DISEÑO E IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA SEGURA EN GNU/LINUX USANDO ENDIAN FIREWALL

Katherin Julieth Chacón Valbuena
kjchaconva@unadvirtual.edu.co
Brayan Antonio Baez Cumaco
babaezc@unadvirtual.edu.co
Alejandro Palacios Arévalo
apalaciosar@unadvirtual.edu.co
Alejandro Ruiz Cristancho
aruizcr@unadvirtual.edu.co
Edison Javier Florez Barrera
Ejflorezb@unadvirtual.edu.co

RESUMEN: *Este artículo presenta la implementación de una infraestructura de seguridad perimetral basada en GNU/Linux utilizando la distribución Endian Firewall Community (EFW) en un entorno virtualizado con VirtualBox. El proyecto contempla la configuración de zonas de red LAN, WAN y DMZ, así como la aplicación de reglas NAT, control de acceso, habilitación de servicios HTTP y FTP, y la implementación de un proxy HTTP con políticas de autenticación y filtrado web. Además, se realizaron pruebas de conectividad y restricciones de tráfico mediante comandos ejecutados desde consola, garantizando el cumplimiento de buenas prácticas de administración y seguridad en sistemas Linux. Los resultados obtenidos evidencian una correcta segmentación de red y un control eficiente del tráfico entre zonas, fortaleciendo la protección de servidores y servicios críticos en la infraestructura.*

PALABRAS CLAVE: *DMZ, Endian Firewall, seguridad perimental, redes LAN/WAN.*

ABSTRACT: *This article presents the implementation of a perimeter security infrastructure based on GNU/Linux using the Endian Firewall Community (EFW) distribution in a virtualized environment with VirtualBox. The project includes the configuration of LAN, WAN, and DMZ network zones, as well as the application of NAT rules, access control, enabling HTTP and FTP services, and implementing an HTTP proxy with authentication and web filtering policies. Connectivity and traffic restriction tests were also performed using commands executed from the console, ensuring compliance with best practices for Linux administration and security. The results obtained demonstrate proper network segmentation and efficient traffic control between zones, strengthening the protection of critical servers and services within the infrastructure.*

1 INTRODUCCIÓN

La seguridad perimetral constituye uno de los componentes fundamentales en la protección de infraestructuras tecnológicas modernas, especialmente en entornos donde los servicios web, bases de datos y aplicaciones empresariales se encuentran expuestos a redes externas. En este contexto, las distribuciones GNU/Linux ofrecen herramientas robustas y flexibles para la administración segura de redes y servicios.

El presente trabajo tiene como finalidad implementar una solución de seguridad basada en GNU/Linux mediante la utilización de Endian Firewall Community (EFW) como plataforma principal de protección y administración del tráfico de red. Para ello, se diseñó una arquitectura compuesta por una red interna (LAN), una zona desmilitarizada (DMZ) y una red externa (WAN), permitiendo establecer políticas de acceso, traducción de direcciones NAT, control de servicios y filtrado de contenido web.

Asimismo, se desarrollaron configuraciones relacionadas con reglas de firewall, servicios HTTP y FTP, políticas de autenticación y restricciones de navegación, con el propósito de fortalecer la seguridad de la infraestructura y garantizar la integridad de los recursos alojados en el servidor GNU/Linux. Todas las configuraciones y validaciones fueron realizadas desde consola, siguiendo las recomendaciones establecidas en la guía de actividades.

2 OBJETIVOS

2.1 OBJETIVO GENERAL

Implementar una infraestructura de seguridad perimetral en GNU/Linux utilizando Endian Firewall Community, mediante la configuración de redes LAN, WAN y DMZ, aplicando políticas de control de acceso, NAT y servicios de red para garantizar la protección y administración segura del tráfico.

2.2 OBJETIVOS ESPECÍFICOS

Configurar una instancia de GNU/Linux Endian en VirtualBox mediante la implementación de las zonas LAN, WAN y DMZ para segmentar adecuadamente la red.

Implementar reglas NAT y políticas de firewall que permitan controlar el tráfico entre las diferentes zonas de red y garantizar la conectividad segura.

Habilitar y administrar servicios HTTP y FTP en un servidor GNU/Linux dentro de la zona DMZ, aplicando restricciones de acceso y pruebas de funcionamiento.

Configurar un proxy HTTP con autenticación de usuarios y listas negras para restringir el acceso a sitios web específicos desde la red LAN.

Verificar el funcionamiento de los servicios y políticas de seguridad mediante pruebas ejecutadas desde consola en sistemas GNU/Linux.

3 MARCO TEÓRICO

3.1 FIREWALL

Un firewall o cortafuegos es un sistema de seguridad encargado de supervisar, filtrar y controlar el tráfico de red entre diferentes segmentos o redes, permitiendo o bloqueando conexiones según reglas previamente definidas. Su objetivo principal es proteger los recursos internos frente a accesos no autorizados, ataques externos y amenazas provenientes de Internet. Los firewalls pueden implementarse mediante hardware, software o una combinación de ambos, y constituyen uno de los mecanismos fundamentales en la seguridad perimetral de las organizaciones. Diversos estudios destacan que una configuración adecuada de las reglas de firewall es esencial para garantizar la protección efectiva de la infraestructura de red.

De acuerdo con Stallings (2018), los firewalls funcionan como una barrera entre redes confiables y no confiables, inspeccionando paquetes de datos y aplicando políticas de seguridad para controlar el acceso a servicios y recursos compartidos

3.2 ENDIAN FIREWALL COMMUNITY

Endian Firewall Community es una distribución GNU/Linux especializada en seguridad perimetral y gestión unificada de amenazas (UTM). Esta plataforma permite implementar servicios de firewall, proxy, VPN, filtrado de contenidos y control de acceso mediante una interfaz de administración web centralizada. Su arquitectura facilita la segmentación de redes y el monitoreo del tráfico, convirtiéndose en una herramienta ampliamente utilizada en entornos educativos y empresariales.

Endian utiliza un modelo de segmentación basado en colores para identificar las diferentes zonas de seguridad, permitiendo separar redes internas, externas y desmilitarizadas (DMZ). Además, ofrece soporte para NAT, detección de intrusos, autenticación de usuarios y filtrado web, lo cual fortalece la protección de los servicios publicados en Internet.

Según la documentación oficial de Endian, la plataforma está diseñada para facilitar la administración de la seguridad de red mediante herramientas centralizadas y políticas de filtrado configurables.

3.3 VIRTUALIZACIÓN

La virtualización es una tecnología que permite ejecutar múltiples sistemas operativos y servicios sobre un mismo equipo físico mediante el uso compartido de recursos de hardware. Esta técnica facilita la creación de entornos de prueba, simulación y laboratorios académicos sin necesidad de disponer de múltiples equipos físicos.

Una de las herramientas más utilizadas para este propósito es Oracle VirtualBox, un software de virtualización que permite crear y administrar máquinas virtuales de manera eficiente. En el ámbito académico, VirtualBox es ampliamente empleado para implementar laboratorios de redes, servidores y escenarios de ciberseguridad debido a su facilidad de uso y compatibilidad con diferentes sistemas operativos.

La virtualización también contribuye a optimizar recursos, reducir costos de infraestructura y mejorar la flexibilidad en la administración de sistemas. Según Smith y Nair (2005), esta tecnología representa una de las bases fundamentales de la computación moderna al permitir el aislamiento y la administración eficiente de entornos operativos.

3.4 SEGMENTACIÓN DE REDES

La segmentación de redes consiste en dividir una infraestructura de comunicación en diferentes zonas o subredes con el propósito de mejorar la seguridad, controlar el tráfico y limitar el alcance de posibles ataques informáticos. Este enfoque permite aplicar políticas específicas de acceso y protección según el nivel de confianza de cada segmento de red.

En Endian Firewall las principales zonas utilizadas son GREEN, RED y ORANGE. La zona GREEN corresponde a la red LAN o red interna segura; la zona RED representa la conexión WAN o salida hacia Internet; y la zona ORANGE corresponde a la DMZ, destinada a alojar servidores accesibles desde redes externas.

