# IMPLEMENTACIÓN COLABORATIVA DE SEGURIDAD PERIMETRAL MEDIANTE LA CONFIGURACIÓN DE UNA DMZ UTILIZANDO ENDIAN FIREWALL Y PLATAFORMAS GNU/LINUX

Juan José Bocanegra Vergara
e-mail: jjbocanegrav@unadvirtual.edu.co
Rodrigo Hernando Martínez Romero
e-mail: rhmartinezr@unadvirtual.edu.co
Karol Jiseth Martínez Páez
E-mail: kjmartinezpae@unadvirtual.edu.co
Andrés Camilo Calderón Ciro
e-mail: accalderonci@unadvirtual.edu.co
David Santiago Montoya
e-mail: dsantiagom@unadvirtual.edu.co

**RESUMEN:** *El presente trabajo se centra en la implementación de un entorno seguro de red mediante el uso de la distribución GNU/Linux Endian Firewall (EFW) para proteger los servidores y servicios críticos alojados en una arquitectura LAN, WAN y DMZ. A través de un proceso colaborativo, cada integrante realiza la instalación, configuración y validación de servicios clave usando Endian como solución de seguridad perimetral, permitiendo controlar el acceso interno y externo, aplicar reglas de filtrado y traducir direcciones mediante NAT. El proyecto abarca la creación de zonas de seguridad, la administración de puertos y servicios, y el uso de proxy para fortalecer el control de navegación, asegurando la integridad y disponibilidad de aplicaciones y bases de datos corporativas.*

**PALABRAS CLAVE**: Seguridad perimetral, DMZ, Endian Firewall, GNU/Linux, NAT, Proxy, LAN/WAN, Acceso controlado, Filtrado de tráfico, Infraestructura protegida.

## 1 INTRODUCCIÓN

La seguridad de la información en entornos empresariales requiere mecanismos sólidos que permitan minimizar riesgos asociados a accesos no autorizados, ataques externos y fallas en la disponibilidad de servicios. Para ello, las redes deben diseñarse con zonas de seguridad diferenciadas y sistemas de firewall perimetral capaces de controlar y monitorear el tráfico entrante y saliente. En el contexto académico y profesional, se plantea la implementación de un esquema de red bajo GNU/Linux utilizando Endian Firewall (EFW) como herramienta principal de protección, acompañada de servicios hospedados en una DMZ que permitan asegurar aplicaciones web y bases de datos. Este proyecto se desarrolla de forma colaborativa, aplicando conceptos prácticos de gestión de servidores, redes y ciberseguridad.

## 2 CARACTERISITICAS GENERALES

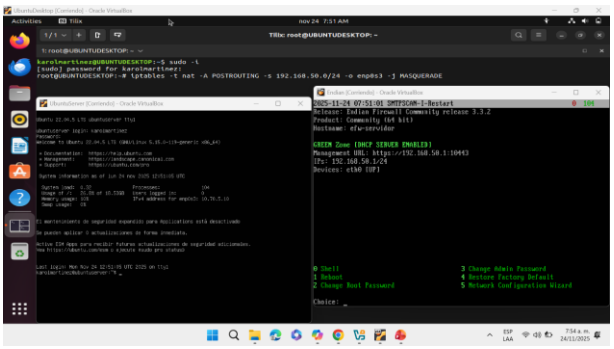
1. Modelo de Seguridad Perimetral Basado en Segmentación de Red:
   El diseño de la infraestructura incluye tres zonas de seguridad diferenciadas mediante Endian Firewall:
   - Zona Verde (LAN): Área interna y de uso exclusivo de los equipos de trabajo.
   - Zona Roja (WAN): Acceso a Internet y redes externas no confiables.
   - Zona Naranja (DMZ): Segmento aislado donde residen los servicios públicos expuestos, tales como aplicaciones web y bases de datos.
2. Uso de GNU/Linux como Base Tecnológica:
   Los servicios de red, servidores y estaciones de trabajo se configuran bajo sistemas operativos de código abierto, lo cual permite flexibilidad, escalabilidad, personalización y seguridad mediante herramientas libres.
3. Firewall UTM (Unified Threat Management):
   Endian Firewall integra diversas funcionalidades de seguridad en un solo dispositivo, tales como:
   - Control de tráfico
   - NAT y reenvío de puertos
   - Filtrado de contenido
   - IDS/IPS
   - Proxy con autenticación
   - VPN
4. Administración Centralizada de Políticas de Acceso y Filtrado:
   Desde la interfaz de administración de Endian es posible gestionar reglas específicas entre zonas, permitiendo o denegando tráfico en función de puertos, protocolos o direcciones IP.

5. Aprendizaje Colaborativo y Práctico:
   El desarrollo se realiza de manera individual y colaborativa, permitiendo la consolidación de conocimientos prácticos en redes, seguridad informática y administración de servidores.

6. Validación mediante Comprobación de Servicios y Comandos:
   Cada participante debe demostrar funcionalmente la configuración mediante pruebas operativas, evidenciando fecha, hora, conectividad y comportamiento de los servicios configurados.

## 3 IMPLEMENTACIÓN DE SEGURIDAD PERIMETRAL MEDIANTE LA CONFIGURACIÓN DE ZONAS UTILIZANDO ENDIAN FIREWALL EN ENTORNOS GNU/LINUX

Esta implementación consiste en diseñar y configurar una infraestructura de seguridad de red destinada a proteger servicios y servidores críticos mediante la creación de una zona desmilitarizada (DMZ). Para ello se emplea la solución de seguridad perimetral Endian Firewall sobre sistemas GNU/Linux, con el objetivo de segmentar la red en zonas de acceso controlado (LAN, WAN y DMZ), aplicar reglas de filtrado, realizar traducción de direcciones mediante NAT y garantizar un monitoreo efectivo del tráfico. Esta arquitectura permite reducir vulnerabilidades, evitar accesos no autorizados y asegurar la disponibilidad, integridad y confidencialidad de los servicios y datos corporativos.



Lo primero que se debe realizar antes de la instalación es el diseño, el cual se explica en detalle en la temática 1. En este apartado se aborda el proceso de preparación del entorno y la instalación de Endian, dado que corresponde a una descripción general del procedimiento.

Se descarga la imagen ISO de Endian desde su repositorio oficial en https://sourceforge.net/projects/efw

. Una vez obtenida la ISO, se configuran los recursos de la máquina virtual, asignando como base 2 CPU, 4 GB de RAM y 30 GB de almacenamiento. Tras el aprovisionamiento de recursos, se procede con la configuración de las interfaces o adaptadores de red.

