IMPLEMENTACIÓN DE UN ESQUEMA DE SEGURIDAD PERIMETRAL CON GNU/LINUX ENDIAN FIREWALL PARA LA PROTECCIÓN DE REDES LAN, DMZ Y WAN

David Steven Jaramillo Molano
e-mail: dsjaramillom@unadvirtual.edu.co
Miguel Alejandro Parra Sánchez
e-mail: maparrasa@unadvirtual.edu.co
Diego Fernando Torrado Duarte
e-mail: dftorradod@unadvirtual.edu.co
Joaquin Rafael Vides Beleño
e-mail: jrvidesb@unadvirtual.edu.co
Agustín Alberto Vega Basto
e-mail: aavegab@unadvirtual.edu.co

RESUMEN: *Este artículo describe la implementación de un entorno de seguridad perimetral utilizando la distribución GNU/Linux Endian Firewall (EFW) en un ambiente virtualizado con VirtualBox. El propósito principal fue configurar una infraestructura compuesta por una red LAN, una zona DMZ y la conexión hacia la WAN, garantizando la protección de servidores internos, bases de datos y servicios web. Para ello, cada integrante del grupo desarrolló una de las cinco temáticas planteadas: instalación y configuración inicial de Endian, reglas de NAT, habilitación de servicios para la DMZ, políticas de acceso mediante firewall e implementación de un proxy HTTP con autenticación. Durante la práctica se configuraron servicios esenciales, se gestionaron interfaces de red, se implementaron políticas de enmascaramiento y se establecieron esquemas de filtrado y control de tráfico. Los resultados evidencian una correcta comunicación entre las redes, un aislamiento seguro de la DMZ y el funcionamiento efectivo de las políticas de seguridad, logrando cumplir el objetivo de fortalecer la administración de sistemas GNU/Linux y la gestión integral de la seguridad perimetral.*

PALABRAS CLAVE: Seguridad perimetral; Endian Firewall; DMZ; NAT; Proxy; GNU/Linux; Firewall; Redes; VirtualBox.

1 INTRODUCCIÓN

La creciente dependencia de los servicios digitales dentro de las organizaciones exige la implementación de esquemas de seguridad perimetral robustos, capaces de proteger servidores, aplicaciones y bases de datos frente a amenazas internas y externas. En este contexto, las distribuciones GNU/Linux orientadas a la seguridad, como Endian Firewall (EFW), ofrecen una solución integral para la segmentación de redes, la administración del tráfico y el aseguramiento de los servicios críticos.

La actividad desarrollada tiene como finalidad aplicar los conocimientos adquiridos sobre administración de sistemas GNU/Linux y la gestión de servicios esenciales para alcanzar el resultado de aprendizaje: configurar interfaces de usuario y escritorio mediante tareas administrativas, garantizando un óptimo nivel de seguridad en el sistema operativo. Para ello, se implementó un entorno de red compuesto por una LAN, una zona DMZ y la conexión hacia la WAN, delimitadas y administradas a través de Endian como firewall perimetral.

El trabajo se organizó en cinco temáticas, abordadas individualmente por cada integrante del grupo:

- Configuración inicial de la instancia en VirtualBox.
- Configuración de NAT.
- Habilitación de servicios para la DMZ.
- Reglas de acceso para permitir o denegar tráfico.
- Implementación de un proxy HTTP con autenticación.

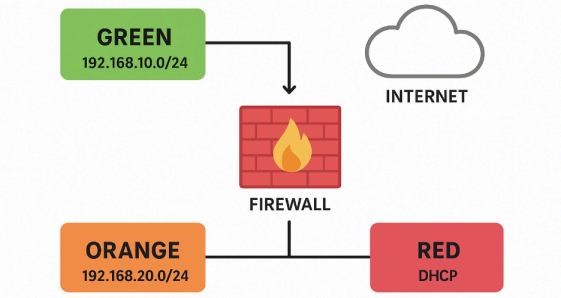
El presente artículo consolida los resultados obtenidos y detalla, especialmente, el desarrollo de la Temática 2 correspondiente a la configuración de NAT en Endian Firewall.

2 IMPLEMENTACIÓN DE LA ARQUITECTURA DE SEGURIDAD PERIMETRAL CON ENDIAN FIREWALL

La implementación de la arquitectura de seguridad perimetral se desarrolló a partir de cinco temáticas que abarcan desde la instalación inicial del firewall hasta la configuración de políticas avanzadas de control de tráfico. Cada integrante del grupo asumió una temática específica con el fin de construir, de manera colaborativa, una infraestructura funcional y segura basada en la distribución GNU/Linux Endian Firewall (EFW). Este proceso incluyó la configuración de interfaces de red, la habilitación de servicios esenciales, el establecimiento de reglas de traducción de direcciones, la definición de políticas de acceso y la implementación de mecanismos de filtrado y autenticación. Antes de iniciar con el desarrollo de las temáticas propuestas, fue necesario realizar la instalación y configuración base de la distribución Endian Firewall Community, la cual funcionó como plataforma de seguridad perimetral del entorno LAN–DMZ–WAN. Este proceso incluyó la descarga de la imagen ISO, la creación de la máquina virtual en VirtualBox, la asignación de las zonas de red y la ejecución del asistente inicial de configuración. Se descargó la imagen oficial de Endian Firewall Community

desde el sitio web del proyecto y se almacenó localmente para proceder con su instalación en VirtualBox y para el diseño de la solución se definió un esquema de direccionamiento y segmentación basado en tres zonas de seguridad: VERDE (LAN interna), NARANJA (DMZ) y ROJA (WAN).