La implementación de una DMZ permite aislar servicios públicos, como servidores web o FTP, evitando el acceso directo desde Internet hacia la red interna. Este modelo de arquitectura es ampliamente utilizado en organizaciones para fortalecer la seguridad perimetral y reducir riesgos de intrusión.

Según Comer (2018), la segmentación de redes mejora significativamente la administración del tráfico y permite establecer mecanismos de protección más eficientes frente a amenazas externas.

3.5 DMZ (ZONA DESMILITARIZADA)

Para Belen (2023) La DMZ (Demilitarized Zone) es una subred utilizada para alojar servicios que deben ser accesibles desde redes externas, como servidores web, FTP, DNS o correo electrónico, sin exponer directamente la red interna de la organización. Esta arquitectura permite aislar los servicios públicos y reducir el riesgo de acceso no autorizado hacia los equipos de la red LAN.

En una infraestructura segmentada, la DMZ actúa como una zona intermedia entre la red interna segura y la red externa o Internet. Los firewalls controlan el tráfico que entra y sale de esta zona mediante reglas específicas, permitiendo únicamente los servicios necesarios.

La utilización de una DMZ constituye una práctica fundamental en seguridad informática debido a que limita el impacto de posibles ataques dirigidos a servidores públicos, la implementación de zonas desmilitarizadas mejora significativamente la protección de la red interna frente a amenazas externas.

3.6 PROTOCOLO ICMP

El protocolo ICMP (Internet Control Message Protocol) es un protocolo de red utilizado para el intercambio de mensajes de control, diagnóstico y notificación de errores entre dispositivos IP. Una de sus funciones más conocidas es permitir la utilización del comando ping para verificar la conectividad entre equipos.

Aunque ICMP cumple funciones importantes dentro de las comunicaciones de red, también puede ser utilizado por atacantes para realizar tareas de reconocimiento y exploración de hosts activos. Por esta razón, muchas organizaciones implementan restricciones sobre determinados tipos de mensajes ICMP mediante reglas de firewall.

El bloqueo de solicitudes Echo Request permite reducir la visibilidad de los dispositivos dentro de una red y disminuir posibles riesgos relacionados con escaneos y descubrimiento de infraestructura (Markova & Markova, 2026).

4 METODOLOGÍA

4.1 TEMÁTICA 1: CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX

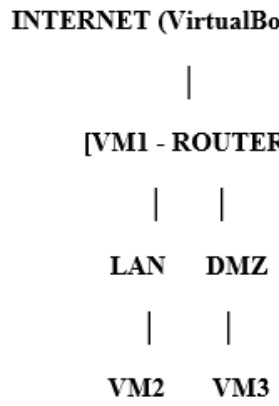
La metodología desarrollada durante la práctica se realizó mediante un entorno virtualizado utilizando Oracle VirtualBox. Inicialmente se configuraron redes Host-Only y NAT para permitir la comunicación entre las diferentes máquinas virtuales.

Posteriormente se implementó Endian Firewall Community utilizando tres interfaces de red correspondientes a las zonas GREEN, RED y ORANGE. Adicionalmente, se configuraron Ubuntu Desktop y Ubuntu Server mediante direccionamiento IP estático utilizando Netplan.

Finalmente, se realizaron pruebas de conectividad y validación de servicios para comprobar el funcionamiento de la arquitectura de red implementada.

4.2 TEMÁTICA 2: CONFIGURACIÓN NAT

Figura 1. Proceso de configuración NAT



Fuente: Autoría Propia

En las redes modernas, la comunicación entre diferentes segmentos (LAN, DMZ Y WAN) se gestiona mediante mecanismos que permiten controla, traducir y asegurar el tráfico de datos. Uno de los más importantes es el Network Address Translation (NAT), que permite que múltiples dispositivos con direcciones IP privadas puedan acceder a redes externas como internet utilizando una única dirección IP publica o de salida. Este proceso optimiza el uso de direcciones IP y también añade una capa básica de seguridad al ocultar la estructura interna de la red.

En ese contexto, la implementación de NAT en un entorno virtualizado con Ubuntu permite simular un escenario real donde se diferencian zonas de red: la LAN (red interna), la DMZ (zona desmilitarizada) y la WAN (red externa simulada). La DMZ se utiliza comúnmente para alojar servicios accesibles desde el exterior (como servidores web), manteniendo aislada la red interna. A través de regla de enrutamiento y traducción de direcciones, se puede controlar el flujo de tráfico entre estas zonas, garantizando conectividad y seguridad.

La actividad tiene como objetivo configurar reglas NAT que permitan la comunicación desde LAN hacia la WAN, así como desde la DMZ hacia internet, verificando además el correcto funcionamiento del reenvió de puestos. Esto permite comprender de forma práctica como operan los dispositivos de red en escenarios reales, fortaleciendo competencias en administración de redes y seguridad informática. La actividad tiene como objetivo configurar reglas NAT que permitan la comunicación desde LAN hacia la WAN, así como desde la DMZ hacia internet, verificando además el correcto funcionamiento del reenvió de puestos. Esto permite comprender de forma práctica como operan los dispositivos de red en escenarios reales, fortaleciendo competencias en administración de redes y seguridad informática.

Escenario Completo:

Tabla 1. distribución de las zonas

Maquina	Función	Red	IP
VM1	Router	WAN + LAN + DMZ	Automático
VM2	Cliente LAN	LAN	192.168.10.1
VM3	Cliente DMZ	DMZ	192.168.20.1

Fuente: Autoría Propia

4.3 TEMÁTICA 3: PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

Para el desarrollo de esta práctica se utilizó una metodología basada en la implementación progresiva de una infraestructura de seguridad en GNU/Linux mediante el uso de virtualización y segmentación de redes. Inicialmente, se realizó el diseño de la arquitectura de red definiendo las zonas de seguridad GREEN, ORANGE y RED, con el propósito de separar la red interna, la zona desmilitarizada (DMZ) y la conexión hacia Internet. Esta distribución permitió establecer un entorno controlado para aplicar políticas de seguridad y monitoreo de tráfico.

se procedió a la creación y configuración de las máquinas virtuales en VirtualBox. Se implementó el firewall Endian como dispositivo central de administración y filtrado de tráfico, asignándole interfaces de red correspondientes a cada zona definida. De igual forma, se configuró un servidor Ubuntu Server ubicado en la zona ORANGE (DMZ), el cual alojó los servicios HTTP y FTP, mientras que Kali Linux fue configurado

como equipo cliente perteneciente a la zona GREEN. Todas las máquinas fueron configuradas con direccionamiento IP estático para garantizar una comunicación estable dentro de la topología de red.

Una vez configuradas las máquinas virtuales y la conectividad básica, se realizó la instalación y activación de los servicios Apache y VSFTPD en Ubuntu Server. Esto permitió disponer de un servidor web y un servidor FTP funcionales para las pruebas de acceso desde la red interna. Posteriormente, se accedió a la interfaz administrativa de Endian Firewall mediante navegador web para realizar la configuración de las reglas de seguridad.

En la etapa de configuración del firewall se implementaron reglas de filtrado específicas. Primero, se creó una política que permitió el tráfico HTTP desde la red GREEN hacia el servidor Ubuntu en la zona ORANGE utilizando el puerto 80. Después, se configuró una segunda regla para habilitar el servicio FTP mediante el puerto 21. Estas reglas fueron definidas bajo políticas de acceso controlado, permitiendo únicamente los servicios necesarios entre las zonas de seguridad.

se implementó una regla de denegación para el protocolo ICMP con el fin de bloquear las solicitudes de ping entre las redes. Esta medida permitió fortalecer la seguridad de la infraestructura evitando mecanismos básicos de reconocimiento y detección de equipos dentro de la red.

se realizaron pruebas de funcionamiento y validación de las configuraciones implementadas. Desde Kali Linux se verificó el acceso correcto a los servicios HTTP y FTP alojados en Ubuntu Server, así como la restricción del protocolo ICMP. Complementariamente, se revisaron los logs y registros generados por Endian Firewall para comprobar que el tráfico autorizado era aceptado y que las conexiones bloqueadas eran registradas correctamente. De esta manera, se confirmó el adecuado funcionamiento de las políticas de seguridad implementadas en la práctica.

