IMPLEMENTACIÓN DE SEGURIDAD PERIMETRAL CON ENDIAN FIREWALL: GESTIÓN DE ZONAS, NAT Y PROXY HTTP EN SOFTWARE LIBRE

Andrés Felipe Roldan Higuera
e-mail: afroldanh@unadvirtual.edu.co

Duván Eduardo Vergara Bolivar
e-mail devergarab@unadvirtual.edu.co

Lenin David Pineda Cueva
e-mail Ldpinedacu@unadvirtual.edu.co

Wilson Andrés Zambrano Porras
e-mail wazambranop@unadvirtual.edu.co

RESUMEN: *El presente artículo describe la configuración e implementación de seguridad perimetral mediante Endian Firewall en un entorno virtualizado con GNU/Linux sobre Oracle VirtualBox, abarcando desde la configuración de las tarjetas de red y la instalación del sistema hasta la validación de políticas de seguridad entre zonas, se aborda la implementación de reglas de Traducción de Direcciones de Red (NAT) para habilitar la comunicación entre la zona LAN (GREEN) y la WAN (RED), así como desde la zona DMZ (ORANGE) hacia Internet, posterior a esto se configuraron reglas de tráfico inter-zona para permitir los servicios HTTP (puerto 80) y FTP (puerto 21), y se aplicaron políticas de denegación del protocolo ICMP con el fin de restringir el uso del comando ping en la red. Adicionalmente, se implementó un Proxy HTTP no transparente con autenticación por usuario y grupo, estableciendo listas negras para bloquear el acceso a sitios web específicos desde la zona LAN, cada configuración fue verificada mediante pruebas prácticas desde navegadores web y terminales de consola, evidenciando la correcta segmentación de la red y la aplicación efectiva de políticas de seguridad perimetral, los resultados demuestran que Endian Firewall constituye una solución robusta y accesible para la gestión de tráfico y control de acceso en redes con múltiples zonas de seguridad.*

PALABRAS CLAVE: Firewall, GNU/Linux, Proxy, Segmentación.

ABSTRACT: *This article describes the configuration and implementation of perimeter security using Endian Firewall in a virtualized environment with GNU/Linux on Oracle VirtualBox, covering from the network card configuration and system installation to the validation of security policies between zones. The implementation of Network Address Translation (NAT) rules is addressed to enable communication between the LAN zone (GREEN) and the WAN (RED), as well as from the DMZ zone (ORANGE) toward the Internet. Subsequently, inter-zone traffic rules were configured to allow HTTP (port 80) and FTP (port 21) services, and ICMP protocol denial policies were applied in order to restrict the use of the ping command on the network. Additionally, a non-transparent HTTP Proxy was implemented with user and group authentication, establishing blacklists to block access to specific websites from the LAN zone. Each configuration was verified through practical tests from web browsers and console terminals, evidencing the correct network segmentation and the effective application of perimeter security policies. The results demonstrate that Endian Firewall constitutes a robust and accessible solution for traffic management and access control in networks with multiple security zones.*

KEYWORDS: Firewall, GNU/Linux, Proxy, Segmentation.

1 INTRODUCCIÓN

En la actualidad, la gestión del tráfico de red y la segmentación por zonas de seguridad representan aspectos fundamentales en el diseño de infraestructuras informáticas confiables, las organizaciones enfrentan el reto constante de proteger sus recursos internos frente a amenazas externas, garantizando al mismo tiempo la disponibilidad de los servicios para los usuarios autorizados, en este contexto, el uso de soluciones de software libre como Endian Firewall ofrece una alternativa robusta, flexible y de bajo costo para la implementación de políticas de seguridad perimetral.

Endian Firewall es una distribución GNU/Linux orientada a la seguridad de redes, que permite definir zonas diferenciadas de tráfico: la zona LAN o GREEN, destinada a la red interna; la zona WAN o RED, correspondiente al acceso a Internet; y la zona DMZ u ORANGE, reservada para los servidores expuestos, esta arquitectura de tres zonas facilita la aplicación de políticas de control de acceso precisas, reduciendo la superficie de ataque y mejorando la visibilidad del tráfico en la red.

Para el despliegue del entorno, se utilizó Oracle VirtualBox como plataforma de virtualización, sobre la cual se configuraron las tarjetas de red y se realizó la instalación de Endian Firewall Community, estableciendo las zonas GREEN, ORANGE y RED como base para las configuraciones

posteriores. Este paso es fundamental, ya que la correcta asignación de interfaces de red determina el comportamiento de todas las políticas de seguridad implementadas en las etapas siguientes.

El presente trabajo documenta la configuración de reglas NAT para permitir la comunicación entre las zonas LAN y WAN, así como desde la DMZ hacia Internet, además, se establecieron reglas de tráfico inter-zona para los servicios HTTP y FTP, se restringió el protocolo ICMP mediante políticas de denegación, y se implementó un Proxy HTTP no transparente con autenticación por usuario, incluyendo listas negras para el bloqueo de sitios web específicos.

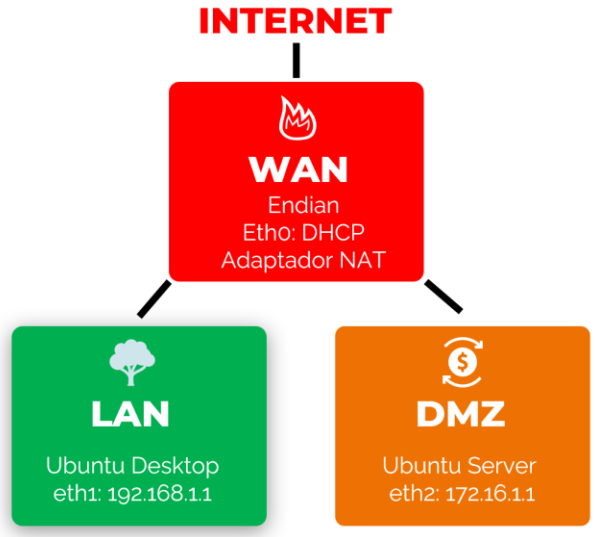
2 TEMÁTICAS

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

Endian Firewall Community (EFW) es una solución de seguridad de red basada en GNU/Linux que funciona como appliance UTM (Gestión Unificada de Amenazas). Permite segmentar redes en zonas de confianza diferenciadas y aplicar políticas de control de tráfico. Su implementación en entornos virtualizados como VirtualBox facilita la enseñanza y práctica de conceptos de seguridad perimetral. La segmentación consiste en dividir la infraestructura en zonas lógicas con distintos niveles de confianza:

1. Zona Roja (RED/WAN): conexión hacia Internet, considerada no confiable.
2. Zona Verde (GREEN/LAN): red interna segura para clientes.
3. Zona Naranja (ORANGE/DMZ): servidores expuestos, aislados de la LAN.

Figura 1
Esquema de segmentación



Fuente: Autoría propia

2.1.1 INSTALACIÓN Y PREPARACIÓN DEL ENTORNO

Con el esquema de segmentación previamente diseñado, procedemos a reunir los componentes necesarios para el desarrollo de la temática. En primer lugar, se realizó la adquisición del software accediendo al repositorio oficial en SourceForge, donde se localizó y descargó la imagen ISO de Endian Firewall Community (community_x64_3.3.2_recovery_softwarex8664_2020110122 0035).