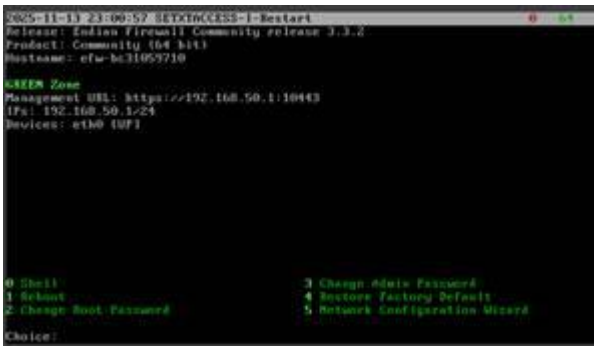
Para esta configuración se utilizan tres adaptadores de red: el adaptador 1 para la zona verde, correspondiente a la red LAN y configurado como red interna; el adaptador 2 para la zona naranja, correspondiente a la red DMZ, también configurado como red interna; y el adaptador 3 para la zona roja, correspondiente a la red NAT y configurado como tipo NAT.

Figura 1. Máquina virtual de Endian con recursos.

Fuente: Autoría Rodrigo Martinez

Una vez configurado el entorno, se inicia la máquina virtual y se selecciona la imagen ISO para realizar la instalación del firewall a nivel de software. Durante este proceso se selecciona el idioma y se configura la zona verde, a la cual se debe asignar la dirección IP de la puerta de enlace, ya que mediante esta dirección se accede a la interfaz web para las configuraciones y la administración posteriores. Con esto se finaliza la instalación de Endian, quedando listo para ser utilizado tanto desde su modo consola como desde su interfaz web.

Figura 2. Consola de Endian finalizada la instalación



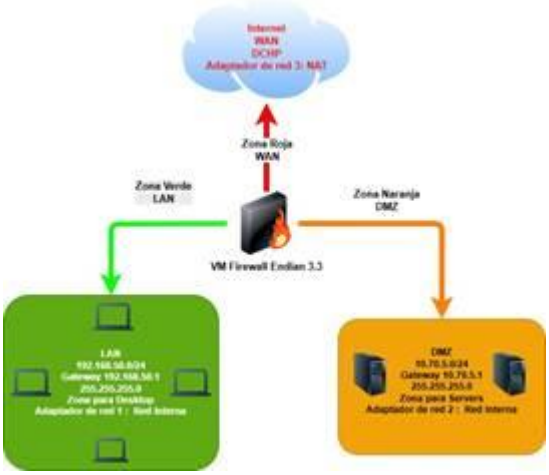

Fuente: Autoría Rodrigo Martinez

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

Para el proceso de implementación, se realiza como primera medida la fase de diseño, en la cual se elabora un diagrama que

representa las zonas: zona verde para la red LAN, zona naranja para la red DMZ y zona roja para la red NAT. En esta misma etapa se definen los segmentos de direcciones IP a utilizar y la gateway o puerta de enlace, que será la encargada de permitir la comunicación entre cada una de las zonas.

Figura 3. Diagrama y segmentación de zonas.




Fuente: Autoría Rodrigo Martinez

Una vez finalizado el diseño, se procedió con la instalación y la configuración inicial de Endian, según lo descrito previamente. Durante esta fase se implementaron las dos primeras zonas: la zona roja, correspondiente a la red NAT, encargada de permitir la comunicación de las demás zonas hacia Internet, y la zona verde, correspondiente a la red LAN, destinada al uso de los equipos de escritorio.

Figura 4. Configuración zona verde

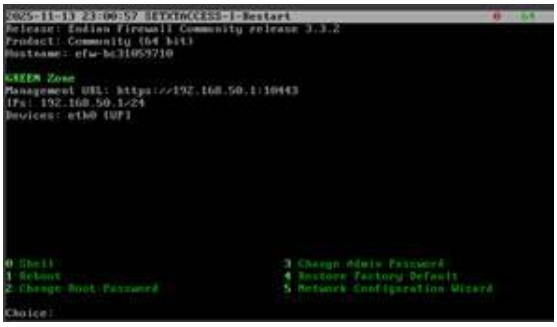

Fuente: Autoría Rodrigo Martinez

Una vez se implementó la zona verde durante la configuración inicial de Endian, quedó habilitado el acceso a la interfaz web a través del navegador, utilizando la dirección https://192.168.50.1:10443, correspondiente a la puerta de enlace de la zona verde (zona LAN). Con este acceso disponible y con Endian funcionando correctamente como firewall, se continuó con la implementación de la zona naranja, correspondiente a la DMZ.

Figura 5. Zona verde configurada


Fuente: Autoría Rodrigo Martinez

Figura 6. Consola de Endian




Fuente: Autoría Rodrigo Martinez

Una vez finalizada la configuración de Endian, se procedió con la configuración de las tarjetas de red de las máquinas clientes que utilizarán las zonas verde y naranja. En este proceso, cada tarjeta de red debía configurarse como red interna y, posteriormente, asignarse a la zona correspondiente: zona naranja (DMZ) o zona verde (LAN). La zona DMZ se destinó para los servidores, mientras que la zona LAN se asignó a los equipos de escritorio.

Finalizada la configuración del hardware virtual de los equipos clientes, se accedió desde el equipo de escritorio conectado a la zona verde (LAN) mediante el navegador, con el fin de completar la configuración e implementar la zona naranja (DMZ).

En la interfaz web se procedió a aceptar la licencia de Endian y a confirmar la configuración de la zona roja, para la cual se seleccionó el modo de red enrutamiento y el tipo de enlace DHCP. Posteriormente, se validó la configuración de la zona verde, cuya puerta de enlace corresponde a 192.168.50.1, verificando además que la interfaz asociada fuera el adaptador 1. A continuación, se configuró la zona naranja, asignándole la puerta de enlace 10.70.5.1, correspondiente al segmento 10.70.5.0/24. Todos los segmentos utilizados emplearon una máscara /24, lo que proporciona una disponibilidad de hasta 254 direcciones IP por cada segmento.

Por último, en esta sección de la configuración se definió el nombre de host, correspondiente al nombre asignado a Endian.

Asimismo, se validó que las interfaces de los adaptadores de red coincidieran con la zona que les correspondía, de acuerdo con las direcciones MAC de cada adaptador. Se configuró un DNS automático y, con ello, se dio por finalizada la configuración e implementación de las tres zonas requeridas: la zona roja para la NAT, la zona verde para la LAN y la zona naranja para la DMZ.