4.4 TEMÁTICA 4: REGLAS DE ACCESO PARA EPRMITIR O DENEGAR EL TRAFICO

La metodología aplicada en esta temática consistió en la configuración de reglas de control de acceso en Endian Firewall Community 3.3.2 desde el panel de administración web, accediendo mediante la dirección https://192.168.0.1:10443 desde la estación de trabajo de la zona LAN.

Inicialmente se configuraron las reglas de tráfico Inter-Zona en la sección Firewall, Inter-Zone Traffic, creando dos reglas que permiten la comunicación entre la zona Verde (LAN) y la zona Naranja (DMZ) mediante los protocolos HTTP en el puerto 80 y FTP en el puerto 21, aplicando política ALLOW sobre el tráfico TCP entre ambas zonas.

Posteriormente se configuraron reglas de Port Forwarding y Destination NAT en la sección Firewall, Port Forwarding / NAT, estableciendo el reenvío del tráfico entrante desde Internet en los puertos 80 y 21 hacia el servidor DMZ en la dirección 172.16.1.10, permitiendo la publicación controlada de los servicios web y FTP hacia redes externas.

Finalmente, se realizaron pruebas de conectividad desde el navegador Firefox y la terminal de las máquinas virtuales, verificando el acceso HTTP y FTP entre todas las zonas definidas en la infraestructura y documentando los resultados obtenidos con fecha y hora como evidencia del funcionamiento de las reglas configuradas.

4.5 TEMÁTICA 5: IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE) CON POLITICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET

La metodología aplicada en esta práctica se basó en la implementación de servicios de seguridad de capa de aplicación sobre un entorno virtualizado en Oracle VirtualBox. Inicialmente, se procedió con la configuración de las interfaces de red del Endian Firewall, asegurando el aislamiento de los segmentos mediante la definición de zonas GREEN (Red Local), ORANGE (DMZ) y RED (WAN/Internet).

Posteriormente, se realizó el aprovisionamiento del servicio HTTP Proxy en modo no transparente, configurando el puerto 8080 y estableciendo un esquema de autenticación local mediante la creación de una base de datos de usuarios en el firewall. Para el control de navegación, se implementaron perfiles de filtrado de contenido (Web Filter) y políticas de acceso (Access Policies) basadas en listas negras (Blacklists) para restringir dominios específicos como YouTube y Hotmail.

Finalmente, se realizó la configuración del cliente Lubuntu mediante direccionamiento IP estático y la parametrización manual del navegador Firefox. La validación de la arquitectura se efectuó mediante pruebas de interceptación de tráfico, verificación de credenciales de usuario y comprobación de la efectividad del bloqueo de dominios prohibidos.

5 DESARROLLO DE LAS TEMATICAS IMPLEMENTADAS

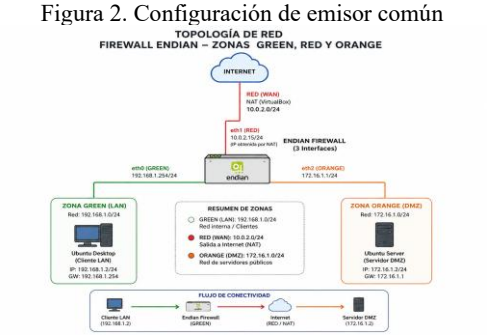
La presente investigación fue desarrollada tomando como base las cinco temáticas establecidas en la guía de aprendizaje de la Etapa 7 Implementando Seguridad en GNU/Linux, las cuales permitieron implementar mecanismos de seguridad perimetral utilizando GNU/Linux Endian Firewall Community en un entorno virtualizado.

5.1 TEMÁTICA 1: CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX

5.1.1 TOPOLOGÍA DE RED

La arquitectura se dividió en tres zonas: RED para la conexión WAN mediante NAT, GREEN para la red LAN interna y ORANGE para la DMZ donde se alojó el servidor Ubuntu Server. Esta segmentación permitió aislar servicios y mejorar la seguridad de la infraestructura.

Figura 2. Configuración de emisor común



Fuente: Autoría Propia

5.1.2 CREACIÓN DE REDES VIRTUALES

En VirtualBox se configuraron redes Host-Only y NAT para separar correctamente las zonas GREEN, RED y ORANGE. Cada segmento de red fue asignado de acuerdo con su función dentro de la arquitectura implementada.

Figura 3. Creación de redes virtuales en VirtualBox

Fuente: Autoría Propia

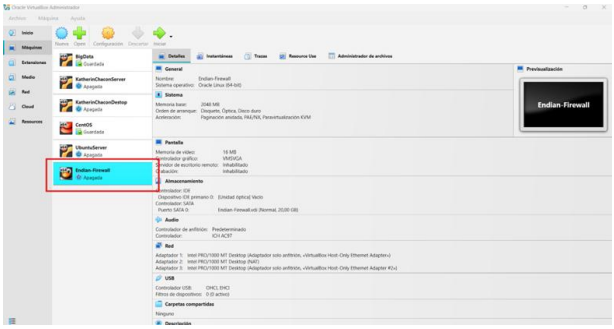
5.1.3 CREACIÓN DE MAQUINA VIRTUAL ENDIAN

Se creó una máquina virtual con sistema operativo Linux, 2 GB de RAM, 20 GB de disco duro y tres adaptadores de red. Esta VM fue destinada a la instalación del firewall GNU/Linux Endian Firewall Community.

Figura 4. Creación de máquina virtual de Endian

Fuente: Autoría Propia

Figura 5. Finalización de creación de máquina virtual Endian



Fuente: Autoría Propia

5.1.4 CONFIGURACION DE ADAPTADORES DE RED

Se configuraron tres interfaces virtuales: GREEN para la LAN, RED para Internet y ORANGE para la DMZ. Esta distribución permitió separar el tráfico de red y administrar adecuadamente las comunicaciones.

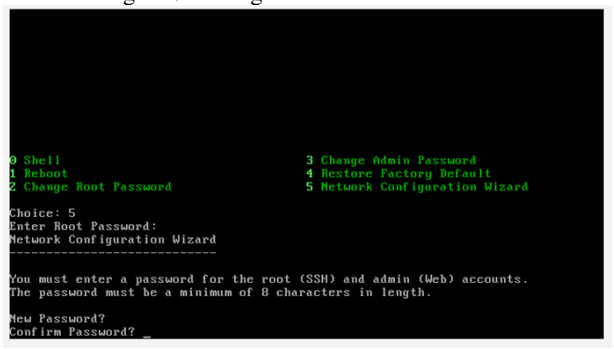
Figura 6. Configurar redes en máquina virtual Endian

Fuente: Autoría Propia

5.1.5 INSTALACIÓN Y CONFIGURACION DE ENDIAN

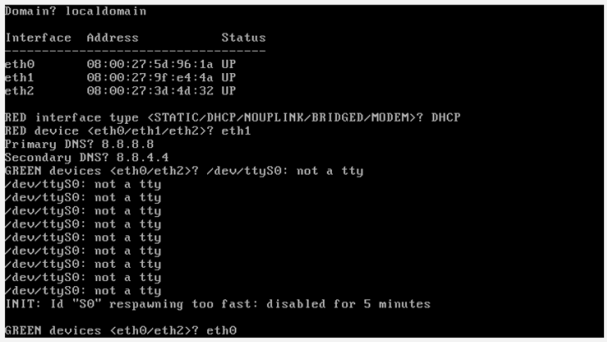
Durante la instalación se configuraron la contraseña de administrador, las interfaces de red y el acceso SSH. Además, se asignaron direcciones IP específicas a las zonas GREEN y ORANGE, mientras que la interfaz RED obtuvo su configuración mediante DHCP.