Adicionalmente, se incorporaron las siguientes herramientas:

1. VirtualBox, utilizado como hipervisor para la creación y gestión de las máquinas virtuales.

2. Ubuntu Desktop (ubuntu-24.04.4-desktop-amd64), que funcionará como cliente en la zona GREEN (LAN).

3. Ubuntu Server (ubuntu-24.04.4-live-server-amd64), destinado a la zona ORANGE (DMZ).

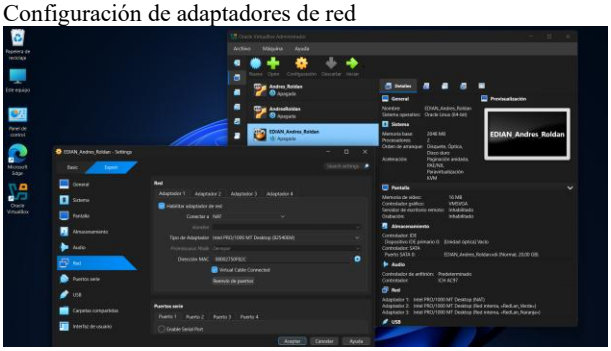
Figura 2
Creación de máquinas virtuales en VirtualBox

Fuente: Autoría Propia

Con VirtualBox disponible en el sistema anfitrión, se procedió a crear las máquinas virtuales correspondientes para el montaje de las ISOs de Endian, Ubuntu Desktop y Ubuntu Server. Cada máquina fue configurada con parámetros básicos: [1]

- Tipo de sistema: Linux (64-bit).
- Memoria RAM asignada: 2 GB.
- Núcleos asignados: 2
- Disco duro virtual: 10 GB.

Figura 3
Configuración de adaptadores de red



Fuente: Autoría Propia

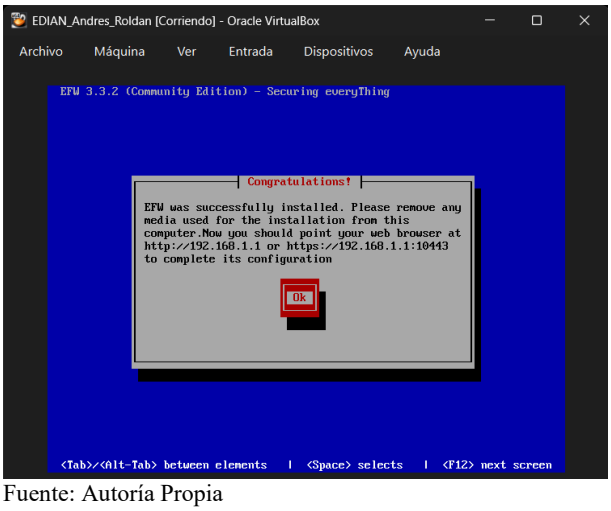
Esta preparación constituye el entorno adecuado para iniciar la configuración del firewall y establecer la arquitectura segmentada de seguridad perimetral. La correcta asignación de los adaptadores de red es un aspecto fundamental, ya que garantiza el funcionamiento apropiado de cada zona dentro del esquema planteado. Para ello se definió la siguiente disposición:

4. Adaptador 1: configurado en modo NAT, destinado a proporcionar salida hacia Internet (Zona Roja – RED/WAN).

5. Adaptador 2: configurado como Red Interna, asignado al cliente Ubuntu Desktop (Zona Verde – GREEN/LAN).

6. Adaptador 3: configurado también como Red Interna, destinado al servidor Ubuntu Server (Zona Naranja – ORANGE/DMZ).

Figura 4
Instalación inicial de Endian Firewall



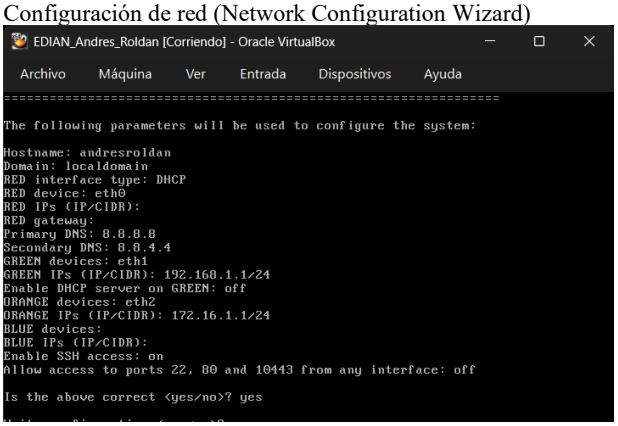
Fuente: Autoría Propia

Al arrancar la máquina virtual de Endian Firewall, se inicia el asistente de instalación, donde se aceptan las opciones básicas de idioma y teclado, y se establecen los parámetros de red, para esta fase se define la dirección IP y la máscara de red para la zona GREEN, que funcionará como gateway de la red interna. [2]

Finalizado el proceso de instalación y configuración, el sistema proporciona el enlace y puerto de acceso a la interfaz web de administración, al cual se puede ingresar desde el navegador de la máquina Ubuntu Desktop ubicada en la zona GREEN. El acceso se realiza mediante protocolo seguro HTTPS en la dirección: https://192.168.1.1:10443. [3]

Este portal permite gestionar las reglas de firewall, monitorear las interfaces y administrar los servicios de seguridad de manera centralizada.

Figura 5
Configuración de red (Network Configuration Wizard)



Fuente: Autoría Propia

En la máquina virtual de Endian Firewall se procedió a ejecutar el asistente de configuración de red (Network Configuration Wizard). En este punto, el sistema solicita ingresar la contraseña previamente definida durante la instalación del firewall. Posteriormente, se requiere establecer un hostname para identificar el dispositivo dentro de la infraestructura.

A continuación, se accede a la sección RED interface type, donde se listan las tarjetas de red instaladas en la máquina virtual. En esta fase se procede con la configuración de cada interfaz, asignando las zonas correspondientes:

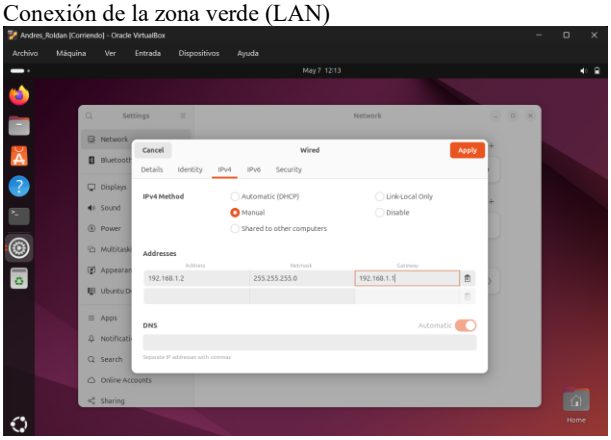
- eth0: RED (DHCP)
- eth1: GREEN (192.168.1.1/24)
- eth2: ORANGE (172.16.1.1/24)

Además, se configuraron los servidores DNS:

- Primario: 8.8.8.8
- Secundario: 8.8.4.4

Se habilitó el servicio DHCP en las interfaces necesarias y se definieron los protocolos de acceso permitidos, incluyendo los puertos 22 (SSH) y 80 (HTTP), finalmente, se guardaron los parámetros, quedando el sistema preparado para administrar las zonas de seguridad y garantizar la conectividad entre ellas bajo las políticas del firewall.