Figura 1. Esquema, el direccionamiento y asignación de zonas (verde, naranja y roja) para el desarrollo de la actividad.



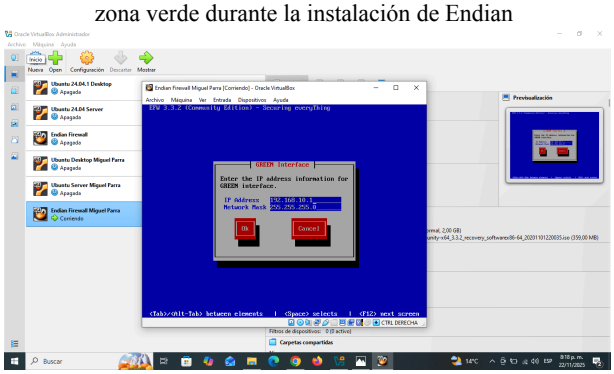
Fuente: Autoría Propia

Con el fin de replicar un entorno real de firewall perimetral con segmentación por zonas, se configuraron tres adaptadores de red en la máquina virtual de Endian, asignando cada uno a una zona específica:

- Adaptador 1 – Zona VERDE (LAN interna)
  - Modo: Red interna
  - Nombre: lan
  - Función: conectar usuarios internos (Ubuntu Desktop)
- Adaptador 2 – Zona NARANJA (DMZ)
  - Modo: Red interna
  - Nombre: dmz
  - Función: conectar el servidor (Ubuntu Server)
- Adaptador 3 – Zona ROJA (WAN)
  - Modo: NAT
  - Función: acceso a Internet simulado
  - IP asignada automáticamente por DHCP

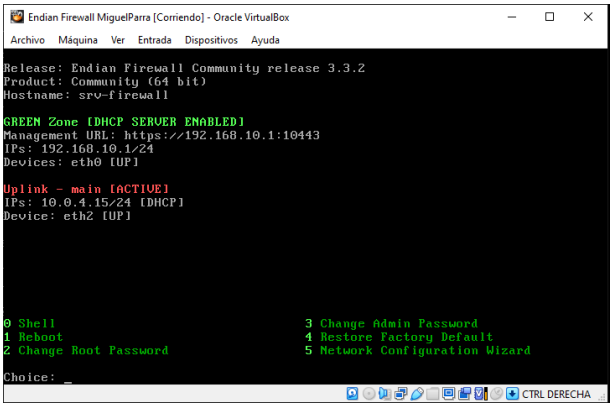
Esta configuración garantiza una segmentación adecuada para implementar políticas de seguridad diferenciadas. Para la instalación de Endian Firewall se inició la máquina virtual desde la ISO y se ejecutó el asistente de instalación, completando: selección del idioma, zona horaria, aceptación de la licencia, instalación del sistema en disco y reinicio.

Figura 2. Asignación de dirección IP y máscara de red para la zona verde durante la instalación de Endian



Fuente: Autoría Propia

Figura 3. Interfaz principal de Endian tras completar la instalación exitosamente.



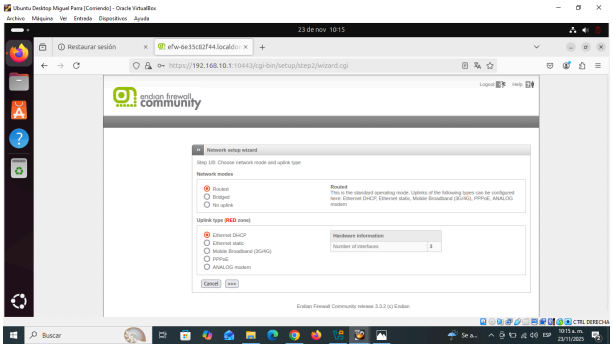
Fuente: Autoría Propia

Después del reinicio se ejecutó el Network Setup Wizard, compuesto por ocho pasos que permiten configurar el modo de operación del firewall, las zonas de red y sus direcciones IP.