Figura 7. Configurar contraseña en Endian



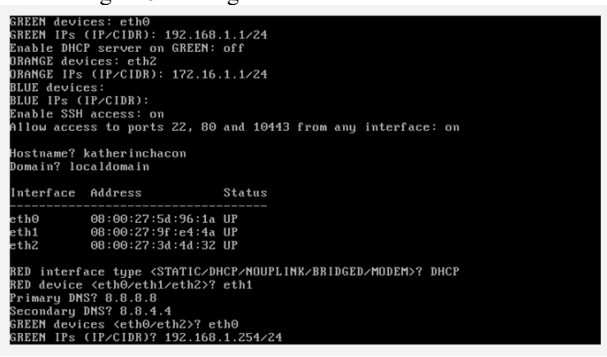
Fuente: Autoría Propia

Figura 8. Configuración de la interfaz RED



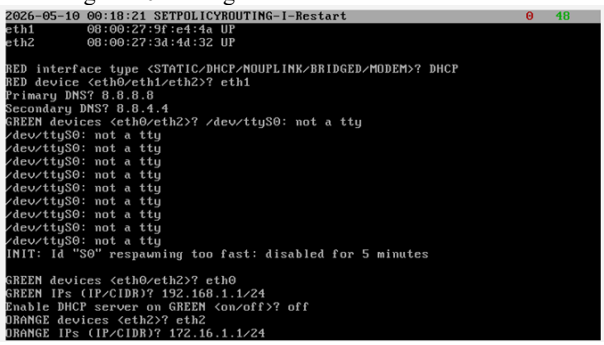
Fuente: Autoría Propia

Figura 9. Configuración de la interfaz GREEN



Fuente: Autoría Propia

Figura 10. Configuración de la interfaz ORANGE

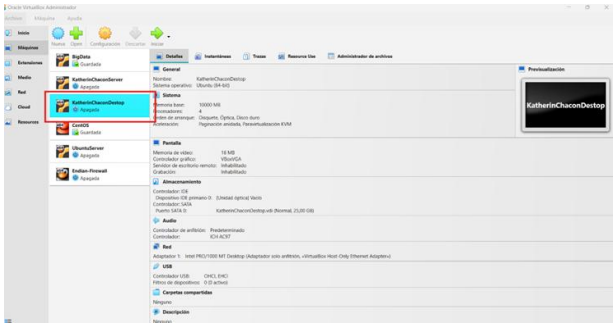


Fuente: Autoría Propia

5.1.6 CONFIGURACIÓN DE UBUNTU DESKTOP Y UBUNTU SERVER

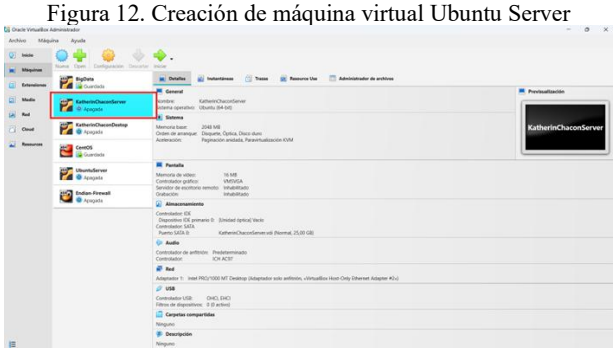
Se implementó Ubuntu Desktop en la zona GREEN y Ubuntu Server en la zona ORANGE utilizando direccionamiento IP estático mediante Netplan. Estas configuraciones permitieron establecer comunicación adecuada entre clientes y servidores.

Figura 11. Creación de máquina virtual Ubuntu Desktop



Fuente: Autoría Propia

Figura 12. Creación de máquina virtual Ubuntu Server



Fuente: Autoría Propia

5.1.7 ACCESO A LA INTERFAZ WEB DE ENDIAN

Desde Ubuntu Desktop se accedió al panel administrativo de Endian mediante HTTPS. Allí se realizó el registro inicial, activación de cuenta y autenticación administrativa para gestionar el firewall.

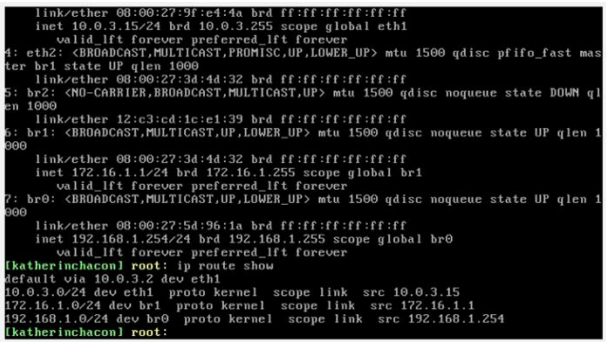
Figura 13. Acceso a Dashboard de Endian

Fuente: Autoría Propia

5.1.8 VERIFICACIÓN DE INTERFACES Y CONECTIVIDAD

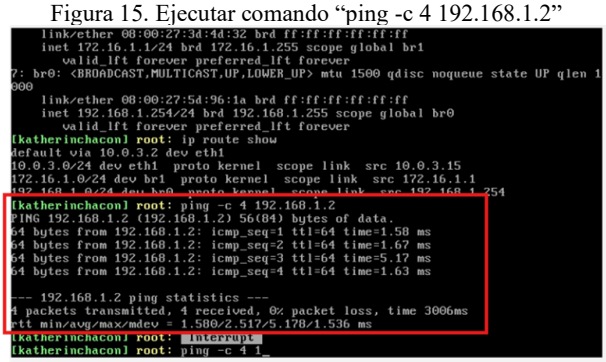
Se utilizaron comandos como ip addr show, ip route show y ping para validar la configuración de interfaces, el enrutamiento y la conectividad entre las diferentes zonas de red y el acceso a Internet.

Figura 14. Ejecutar comando “ip addr show”



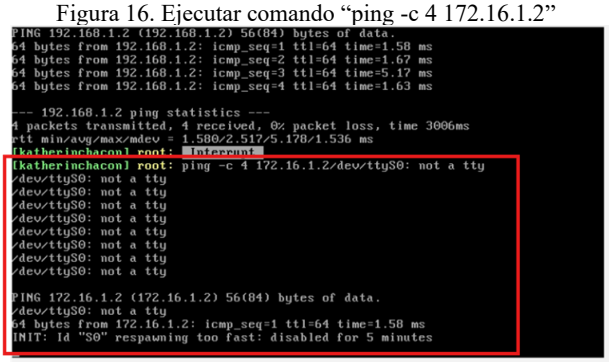
Fuente: Autoría Propia

Figura 15. Ejecutar comando “ping -c 4 192.168.1.2”



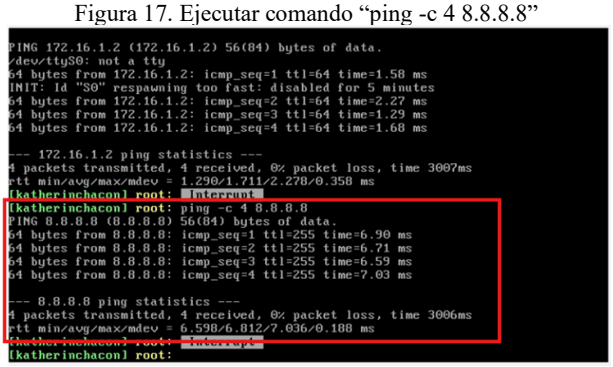
Fuente: Autoría Propia

Figura 16. Ejecutar comando “ping -c 4 172.16.1.2”



Fuente: Autoría Propia

Figura 17. Ejecutar comando “ping -c 4 8.8.8.8”



Fuente: Autoría Propia

5.2 TEMÁTICA 2: CONFIGURACIÓN NAT

5.2.1 CONFIGURACION DE RED

En este paso se configuran las tres interfaces de red del router, asignando a cada una un rol especifico: WAN para acceso a Internet, LAN para la red interna y DMZ para servicios expuestos. Esta separación permite controlar el tráfico entre redes y aplicar reglas de seguridad. Además, al definir direcciones IP estáticas en LAN y DMZ, se garantiza estabilidad en la comunicación. Esta configuración es la base para implementar NAT y enrutamiento. Sin este esquema, no sería posible segmentar correctamente la red.