Figura 6
Conexión de la zona verde (LAN)



Fuente: Autoría propia

La conexión de la zona verde **(LAN)** se realiza accediendo a la máquina virtual Ubuntu Desktop, la cual está vinculada al Adaptador 2 configurado como Red Interna correspondiente a la zona GREEN. Desde allí, ingresamos a la sección de configuración de red cableada (IPv4) y aplicamos la configuración manual de los parámetros de red:

- Dirección IP: 192.168.1.2
- Máscara de red: 255.255.255.0
- Puerta de enlace (Gateway): 192.168.1.1
- Servidor DNS: 8.8.8.8

Con esta configuración, el cliente Ubuntu Desktop queda correctamente integrado en la zona GREEN, utilizando al firewall Endian como puerta de enlace y servidor de resolución de nombres.

Con la red ya configurada, desde la zona LAN (GREEN) se puede validar la conectividad hacia Internet y la comunicación con el servidor, se accede a la interfaz web de Endian Firewall desde la máquina virtual Ubuntu Desktop conectada al adaptador 2 (Red Interna – GREEN).

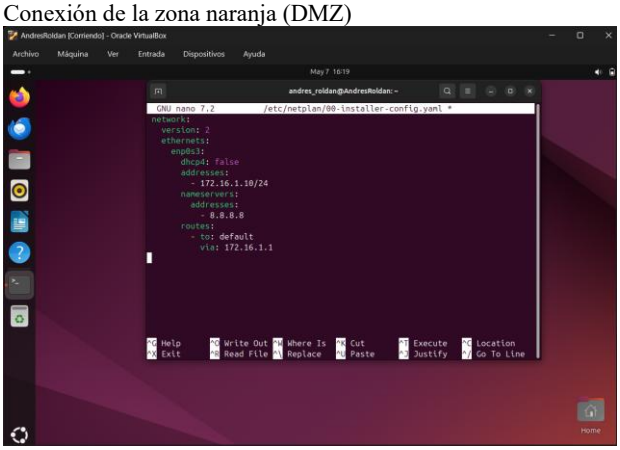
Figura 7
Validación de conectividad y acceso a la interfaz web

Fuente: Autoría Propia

En este punto se realiza el registro inicial y primer inicio de sesión, utilizando el usuario administrador y la contraseña definida durante la instalación. Una vez dentro de la interfaz gráfica de administración, se visualizan las interfaces de red previamente configuradas (RED, GREEN y ORANGE), confirmando que cada una se encuentra activa y correctamente asignada a su respectiva zona de seguridad.

Este acceso permite gestionar de manera centralizada las políticas de firewall, monitorear el estado de las zonas y administrar los servicios habilitados, garantizando así la operatividad del esquema de segmentación y la seguridad perimetral del laboratorio.

Figura 8
Conexión de la zona naranja (DMZ)



Fuente: Autoría Propia

Finalmente, nos dirigimos a la máquina virtual Ubuntu Server para habilitar la conexión correspondiente a la zona naranja **(DMZ)**. Esta VM está vinculada al Adaptador 3, configurado como Red Interna, lo que la integra directamente en la zona ORANGE definida en el esquema de segmentación. [4]

Desde allí, se procede a configurar el acceso a la red mediante la edición del archivo YAML de Netplan ubicado en nano */etc/netplan/00-installer-config.yaml*.

Figura 9
Configuración ipv4 en archivo nano /etc/netplan

Fuente: Autoría propia

Una vez guardados los cambios, se aplica la configuración con: *sudo netplan apply*, con esta configuración, el servidor Ubuntu quedó correctamente integrado en la **zona ORANGE (DMZ)**, asegurando comunicación con el firewall Endian y permitiendo la gestión de servicios en un entorno aislado y controlado.

2.2 TEMÁTICA 2: CONFIGURACIÓN NAT.

2.2.1 CONFIGURACIÓN DE REGLAS NAT EN ENDIAN FIREWALL

En un entorno de seguridad de redes, es importante tener una adecuada configuración del protocolo NAT(Network Address Traslation) ya que permite la comunicación de una forma controlada esto entre diferentes zonas de redes. Seguidamente se realiza un análisis en la implementación de practica de reglas NAT en firewall ENDIAN, permitiendo de este modo que los equipos de cómputo que se encuentran en red interna (LAN) como servidores en zona desmilitarizada (DMZ) puedan tener acceso a la red WAN (internet), garantizado la seguridad de la red, esto mientras se mantiene un estricto control en la salida y entrada de redes.

2.2.2 ARQUITECTURA DE RED

Tabla 1
Arquitectura de red

Zona	Tipo de red VirtualBox	Interfaz VirtualBox	Rango IP
Green (LAN)	Adaptador solo Anfitrión	Adaptador 1	192.168.1.1/24
Orange (DMZ)	Adaptador solo Anfitrión	Adaptador 2	172.16.1.1/24
Red (WAN)	NAT	Adaptador 3	10.0.2.15/24

Nota: Asignación de interfaces virtuales y direccionamiento IP para las zonas GREEN, ORANGE y RED del firewall.
Fuente: Autoría propia

2.2.3 NAT Y REENVIO DE PUERTOS

NAT es un mecanismo funcional el cual permite la conexión de múltiples dispositivos esto en un entorno de red privada comparta una conexión única con direcciones de IP pública, este mecanismo opera traduciendo las diferentes direcciones IP privadas de los dispositivos de una red interna a un protocolo de IP publica, es decir cuando existe un tráfico de internet este regresa. [5]

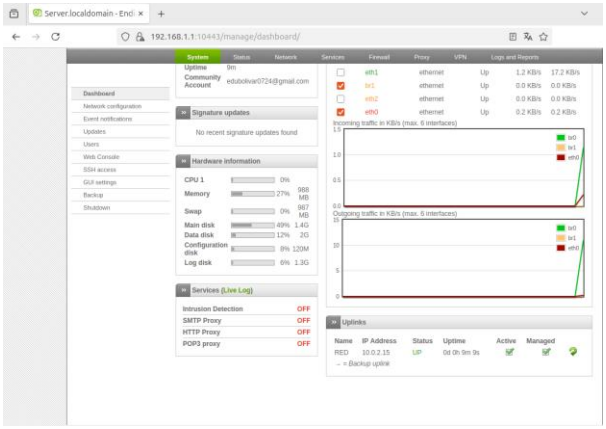
2.2.4 REENVIO DE PUERTOS

El reenvió de puertos es un servicio el cual permite un acceso restringido a redes LAN que no estén permitidas dentro de la configuración de privacidad interna es decir los equipos externos no tendrán acceso, esto permite que el tráfico de internet llegue de una mara segura y especifica esto en los servidores de una red privada. Cuando se realiza una configuración de reenvió de puertos en un firewall esta define una regla la cual especifica que el tráfico entrante sea dirigido a una IP privada y un puesto especifico de red. [6]

2.2.5 CONFIGURACIÓN DE REGLA NAT DEMOSTRADA.

En la página web se realiza la configuración de la regla NAT y sus respectivas pruebas de navegabilidad.

