Implementación de Seguridad Perimetral mediante Endian Firewall en Entornos GNU/Linux Virtualizados

Ana María Mesa González
e-mail: ammesames@unadvirtual.edu.co
Julián Esteban Herrera Rey
e-mail: jeherrerare@unadvirtual.edu.co
Oscar Esteban Cano Barbosa
e-mail: oecanob@unadvirtual.edu.co
Shirley Yurani Pereira Cubillos
e-mail: sypereirac@unadvirtual.edu.co
Elian Antonio Moyano Oviedo
e-mail: eamoyanoo@unadvirtual.edu.co

RESUMEN: *La seguridad en el perímetro de una red es fundamental para proteger los sistemas y servicios de una infraestructura tecnológica. En este proyecto se busca asegurar los servidores ubicados tanto en la red interna (LAN) como en la red externa (WAN), mediante la implementación de una zona DMZ utilizando la herramienta Endian UTM. A través del uso de un firewall y la definición de políticas de acceso, se logra controlar y proteger la comunicación entre las diferentes zonas de la red. Para ello, se realizaron configuraciones como la traducción de direcciones (NAT), la activación de servicios en la DMZ y la implementación de un proxy HTTP con autenticación, permitiendo así un filtrado más seguro del tráfico hacia Internet.*

PALABRAS CLAVE: Seguridad perimetral, DMZ, Endian, Firewall, GNU/Linux.

ABSTRACT: ***Network*** *perimeter security plays a key role in safeguarding IT infrastructures. This project focuses on protecting servers located in both internal (LAN) and external (WAN) networks by implementing a DMZ using Endian UTM. By configuring an Endian firewall and applying access control policies, secure communication between network segments is achieved. The process includes setting up NAT rules, enabling services within the DMZ, and configuring an authenticated HTTP proxy to properly filter web traffic.*

KEY WORDS: Perimeter Security, DMZ, Endian, Firewall, GNU/Linux.

1. INTRODUCCIÓN

En la actualidad, la protección de la información y de los sistemas informáticos se ha convertido en una necesidad fundamental para cualquier organización. Las redes no solo permiten la comunicación y el acceso a servicios, sino que también representan un punto vulnerable frente a posibles amenazas externas. Por esta razón, es importante implementar mecanismos que permitan controlar y asegurar el tráfico que entra y sale de la red.

En este trabajo se aborda el concepto de seguridad perimetral mediante la implementación de un firewall basado en GNU/Linux, utilizando la distribución Endian Firewall Community. A través de este entorno, se configuraron diferentes zonas de red como la LAN, la WAN y la DMZ, con el fin de segmentar el tráfico y proteger los recursos internos. Además, se aplicaron reglas de traducción de direcciones de red (NAT), permitiendo que los equipos de la red interna y de la zona DMZ puedan comunicarse de manera segura con el exterior.

2. TEMÁTICAS

2.1 TEMÁTICA 1: Configurar la regla de NAT (Network Address Translation / Traducción de Direcciones de Red). Configurar la regla de NAT. Verificar en el reenvió de puertos / NAT, la creación de las reglas.

2.1.1 CONFIGURACIÓN DE ENDIAN FIREWALL - CONSOLA

Se procedió con la descarga, instalación y configuración de GNU/Linux Endian Firewall Community 3.3.25 en una máquina. La configuración de las zonas de red se realizó mediante el Network Configuration Wizard desde la consola de Endian.

Tabla 1.
Configuración de zonas de red en Endian Firewall

Zona	Interfaz	Segmento de Red	IP Endian (Gateway)
Verde (LAN)	eth0	192.168.10.0/24	192.168.10.1
Naranja (DMZ)	eth1	192.168.20.0/24	192.168.20.1
Roja (WAN)	eth2	DHCP (Internet)	Asignada por router

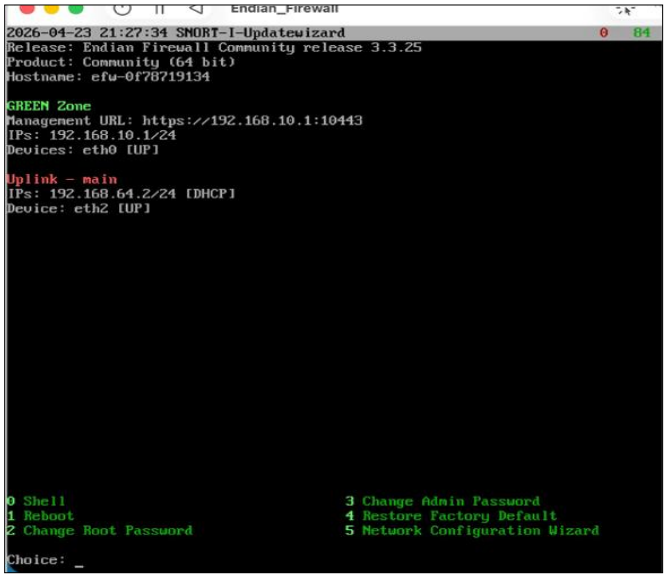
Fuente: Autoría propia.

2.1.2 PANTALLA PRINCIPAL DE ENDIAN CON ZONAS GREEN Y RED ACTIVAS

La siguiente captura evidencia la pantalla principal de Endian Firewall Community 3.3.25 luego de completar la configuración mediante el Network Configuración Wizard. Se observa la Zona Verde (GREEN) con la IP 192.168.10.1/24 asignada a eth0, y el Uplink RED activo con IP

DHCP en eth2.

Figura 1.
Pantalla principal de Endian Firewall mostrando GREEN Zone: 192.168.10.1/24 y Uplink RED activo con IP DHCP.

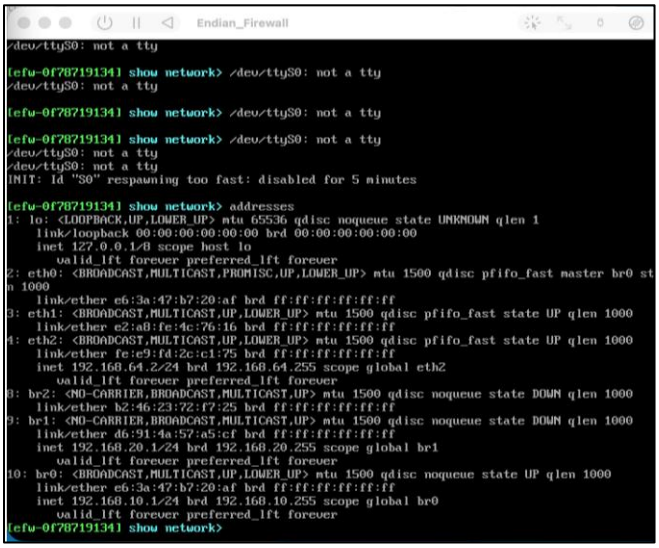


Fuente: Autoría propia.

2.1.3 VERIFICACIÓN DE DIRECCIONES - COMANDO ADDRESSES

La siguiente captura evidencia la ejecución del comando addresses dentro del subcomando show network, mostrando todas las interfaces configuradas: br0 (GREEN 192.168.10.1/24), br1 (ORANGE 192.168.20.1/24) y eth2 (RED 192.168.64.2/24).

Figura 2.
Comando addresses mostrando las tres zonas de red configuradas en Endian Firewall.

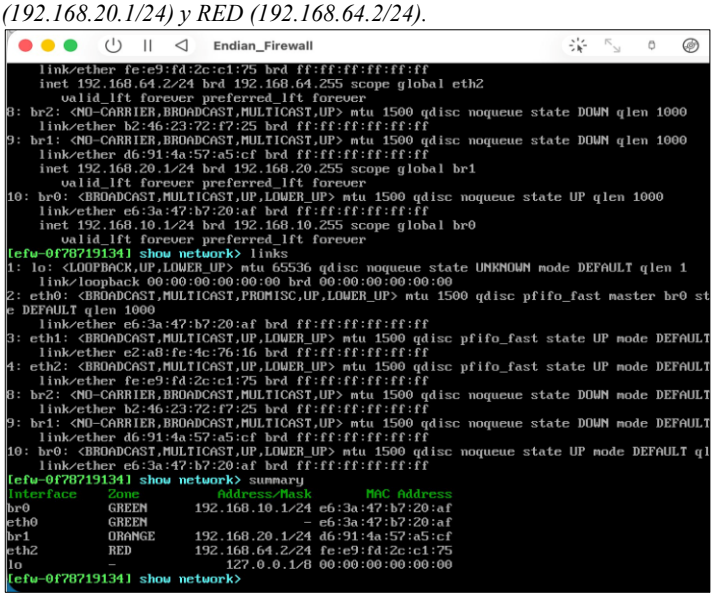


Fuente: Autoría propia.

2.1.4 RESUMEN DE RED - COMANDO SUMMARY

La siguiente captura evidencia el comando summary dentro de show network, presentando de forma organizada todas las zonas con sus interfaces y direcciones IP, confirmando la correcta configuración de la infraestructura de seguridad perimetral.