> sudo nano /etc/netplan/*.yaml

network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: true
    enp0s8:
      addresses:
192.168.10.1/24
    enp0s9:
192.168.20.1/24

> sudo netplan apply

Figura 18. Proceso de configuración de red

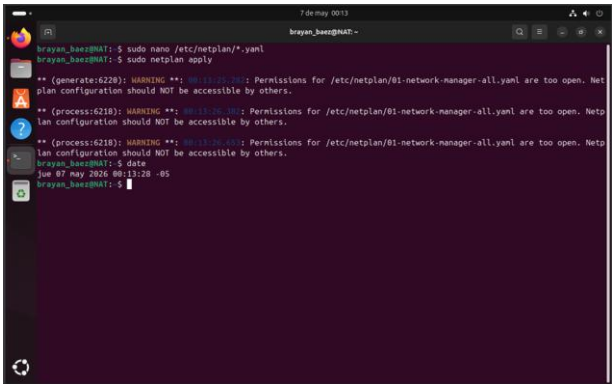
Fuente: Autoría Propia

Figura 19. Proceso de configuración de red

Fuente: Autoría Propia

.

Figura 20. Proceso de configuración de red



Fuente: Autoría Propia

5.2.2 ACTIVAR IP FORWARDING

El IP forwarding permite que el sistema funcione como un router, reenviando paquetes entre diferentes interfaces de red. Por defecto, Linux no realiza esta función, ya que está diseñado como host final. Al habilitar esta opción, el sistema puede recibir paquetes por una interfaz y enviarlos por otra.

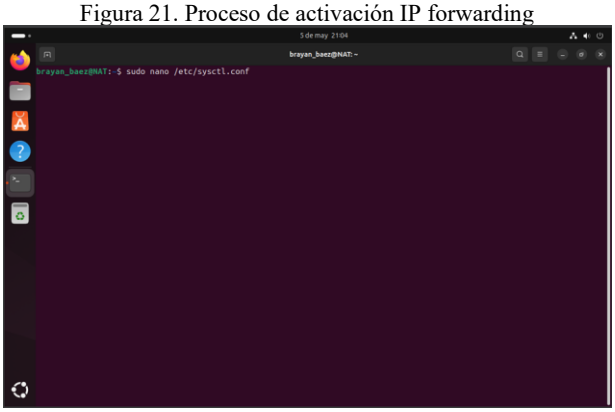
Esto es esencial para que la LAN y la DMZ puedan comunicarse con la WAN. Sin este paso, las reglas NAT no tendrían efecto real. En términos prácticos, convierte la maquina en un dispositivo de interconexión de redes.

> sudo nano /etc/sysctl.conf

net.ipv4.ip_forward=1

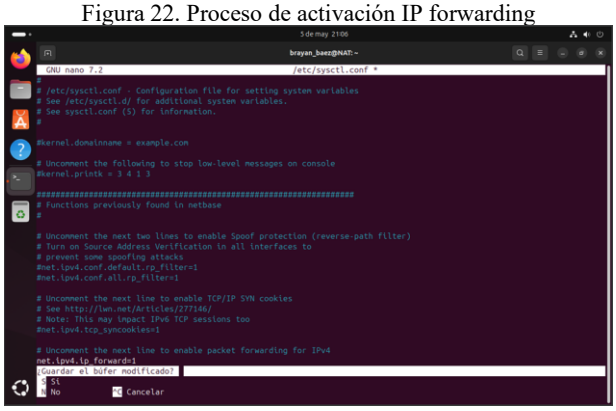
> sudo sysctl –p

Figura 21. Proceso de activación IP forwarding



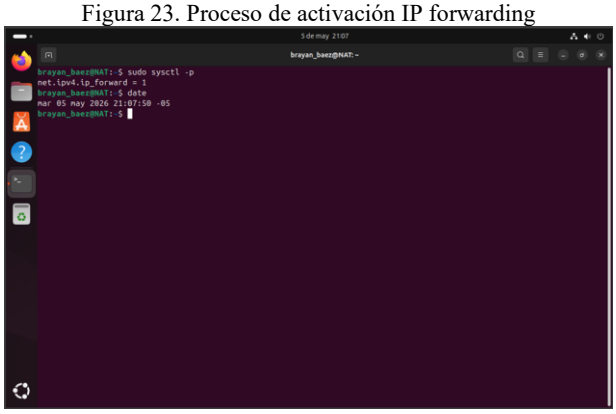
Fuente: Autoría Propia

Figura 22. Proceso de activación IP forwarding



Fuente: Autoría Propia

Figura 23. Proceso de activación IP forwarding



Fuente: Autoría Propia

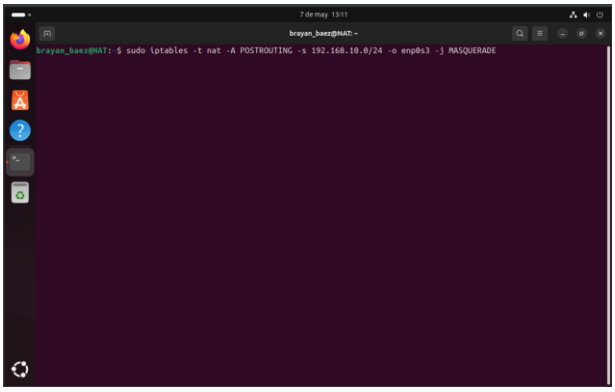
5.2.3 CONFIGURAR NAT PARA LA LAN Y DMZ

En este paso se configura NAT para permitir que los equipos de la LAN accedan a internet. La regla MASQUERADE traduce las direcciones IP privadas a la IP pública del router, permitiendo la comunicación externa. Además, se habilita el tráfico de salida y el entorno de respuesta, garantizando conectividad bidireccional. Este mecanismo es el mismo que utilizan los routers domésticos. También añade una capa básica de seguridad al ocultar la red interna. Es un paso fundamental para la conectividad de la LAN.

NAT para la LAN hacia Internet
> sudo iptables -t nat -A POSTROUTING -s 192.168.10.0/24 -o enp0s3 -j MASQUERADE

NAT para la DMZ hacia Internet
> sudo iptables -t nat -A POSTROUTING -s 182.168.20.0/24 -o enp0s3 -j MASQUERADE

Figura 24. Proceso de configuración NAT para LAN y DMZ



Fuente: Autoría Propia

Figura 25. Proceso de configuración NAT para LAN y DMZ

Fuente: Autoría Propia

5.2.4 CONFIGURAR CLIENTE LAN

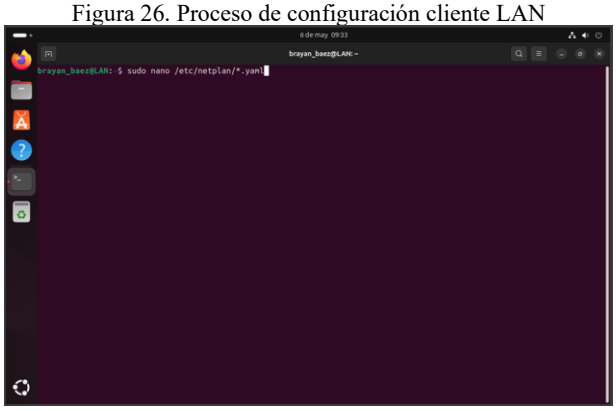
Aquí se configura el cliente de la red LAN con una dirección IP estática dentro del mismo segmento que el router. Se define como puerta de enlace la IP del router, lo que permite que el tráfico salga hacia otras redes. También se establece un servidor DNS para la resolución de nombres. Esta configuración simula un equipo real dentro de una red interna empresarial. Es importante que los parámetros coincidan con los del router para asegurar conectividad. Sin esto, el cliente no podria acceder a internet.