Desde el equipo ubicado en la zona verde se accedió a la consola web mediante la URL:

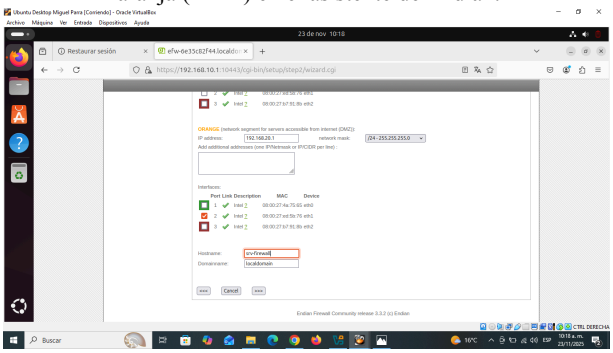
https://192.168.1.1:10443

Figura 4. Selección del modo de red en el asistente de configuración inicial de Endian.



Fuente: Autoría Propia

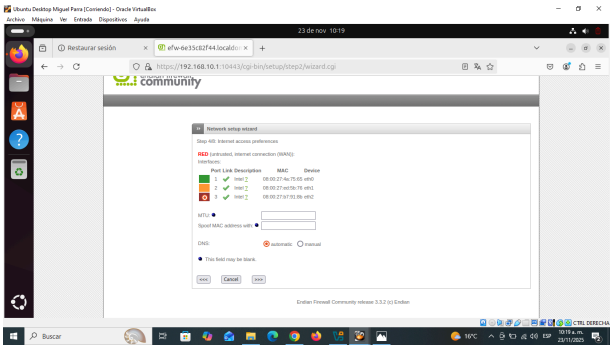
Figura 5. Configuración de las zonas verde (LAN interna) y naranja (DMZ) en el asistente de Endian.



Fuente: Autoría Propia

Cada zona (verde, naranja, roja) cumple un rol específico que facilita la aplicación de políticas de seguridad diferenciadas según el nivel de confianza.

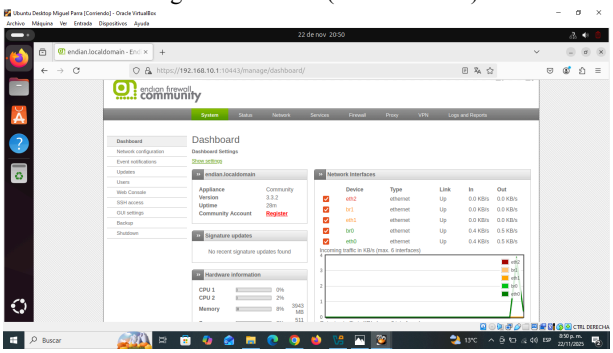
Figura 6. Configuración de la zona RED (WAN) durante el asistente inicial.



Fuente: Autoría Propia

El asistente aplicó los cambios y reinició los servicios de red, dejando el sistema operativo completamente funcional. Finalmente, desde esta interfaz se administran reglas de firewall, NAT, servicios, monitoreo y configuraciones avanzadas.

Figura 7. Pantalla de inicio de sesión al finalizar la configuración inicial (usuario admin).



Fuente: Autoría Propia

2.1 TEMÁTICA 1 – CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN

La implementación del firewall Endian en un entorno virtualizado requiere una correcta definición de las zonas de red y la asignación adecuada de interfaces. Para este ejercicio se habilitaron tres adaptadores de red en la máquina virtual de Endian, correspondientes a las zonas GREEN, ORANGE y RED, siguiendo el modelo clásico de segmentación adoptado por distribuciones de firewall basadas en GNU/Linux.

2.1.1 VALIDACIÓN DE LAS ZONAS DE RED Y CONECTIVIDAD

Una vez asignadas las interfaces, Endian reconoce automáticamente la segmentación y valida las direcciones IP configuradas. A través de su entorno de administración web se verificó la disponibilidad de las tres interfaces, confirmando que la estructura lógica de red se encontraba activa. Para comprobar la funcionalidad de la topología, se realizaron pruebas de conectividad mediante comandos ping desde un cliente simulado hacia el firewall Endian. Los resultados evidenciaron una correcta comunicación entre:

- Cliente → GREEN
- Servidor → ORANGE
- Endian → RED (salida externa)

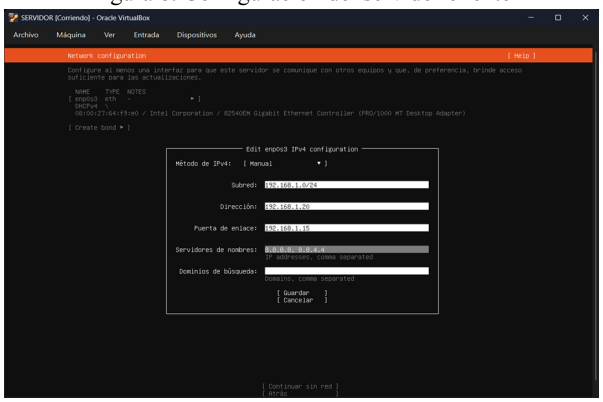
Esto confirma no solo la correcta configuración de las interfaces, sino también la capacidad del firewall para enrutar tráfico entre zonas conforme a las reglas por defecto.