Figura 3.
Comando summary mostrando: GREEN (192.168.10.1/24), ORANGE (192.168.20.1/24) y RED (192.168.64.2/24).



Fuente: Autoría propia.

2.1.5 ACCESO AL PANEL WEB DE ADMINISTRACIÓN DE ENDIAN

Se configuró exitosamente una estación de trabajo Debian 13 en la zona LAN con la dirección IP 192.168.10.20/24, logrando acceso al panel de administración web de Endian Firewall desde el navegador Firefox mediante la URL https://192.168.10.1:10443. Esto demuestra la correcta comunicación entre la zona LAN y el firewall Endian.

2.1.6 DASHBOARD PRINCIPAL DEL PANEL WEB

La siguiente captura evidencia el acceso exitoso al panel de administración web de Endian Firewall Community 3.3.25 desde la estación de trabajo Debian 13 en la zona LAN. Se observa el Dashboard con información del sistema, las interfaces de red (eth2, br0, eth0) todas en estado Up, y las gráficas de tráfico entrante y saliente.

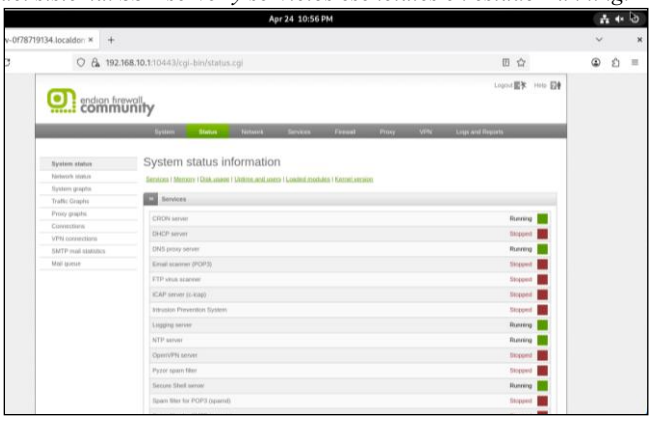
Figura 4.
Dashboard del panel web de Endian Firewall accedido desde Debian 13 en la zona LAN (192.168.10.20) vía https://192.168.10.1:10443. versión 3.3.25, Uptime 1h 22m.

Fuente: Autoría propia.

2.1.7 ESTADO DEL SISTEMA - STATUS

La siguiente captura evidencia la sección de estado del sistema en el panel web, mostrando el estado de todos los servicios de Endian. Se observa que el CRON server, DNS proxy server, Logging server, NTP server y Secure Shell server están en estado Running (activos), mientras que servicios no configurados como DHCP server, OpenVPN y otros permanecen Stopped.

Figura 5.
Sección Status del panel web mostrando el estado de los servicios del sistema. SSH server y servicios esenciales en estado Running.

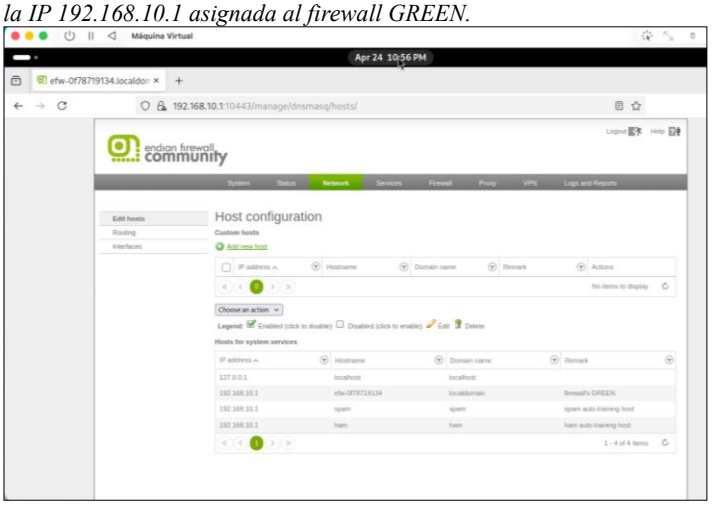


Fuente: Autoría propia.

2.1.8 CONFIGURACIÓN DE RED - NETWORK

La siguiente captura evidencia la sección de configuración de red del panel web, mostrando los hosts del sistema configurados. Se observan las entradas para localhost (127.0.0.1), el firewall GREEN (192.168.10.1 con hostname efw-0f78719134.localdomain), y los hosts de servicios spam y ham.

Figura 6.
sección Network del panel web mostrando la configuración de hosts con la IP 192.168.10.1 asignada al firewall GREEN.

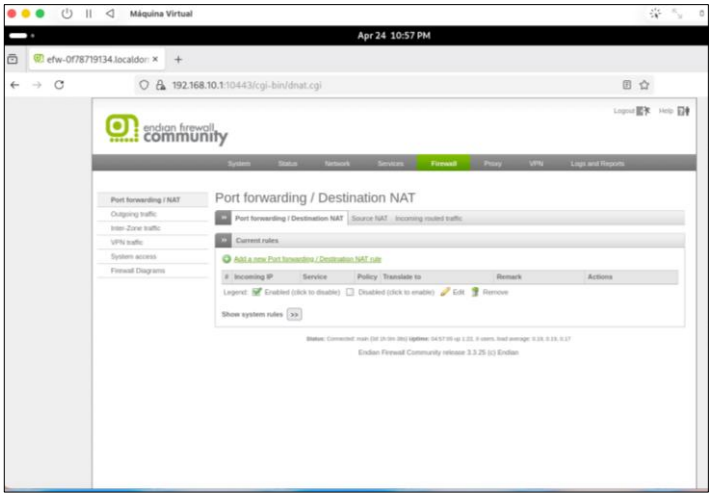


Fuente: Autoría propia.

2.1.9 REGLAS DE FIREWALL - PORT FORWARDING / NAT

La siguiente captura evidencia la sección Firewall del panel web, mostrando la configuración de Port Forwarding / Destination NAT. Se observa la interfaz con las opciones para crear reglas NAT, el menú de tráfico de salida, tráfico interzonal, acceso al sistema y diagramas del firewall. En este estado inicial no hay reglas NAT configuradas, listas para ser definidas según los requerimientos de las Temáticas 2 y 4.

Figura 7.
Seccion Firewall del panel web mostrando la configuracion de Port Forwarding/Destination NAT. Estado Connected: main, Uptime 4:57:05. Endian Firewall Community 3.3.25.



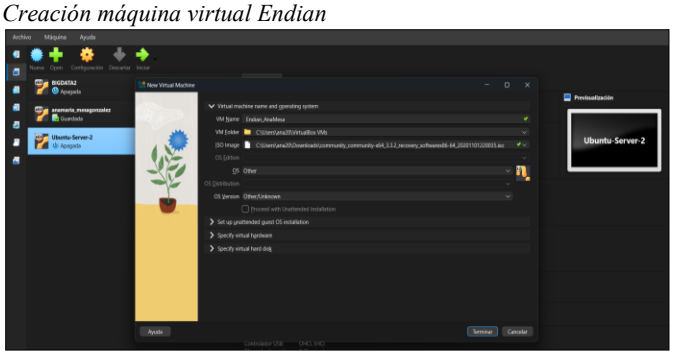
Fuente: Autoría propia.

3. TEMÁTICA 2: CONFIGURACIÓN NAT

3.1.1 INSTALACIÓN DE ENDIAN EN VIRTUALBOX

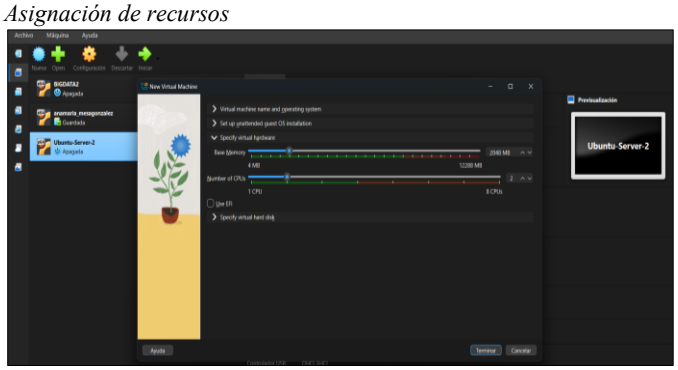
En este paso se realizó la creación de la máquina virtual en VirtualBox para instalar el firewall Endian. Se definieron los recursos básicos como memoria RAM, almacenamiento y tipo de sistema operativo. Posteriormente, se cargó la imagen ISO de Endian para iniciar el proceso de instalación dentro de la máquina virtual.