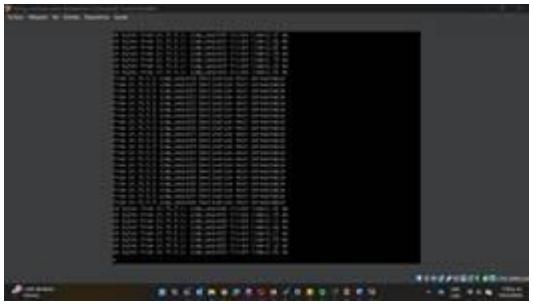
Figura 7. Configuración de zona naranja

Fuente: Autoría Rodrigo Martinez

Finalizada la implementación, se realizaron las pruebas de conectividad entre las zonas. En este punto se tenía garantizado el acceso del equipo de escritorio a la zona LAN, ya que desde esta se configuró la zona naranja mediante la interfaz gráfica de Endian. Adicionalmente, se ejecutaron pruebas de ping tanto desde el servidor como desde el equipo de escritorio, con el fin de confirmar el correcto funcionamiento de las zonas implementadas.

Se ejecutó una prueba de conectividad mediante ping desde el servidor hacia la gateway 10.70.5.1, correspondiente a la zona DMZ. También se realizó un ping hacia una zona inexistente y, finalmente, se efectuó un reinicio de Endian manteniendo el ping en ejecución, con el fin de confirmar que la comunicación con la zona no dependía de un estado previo y que no existía conectividad mientras Endian se encontraba fuera de servicio.

Figura 8. Prueba de ping server a DMZ



Fuente: Autoría Rodrigo Martinez

Finalizada la prueba realizada desde el servidor, se efectuó la prueba de ping desde el equipo de escritorio. Primero se envió un ping a una dirección IP perteneciente a una zona inexistente, lo cual resultó fallido, tal como se esperaba. Posteriormente, se realizó un ping a la zona LAN, específicamente a la dirección IP de la puerta de enlace, obteniéndose una respuesta exitosa. Finalmente, se verificó la dirección IP asignada por DHCP al equipo de escritorio, confirmando que recibió la 192.168.50.2, correspondiente a la siguiente dirección disponible según el orden del servidor DHCP.

Figura 9. Prueba de ping desktop a LAN

Fuente: Autoría Rodrigo Martinez

Por último, se validó el tráfico desde todas las zonas a través de la interfaz de Endian, donde se evidenció el funcionamiento correcto del tráfico correspondiente a las zonas DMZ, NAT y LAN. De esta manera, se garantizó que la implementación se realizó correctamente y conforme al diseño establecido.

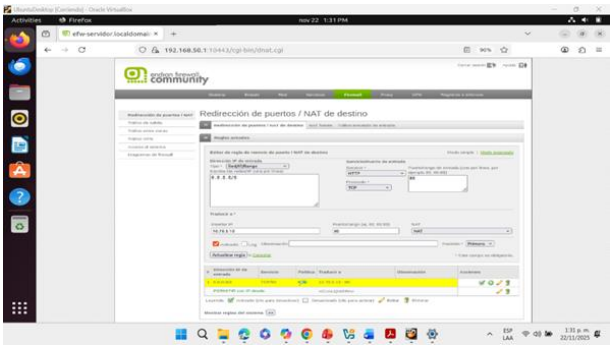
Figura 10. Validación de tráfico desde Endian

Fuente: Autoría Rodrigo Martinez

Las zonas fueron implementadas correctamente según el diseño establecido. Se evidenció el adecuado funcionamiento de la comunicación entre ellas, confirmándose la conectividad de la zona naranja (DMZ), la zona verde (LAN) y la zona WAN, esta última con acceso a Internet.

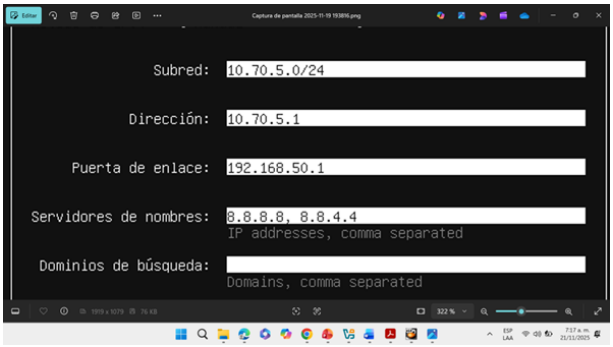
## 5 TEMÁTICA 2: CONFIGURACIÓN NAT

Figura 11. Configuración de DHCP – Definición de reglas



Fuente: Autoría Karol Martínez

Figura 12. Parámetros de red – Instalación ubuntu-22.04.5-live-server

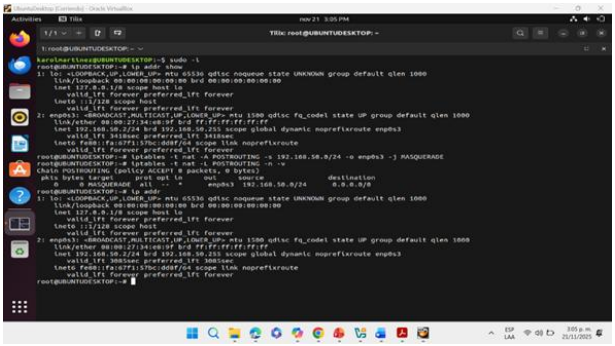



Fuente: Autoría Karol Martínez

El objetivo es permitir que equipos en la LAN y DMZ accedan a internet simulada mediante reglas NAT, y verificar el reenvío de puertos.