2.1.2 ANÁLISIS CRÍTICO DE LA CONFIGURACIÓN

Si bien la estructura planteada cumple los requisitos básicos de segmentación de redes, existen aspectos que pueden mejorarse desde un enfoque profesional y alineado con buenas prácticas:

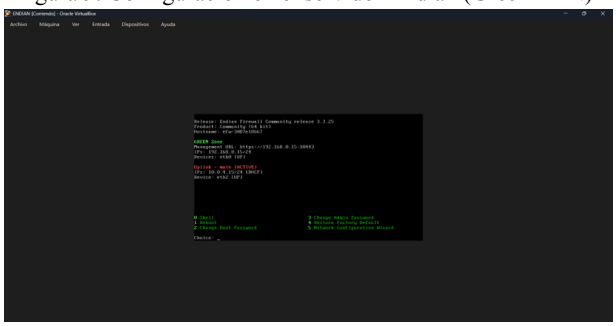
- Ausencia de reglas explícitas de filtrado: El ejercicio se centró en la configuración de interfaces, pero no se documentaron políticas de firewall. Para un entorno productivo, es indispensable definir reglas de acceso específicas para la DMZ y los clientes internos.
- Falta de mecanismos de monitoreo: Endian proporciona herramientas de registro y monitoreo (logs, IDS/IPS, gráficos de tráfico), que no se describen en esta etapa. Su uso sería esencial para evaluar el comportamiento real de la red.
- Topología estática sin alta disponibilidad: La configuración es funcional, pero carece de redundancia. En escenarios reales, Endian admite configuraciones HA (High Availability) que mejorarían la continuidad del servicio.
- Ausencia de pruebas de servicios en la DMZ: Aunque se configuró la zona ORANGE, no se evaluó la publicación de servicios (HTTP, FTP, SSH). Estas pruebas son claves para justificar el uso de una DMZ.
- En síntesis, la configuración presentada establece una base sólida para comprender la arquitectura de red con Endian, pero puede fortalecerse mediante una gestión más avanzada de políticas, monitoreo y pruebas de servicio, especialmente si va a ser incluida en un artículo técnico o académico.

Figura 8. Configuración del servidor cliente



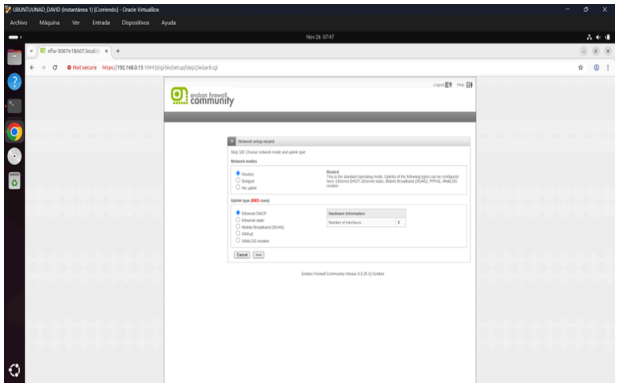
Fuente: Autoría propia.

Figura 9. Configuración en el servidor Endian (Green LAN)



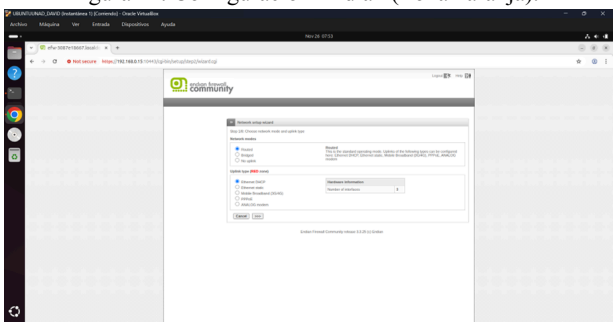
Fuente: Autoría propia.

Figura 10. Apertura inicial Endian desde un equipo cliente dentro de VB.



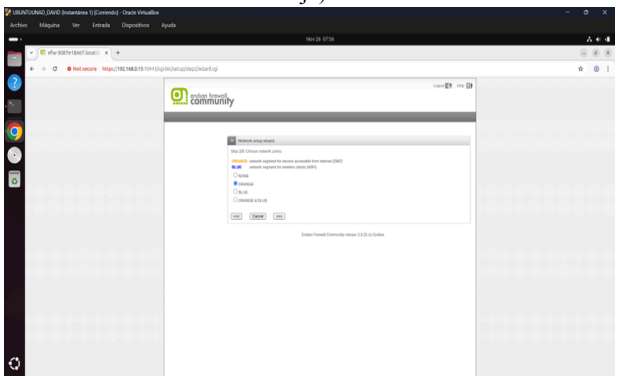
Fuente: Autoría propia.

Figura 11. Configuración Endian (Zona naranja).



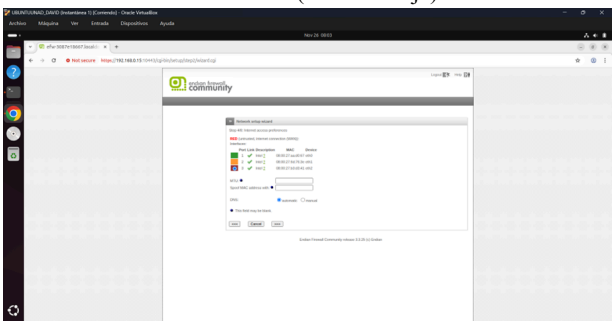
Fuente: Autoría propia.