> sudo nano /etc/netplan/*.yaml

```
network:
  version: 2
  ethernets:
    enp0s3:
      addresses: [192.168.10.10/24]
      routes:
        - to:
          via: 192.168.10.1
      nameservers:
        addresses: [8.8.8.8, 1.1.1.1]
```

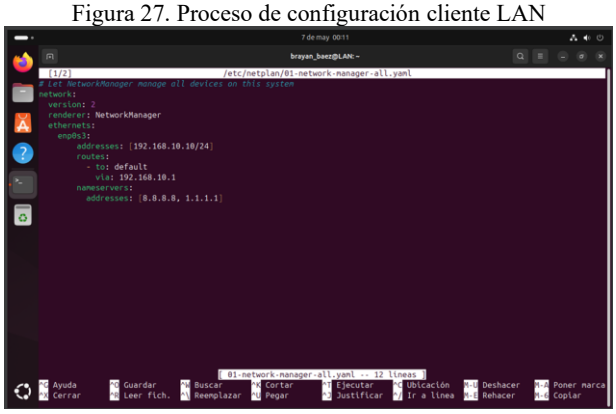
> sudo netplan apply

Figura 26. Proceso de configuración cliente LAN



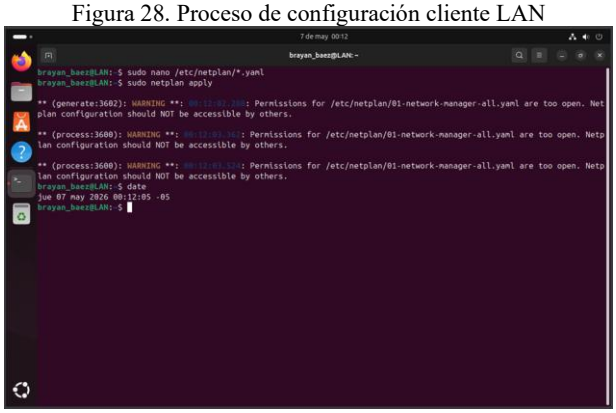
Fuente: Autoría Propia

Figura 27. Proceso de configuración cliente LAN



Fuente: Autoría Propia

Figura 28. Proceso de configuración cliente LAN



Fuente: Autoría Propia

5.2.5 VERIFICAR LAN → INTERNET

Este paso valida que la configuración NAT aplicada en el router funciona correctamente para la LAN. Al hacer ping a una dirección externa, se comprueba que los paquetes salen de la red interna y reciben respuesta. Además, al usar un dominio, se verifica que el servicio DNS está operativo. Esta prueba es fundamental para detectar errores de configuración. Si funciona, significa que la LAN tiene acceso completo a internet. Es una verificación básica pero crucial en redes.

> ping 8.8.8.8

> ping google.com

Figura 29. Proceso de verificación LAN a Internet

Fuente: Autoría Propia

5.2.6 CONFIGURAR CLIENTE/SERVIDOR DMZ

Aquí se configura la maquina ubicada en la DMZ, asignándole una dirección IP dentro de su segmento de red. Se establece como gateway la interfaz DMZ del router, permitiendo la salida hacia internet. Tambien se configura un DNS para resolver nombres de dominio. Esta máquina puede representar un servidor web o de servicios. Es importante que esté correctamente configurada para probar las reglas NAT. Este paso permite simular un entorno empresarial real con servicios expuestos.

> sudo nano /etc/netplan/*.yaml

```
network:
  version: 2
  ethernets:
    enp0s3:
      addresses: [192.168.20.10/24]
      routes:
        - to: default
          via; 192.168.20.1
      nameservers:
        addresses: [8.8.8.8, 1.1.1.1]
sudo netplan apply
```

> sudo netplan apply

Figura 30. Proceso de configuración cliente-servidor DMZ

Fuente: Autoría Propia

Figura 31. Proceso de configuración cliente-servidor DMZ

Fuente: Autoría Propia

Figura 32. Proceso de configuración cliente-servidor DMZ

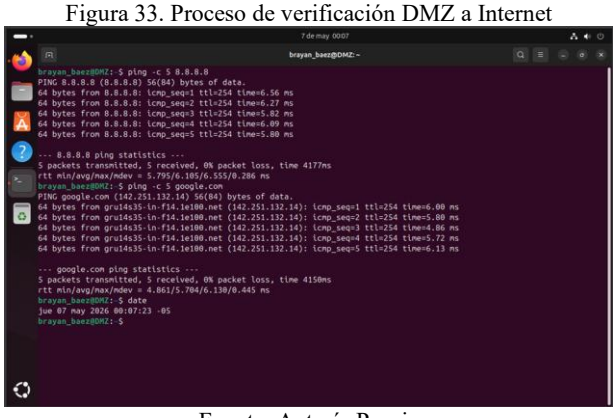
Fuente: Autoría Propia

5.2.7 VERIFICAR DMZ → INTERNET

Este paso comprueba que la DMZ tiene acceso a internet las reglas configuradas en el router. Al realizar pruebas de conectividad, se valida que el tráfico sale correctamente y regresa sin problemas. Esto confirma que el NAT está funcionando también para zona. Es importante porque muchos servicios en la DMZ requieren conectividad externa. Además, ayuda a detectar errores en las reglas de firewall. Si funciona la configuración es correcta.

> ping 8.8.8.8
> ping google.com

Figura 33. Proceso de verificación DMZ a Internet



Fuente: Autoría Propia

5.2.8 VERIFICAR REGLAS → NAT

En este último paso se revisan las reglas NAT configuradas en el sistema para verificar su correcto funcionamiento. Este comando permite visualizar las reglas activas y su comportamiento. Se pueden identificar las reglas de salida (POSTROUTING) y entrada (PREROUTING). Además, muestras estadísticas de tráfico que ayudan a validar su uso. Esta verificación es importante para detectar errores e inconsistencias. Es una práctica común en la administración de redes para asegurar que todo funciona correctamente.

> sudo iptables -t nat -L -n -v

Figura 34. Proceso de verificación de reglas NAT

Fuente: Autoría Propia

5.3 TEMÁTICA 3: PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

De acuerdo a lo establecido en temáticas anteriores se tiene:

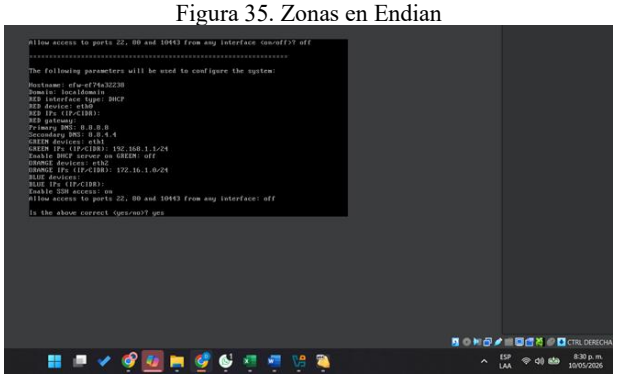
Tabla 2. distribución de las zonas

Zona	Función	Red	Máquina
GREEN	LAN interna	192.168.1.0/24	Kali
ORANGE	DMZ	172.16.1.0/24	Ubuntu Server
RED	Internet/WAN	Red NAT de VirtualBox	Endian hacia Internet

Fuente: Autoría Propia

En endian se configuran las zonas de acuerdo a esta información, como evidencia está la siguiente imagen donde se observa claramente las ips asignadas a cada zona

Figura 35. Zonas en Endian



Fuente: Autoría Propia

El paso siguiente es configurar Ubuntu server, para ello es importante tener en cuenta que el adaptador a usar debe contar con estas características.