Figura 10
Menú firewall -NAT



Fuente: Autoría propia

Figura 11
Configuración regla NAT

Fuente: Autoría propia

2.2.6 PRUEBA DE NAVEGABILIDAD

Desde la maquina servidor se realizan las pruebas de las reglas de acceso. A la red Orange realizando una restricción de acceso.

Figura 12
Restricción de navegación (DMZ)

Fuente: Autoría propia

Figura 13
Acceso internet por la IP servidor

Fuente: Autoría propia

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

Como parte de la formación práctica en Administración de Servicios en Red, se desarrolló un conjunto de actividades orientadas a la configuración de redes segmentadas y a la implementación de políticas de seguridad mediante herramientas basadas en GNU/Linux. En este contexto, se realizó la configuración de una red segmentada utilizando el firewall Endian Firewall Community, abarcando desde la instalación del sistema hasta la validación de servicios permitidos y restringidos entre las diferentes zonas de red. [7]

2.3.1 CREACIÓN DE LA MÁQUINA VIRTUAL ENDIAN FIREWALL

Para la implementación del entorno de pruebas se utilizó Oracle VM VirtualBox, donde se creó la máquina virtual denominada *Endian_Firewall*. Esta fue configurada con un sistema operativo Linux de 64 bits, 1024 MB de memoria RAM y un disco duro virtual tipo VDI con capacidad de 20 GB.

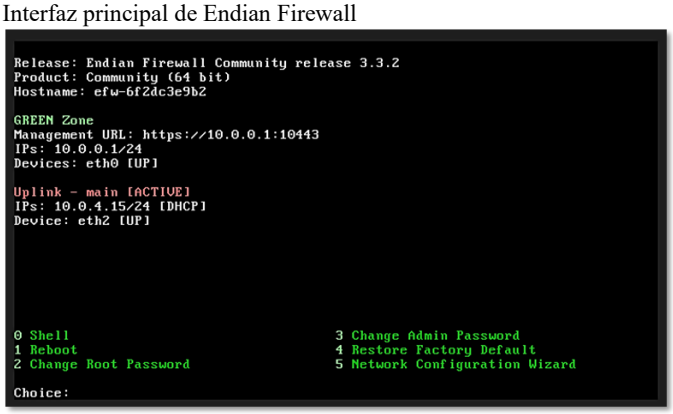
Adicionalmente, se configuraron tres adaptadores de red con el fin de segmentar el entorno de comunicación: [8]

1. Adaptador 1: red interna denominada LAN-Verde.
2. Adaptador 2: red interna denominada DMZ-Naranja.
3. Adaptador 3: modo NAT para acceso a Internet.

2.3.2 INSTALACIÓN DEL SISTEMA ENDIAN FIREWALL

Se montó la ISO EFW-COMMUNITY-3.3.2.iso en la VM y se procedió con la instalación, durante la configuración inicial, se asignó la zona verde con IP estática 10.0.0.1/24. Luego se accedió a la interfaz gráfica desde un navegador en una máquina cliente LAN.

Figura 14
Interfaz principal de Endian Firewall



Fuente: Autoría propia

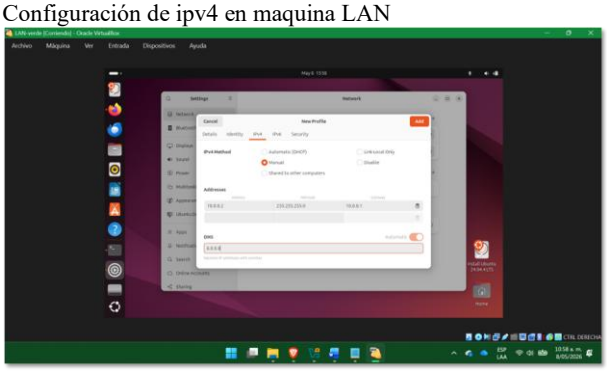
2.3.3 CREACIÓN DE CLIENTE LAN Y SERVIDOR DMZ

Se crearon dos nuevas Máquinas Virtuales:

1. Desktop-LAN con IP 10.0.0.2, red interna LAN
2. Server-DMZ con IP 172.16.0.2, red interna DMZ

Ambas sin ISO, utilizando Ubuntu Desktop y Server previamente instalado

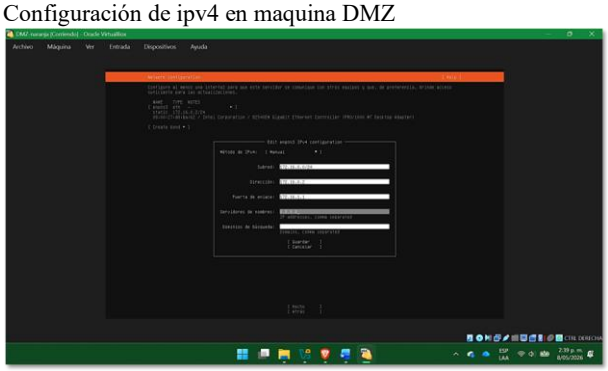
Figura 15
Configuración de ipv4 en maquina LAN



Fuente: Autoría propia

Antes de finalizar la instalación de Ubuntu server, se edita la configuración ipv4, estbleciendo los siguientes parametros:

Figura 16
Configuración de ipv4 en maquina DMZ



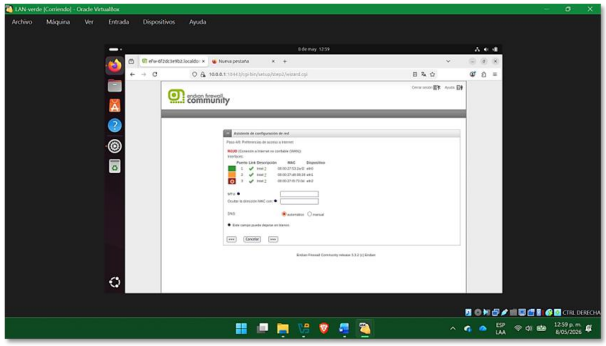
Fuente: Autoría propia

2.3.4 ACCESO AL DASHBOARD Y CONFIGURACIÓN BÁSICA

Desde el navegador de la máquina cliente (con IP 10.0.0.2), se accedió a la dirección https://10.0.0.1 para iniciar sesión en el dashboard de Endian. Se completó el asistente de configuración inicial, se estableció zona roja como ETH02, zona verde como ETH00 y zona naranja como ETH01. Se configuraron las interfaces con IPs:

1. Verde: 10.0.0.1/24
2. Naranja: 172.16.0.1/24
3. Roja: automática por DHCP

Figura 17
Acceso a Dashboard Endian Firewall



Fuente: Autoría propia

2.3.5 PRUEBAS DE CONECTIVIDAD

1. Ping desde Endian Firewall (Endian server) hacia LAN-verde (Ubuntu Desktop) 10.0.0.2 y DMZ-naranja (Ubuntu server) 172.16.0.2

