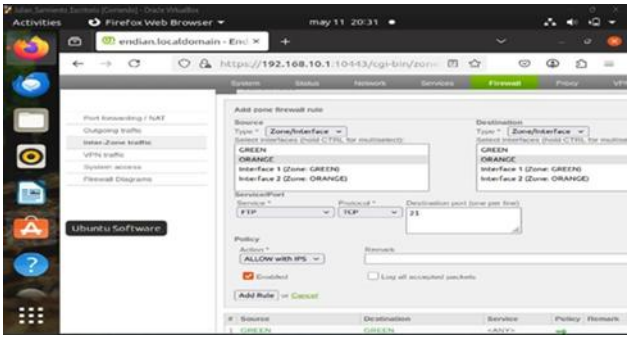
- Permitir HTTP (puerto 80) desde Zona Orange
- Permitir FTP (puerto 21) desde Zona Orange
- Denegar ICMP (ping) desde Any hacia Any (acción Reject)

Figura 22.
Permitir HTTP puerto 80 desde la Zona Orange hacia Orange



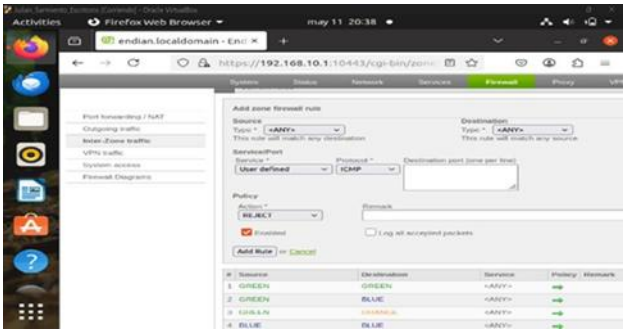
Fuente: Autoría propia

Figura 23.
Permitir FTP puerto 21 desde la Zona Orange hacia Orange



Fuente: Autoría propia

Figura 24.
Denegar ICMP (ping) desde Any hacia Any con acción Reject



Fuente: Autoría propia

Prueba HTTP

Prueba de acceso al sitio web desde la Zona Verde. Se verifica que el sitio WordPress "Portafolio Agronómico Julian Sarmiento" carga correctamente a través del firewall.

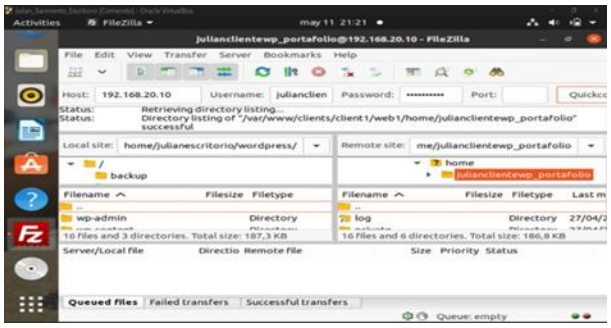
Figura 25.
Sitio WordPress cargando (Portafolio Agronomico)

Fuente: Autoría propia

Prueba FTP

Prueba de conexión FTP mediante FileZilla. Se establece conexión exitosa al servidor en la Zona DMZ utilizando las credenciales del usuario FTP configurado.

Figura 26.
FileZilla conectado exitosamente.

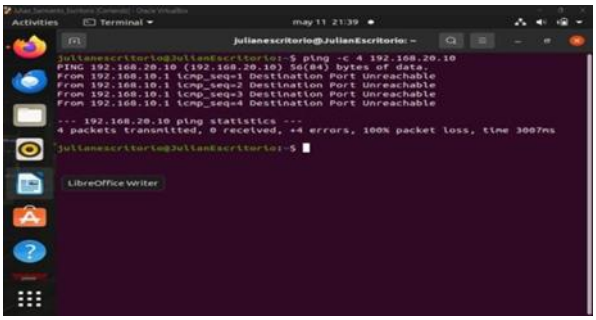


Fuente: Autoría propia

Prueba ICMP (Ping):

Prueba de bloqueo de ICMP. Desde la máquina Desktop se ejecuta ping hacia el servidor (192.168.20.10) y se obtiene 100% de pérdida de paquetes, confirmando que la regla de denegación está activa.

Figura 27.
Captura del ping fallando (100% packet loss)



Fuente: Autoría propia

Con la Temática 3 se logró configurar de forma precisa las reglas de firewall en la sección Inter-Zone traffic de Endian Firewall, permitiendo los servicios HTTP (puerto 80) y FTP (puerto 21) desde la Zona DMZ (Orange) hacia la red interna, al mismo tiempo que se denegaba completamente el protocolo ICMP. Los resultados obtenidos validaron el correcto control del tráfico inter-zona, demostrando que los servicios web y FTP son accesibles desde la LAN mientras se mantiene protegida la red frente a posibles ataques de reconocimiento. Esta práctica fortaleció las competencias en configuración avanzada de reglas de firewall, administración de tráfico segmentado y buenas prácticas de seguridad en entornos GNU/Linux.

4 CONCLUSIONES

La implementación de la Temática 1 permitió configurar correctamente Endian Firewall como elemento central de seguridad perimetral, creando y segmentando las tres zonas de red (GREEN, ORANGE y RED).

Con la Temática 3 se logró controlar de forma precisa el tráfico inter-zona, permitiendo los servicios HTTP y FTP desde la Zona DMZ hacia la red interna, mientras se bloqueaba completamente el protocolo ICMP.

Los resultados obtenidos demuestran que la arquitectura propuesta cumple con los objetivos de seguridad solicitados: los servicios web y FTP son accesibles desde la LAN, mientras se mantiene protegida la integridad de la red frente a posibles ataques de reconocimiento (ping).

Esta práctica fortaleció las competencias en configuración de firewalls UTM, administración de redes segmentadas y buenas prácticas de seguridad en entornos GNU/Linux.

5 REFERENCIAS

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

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

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

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

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

[6] Hernandez, P. F., & Sánchez, J. (2022). Monitoreo y administración de sistemas Linux

[7] Objeto virtual de información OVI]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/53211

[8] Hernández, P. F., & Sánchez, J. (2022). Servidores para administración remota y compartir recursos [Objeto virtual de información OVI]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/53212

[9] Canonical. (2023). Help Ubuntu. Ubuntu. https://help.ubuntu.com/

[10] LaCroix, J. (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

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

[12] Nemeth, E., Snyder, G., Hein, T. R., Whaley, B., & Mackin, D. (2018). UNIX and Linux system administration handbook (5.ª ed.). Addison-Wesley Professional.

[13] Tanenbaum, A. S., & Wetherall, D. J. (2012). Redes de computadoras (5.ª ed.). Pearson Educación.