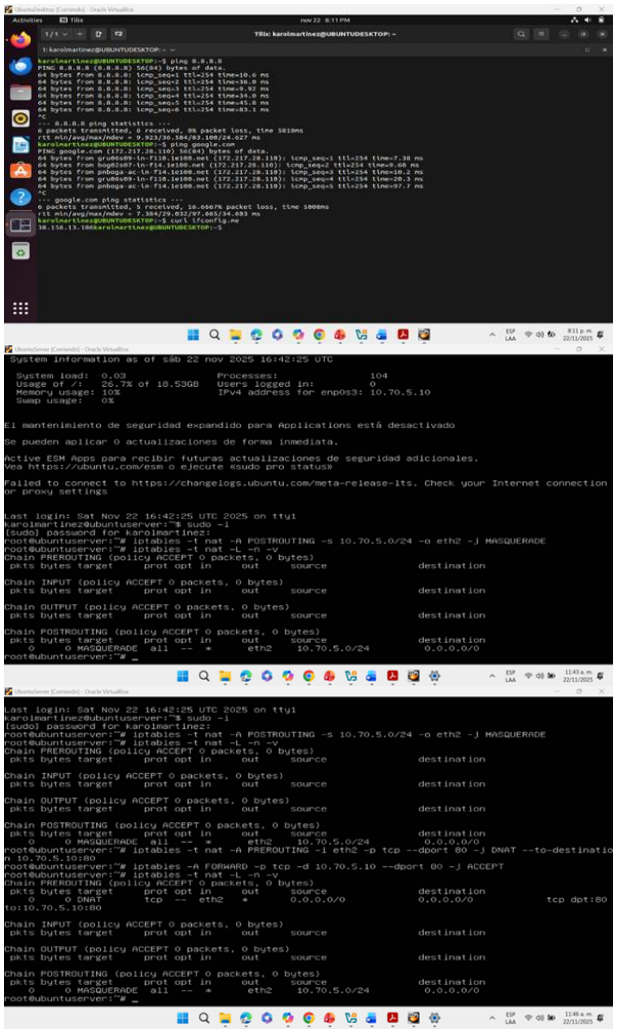
NAT desde LAN hacia WAN
NAT desde DMZ hacia Internet
Reenvío de puertos (DNAT)
Verificación

Figura 13. Conectividad



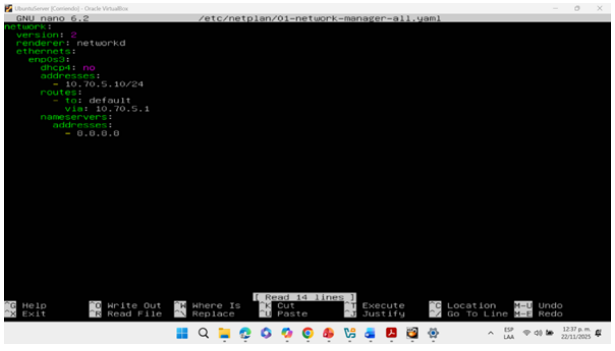
Fuente: Autoría Karol Martínez

Figura 14. Verificación de conectividad desde la LAN (VM Ubuntu)