Figura 18
Ping exitoso desde Endian_Firewall

Fuente: Autoría propia

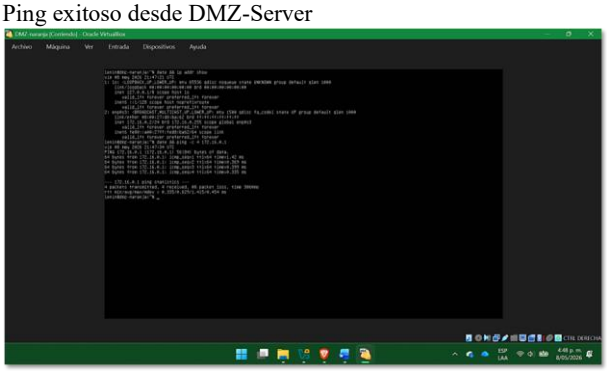
2. Ping desde LAN-verde (Ubuntu desktop) hacia Endian Firewall (Endian server)

Figura 19
Ping exitoso desde LAN-Desktop

Fuente: Autoría propia

3. Ping desde DMZ naranja (Ubuntu server) hacía Endian Web (Ubuntu Desktop)

Figura 20
Ping exitoso desde DMZ-Server



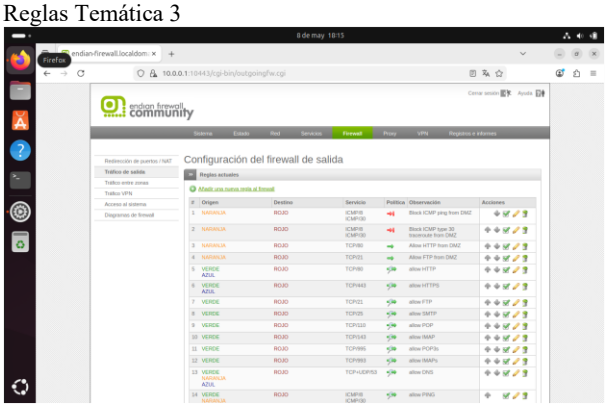
Fuente: Autoría propia

2.3.6 REGLAS DE FIREWALL Y FILTRADO DE SERVICIOS

Configuración y comprobación temática 3: Permitir servicios de la Zona DMZ para la red. [9]

4. Regla1: Permitir los servicios HTTP (Puerto 80)
5. Regla 2: PERMITIR FTP (puerto 21) desde NARANJA
6. Regla 3: BLOQUEAR ICMP tipo 8 (ping) desde NARANJA
7. Regla 4: BLOQUEAR ICMP tipo 30 (traceroute) desde NARANJA

Figura 21
Reglas Temática 3



Fuente: Autoría propia

2.3.7 VERIFICACIÓN DE LAS REGLAS APLICADAS EN LA TEMATICA 3

1. La primera prueba verificó el bloqueo del protocolo ICMP desde la zona DMZ mediante un comando *ping* hacia 8.8.8.8. El resultado fue 100 % de pérdida de paquetes, confirmando el correcto bloqueo configurado en Endian Firewall Community.

2. La segunda prueba validó el acceso HTTP desde la zona DMZ utilizando el comando curl -I hacia Google. La respuesta obtenida confirmó que el tráfico TCP por el puerto 80 se encuentra permitido correctamente.

Figura 22
Verificación de reglas mediante DMZ-Server

Fuente: Autoría propia

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

Una vez establecida la infraestructura, se accede al módulo Inter-Zone Firewall en la interfaz web de Endian. Allí se definen las reglas de acceso precisas, especificando la zona de origen, la zona de destino, el servicio o puerto involucrado y la política de acción para permitir o denegar. Se configuran para permitir tráfico HTTP (puerto 80) y FTP (puerto 21) entre LAN y DMZ, entre LAN y WAN, así como entre WAN y DMZ, Cada regla se guarda y aplica los cambios realizados. [10]

2.4.1 CONFIGURACIÓN DE REGLAS

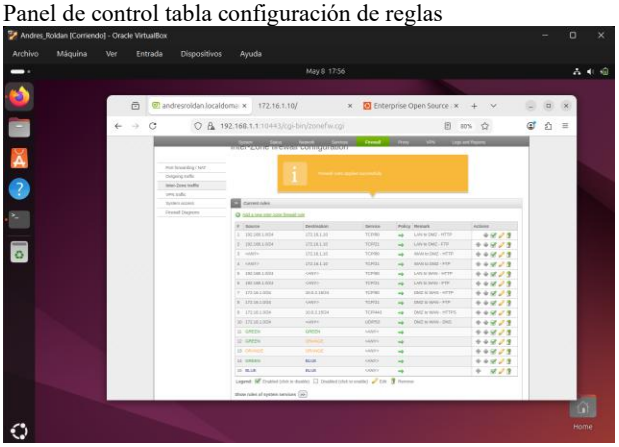
Tabla 2
Panel de control sobre la configuración de reglas

VERDE (LAN) ↔ NARANJA (DMZ)	
LAN a DMZ (HTTP)	LAN a DMZ (FTP)
Source type: 192.168.1.0/24 Destination type: 172.16.1.10 Service/port: HTTP → TCP/80 Policy Action: ALLOW Remark: LAN to DMZ - HTTP Status: Enabled ✓	Source type: 192.168.1.0/24 Destination type: 172.16.1.10 Service/port: FTP → TCP/21 Policy Action: ALLOW Remark: LAN to DMZ - FTP Status: Enabled ✓
INTERNET (WAN)	
WAN a DMZ (HTTP)	WAN a DMZ (FTP)
Source type: Any (0.0.0.0/0) Destination type: 172.16.1.10 Service/port: HTTP → TCP/80 Policy Action: ALLOW Remark: WAN to DMZ – HTTP Status: Enabled ✓	Source type: Any (0.0.0.0/0) Destination type: 172.16.1.10 Service/port: FTP → TCP/21 Policy Action: ALLOW Remark: WAN to DMZ - FTP Status: Enabled ✓
LAN a WAN (HTTP)	LAN a WAN (FTP)
Source type: 192.168.1.0/24 Destination type: Any (0.0.0.0/0) Service/port: HTTP → TCP/80 Policy Action: ALLOW Remark: LAN to WAN - HTTP Status: Enabled ✓	Source type: 192.168.1.0/24 Destination type: Any (0.0.0.0/0) Service/port: FTP → TCP/21 Policy Action: ALLOW Remark: LAN to WAN - FTP Status: Enabled ✓
DMZ a WAN (HTTP)	DMZ a WAN (FTP)
Source type: 172.16.1.0/24 Destination type: Any (0.0.0.0/0) Service/port: HTTP → TCP/80 Policy Action: ALLOW Remark: DMZ to WAN – HTTP Status: Enabled ✓	Source type: 172.16.1.0/24 Destination type: Any (0.0.0.0/0) Service/port: FTP → TCP/21 Policy Action: ALLOW Remark: DMZ to WAN - FTP Status: Enabled ✓

Nota: Configuración de políticas de filtrado y control de acceso implementadas entre las zonas de red LAN, DMZ y WAN mediante Endian Firewall.
Fuente. Autoría Propia

Se muestra la tabla completa de las configuraciones en el apartado de inter-zone traffic.