Figura 12. Validación de configuración (Zona verde, Zona roja)



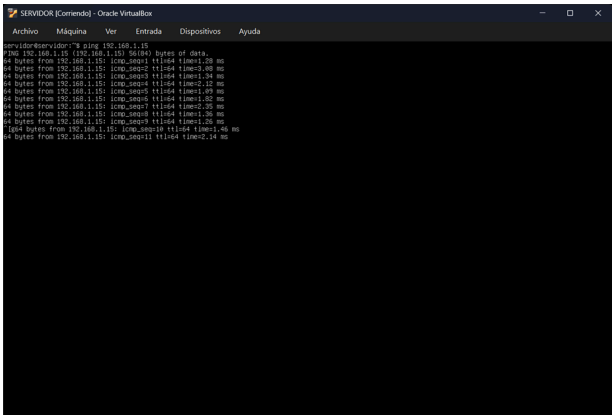
Fuente: Autoría propia.

Figura 13. Validación de configuración previa con la ip seleccionada (Zona naranja)



Fuente: Autoría propia.

Figura 14. Ping sostenido desde el servidor cliente a través de Endian.



Fuente: Autoría propia

2.2 TEMÁTICA 2 – CONFIGURACIÓN NAT

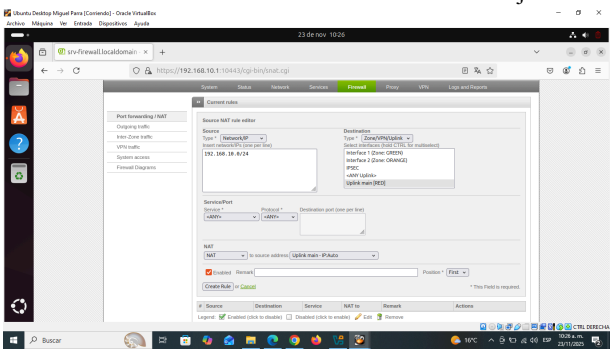
La Temática 2 se centró en la configuración de NAT (Network Address Translation) dentro de Endian Firewall, un componente esencial para permitir la comunicación entre la red LAN (zona verde) y la red externa (zona roja). El objetivo principal fue habilitar el enmascaramiento de direcciones privadas para que los dispositivos internos pudieran acceder a Internet de manera segura, sin exponer sus direcciones reales.

2.2.1 CONFIGURACIÓN DE LA PRIMERA REGLA NAT ENTRE LA ZONA VERDE (LAN) Y LA ZONA ROJA (WAN)

Para habilitar la comunicación de los equipos ubicados en la red LAN (zona GREEN) hacia la red simulada de Internet (zona RED), se configuró una regla de traducción de direcciones (NAT).

Para ello, se ingresó al menú Firewall > Port Forwarding / NAT, y en la sección Source NAT se creó una nueva regla. Esta regla se configuró definiendo como origen la zona verde (192.168.10.0/24), como destino la zona roja, permitiendo cualquier servicio (ANY) y utilizando el tipo de NAT Uplink main con la dirección configurada en modo Auto. Una vez creada la regla, se habilitó y se aplicaron los cambios correspondientes.

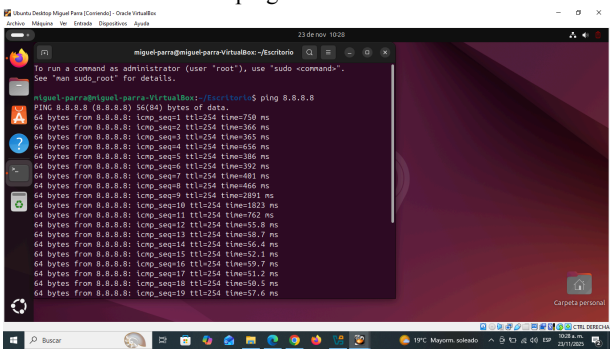
Figura 15. Implementación de NAT para habilitar la comunicación de la zona verde hacia la zona roja.



Fuente: Autoría Propia

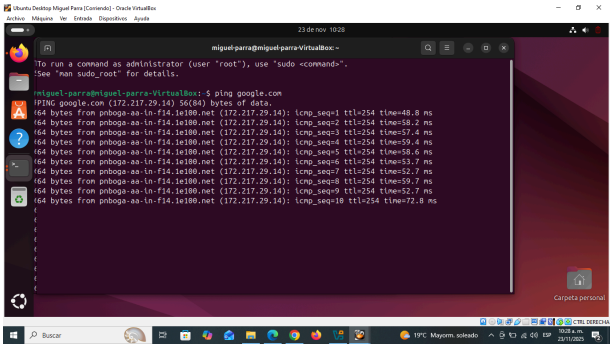
Desde el equipo Ubuntu Desktop ubicado en la zona verde se realizaron pruebas de conectividad para validar la correcta salida hacia la red WAN. Como resultado, los equipos de la LAN lograron establecer comunicación hacia la red WAN simulada, verificando así el funcionamiento adecuado del NAT para tráfico saliente.