Figura 8.
Creación máquina virtual Endian



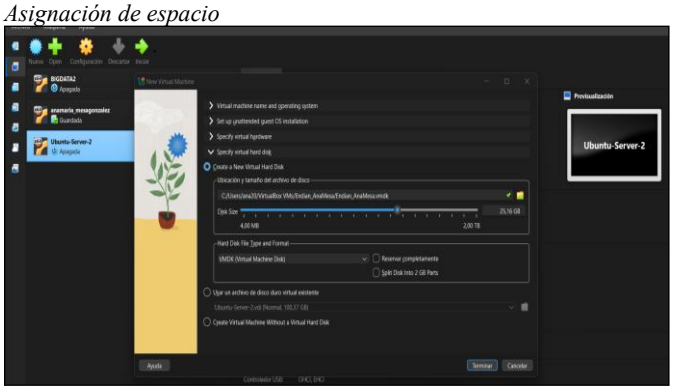
Fuente: Autoría propia.

Figura 9.
Asignación de recursos



Fuente: Autoría propia.

Figura 10.
Asignación de espacio

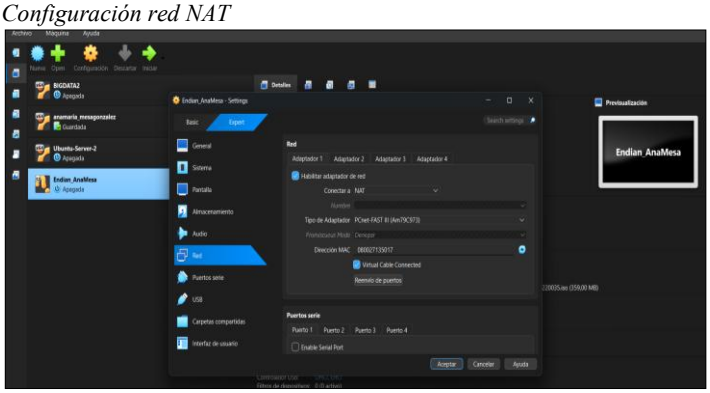


Fuente: Autoría propia.

3.1.2 CONFIGURACIÓN DE RED NAT – LAN – DMZ EN VIRTUALBOX

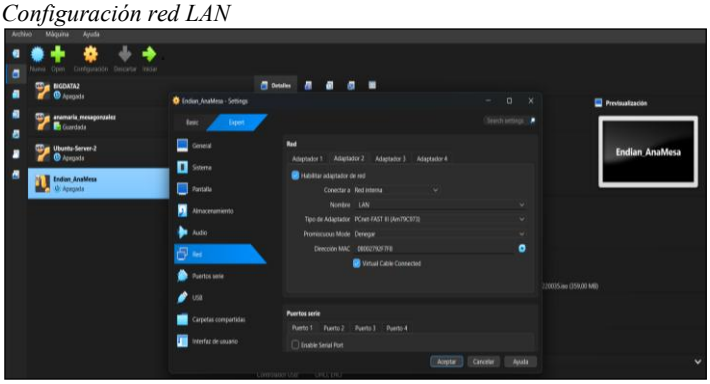
Aquí se configuraron los adaptadores de red de la máquina virtual para simular diferentes tipos de red. Se asignaron tres interfaces: una para la red externa (NAT o Internet), otra para la red interna (LAN) y una adicional para la zona DMZ. Esto permite separar el tráfico y simular un entorno real de red.

Figura 11.
Configuración red NAT



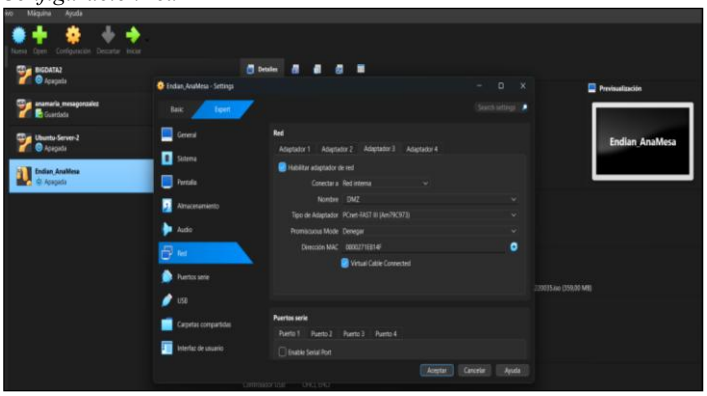
Fuente: Autoría propia.

Figura 12.
Configuración red LAN



Fuente: Autoría propia.

Figura 13.
Configuración red DMZ



Fuente: Autoría propia.

3.1.3 INSTALACIÓN Y CONFIGURACIÓN INICIAL DE ENDIAN

En este paso se llevó a cabo la instalación del sistema Endian. Se seleccionó el idioma, se aceptaron las configuraciones básicas y se completó el proceso de instalación. También se configuraron parámetros iniciales como red, hostname y acceso administrativo.

Figura 14.
Selección de idioma para Endian

Fuente: Autoría propia.

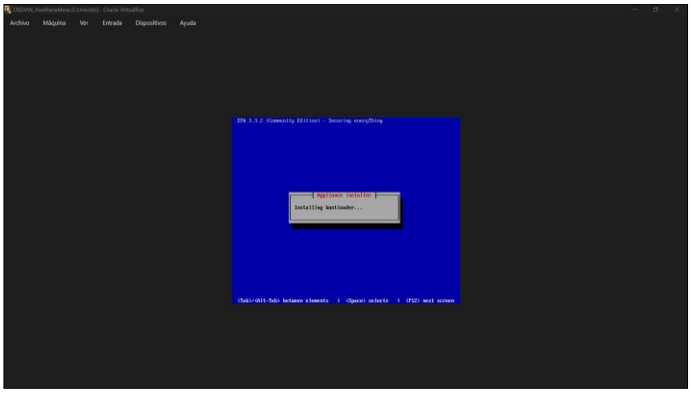
Figura 15.
Seleccionamos "yes" para continuar la instalación

Fuente: Autoría propia.

Figura 16.
Configuramos el segmento de red

Fuente: Autoría propia.

Figura 17.
Conti*núa la instalación*



Fuente: Autoría propia.

Figura 18.
Seleccionamos "ok" para continuar la instalación

Fuente: Autoría propia.

lustración 19.
Seleccionamos "ok" para finalizar la instalación

Fuente: Autoría propia

3.1.4 INTERFAZ DE ENDIAN

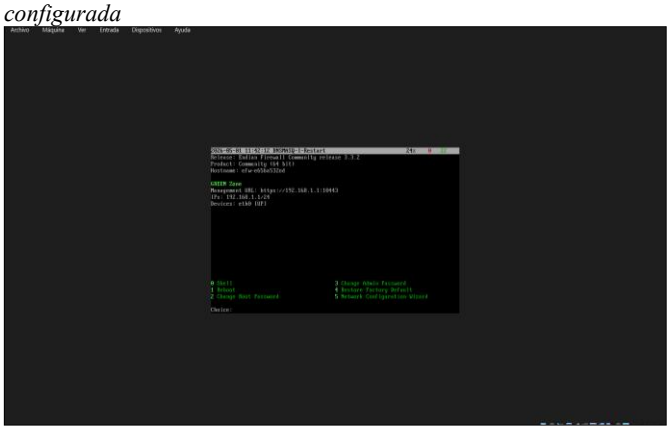
Una vez finalizada la instalación, se accedió a la interfaz principal de Endian desde la consola. Aquí se verificó que el sistema

estuviera correctamente instalado y que las interfaces de red estuvieran activas.

Figura 20.
Interfaz principal de Endian

Fuente: Autoría propia.

Figura 21.
Interfaz principal de Endian, se identifica la red previamente configurada



Fuente: Autoría propia

3.1.5 CONFIGURACIÓN DE RED LAN – WAN – DMZ DENTRO DE ENDIAN

En este paso se configuraron las zonas de red dentro de Endian:

- GREEN (LAN) como red interna
- RED como conexión a Internet
- ORANGE como zona DMZ

Se asignaron las interfaces correspondientes a cada zona, permitiendo una correcta segmentación de la red.

Figura 22.
Seleccionamos "ok" para finalizar la instalación

Fuente: Autoría propia

Figura 23.
Configuración de las zonas de red

Fuente: Autoría propia

3.1.6 ACCESO A LA INTERFAZ WEB DE ENDIAN

Se accedió a la interfaz web de administración ingresando la dirección IP del firewall en el navegador: https://192.168.10.1:10443

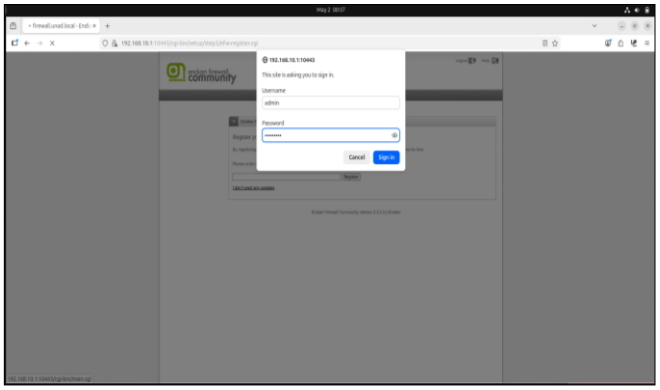
Desde allí se inició sesión con el usuario administrador para continuar con la configuración del sistema.