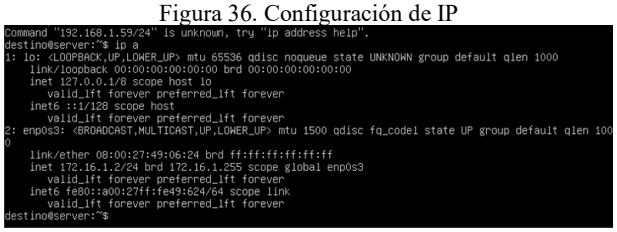
Tabla 3. Adaptadores de red

Adaptador	***Configuración***
Adaptador 1	*Red interna*
Nombre	*ORANGE*

Fuente: Autoría Propia

La IP asignada debe coincidir con la configurada en Endian, como se observa a continuación

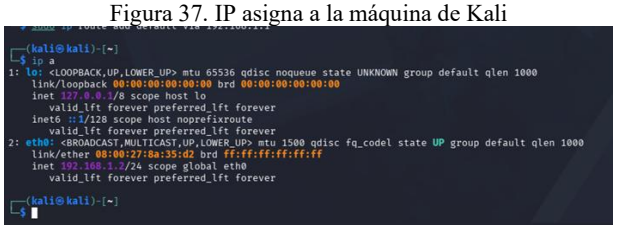
Figura 36. Configuración de IP



Fuente: Autoría Propia

Siguiendo los mismos pasos, se asigna la ip a la red Green que va a ser representada por un sistema Kali Linux, dicho dispositivo tiene adaptador por red interna “green”

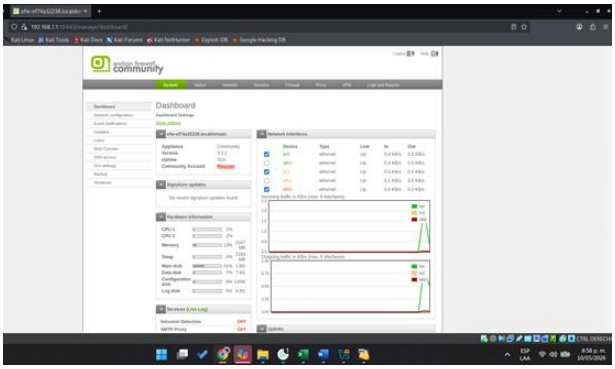
Figura 37. IP asigna a la máquina de Kali



Fuente: Autoría Propia

Ahora se ingresa a la red por medio de la dirección https://192.168.1.1:10443 se observa la interfaz del firewall

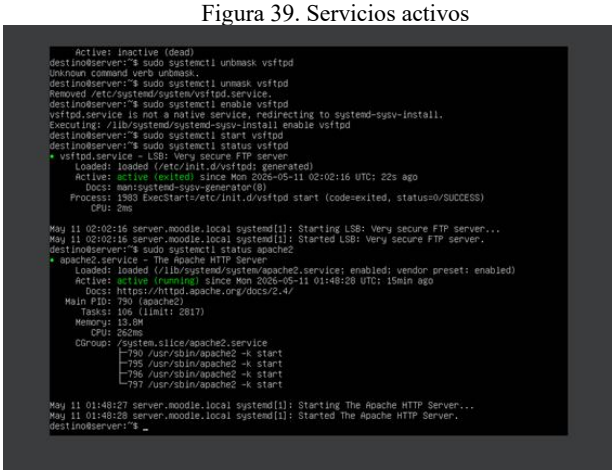
Figura 38. Interfaz gráfica del firewall



Fuente: Autoría Propia

En el servidor se debe contar con los servicios de apache y vstfpd activos como se observa

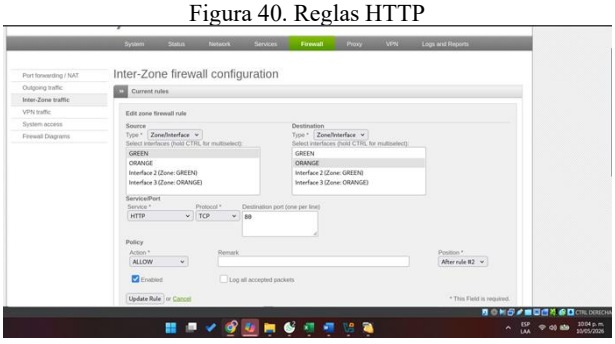
Figura 39. Servicios activos



Fuente: Autoría Propia

5.3.1 CONFIGURACIÓN DE LA REGLA HTTP

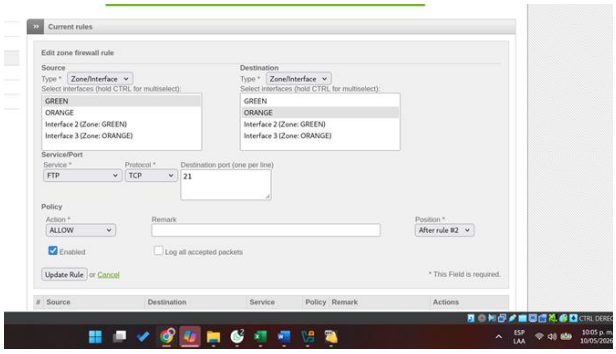
Figura 40. Reglas HTTP



Fuente: Autoría Propia

Se realiza la regla para FTP

Figura 41. Reglas FTP



Fuente: Autoría Propia

Durante la práctica se implementaron reglas de filtrado dentro del firewall Endian con el propósito de controlar el acceso entre la red interna GREEN y la zona ORANGE (DMZ). Estas reglas permitieron aplicar políticas de seguridad específicas sobre los protocolos autorizados y restringidos.

La primera regla configurada correspondió al servicio HTTP. Esta regla permitió el tráfico TCP desde la zona GREEN hacia el servidor Ubuntu ubicado en la DMZ utilizando el puerto 80. Gracias a esta configuración, los equipos de la red interna pudieron acceder correctamente al servidor web mediante navegador o utilizando herramientas como curl. La finalidad de esta regla fue habilitar el acceso controlado al servicio web alojado en Ubuntu Server.

se creó una segunda regla para permitir el servicio FTP utilizando el puerto 21. Esta configuración permitió establecer conexiones FTP desde la red GREEN hacia el servidor Ubuntu en la zona ORANGE. De esta manera, fue posible realizar pruebas de acceso y comunicación utilizando clientes FTP desde Kali Linux, verificando el correcto funcionamiento del servicio y la política de filtrado aplicada.

se implementó una regla de denegación para el protocolo ICMP. Esta regla tuvo como objetivo bloquear las solicitudes de tipo Echo Request, evitando así la utilización del comando ping entre los equipos de la red. Con esta configuración se incrementó el nivel de seguridad de la infraestructura, limitando la detección y reconocimiento de hosts dentro de la red interna y la DMZ.

se verificó el funcionamiento de todas las reglas mediante las herramientas de monitoreo y logs incluidas en Endian Firewall. En los registros se observó el tráfico permitido correspondiente a HTTP y FTP bajo acciones ACCEPT, así como el tráfico ICMP bloqueado bajo acciones DROP, confirmando el correcto comportamiento de las políticas implementadas.

5.4 TEMÁTICA 4: REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRAFICO

La cuarta temática consistió en la configuración de reglas de acceso en Endian Firewall Community 3.3.2 para controlar y permitir el tráfico entre las zonas Verde (LAN), Naranja (DMZ) y Roja (Internet), mediante la creación de políticas de firewall basadas en los protocolos HTTP y FTP.

Para la comunicación entre la zona Verde y la zona Naranja se crearon dos reglas de tráfico Inter-Zona en la sección Firewall → Inter-Zone Traffic, permitiendo el acceso HTTP en el puerto 80 y FTP en el puerto 21 desde la red LAN hacia el

servidor Apache2 ubicado en la DMZ, con política ALLOW sobre el protocolo TCP.

Para la comunicación entre Internet y la zona DMZ se configuraron reglas de Port Forwarding y Destination NAT, redirigiendo el tráfico entrante desde cualquier dirección de Internet en los puertos 80 y 21 hacia el servidor DMZ en la dirección 172.16.1.10, publicando de forma controlada los servicios web y FTP hacia redes externas.