Figura 16. Validación de acceso a Internet desde la zona verde mediante ping al servidor 8.8.8.8.



Fuente: Autoría Propia

Figura 17. Validación de acceso a internet desde la zona verde mediante ping al servidor de google.com

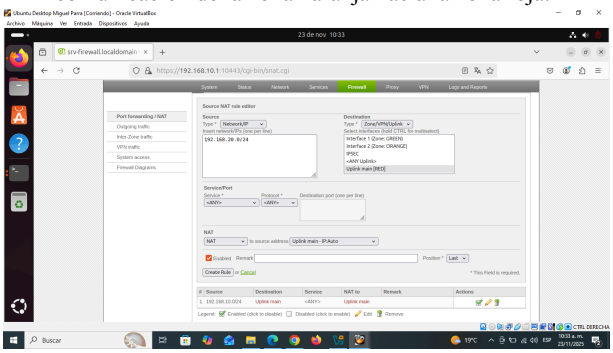


Fuente: Autoría Propia

2.2.2 CONFIGURACIÓN DE LA SEGUNDA REGLA NAT ENTRE LA ZONA NARANJA (DMZ) Y LA ZONA ROJA (WAN)

Para habilitar la comunicación de los servidores ubicados en la zona DMZ (ORANGE) hacia la red WAN/Internet (zona RED), se configuró una segunda regla de NAT. Para ello, desde el menú Firewall > Port Forwarding / NAT, en la sección Source NAT, se añadió una nueva regla en la cual se definió como origen la zona ORANGE y como destino la zona RED, permitiendo cualquier servicio (ANY) y empleando el tipo de NAT Uplink main con la dirección configurada en modo Auto. Tras habilitar la regla y aplicar los cambios, los equipos ubicados en la DMZ lograron comunicarse correctamente con la red WAN simulada, confirmando el funcionamiento adecuado del NAT para esta zona.

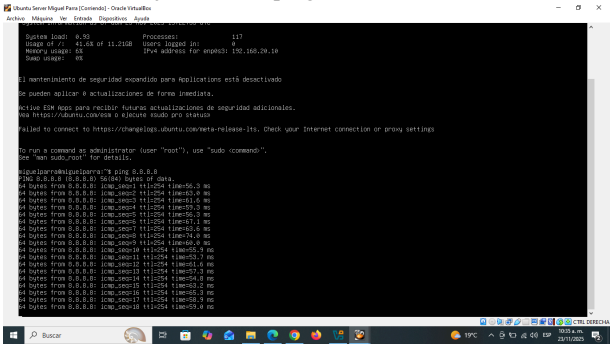
Figura 18. Implementación de NAT para habilitar la comunicación de la zona naranja hacia la zona roja.



Fuente: Autoría Propia

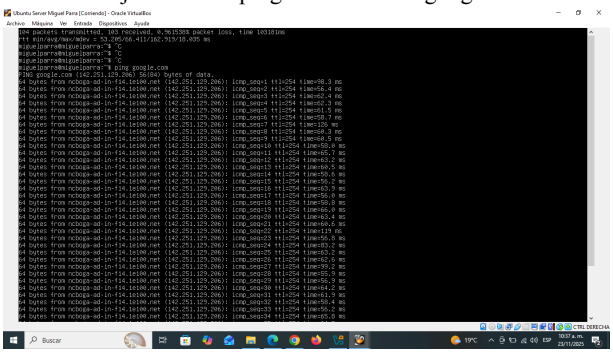
Desde el equipo Ubuntu Server ubicado en la zona naranja se realizaron pruebas de conectividad para validar la correcta salida hacia la red WAN.

Figura 19. Validación de acceso a Internet desde la zona naranja mediante ping al servidor 8.8.8.8.



Fuente: Autoría Propia

Figura 20. Validación de acceso a internet desde la zona naranja mediante ping al servidor de google.com

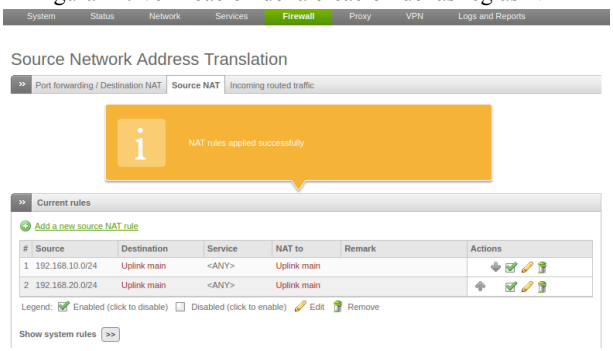


Fuente: Autoría Propia

Como resultado, los equipos de la DMZ lograron establecer comunicación hacia la red WAN simulada, verificando así el funcionamiento adecuado del NAT para tráfico saliente.