Figura 24.
Ingreso a la interfaz web por medio de la url https://192.168.10.1:10443

Fuente: Autoría propia

Figura 25.

Se ingresan credenciales configuradas durante la instalación de Endian



Fuente: Autoría propia

3.1.7 VERIFICACIÓN DEL DASHBOARD

En este paso se revisó el panel principal (dashboard) de Endian, donde se puede visualizar el estado de la red, tráfico, conexiones activas y funcionamiento general del firewall. Esto permitió confirmar que las interfaces estaban funcionando correctamente.

Figura 26.

Panel principal de Endian

Fuente: Autoría propia

Figura 27.

Identificación de los colores establecidos para la red

Fuente: Autoría propia.

Figura 28.

Configuración correcta para red LAN

Fuente: Autoría propia.

Figura 29.

Selección de puerto por defecto

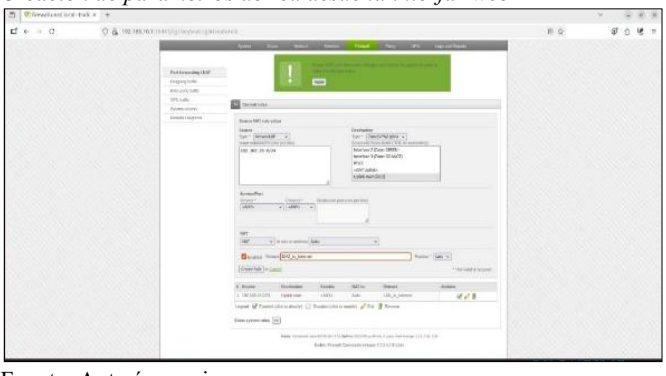
Fuente: Autoría propia.

3.1.8 CONFIGURACIÓN DE RED EN ENDIAN

Se ajustaron los parámetros de red desde la interfaz web, verificando direcciones IP, máscaras de red y asignación de interfaces. Se aseguró que la red LAN y la DMZ estuvieran correctamente configuradas para permitir la comunicación.

Figura 30.

Creación de parámetros de red desde la interfaz web



Fuente: Autoría propia.

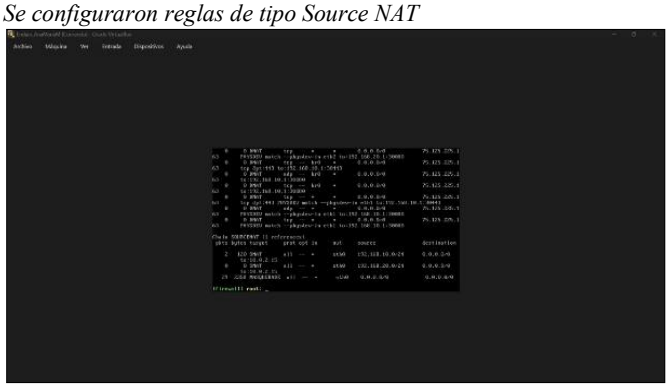
Figura 31.
Parámetros creados

Fuente: Autoría propia.

3.1.9 CONFIGURACIÓN DE REGLAS NAT

En este paso se crearon las reglas de NAT (traducción de direcciones de red), permitiendo que los equipos de la red interna (LAN) y la zona DMZ pudieran acceder a Internet. Se configuraron reglas de tipo Source NAT para traducir las direcciones privadas a la dirección pública del firewall.

Figura 32.
Se configuraron reglas de tipo Source NAT

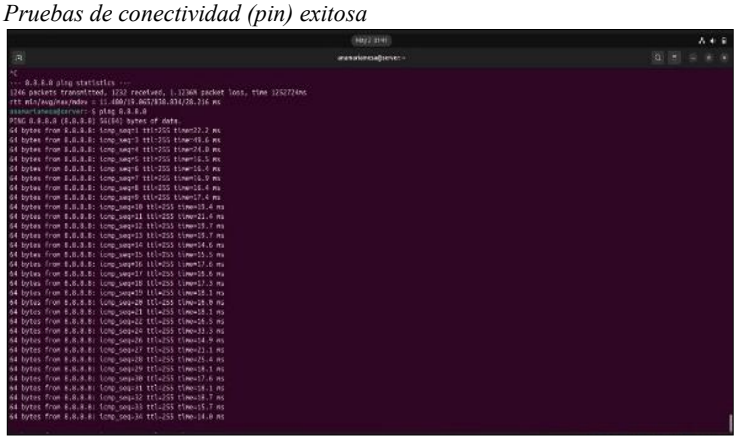


Fuente: Autoría propia.

3.1.10 VERIFICACIÓN DE CONECTIVIDAD

Finalmente, se realizaron pruebas de conectividad mediante comandos como ping, comprobando que los equipos de la red LAN y la DMZ podían comunicarse con Internet. Además, se validó la correcta aplicación de las reglas NAT revisando el tráfico en el sistema.

Figura 33.
Pruebas de conectividad (pin) exitosa



Fuente: Autoría propia.

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

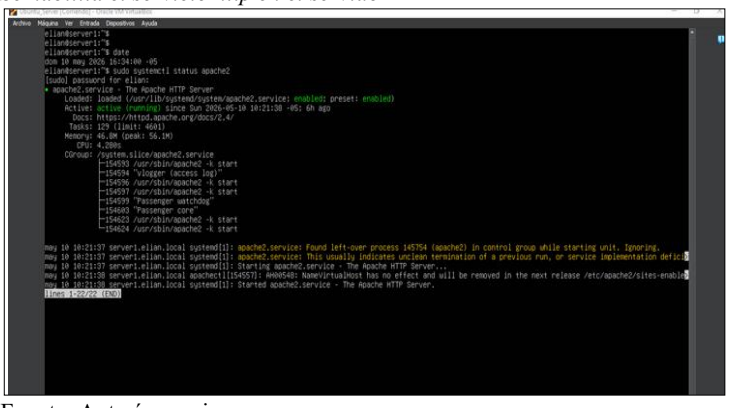
4.1.1 FUNDAMENTO TEÓRICO

Endian EFW administra el tráfico entre las diferentes zonas de red mediante reglas de firewall. En esta práctica se gestionaron servicios HTTP y FTP desde una zona DMZ, además del bloqueo de mensajes ICMP tipo Echo Request y Traceroute para evitar el reconocimiento de la topología de red.

4.1.2 HABILITACIÓN DEL SERVICIO HTTP

Se instaló el servidor Apache2 en Ubuntu Server con la dirección 192.168.20.11 utilizando el comando sudo apt install apache2 -y. Posteriormente se habilitó el servicio y se verificó que escuchara correctamente sobre el puerto TCP 80.

Figura 34.
Se habilita el servicio http en el servidor



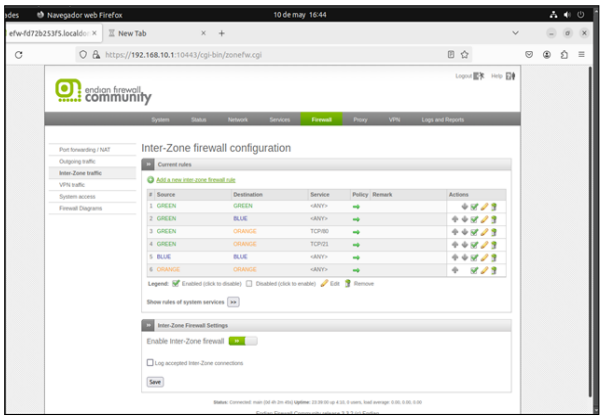
Fuente: Autoría propia.

4.1.3 CONFIGURACIÓN DE LA REGLA HTTP EN ENDIAN EFW

Se creó una regla de firewall en Endian EFW permitiendo tráfico TCP desde la zona ORANGE (DMZ) hacia GREEN (LAN) mediante el

puerto 80. La regla se configuró con acción ACCEPT.

Figura 35.
Se observa la configuración personalizada

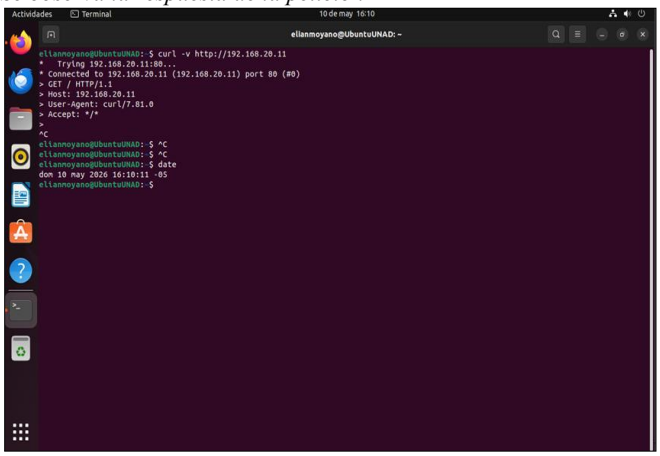


Fuente: Autoría propia.