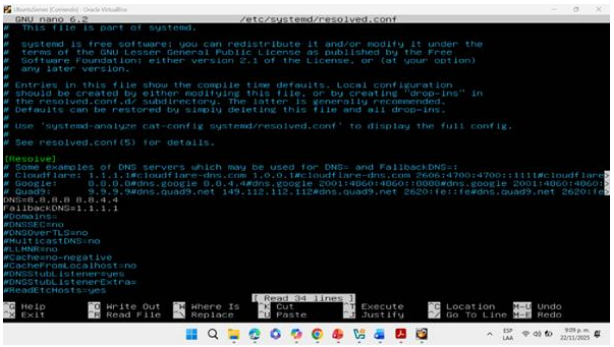
Fuente: Autoría Karol Martínez

Figura 15. Configuración de IP estática con Netplan



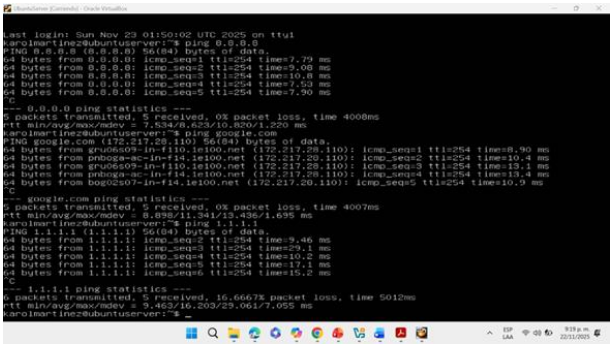
Fuente: Autoría Karol Martínez

Figura 16. Configuración de DNS con systemd-resolved



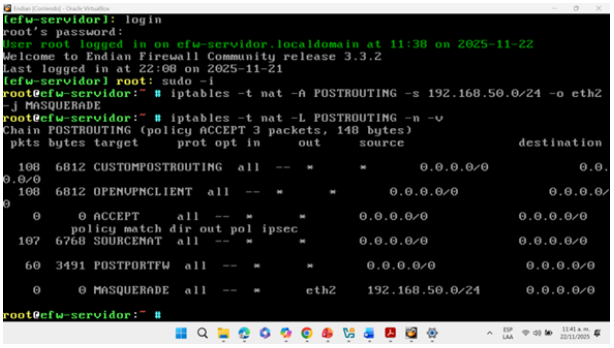
Fuente: Autoría Karol Martínez

Figura 17. Verificación de conectividad LAN, DMZ e Internet



Fuente: Autoría Karol Martínez

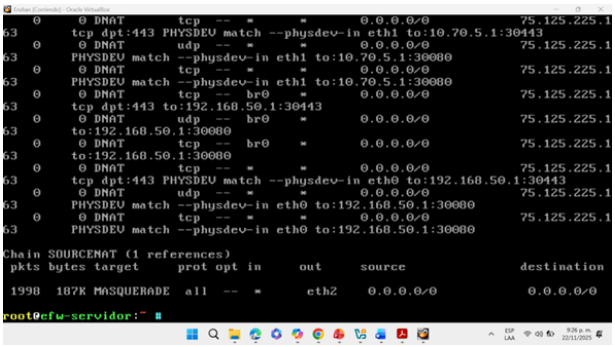
Figura 18. NAT en Endian Firewall



Fuente: Autoría Karol Martínez

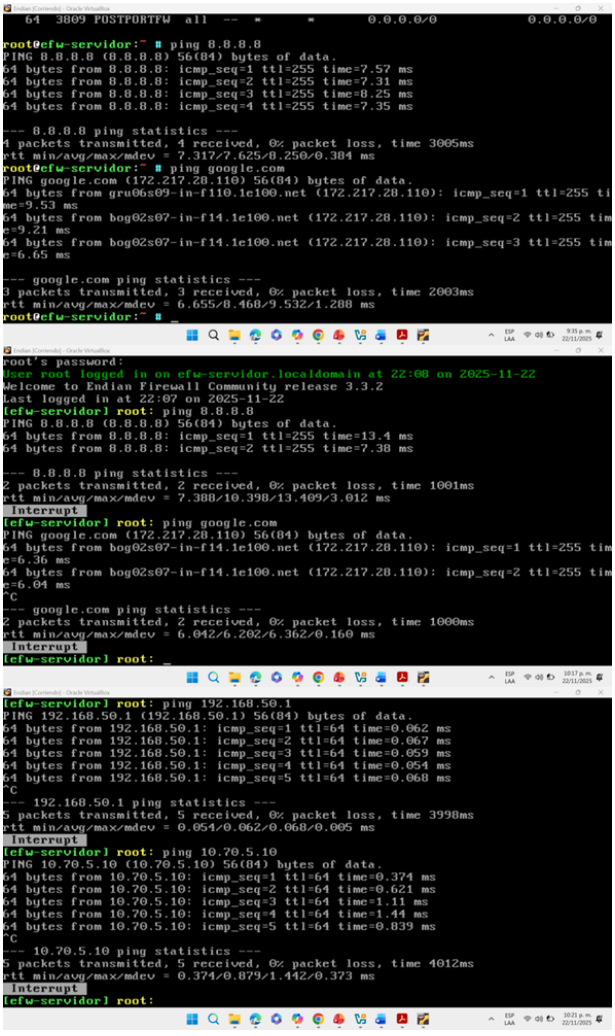
Regla activa en la tabla NAT
Configuración NAT
Redirección de puertos (DNAT)
Reglas DNAT activas
Regla de enmascaramiento (MASQUERADE)

Figura 19. Estado final de la configuración NAT



Fuente: Autoría Karol Martínez

Figura 20. Configuración NAT – Verificación – Pruebas de conectividad



Fuente: Autoría Karol Martínez

## 6 TEMÁTICA 3: PERMITIR SERVICIOS DE LA ZONA DMZ

Se configuraron reglas de firewall que permitieron habilitar los servicios HTTP (puerto 80) y FTP (puerto 21) para el servidor ubicado en la DMZ

Figura 21. Regla configurada de HTTP

Fuente: Autoría David Montoya

Figura 22. Regla configurada de FTP

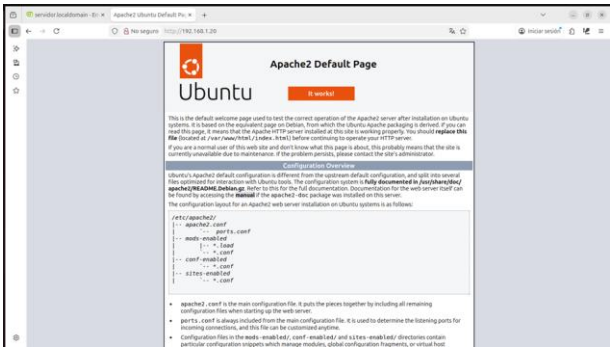
Fuente: Autoría David Montoya

Se configura una regla de denegación del protocolo ICMP para impedir la ejecución de ping desde cualquier máquina interna. Finalmente, se realizaron pruebas de funcionamiento para comprobar la correcta aplicación de las políticas, validando la salida de tráfico permitido y el bloqueo de protocolos restringidos.

Figura 23. Regla configurada de denegación ICMP

Fuente: Autoría David Montoya

Figura 24. Validación de servicios HTTP y FTP

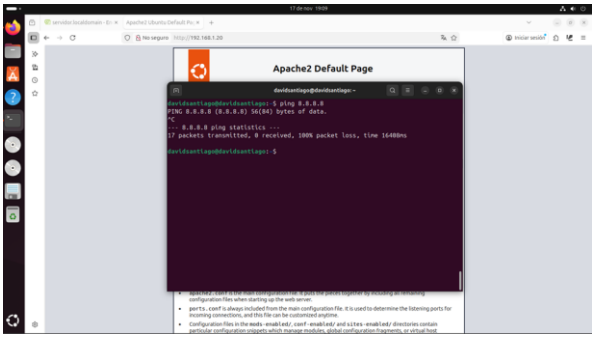



Fuente: Autoría David Montoya

Figura 25. Validación de HTTP

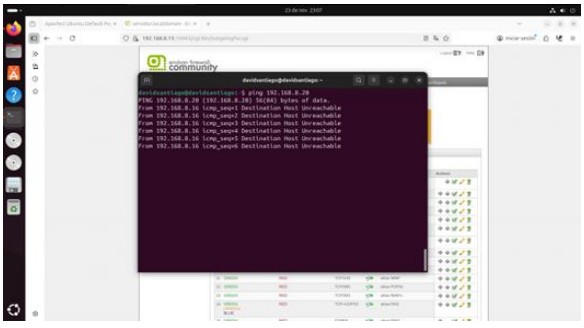
Fuente: Autoría David Montoya

Figura 26. regla configurada de FTP




Fuente: Autoría David Montoya

Figura 27. validación denegación de PING



Fuente: Autoría David Montoya

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

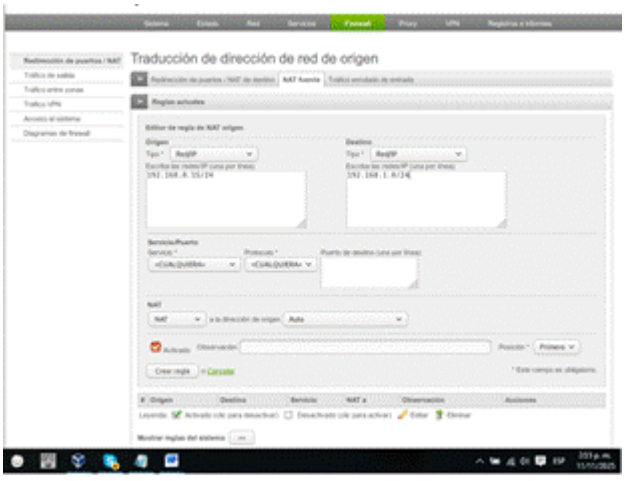
Para continuar con la configuración del firewall, el primer paso que realizamos fue crear la regla de NAT, ya que esta nos permite traducir el tráfico que sale desde la red LAN hacia la red WAN. Para hacerlo, ingresamos al menú de *Cortafuegos*, elegimos la opción *NAT fuente* y, desde allí, añadimos una nueva regla de tipo fuente. Este proceso es sencillo, pero requiere atención para evitar errores.

Figura 28. Configuración de NAT.


Fuente: Autoría Juan Jose Bocanegra

Después de esto, indicamos como origen nuestra red local (LAN) y como destino la red que usamos para simular la conexión a Internet (WAN). Esta configuración nos permite que el tráfico salga correctamente hacia el exterior y regrese de forma segura.