Figura 23
Panel de control tabla configuración de reglas

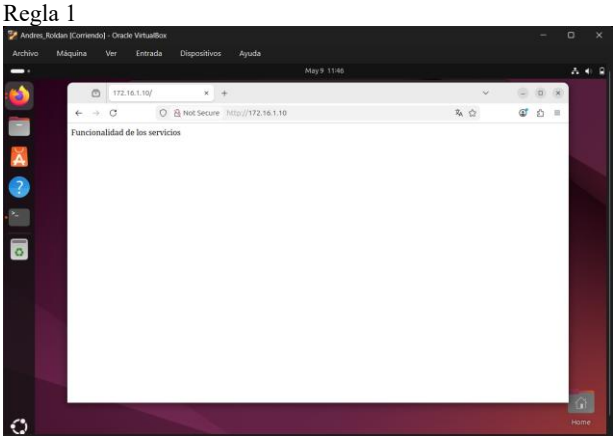


Fuente: Autoría Propia

2.4.2 PRUEBA DE REGLAS

La primera regla configurada en el módulo Inter-Zone Firewall de Endian permite el tráfico HTTP desde la zona LAN (GREEN) hacia la zona DMZ (ORANGE), habilitando así la comunicación web entre la red interna y los servidores alojados en la zona desmilitarizada, esta regla fue definida especificando como origen la red 192.168.1.0/24, como destino la dirección IP 172.16.1.10 del servidor, y el puerto TCP 80 como servicio permitido. Para verificar su correcto funcionamiento, se accedió desde el navegador web de la máquina cliente LAN a la dirección http://172.16.1.10.

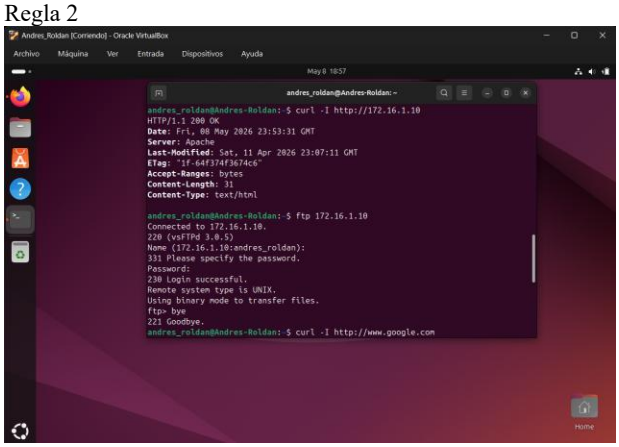
Figura 24
Regla 1



Fuente: Autoría Propia

La segunda regla habilita el protocolo FTP desde la zona LAN (GREEN) hacia la zona DMZ (ORANGE), permitiendo la transferencia de archivos entre los equipos de la red interna y los servidores, esta regla fue configurada con origen en la red 192.168.1.0/24, destino en la dirección 172.16.1.10 y el puerto TCP 21 como servicio autorizado, se verifico desde la terminal de la máquina cliente LAN ejecutando el comando ftp 172.16.1.10.

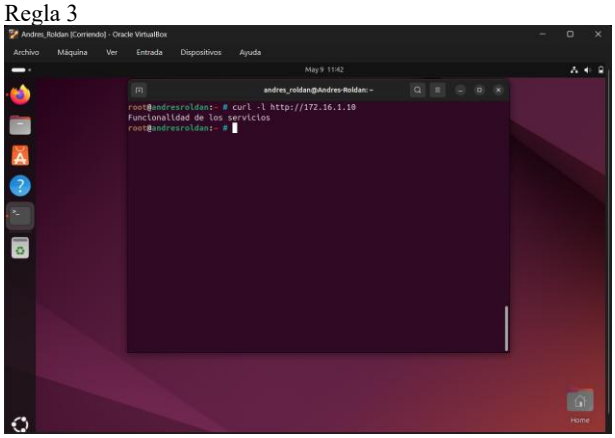
Figura 25
Regla 2



Fuente: Autoría Propia

La tercera regla permite el acceso HTTP desde la zona WAN hacia la zona DMZ, para la verificación se utilizó la terminal de Endian Firewall ejecutando el comando curl -I http://172.16.1.10, el cual retornó las cabeceras HTTP del servidor, confirmando que las solicitudes web provenientes desde Internet hacia los servicios de la DMZ son procesadas correctamente.

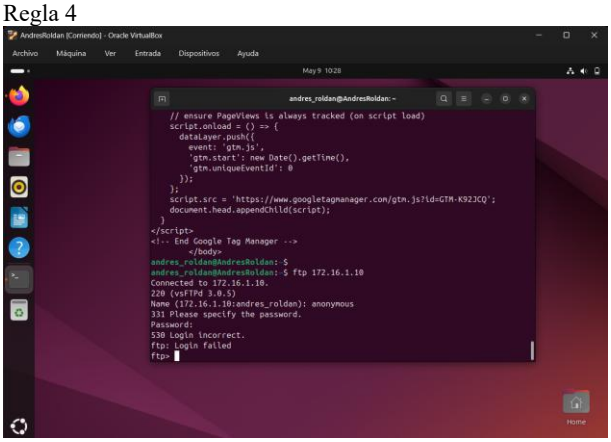
Figura 26
Regla 3



Fuente: Autoría Propia

La cuarta regla habilita el protocolo FTP desde la zona WAN hacia la zona DMZ, la prueba se ejecutó desde la terminal de Endian Firewall con el comando ftp 172.16.1.10, permitiendo verificar que las conexiones FTP originadas desde Internet logran alcanzar el servidor ubicado en la DMZ.

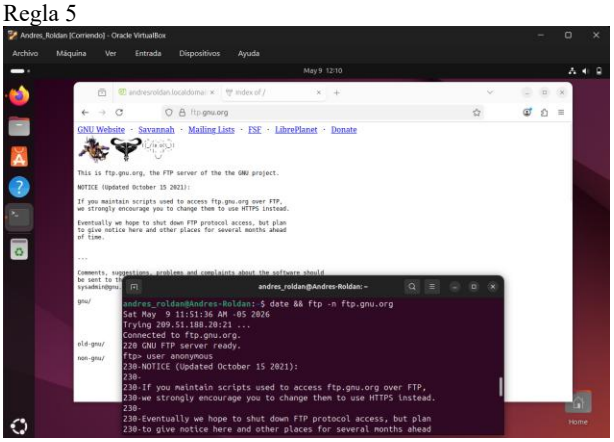
Figura 27
Regla 4



Fuente: Autoría Propia

La quinta regla permite el tráfico HTTP desde la zona LAN hacia la WAN, realizada desde el navegador web de la máquina cliente LAN accediendo a http://www.google.com.