4.1.4 VERIFICACIÓN DEL SERVICIO HTTP

La validación del servicio se realizó desde Ubuntu Desktop mediante el comando curl -I http://192.168.20.11, confirmando la respuesta correcta del servidor web.

Figura 36.
Se observa la respuesta de la petición HTTP

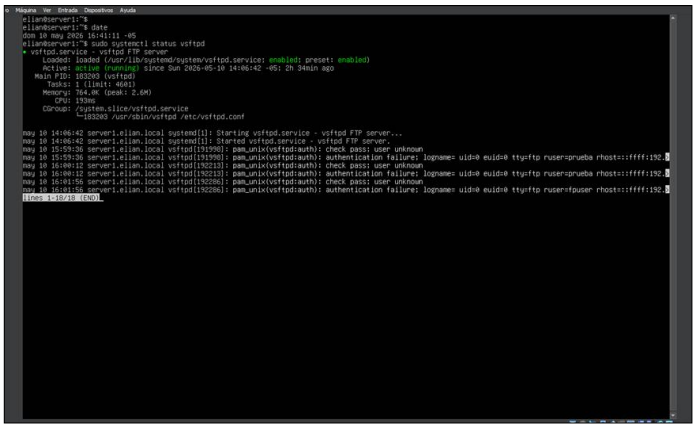


Fuente: Autoría propia.

4.1.5 HABILITACIÓN DEL SERVICIO FTP

Se instaló y configuró el servidor vsftpd utilizando el comando sudo apt install vsftpd -y. Se habilitó el acceso local y el modo pasivo para permitir transferencias seguras de archivos.

Figura 37.
Se observa el servicio corriendo correctamente

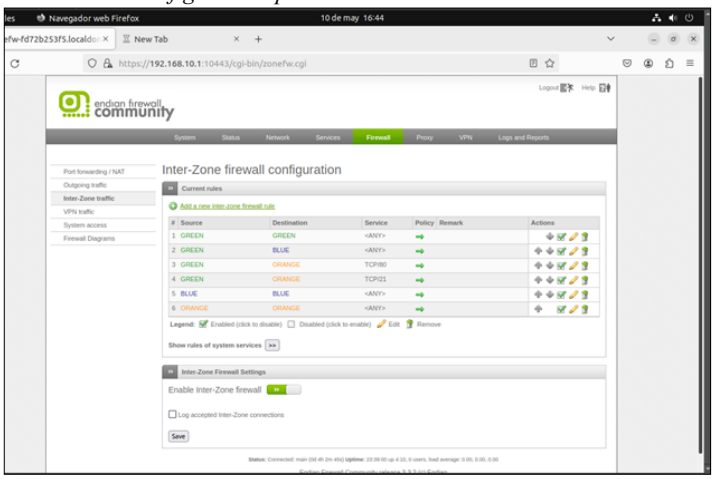


Fuente: Autoría propia.

4.1.6 CONFIGURACIÓN DE LA REGLA FTP

En Endian EFW se creó una regla TCP permitiendo el puerto 21 desde la zona DMZ hacia la LAN. La conectividad fue validada mediante telnet 192.168.20.11 21.

Figura 38.
Se observa la configuración personalizada



Fuente: Autoría propia.

4.1.7 BLOQUEO DEL PROTOCOLO ICMP

Se configuraron reglas de firewall para bloquear mensajes ICMP tipo 8 (Echo Request) y tipo 30 (Traceroute). Las reglas fueron aplicadas en INPUT y FORWARD para todas las zonas de red.

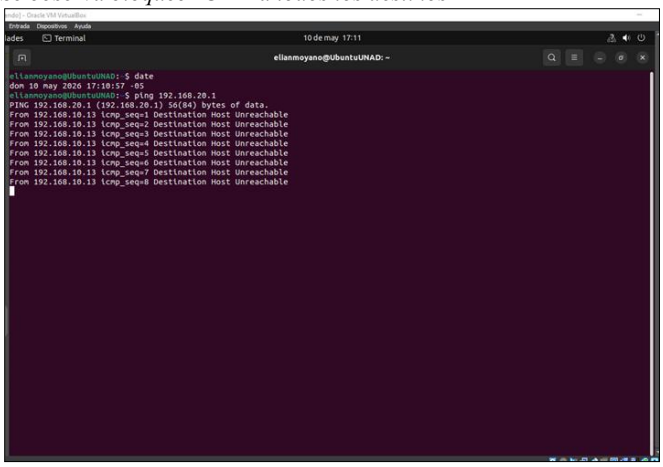
Figura 39.
Se observa el bloqueo de ICMP en el Firewall

Fuente: Autoría propia.

4.1.8 RESULTADOS DEL BLOQUEO

Las pruebas realizadas demostraron el correcto funcionamiento de los servicios HTTP y FTP en la DMZ, así como la efectividad del bloqueo ICMP al impedir respuestas a solicitudes ping y traceroute.

Figura 40.
Se observa bloqueo ICMP a todos los destinos



Fuente: Autoría propia.

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

5.1.1 DESCRIPCIÓN GENERAL

En esta Temática se implementaron reglas de acceso inter-zona en Endian Firewall Community, permitiendo controlar la comunicación entre las zonas LAN (GREEN), DMZ (ORANGE) y WAN (RED). El objetivo principal fue validar el funcionamiento de políticas de seguridad perimetral mediante reglas HTTP y FTP, aplicando segmentación de red y filtrado de tráfico.

Para el desarrollo de la práctica se utilizó Oracle VirtualBox como entorno de virtualización, configurando tres máquinas virtuales:

Tabla 2.
Máquinas virtuales y direccionamiento IP utilizado en la práctica

Máquina Virtual	Zona	Dirección IP
Endian Firewall	Firewall	192.168.10.1 / 192.168.20.1
Ubuntu Desktop	LAN (GREEN)	192.168.10.10
Ubuntu Server	DMZ (ORANGE)	192.168.20.10

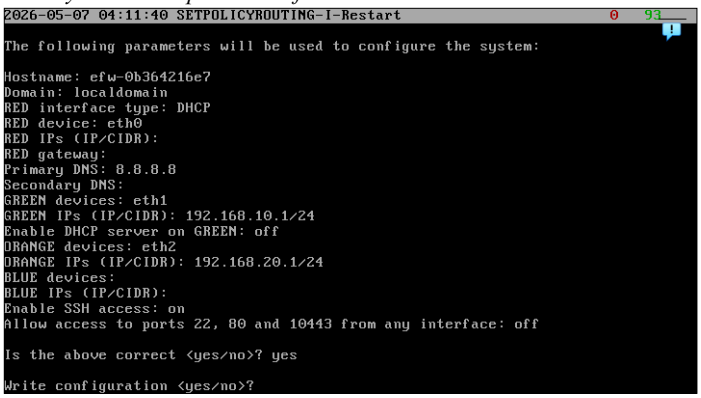
Fuente: Autoría propia.

5.1.2 CONFIGURACIÓN DE INTERFACES EN ENDIAN

Mediante el asistente de configuración de red de Endian se asignaron las siguientes interfaces:

- eth0 → RED (WAN) – DHCP
- eth1 → GREEN (LAN) – 192.168.10.1/24
- eth2 → ORANGE (DMZ) – 192.168.20.1/24

Figura 41.
Esta configuración permitió segmentar correctamente la infraestructura de red y establecer políticas diferenciadas de acceso entre zonas.



Fuente: Autoría propia.

5.1.3 CONFIGURACIÓN DE SERVICIOS EN LA DMZ

En el servidor Ubuntu ubicado en la zona DMZ se instalaron y configuraron los servicios Apache2 y vsftpd, habilitando comunicación mediante los protocolos HTTP y FTP.

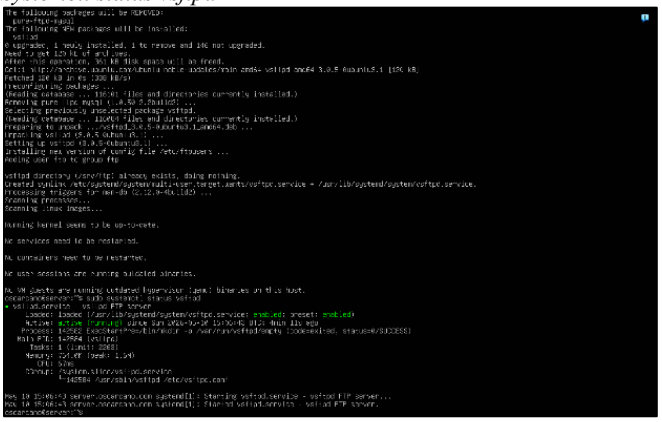
Comandos utilizados:
sudo apt update
sudo apt install apache2 -y
sudo apt install vsftpd -y

Posteriormente se verificó el estado de los servicios:

Figura 42.
Sudo systemctl status apache2

Fuente: Autoría propia.