Tabla 4. Reglas de acceso configuradas en Endian Firewall

Tipo de Regla	Origen	Destino	Puerto	Protocolo	Política
Inter-zone	Green	Orange	80	TCP	Allow
Inter-zone	Green	Orange	21	TCP	Allow
Port Forwarding	Uplink ANY	172.16.1.10	80	TCP	NAT

Fuente: Autoría Propia

5.5 TEMÁTICA 5: IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE) CON POLITICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET

5.5.1 CONFIGURACIÓN DEL ENTORNO VIRTUALIZADO

Para la simulación del escenario, se empleó el hipervisor Oracle VM VirtualBox. La infraestructura se fundamenta en el despliegue de un appliance Endian UTM Firewall, el cual fue provisto de tres interfaces de red lógicas para segmentar el tráfico: una interfaz en modo NAT para el acceso a redes externas (Zona RED) y dos interfaces en modo "Red Interna" para la gestión de la red de área local (Zona GREEN) y la zona desmilitarizada (Zona ORANGE). Se integró una estación de trabajo Lubuntu vinculada al segmento GREEN para las pruebas de validación.

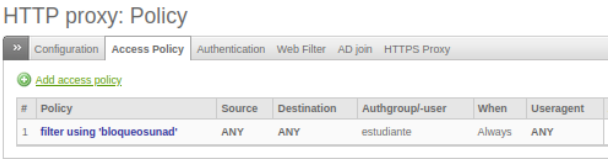
Figura 42. configuración de red en VirtualBox donde se visualicen los tres adaptadores del Firewall.

Fuente: Autoría Propia

5.5.2 PARAMETRIZACIÓN DEL FIREWALL ENDIAN

Se procedió con la configuración del servicio HTTP Proxy bajo el esquema de funcionamiento No Transparente, utilizando el puerto de escucha 8080. El control de acceso se basó en una política de autenticación local, vinculando un perfil de usuario específico para la validación de credenciales. Asimismo, se implementó un perfil de filtrado de contenido (Web Filter) donde se definieron listas negras (Blacklists) para restringir el acceso a los dominios de alto consumo de ancho de banda o externos a la operación: youtube.com, hotmail.com y elnuevodia.com.co.

Figura 43. interfaz de administración de Endian, específicamente en la sección Proxy > HTTP > Access Policy, mostrando la regla de denegación y los dominios afectados.

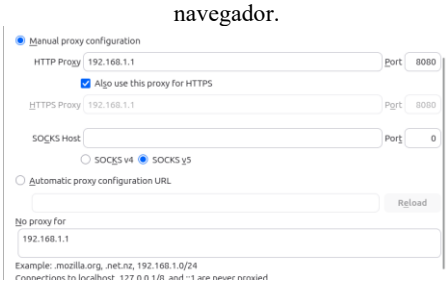


Fuente: Autoría Propia

5.5.3 CONFIGURACIÓN Y APROVISIONAMIENTO DEL CLIENTE

En el host cliente (Lubuntu), se realizó la configuración de red estática dentro del segmento 192.168.1.0/24. Para garantizar la interoperabilidad con el firewall, se configuró manualmente el navegador Mozilla Firefox, direccionando las peticiones de red hacia el Gateway de seguridad (192.168.1.1). Esta configuración asegura que el tráfico web sea interceptado y analizado por el proxy antes de ser conmutado hacia la zona WAN.

Figura 44. ventana de configuración del proxy en el navegador.



Fuente: Autoría Propia

5.5.4 PRUEBAS DE VALIDACIÓN Y FUNCIONAMIENTO

Se ejecutaron pruebas de estrés y validación para confirmar la integridad de las políticas de seguridad:

Validación de Identidad: Se verificó la interrupción de la sesión de navegación para la solicitud de credenciales de usuario.

Filtrado de Dominios: Se comprobó la eficacia de la lista negra; al intentar acceder a los dominios restringidos, el sistema generó un paquete de respuesta tipo "Access Denied" originado por el Firewall.

Conectividad Permitida: Se validó el acceso exitoso a recursos web no listados en las restricciones, confirmando el correcto enrutamiento del tráfico.

Figura 45. mensaje de bloqueo generado por Endian al intentar acceder a un sitio no permitido

Fuente: Autoría Propia

6 CONCLUSIONES

La implementación de Endian Firewall Community permitió establecer una infraestructura de seguridad perimetral eficiente mediante la segmentación de las zonas LAN, WAN y DMZ, garantizando la protección de los servicios y recursos críticos de la red.

Asimismo, la configuración de reglas NAT, políticas de firewall y restricciones de tráfico facilitó el control de acceso entre las diferentes zonas, permitiendo únicamente las comunicaciones autorizadas y fortaleciendo la seguridad de la infraestructura. De igual manera, la habilitación de servicios HTTP y FTP en la zona DMZ evidenció la importancia de aplicar mecanismos de administración y monitoreo en servidores GNU/Linux para reducir riesgos de acceso no autorizado.

La implementación de reglas de acceso Inter-Zona en Endian Firewall Community permitió establecer comunicación controlada entre las zonas LAN, DMZ e Internet mediante los protocolos HTTP y FTP, demostrando que la correcta configuración de políticas de firewall garantiza la exposición segura de servicios hacia redes externas sin comprometer la integridad de la red interna. La segmentación mediante zonas GREEN, ORANGE y RED, combinada con reglas de Port Forwarding y Destination NAT, constituyó un mecanismo eficiente para publicar los servicios del servidor DMZ hacia Internet de forma transparente y controlada, fortaleciendo la arquitectura de seguridad perimetral de la infraestructura implementada.

Además, la implementación del proxy HTTP con autenticación de usuarios y filtrado web mediante listas negras permitió mejorar las políticas de navegación y control de acceso a Internet.

Finalmente, el desarrollo de todas las configuraciones desde consola contribuyó al fortalecimiento de competencias técnicas en administración de sistemas GNU/Linux y gestión de servicios de red, cumpliendo con los lineamientos establecidos en la guía de actividades.

7 REFERENCIAS

[1] *Stallings, W. (2018). Network Security Essentials: Applications and Standards (6th ed.). Pearson. https://api.pageplace.de/preview/DT0400.9781292154916_A37747529/preview-9781292154916_A37747529.pdf*

[2] *Endian SRL. (n.d.). Free open source firewall for home networks | Europe | EndiaN. https://www.endian.com/en/community/*

[3] *Smith, J., & Nair, R. (2005). Virtual Machines: Versatile Platforms for Systems and Processes. Elsevier. https://ndl.ethernet.edu.et/bitstream/123456789/42492/1/14.pdf*

[4] *Belen. (2023, March 31). Zona DMZ: la zona segura de la red a salvo de intrusos. Tecnozero Soluciones Informaticas. https://www.tecnozero.com/blog/zona-dmz-zona-segura-contra-intrusos/*

[5] *Markova, V., & Markova, V. (2026, April 30). What is ICMP (Internet Control Message Protocol)? ClouDNS Blog. https://www.cloudns.net/blog/what-is-icmp-internet-service-message-protocol/*

[6] *Apache Software Foundation, "Apache HTTP Server Documentation Version 2.4," Apache Software Foundation, 2023. [Online]. Available: https://httpd.apache.org/docs/2.4/*

[7] *Canonical Ltd., "Ubuntu Server Guide — Network Configuration," Canonical Ltd., 2023. [Online]. Available: https://ubuntu.com/server/docs/network-configuration*

[8] *Linux Professional Institute, "LPIC-1 Exam 101: Topic 109 — Fundamentals of Internet Protocols," Linux Professional Institute, 2022. [Online]. Available: https://learning.lpi.org/es/learning-materials/101-500/109/*

[9] *Internet Engineering Task Force, "RFC 959: File Transfer Protocol (FTP)," IETF, Oct. 1985. [Online]. Available: https://www.rfc-editor.org/rfc/rfc959*

[10] *Internet Engineering Task Force, "RFC 2663: IP Network Address Translator (NAT) Terminology and Considerations," IETF, Aug. 2000. [Online]. Available: https://www.rfc-editor.org/rfc/rfc2663*