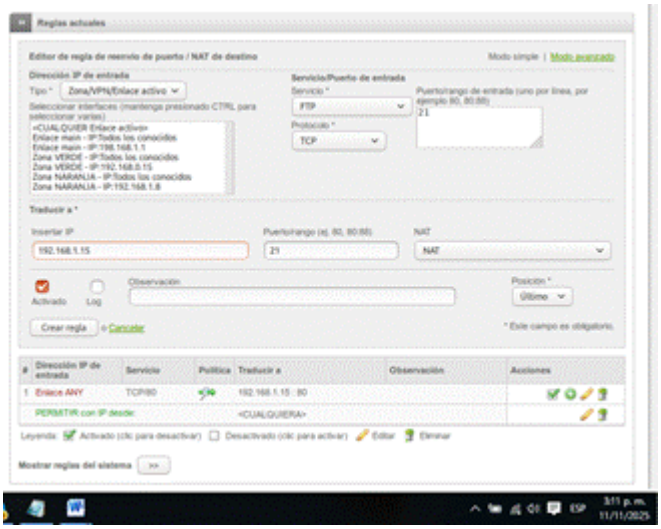
Figura 29. Origen de la red local.




Fuente: Autoría Juan Jose Bocanegra

También confirmamos que el protocolo seleccionado fuera el adecuado para lo que queríamos publicar, sobre todo cuando se trata de servicios que necesitamos exponer desde la zona DMZ hacia Internet. Una elección correcta evita fallos más adelante.

Figura 30. Definición del protocolo.



Fuente: Autoría Juan Jose Bocanegra

**REGLAS ENTRE ZONAS:**

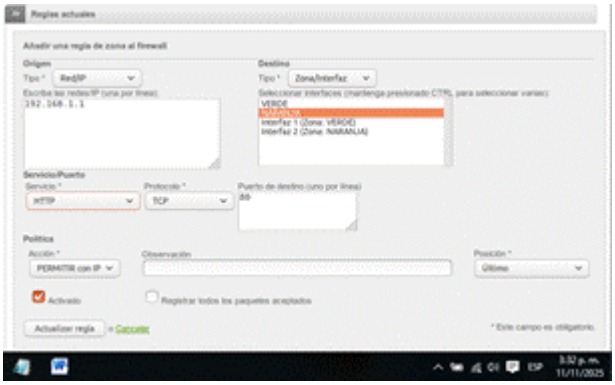
Una vez configurado el NAT, pasamos a crear las reglas que permiten —o bloquean— la comunicación entre las distintas zonas de la red. Este paso es clave, porque aquí definimos cómo se comportará realmente el tráfico dentro de nuestro entorno.

Figura 31. Configuración del firewall.


Fuente: Autoría Juan Jose Bocanegra

Entre estas reglas, una de las más importantes fue permitir la comunicación entre la zona Internet y la zona DMZ, ya que allí ubicamos los servicios que deben ser visibles desde el exterior.

Figura 32. Comunicación de zona DMZ.



Fuente: Autoría Juan Jose Bocanegra

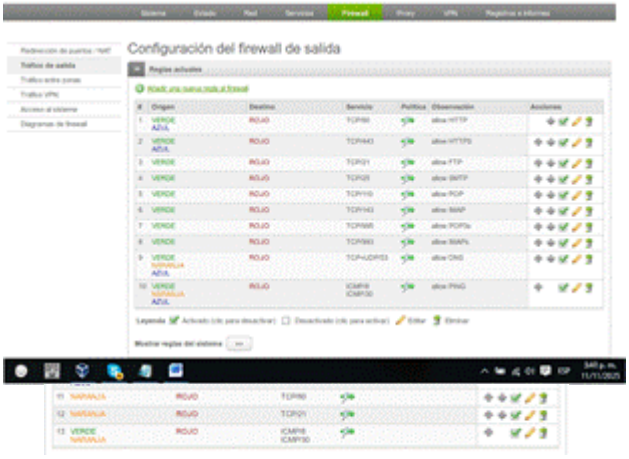
Luego de añadir todas las políticas necesarias, pudimos ver el listado completo de reglas aplicadas entre zonas. Este panorama general nos ayudó a validar que todo estuviera organizado y en el orden correcto.

Figura 33. Todas las reglas creadas.

Fuente: Autoría Juan Jose Bocanegra

En cuanto al tráfico de salida, configuramos tres reglas principales que permiten un control más claro de lo que la red puede realizar hacia el exterior.

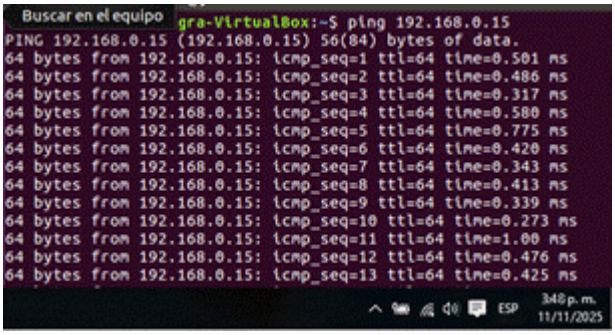
Figura 34. Gráfico de reglas de salidas.




Fuente: Autoría Juan Jose Bocanegra

Finalmente, procedimos a realizar las pruebas correspondientes para confirmar que el firewall aplicara las políticas tal como las configuramos. Estas pruebas nos permitieron verificar la navegación, la respuesta de los servicios y el bloqueo correcto de protocolos determinados.

Figura 35. Ejecución de pruebas



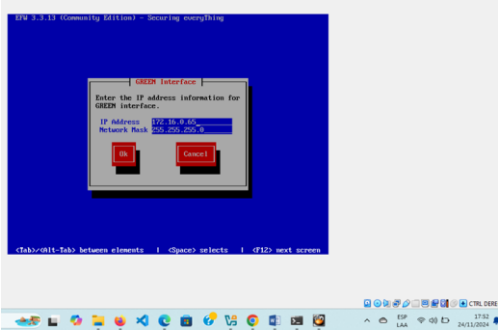

Fuente: Autoría Juan Jose Bocanegra

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

La instalación de Endian Firewall constituye el punto de partida para la implementación de un sistema de filtrado y control de navegación. Durante el proceso se asignan las interfaces de red correspondientes a las zonas Verde (LAN), Roja (WAN) y Naranja (DMZ), garantizando una segmentación segura

Una vez se realiza el proceso de instalación y configuración de Endian se prepara la máquina virtual para gestionar las conexiones entrantes y salientes de la red.

Figura 36. Configuración Endian.