Finalmente, en el menú Firewall > Port Forwarding / NAT, se verificó la correcta creación y funcionamiento de las reglas NAT configuradas para permitir el tráfico saliente desde las zonas VERDE y NARANJA hacia la WAN. Ambas reglas se encuentran activas y aplicadas correctamente.

Figura 21. Verificación de la creación de las reglas NAT

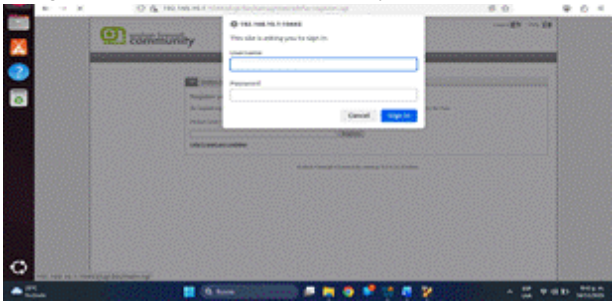


Fuente: Autoría Propia

2.3 TEMÁTICA 3 – PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

La configuración de servicios dentro de la zona DMZ es un componente crítico de la seguridad perimetral, ya que permite publicar servidores hacia el exterior sin comprometer la red interna. En esta temática se habilitaron únicamente los puertos necesarios (HTTP y FTP), aplicando el principio de mínimo privilegio, lo que reduce significativamente la superficie de ataque. Al mismo tiempo, el bloqueo de ICMP fortalece la protección del servidor al evitar respuestas que puedan ser utilizadas para reconocimiento o ataques de red. Esta gestión detallada del tráfico entrante y saliente demuestra la importancia de controlar selectivamente los servicios expuestos en la DMZ para mantener un entorno seguro y funcional. El producto esperado es habilitar los servicios HTTP y FTP en el servidor web bajo Ubuntu Server permitiendo el acceso a los puertos 80 y 21 desde la zona DMZ. Además, se debe denegar el protocolo ICMP bloqueando los puertos 8 y 30 para evitar respuestas de ping en la red. Finalmente, se debe verificar en el tráfico de salida la creación de las reglas de firewall implementadas.

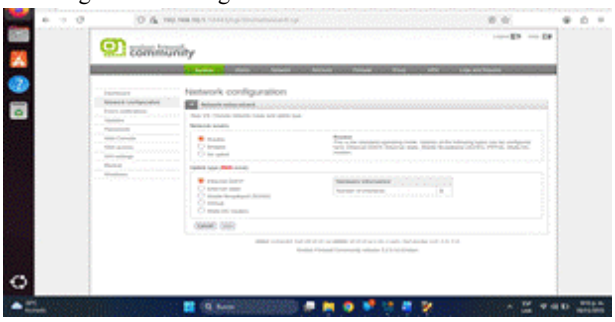
Figura 22. Autenticación de usuario y contraseña Endian.



Fuente: Autoría propia

Desde desktop accedemos a Endian por medio de https://192.168.10.1:10443 y nos loguemos.

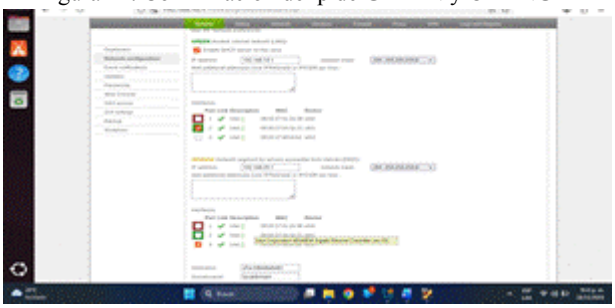
Figura 23. Configuración de RED en modo DHCP.



Fuente: Autoría propia

Confirmamos la configuración de RED (WAN).

Figura 24. Confirmación de ip de GREEN y ORANGE



Fuente: Autoría propia

Confirmamos la configuración de GREEN y ORANGE con sus respectivas ip.

Figura 25. Confirmación de configuración de RED en DHCP.

Fuente: Autoría propia

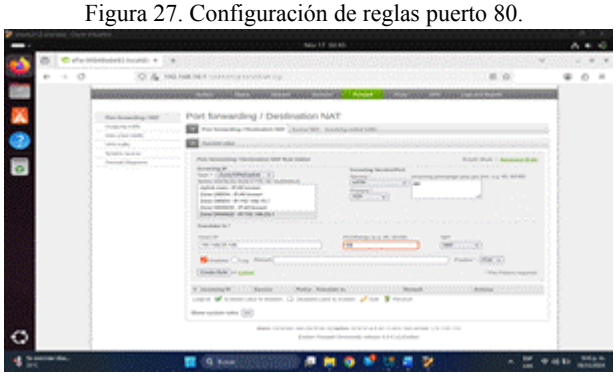
Confirmamos eth0 para RED.