Figura 43.
Systemctl status vsftpd

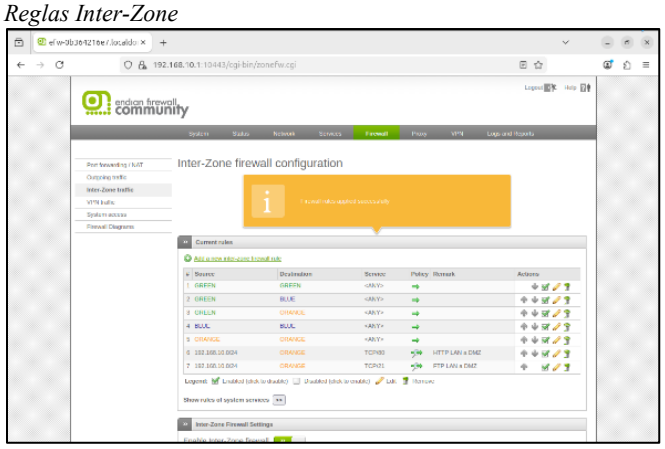


Fuente: Autoría propia

5.1.4 IMPLEMENTACIÓN DE REGLAS INTER-ZONE TRAFFIC

Desde la sección Firewall → Inter-Zone Traffic se crearon las reglas necesarias para permitir tráfico desde la zona GREEN hacia la zona ORANGE.

Figura 44.
Reglas Inter-Zone



Fuente: Autoría propia.

Tabla 3.
Reglas de firewall entre zonas GREEN y ORANGE

Regla	Origen	Destino	Protocolo	Puerto	Acción
6	GREEN	ORANGE	TCP	80	ALLOW
7	GREEN	ORANGE	TCP	21	ALLOW

Fuente: Autoría propia.

Estas reglas permitieron:

- Acceso HTTP desde la LAN hacia el servidor web ubicado en la DMZ.
- Acceso FTP desde la LAN hacia el servidor FTP ubicado en la DMZ.

5.1.5 CONFIGURACIÓN DE PORT FORWARDING / NAT

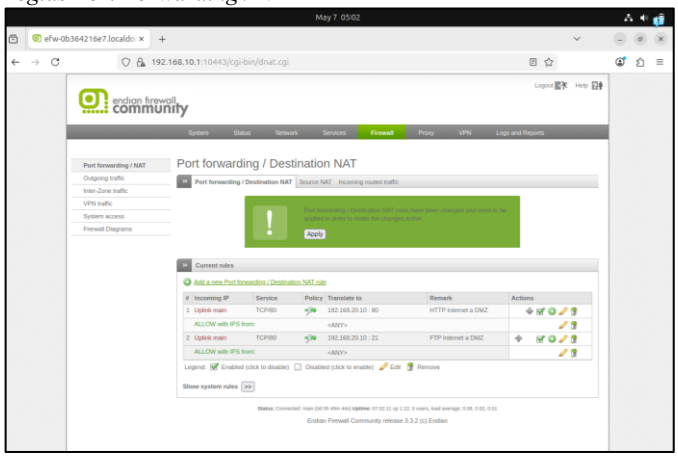
Para permitir el acceso desde la WAN hacia los servicios publicados en la DMZ, se configuraron reglas de Destination NAT.

Tabla 4.
Reglas de Port Forwarding / NAT configuradas en Endian Firewall

Regla	Uplink	Puerto	Destino NAT	Acción
1	main	TCP/80	192.168.20.10:80	ALLOW
2	main	TCP/21	192.168.20.10:21	ALLOW

Fuente: Autoría propia.

Figura 45.
Reglas Port Forwarding / NAT



Fuente: Autoría propia.

La configuración se realizó desde: Firewall → Port Forwarding / NAT

5.1.6 VERIFICACIÓN DE CONECTIVIDAD

Se realizaron pruebas de conectividad para validar el correcto funcionamiento de las reglas implementadas.

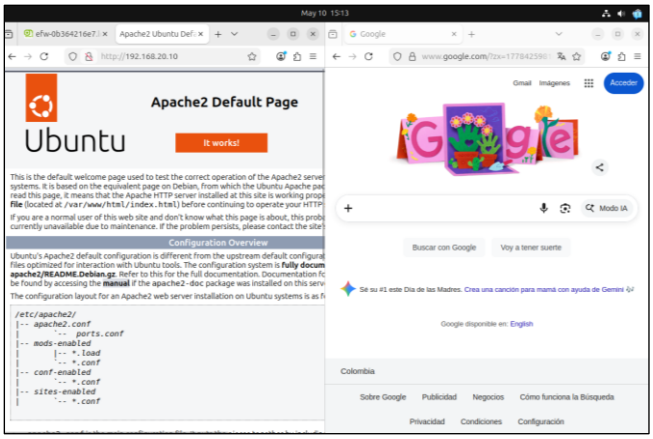
Tabla 5.
Verificación de conectividad entre zonas de red

Prueba	Origen	Destino	Herramienta	Resultado
1	LAN	DMZ	Firefox HTTP	Conexión exitosa
2	LAN	WAN	Navegador Web	Acceso a Internet exitoso

3	DMZ	WAN	curl -I	Respuesta HTTP válida
4	LAN	DMZ FTP	Cliente FTP	Login exitoso
5	WAN	DMZ	NAT	Regla activa

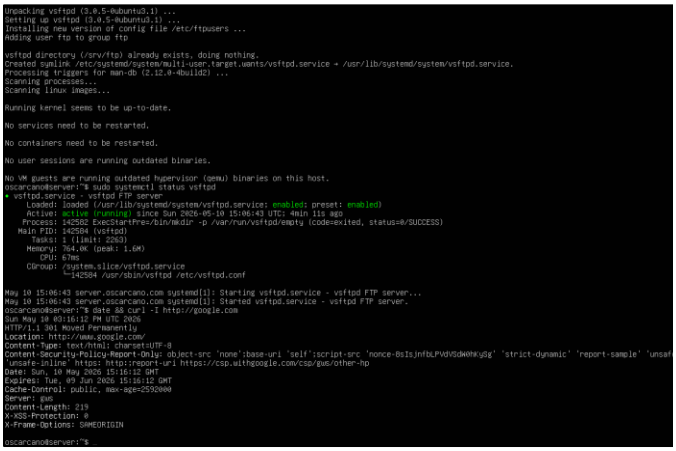
Fuente: Autoría propia.

Figura 46.
Prueba 1 — HTTP desde LAN → DMZ y Prueba 2 — HTTP desde LAN → WAN



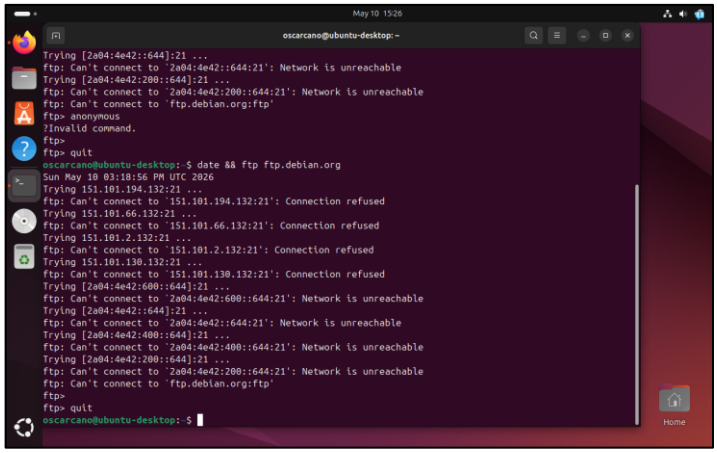
Fuente: Autoría propia.

Figura 47.
Prueba 3 — HTTP desde DMZ → WAN



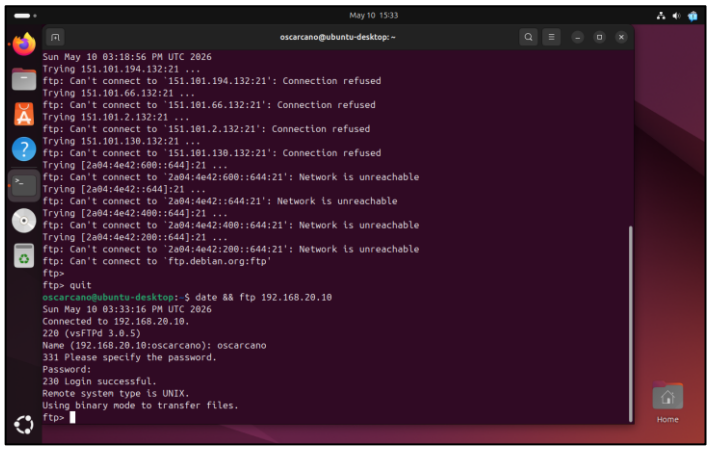
Fuente: Autoría propia.