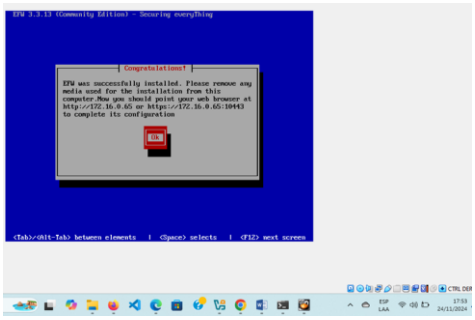


Fuente: Autoría Andres Calderon

Configuración Zona Verde, utilizando Subneteo. En la configuración de la Zona Verde de Endian Firewall, se asignó la dirección IP 172.16.0.65 y la máscara de subred 255.255.255.0. Esto permite segmentar la red interna (LAN) en subredes más pequeñas utilizando subneteo, lo

que optimiza el uso de las direcciones IP disponibles. La máscara de subred 255.255.255.0 divide el rango de direcciones en varias subredes, proporcionando un control más eficiente de los dispositivos dentro de la Zona Verde y mejorando la seguridad y el rendimiento de la red interna.

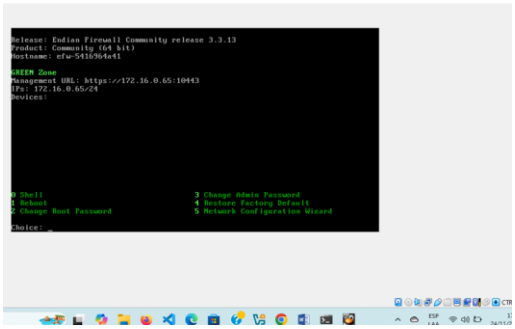
Figura 37. Finalización configuración Endian



Fuente: Autoría Andres Calderon

Acceso a zona verde. Se da ok para acceder a la zona verde de Endian.

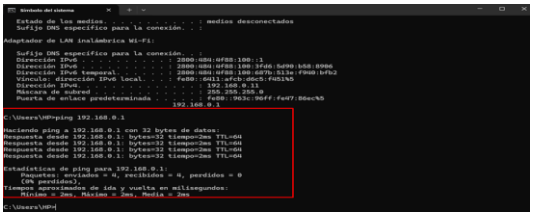
Figura 38. Zona verde configurada



Fuente: Autoría Andres Calderon

Zona Verde. Se muestra la configuración de la Zona Verde en Endian Firewall. Se ha asignado la dirección IP 172.16.0.65 y la máscara de subred 255.255.255.0 a la interfaz de red correspondiente a la Zona Verde, lo que segmenta la red interna en subredes más pequeñas para mejorar la eficiencia y seguridad. Esta configuración asegura que los dispositivos en la red interna (LAN) puedan comunicarse de manera controlada, y que se establezca una base sólida para las futuras configuraciones de seguridad y acceso entre las zonas verde, roja y naranja. Haciendo Ping desde máquina local a la zona verde.

Figura 39. Prueba de ping

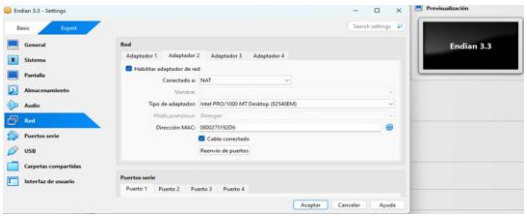


Fuente: Autoría Andres Calderon

El ping fue exitoso, lo que significa que la máquina local tiene conectividad con la Zona Verde de Endian. La respuesta de 172.16.0.65 con un tiempo de 2 ms indica que la comunicación está funcionando correctamente y que la IP de la Zona Verde está accesible desde tu computadora.

La Zona Verde corresponde a la red interna o LAN, donde residen los equipos que serán controlados por el proxy. Se asignó la dirección IP 172.16.0.65/24, lo que garantiza que los dispositivos dentro del rango de la subred puedan comunicarse con Endian. Posteriormente, se verificó la conectividad mediante un ping exitoso, lo cual confirma que los equipos de la LAN pueden acceder a la interfaz de administración de Endian.

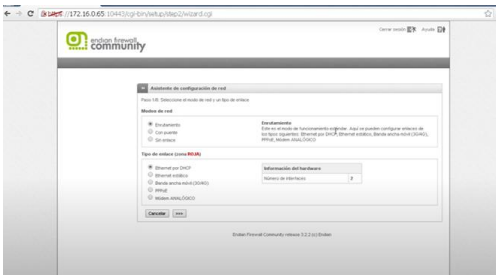
Figura 40. Configuración Adaptador 2 – Rojo



Fuente: Autoría Andres Calderon

Se configura adaptador de red para la zona roja con conexión NAT

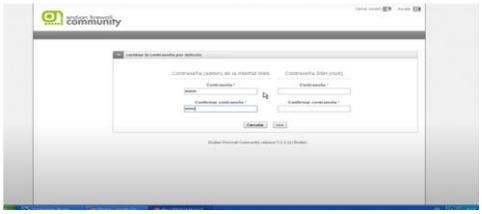
Figura 41. Configuración zona roja en Endian



Fuente: Autoría Andres Calderon

Se ingresa al entorno Endian desde la url: 172.16.0.65:10443 y se configura contraseña

Figura 42. Configuración usuarios y contraseñas

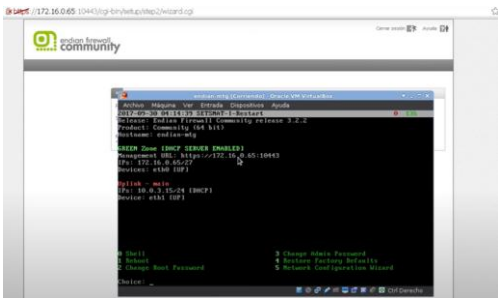


Fuente: Autoría Andres Calderon

Figura 43. Creación zona roja

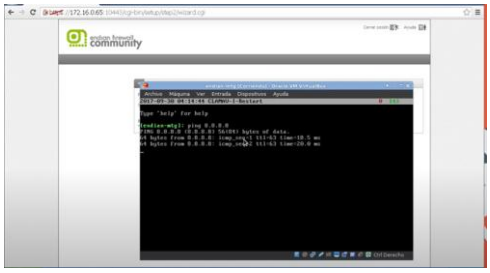
Fuente: Autoría Andres Calderon

Figura 44. Zona roja configurada. Dirección IP otorgada por DHCP



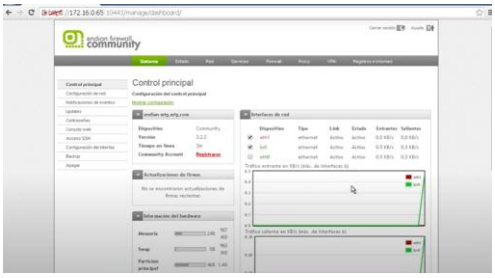
Fuente: Autoría Andres Calderon

Figura 45. Posteriormente se realiza el proceso de comprobación



Fuente: Autoría Andres Calderon

Figura 46. Verificación de las interfaces



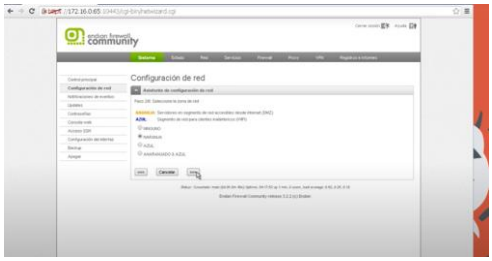
Fuente: Autoría Andres Calderon

La Zona Roja representa la conexión a Internet.