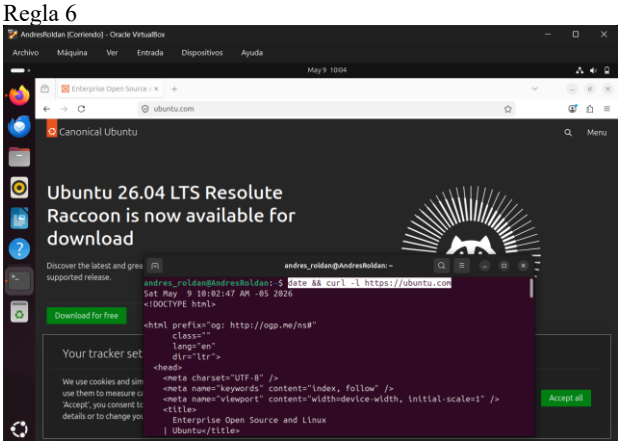
Figura 28
Regla 5



Fuente: Autoría Propia

La sexta regla habilita el tráfico HTTP desde la zona DMZ hacia la WAN, permitiendo que los servidores alojados en la zona desmilitarizada tengan acceso a recursos en Internet.

Figura 29
Regla 6

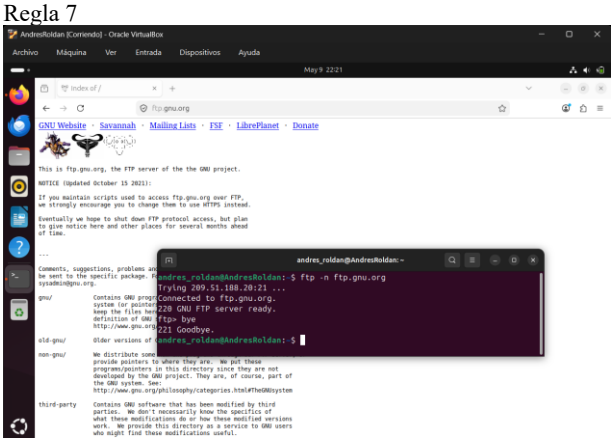


Fuente: Autoría Propia

Esta verificación se realizó desde la terminal de la máquina DMZ ejecutando el comando curl -l https://www.ubuntu.com, obteniendo respuesta exitosa del sitio.

La séptima regla permite el protocolo FTP desde la zona DMZ hacia la WAN, habilitando la transferencia de archivos desde los servidores de la DMZ hacia recursos externos en Internet, la ejecución se realizó mediante el comando ftp -n ftp.gnu.org desde la terminal de la máquina DMZ, logrando establecer conexión con el servidor FTP público de GNU. [11]

Figura 30
Regla 7



Fuente: Autoría Propia

2.5 TEMÁTICA 5 IMPLEMENTACIÓN DE SERVICIOS Y VERIFICACIÓN DE SEGURIDAD EN GNU/LINUX

El tema 5 se centró en la implementación y verificación de servicios de red en un sistema GNU/Linux mediante la aplicación de políticas de seguridad y segmentación utilizando comunidades de firewall Endian. Los objetivos principales fueron verificar que los servicios configurados funcionaran correctamente, que la comunicación entre diferentes zonas de red estuviera controlada y comprobar el comportamiento del firewall para las conexiones permitidas y restringidas.

Los ejercicios utilizaron herramientas de GNU/Linux para la gestión y monitorización de servicios, destacando la importancia de la seguridad perimetral y la correcta configuración de las reglas de acceso en entornos virtualizados. [12]

2.5.1 CONFIGURACION Y VALIDACION

Para la validación del entorno se instalaron y configuraron servicios HTTP y FTP sobre el servidor ubicado en la zona DMZ. Posteriormente se realizaron pruebas de conectividad desde diferentes segmentos de red con el propósito de verificar las políticas de acceso establecidas en Endian Firewall.

El servicio HTTP fue implementado mediante Apache2 en Ubuntu Server, permitiendo comprobar el acceso web desde

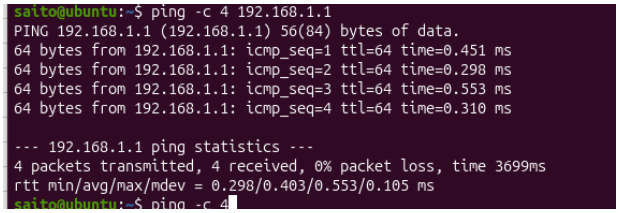
la zona LAN y desde la WAN controlada. De igual manera, el servicio FTP fue habilitado para validar la transferencia y autenticación de archivos utilizando clientes de consola GNU/Linux.

Las verificaciones se realizaron mediante herramientas como:

1. Navegador web para acceso HTTP.
2. Comando curl para validación de cabeceras HTTP.
3. Cliente ftp desde terminal GNU/Linux.
4. Comandos ping y traceroute para pruebas ICMP.

Las pruebas permitieron identificar que las reglas configuradas en el firewall responden correctamente a las políticas definidas, permitiendo únicamente el tráfico autorizado y bloqueando protocolos restringidos desde determinadas zonas.

Figura 31
Validación de servicio HTTP desde LAN hacia servidor DMZ



Fuente: Autoría propia

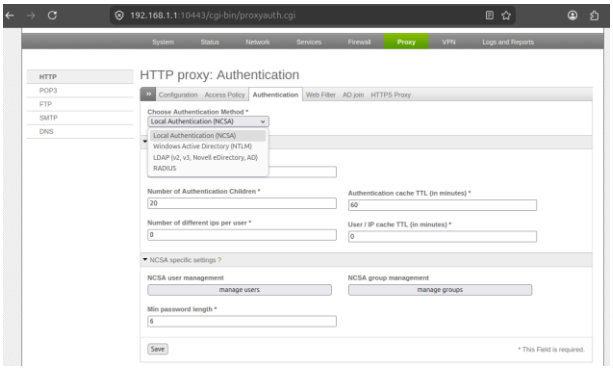
Se habilita el módulo de Proxy en Endian Firewall en modo no transparente, definiendo que los clientes de la zona GREEN deben configurar manualmente el proxy en sus navegadores. [13]

Figura 32
Configuración del proxy http

Fuente: Autoría propia

Luego de haber definido el módulo proxy en Endian Firewall se registra un usuario en el sistema de autenticación NCSA, lo que permite que cada conexión al proxy requiera credenciales validas.

Figura 33
Creación de usuario NCSA



Fuente: Autoría propia

En el navegador del cliente LAN se establece la dirección IP del firewall y el puerto 8080 como proxy, asegurando que todo el tráfico web pase por endian.

Figura 34
Configuración del navegador en Cliente LAN

Fuente: Autoría propia

Se evidencia la aplicación de políticas de seguridad configuradas en el firewall Endian, donde el navegador Mozilla Firefox solicita autenticación para permitir el acceso a la red, lo cual confirma la implementación de restricciones y controles de acceso definidos sobre el tráfico de red, validando el funcionamiento de las reglas de filtrado y protección establecidas durante las pruebas de conectividad.

Figura 35
Verificación de bloqueo ICMP mediante políticas del firewall

Fuente: Autoría propia

2.5.2 MONITOREO Y COMPROBACION DE FIREWALL

Además, se realizaron pruebas de monitorización desde la interfaz de administración de la comunidad de Endian Firewall y se revisaron los registros de conexiones activas,

paquetes filtrados y eventos de seguridad generados por las reglas implementadas.