Figura 48.
Prueba 4 — FTP desde LAN → WA



Fuente: Autoría propia.

Figura 49.
Prueba 5 — FTP LAN → DMZ



Fuente: Autoría propia.

Las pruebas realizadas confirmaron el correcto funcionamiento del firewall y las políticas de seguridad configuradas.

5.1.7 CONCLUSIÓN DE LA TEMÁTICA 4

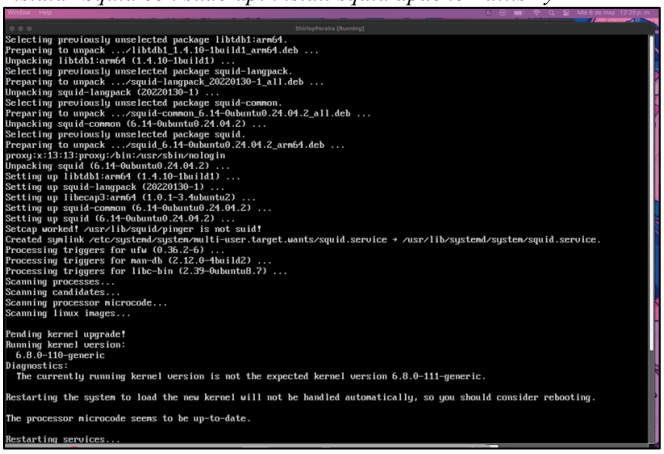
La implementación de reglas inter-zona en Endian Firewall permitió controlar de manera segura el tráfico entre las diferentes zonas de red, aplicando segmentación y filtrado de acceso mediante políticas específicas. Las pruebas realizadas demostraron que los servicios HTTP y FTP funcionaron correctamente entre la LAN, la DMZ y la WAN, validando la efectividad de la seguridad perimetral implementada sobre GNU/Linux.

6. TEMÁTICA 5: AUTENTICACIÓN Y CONFIGURACIÓN DE UN PROXY

En esta Temática se implementó un servidor proxy con autenticación utilizando Squid en GNU/Linux, con el objetivo de controlar y filtrar el acceso a Internet dentro de la red. Además, se configuraron reglas de bloqueo para restringir determinados sitios web y se validó el funcionamiento del proxy mediante pruebas de autenticación y navegación desde los equipos cliente.

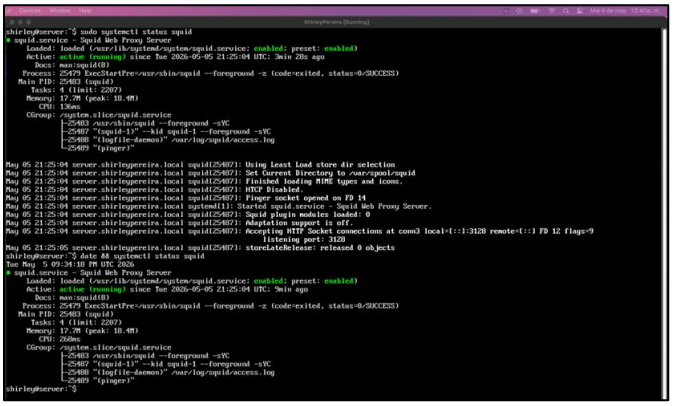
6.1.1 CONFIGURACIÓN EN UBUNTU SERVER (SQUID PROXY)

Figura 50.
Instalar Squid con sudo apt install squid apache2-utils –y



Fuente: Autoría propia.

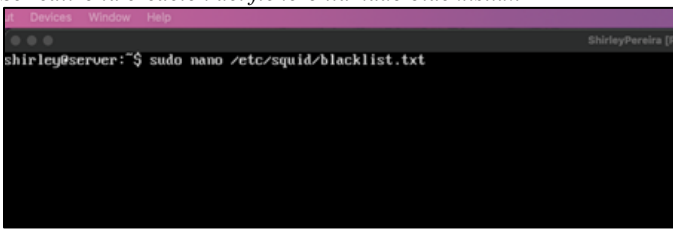
Figura 51.
Verificación del estado del servicio



Fuente: Autoría propia.

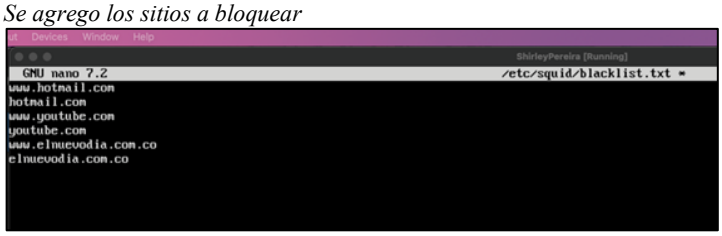
6.1.2 CREAR EL ARCHIVO DE LISTA NEGRA

Figura 52.
Se realizo la creación del fichero llamado blacklist.txt



Fuente: Autoría propia.

Figura 53.
Se agrego los sitios a bloquear



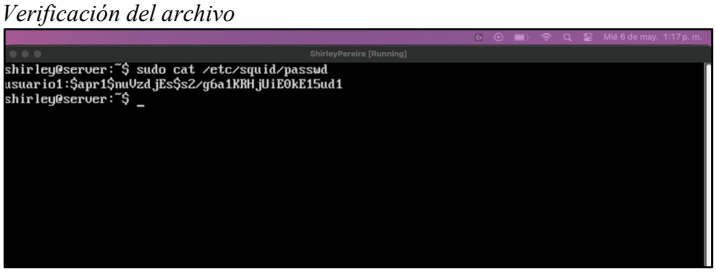
Fuente: Autoría propia.

6.1.3 CREAR USUARIOS CON AUTENTICACIÓN

Figura 54.
Creación de usuario y contraseña

Fuente: Autoría propia.

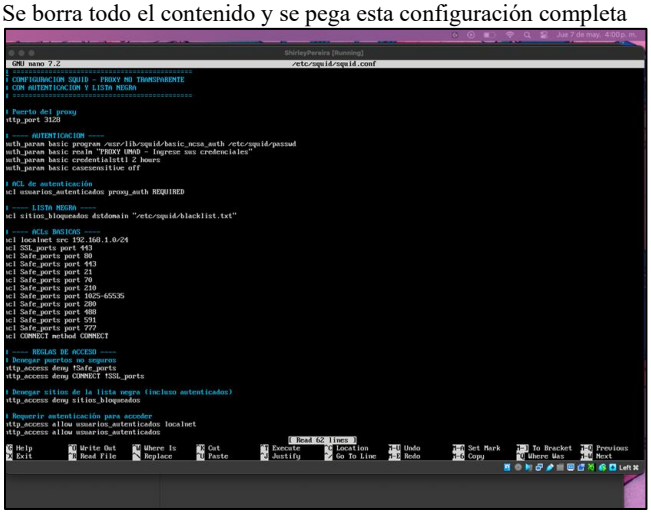
Figura 55.
Verificación del archivo



Fuente: Autoría propia.

6.1.4 CONFIGURAR SQUID.CONF

Figura 56.
Se borra todo el contenido y se pega esta configuración completa



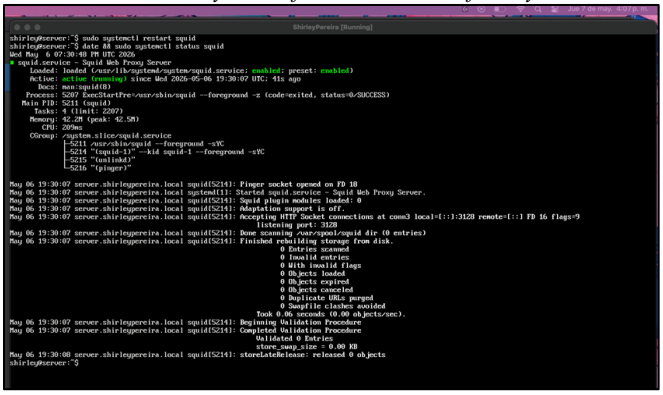
Fuente: Autoría propia.

6.1.5 VALIDAR Y REINICIAR SQUID

Figura 57.
Verificar que la configuración no tenga errores

Fuente: Autoría propia.

Figura 58.
Se reinicio el servicio y se verifico el estado con fecha y hora



Fuente: Autoría propia.

CONFIGURAR FIREWALL EN UBUNTU SERVER

Figura 59.
Se realiza la configuración del firewall en Ubuntu server

Fuente: Autoría propia.