Se configuró el adaptador de red con NAT, permitiendo que Endian reciba una dirección IP automática por DHCP desde el proveedor o desde VirtualBox. Se validó la conectividad mediante un ping hacia Internet, asegurando que Endian puede canalizar tráfico hacia redes externas. También se verificó desde la consola la existencia de ambas interfaces (Roja y Verde), confirmando la estructura inicial de red.

Configuramos el adaptador 3 para interfaz Naranja. Se configura el adaptador 3 para la interfaz Naranja. Se lleva a cabo la configuración Naranja

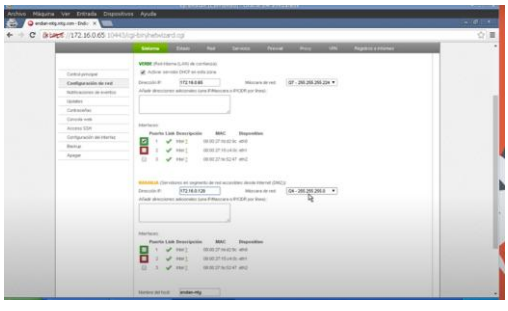
Figura 47. Creación zona naranja



Fuente: Autoría Andres Calderon

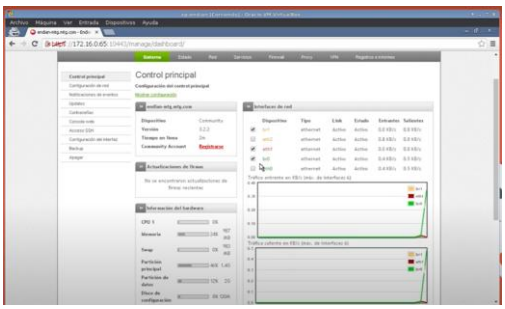
Se le otorga una IP a la red naranja y se realiza su respectiva validación y análisis.

Figura 48. Asignación IP zona naranja



Fuente: Autoría Andres Calderon

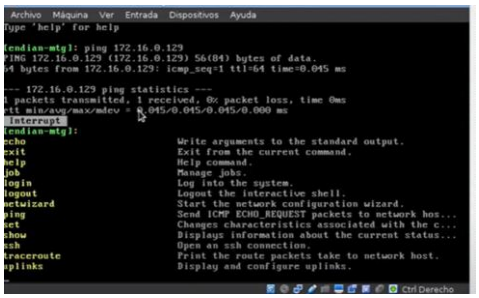
Figura 49. Verificación de tráfico y zonas




Fuente: Autoría Andres Calderon

Finalmente se realiza el proceso de verificar de la zona.

Figura 50. Verificación en consola Endian




Fuente: Autoría Andres Calderon

Al hacer ping verificamos funcionamiento de la zona naranja.

La Zona Naranja (DMZ) es utilizada para ubicar servidores o servicios intermedios. Se habilitó un tercer adaptador y se asignó una dirección IP estática. Finalmente, se comprobó su conectividad con pings internos, verificando que la DMZ quedó correctamente operativa.

# 9 CONCLUSIONES

La fase de diseño para la implementación de un firewall, en la cual se definen las zonas, los rangos de direcciones IP, las puertas de enlace y el rol asignado a cada zona, es fundamental. De esta etapa depende que la implementación se realice de manera adecuada y no de forma improvisada, evitando así retrasos o errores en las fases posteriores.

La implementación de una DMZ es una estrategia esencial para disminuir riesgos de seguridad, ya que evita la exposición directa de los servidores internos y mantiene aislados los servicios críticos frente a posibles amenazas provenientes de internet.

El uso de plataformas GNU/Linux demuestra ser una alternativa robusta, confiable y económica para soluciones de seguridad perimetral, sin necesidad de recurrir a herramientas propietarias de alto costo.

Endian Firewall permite gestionar y monitorear eficientemente el tráfico entre zonas, brindando control granular mediante reglas NAT, controles de acceso (ACLs) y servicios de proxy autenticado, lo cual refuerza la protección y supervisión del entorno de red.

El enfoque colaborativo del proyecto contribuye al fortalecimiento de competencias técnicas reales, especialmente las relacionadas con administración de sistemas, protocolos de red, análisis de tráfico y políticas de seguridad.

La correcta planificación y documentación de la infraestructura es clave para su funcionamiento seguro, ya que una mala asignación de direcciones IP, reglas de firewall o servicios puede generar brechas de seguridad o pérdida de disponibilidad.

En el manejo de los servicios dentro de la DMZ, logramos habilitar los protocolos **HTTP y FTP**, permitiendo que estuvieran disponibles de forma controlada. Al mismo tiempo, decidimos bloquear el protocolo **ICMP**, lo que añadió una capa más de seguridad al evitar respuestas de ping no deseadas. Las reglas entre zonas nos ayudaron a validar el nivel de control que realmente ofrece el firewall, y mediante pruebas con navegadores y herramientas de análisis pudimos confirmar que el comportamiento del tráfico coincidía con las políticas configuradas.

Finalmente, la práctica realizada permite comprender en un entorno controlado los retos y responsabilidades de los administradores de red y seguridad, enfatizando la importancia del monitoreo constante, el principio de menor privilegio y la defensa en profundidad.

# 10 REFERENCIAS

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

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

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

[4] Endian. (2024). Endian Firewall Community Documentation. Endian. https://www.endian.com/community/

.

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

[6] Rouse, M. (2023). Network Address Translation (NAT). TechTarget. https://www.techtarget.com/searchnetworking/definition/NAT

[7] Stallings, W., & Brown, L. (2018). Computer security: Principles and practice (4th ed.). Pearson.