Esta herramienta proporcionó visibilidad en tiempo real del comportamiento del tráfico entre zonas, demostrando que la segmentación de la red reduce significativamente la vulnerabilidad de los servicios internos a conexiones no autorizadas desde la WAN.

Asimismo, se confirmó que el uso de una DMZ es una medida eficaz para alojar servicios públicos sin comprometer directamente la seguridad de la LAN interna.

3 CONCLUSIONES

3.1 TEMÁTICA 1

La configuración de la instancia de Endian Firewall en VirtualBox, mediante la correcta asignación de las tarjetas de red para cada zona, constituye el paso fundamental para el funcionamiento del sistema de seguridad perimetral. La definición precisa de las interfaces GREEN, ORANGE y RED desde el inicio del proceso garantiza que cada zona opere de forma independiente y controlada, sin esta base, ninguna de las políticas de seguridad posteriores tendría efecto, lo que confirma que la infraestructura virtualizada no es simplemente un entorno de pruebas, sino la plataforma sobre la cual se sostiene toda la arquitectura de red segmentada, además este proceso también permitió desarrollar competencias prácticas en la gestión de entornos virtualizados con GNU/Linux, habilidades esenciales para cualquier administrador de sistemas.

3.2 TEMÁTICA 2

La implementación de reglas NAT en Endian Firewall demostró que es posible establecer comunicación controlada entre la zona LAN y la WAN, así como desde la DMZ hacia Internet, sin exponer directamente los recursos internos de la red, el buen uso de estas reglas resulta fundamental para garantizar la salida de tráfico de forma segura y auditable en entornos segmentados, adicional a esto, la configuración del reenvío de puertos evidenció que es posible dirigir tráfico entrante hacia servicios específicos dentro de la red privada, manteniendo en todo momento el control sobre qué conexiones son permitidas y desde qué origen, lo que refuerza el principio de mínimo privilegio en la administración de redes.

3.3 TEMÁTICA 3

En la configuración de reglas de tráfico de salida en la zona DMZ, se evidenció la importancia crítica del orden en la aplicación de las políticas del firewall, las reglas de denegación, como la restricción del protocolo ICMP mediante el bloqueo de los tipos 8 y 30, deben preceder a las de permisión para garantizar su correcta ejecución, las pruebas realizadas con el comando ping confirmaron el bloqueo efectivo del protocolo, mientras que el acceso HTTP mediante curl demostró que los servicios permitidos funcionan correctamente, lo cual confirma que el orden de procesamiento de reglas es un factor determinante en la administración de firewalls y que una mala configuración en este aspecto puede comprometer toda la política de seguridad definida.

3.4 TEMÁTICA 4

Las reglas de tráfico inter-zona permitieron segmentar y controlar de manera precisa la comunicación entre las zonas GREEN, ORANGE y RED, cubriendo los escenarios de comunicación LAN hacia DMZ, LAN hacia WAN, WAN hacia DMZ y DMZ hacia WAN, estas pruebas realizadas mediante navegadores web, el cliente FTP y la herramienta curl evidenciaron que el tráfico autorizado fluye correctamente en cada uno de estos escenarios, mientras que los intentos de acceso no permitidos son bloqueados de forma efectiva, con el fin de reforzar el valor de la DMZ como zona intermedia de seguridad la cual permite exponer servicios al exterior sin comprometer directamente la integridad de la red interna, demostrando que una correcta segmentación es una de las medidas más eficaces en la protección de infraestructuras de red.

3.5 TEMÁTICA 5

La implementación del Proxy HTTP no transparente con autenticación por usuario y grupo demostró que Endian Firewall ofrece mecanismos avanzados de control de navegación web que van más allá del simple filtrado de puertos, la configuración de listas negras permitió bloquear el acceso a sitios específicos desde la LAN, y la exigencia de credenciales para navegar añade una capa adicional de trazabilidad y control sobre el uso de Internet dentro de la organización, validando que las políticas de filtrado de contenido y autenticación son componentes indispensables de seguridad en entornos corporativos y educativos, donde el control del acceso web representa tanto una necesidad de seguridad como una política de uso responsable de los recursos de red.

4 REFERENCIAS

[1]. Oracle, *Manual de usuario VirtualBox*, 2020. [En línea]. Disponible en: https://www.virtualbox.org/manual/ [Accedido: may. 2025].

[2]. Endian, *Endian UTM 3.2 Manual de referencia*, 2016. [En línea]. Disponible en: http://docs.endian.com/3.2/utm/index.html [Accedido: may. 2025].

[3]. Canonical, *Guía del Ubuntu Desktop 20.04 LTS*, 2023. [En línea]. Disponible en: https://help.ubuntu.com/ [Accedido: may. 2025].

[4]. Canonical, *Ubuntu Server Documentation*, 2024. [En línea]. Disponible en: https://ubuntu.com/server/docs/ [Accedido: may. 2025].

[5]. Endian, "The Firewall Menu," *Endian UTM 5.0 Reference Manual*, 2023. [En línea]. Disponible en: https://docs.endian.com/5.0/utm/firewall.html [Accedido: may. 2025].

[6]. Cibersafety, "Guía definitiva sobre la DMZ: cómo implementarla en redes corporativas y mejorar la seguridad perimetral," *Cibersafety*, jul. 2025. [En línea]. Disponible en: https://cibersafety.com/dmz-seguridad-perimetral/ [Accedido: may. 2025].

[7]. N. Barney y B. Lutkevich, "What is a DMZ in networking?," *Search Security, TechTarget*, Feb. 2025. [En línea]. Disponible en: https://www.techtarget.com/searchsecurity/definition/DMZ [Accedido: may. 2025].

[8]. National Institute of Standards and Technology, *NIST Special Publication 800-125B: Secure Virtual Network Configuration for Virtual Machine (VM) Protection*, 2016. [En línea]. Disponible en: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-125B.pdf [Accedido: may. 2025].

[9]. eSecurity Planet, "How To Set Up DMZ on Servers: 7-Step DMZ Configuration," *eSecurity Planet*, Dic. 2024. [En línea]. Disponible en: https://www.esecurityplanet.com/networks/dmz-setup/ [Accedido: may. 2025].

[10]. Automation.com, "Segmenting Networks Using a DMZ," *Automation*, abr. 2024. [En línea]. Disponible en: https://www.automation.com/en-us/articles/april-2024/segmenting-networks-using-dmz [Accedido: may. 2025].

[11]. MCSI Institute, "Network Segmentation," *MCSI Library*, ago. 2023. [En línea]. Disponible en: https://library.mosse-institute.com/articles/2023/08/network-segmentation.html [Accedido: may. 2025].

[12]. Free Software Foundation, "Software libre y educación," *El sistema operativo GNU*, 2016. [En línea]. Disponible en: http://www.gnu.org/education/education.html [Accedido: may. 2025].

[13]. Squid Project, "Proxy Authentication," *Squid Web Cache Wiki*, 2023. [En línea]. Disponible en: https://wiki.squid-cache.org/Features/Authentication [Accedido: may. 2025].