6.1.6 CONFIGURACIÓN EN UBUNTU DESKTOP (CLIENTE)

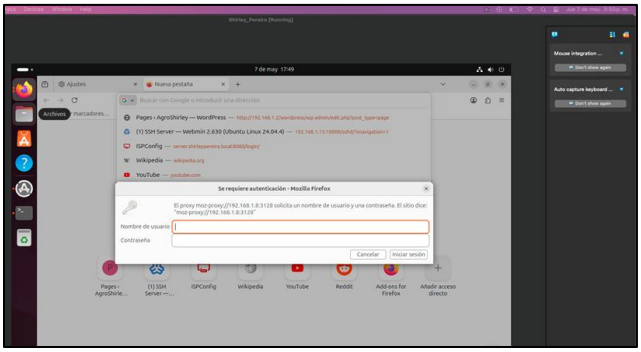
Figura 60.
Configuración del proxy en el navegador Firefox

Fuente: Autoría propia.

6.1.7 PRUEBAS DESDE EL NAVEGADOR

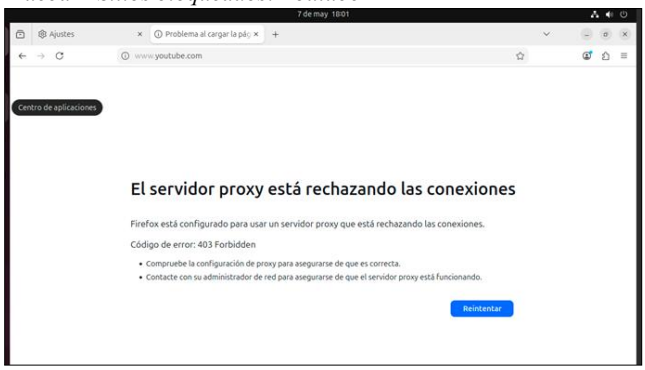
En esta etapa se realizaron pruebas desde el navegador para verificar la autenticación, el acceso a sitios permitidos y el bloqueo de páginas restringidas mediante el proxy configurado.

Figura 61.
Prueba 1- Autenticación



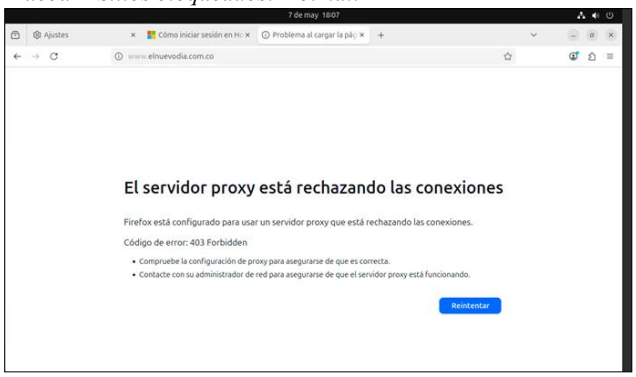
Fuente: Autoría propia.

Figura 62.
Prueba 2-Sitios bloqueados: Youtube



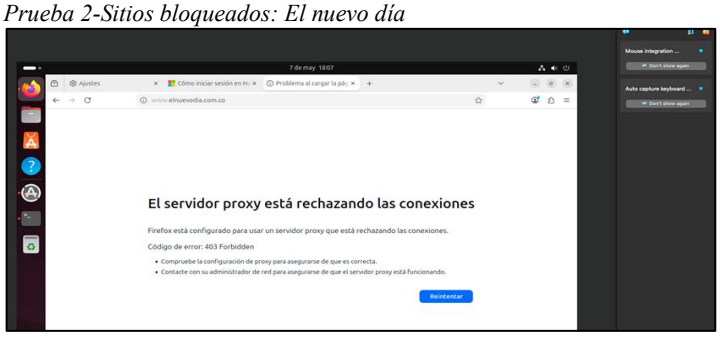
Fuente: Autoría propia.

Figura 63.
Prueba 2-Sitios bloqueados: Hotmail



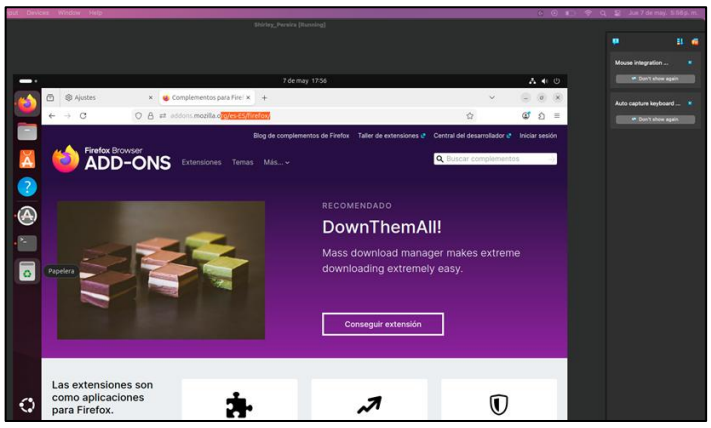
Fuente: Autoría propia.

Figura 64.
Prueba 2-Sitios bloqueados: El nuevo día



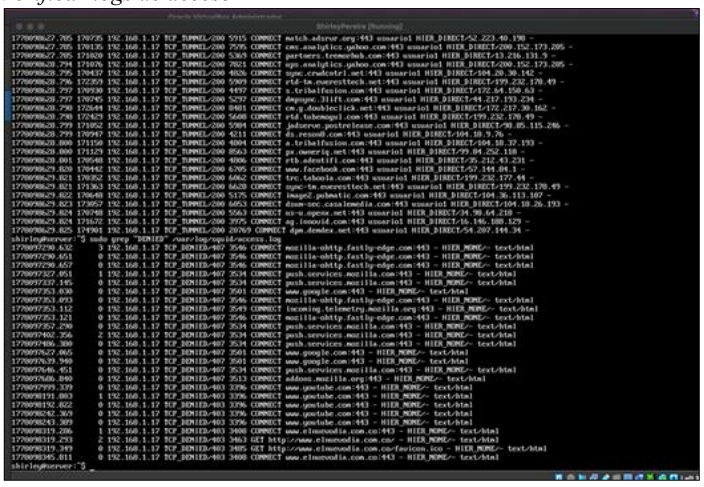
Fuente: Autoría propia.

Figura 64.
Prueba 3 -Sitio permitido



Fuente: Autoría propia.

Figura 65.
Verificar logs de acceso



Fuente: Autoría propia.

7. CONCLUSIONES

La implementación de seguridad perimetral mediante Endian Firewall permitió fortalecer la protección de la infraestructura de red, garantizando un control más eficiente del tráfico entre las zonas LAN, WAN y DMZ. A través de la configuración de reglas NAT, Port Forwarding y políticas de firewall, fue posible gestionar de manera segura la comunicación entre los diferentes segmentos de red, reduciendo riesgos de acceso no autorizado.

Asimismo, la integración de servicios como Apache2, vsftpd y Squid Proxy permitió validar el funcionamiento de mecanismos de acceso, autenticación y filtrado dentro de un entorno basado en GNU/Linux. Las pruebas realizadas mediante herramientas como ping, curl, navegador web y cliente FTP evidenciaron la estabilidad y efectividad de las configuraciones implementadas, confirmando el correcto funcionamiento de los servicios HTTP, FTP y proxy.

Por otra parte, el bloqueo de tráfico ICMP demostró la importancia de aplicar políticas de seguridad que limiten el reconocimiento de red y contribuyan a la protección frente a posibles amenazas externas. Esto permitió comprender cómo las reglas de firewall pueden utilizarse para fortalecer la seguridad perimetral y mejorar el control sobre los servicios expuestos.

Finalmente, el desarrollo de este proyecto permitió integrar conocimientos de virtualización, administración de servidores Linux, redes y ciberseguridad, logrando una solución funcional y adaptable a entornos académicos y empresariales. El uso de herramientas basadas en GNU/Linux demostró ser una alternativa eficiente, flexible y de bajo costo para la implementación de infraestructuras de seguridad perimetral.

8. REFERENCIAS

[1] Apache Software Foundation. (2024). Apache HTTP Server Project. https://httpd.apache.org

[2] Canonical Ltd. (2024). Ubuntu Server Guide. https://ubuntu.com/server/docs

[3] Endian. (2024). Endian Firewall Community. https://www.endian.com

[4] Maiwald, E. (2013). Fundamentals of network security. McGraw-Hill Education.

[5] Nazario, R. (2015). Network security monitoring. Cisco Press.

[6] Oracle. (2024). Oracle VM VirtualBox Documentation. https://www.virtualbox.org

[7] Squid Software Foundation. (2024). Squid Proxy Server. http://www.squid-cache.org

[8] Stallings, W. (2017). Network security essentials: Applications and standards (6th ed.). Pearson.

[9] Tanenbaum, A. S., & Wetherall, D. (2011). Computer networks (5th ed.). Pearson.

[10] The VSFTPD Project. (2024). Very Secure FTP Daemon. https://security.appspot.com/vsftpd.html