Figura 26. Ingresamos al módulo firewall.

Fuente: Autoría propia

Nos dirigimos al módulo de firewall y le damos al botón de añadir una nueva regla.

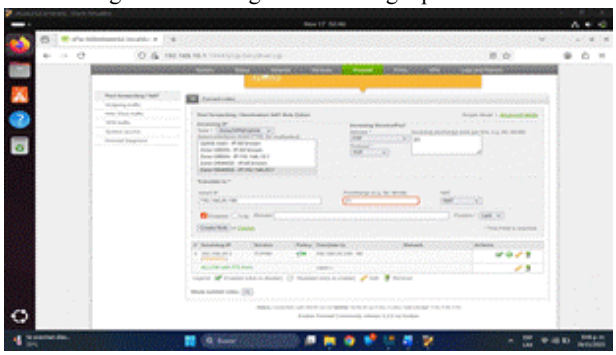
Figura 27. Configuración de reglas puerto 80.



Fuente: Autoría propia

Configuración de port forwarding en Endian Firewall para permitir el tráfico HTTP (puerto 80) hacia el servidor Ubuntu en la zona DMZ con la IP 192.168.20.100.

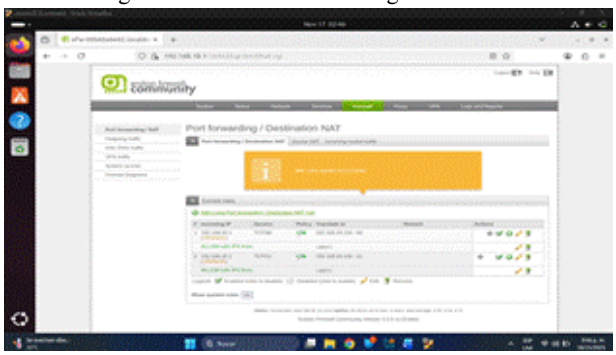
Figura 28. Configuración de regla puerto 21.



Fuente: Autoría propia

Configuración de port forwarding para permitir el tráfico FTP (puerto 21) hacia el servidor Ubuntu en la zona DMZ con la IP 192.168.20.100.

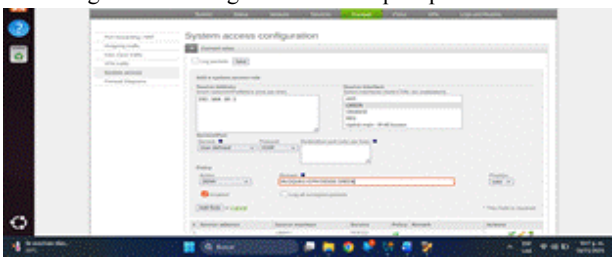
Figura 29. Visualización de reglas creadas.



Fuente: Autoría propia

Reglas creadas correctamente. La creación de reglas NAT es fundamental para permitir que las redes internas accedan a Internet sin exponer directamente sus direcciones privadas, reforzando la seguridad del entorno. Además, estas reglas garantizan un enrutamiento eficiente del tráfico, asegurando que cada zona se comunique correctamente según las políticas establecidas.

Figura 30. Configuración de bloqueo para ICMP.



Fuente: Autoría propia

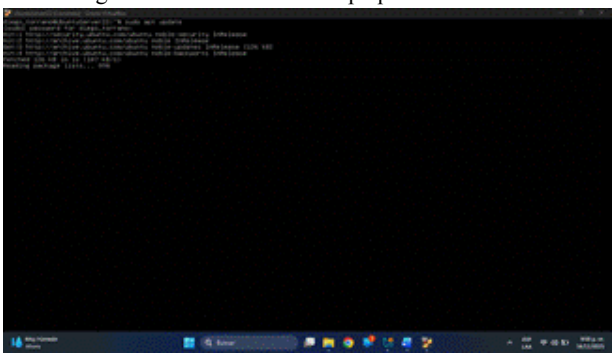
Regla de firewall en Endian Firewall para bloquear el tráfico ICMP desde la IP 192.168.10.1 en la interfaz GREEN (DMZ), con acción de denegar el tráfico.

Figura 31. Visualización de bloqueo.

Fuente: Autoría propia

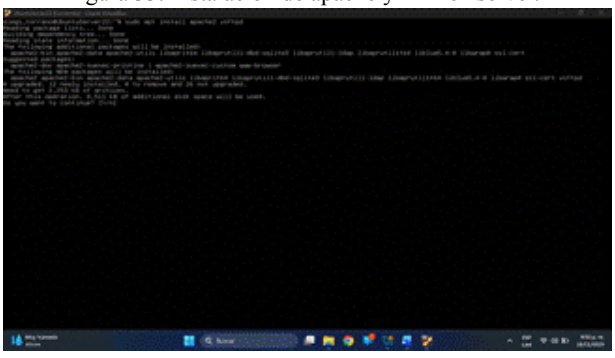
Bloqueo creado.

Figura 32. Actualización de paquetes en server.



Fuente: Autoría propia

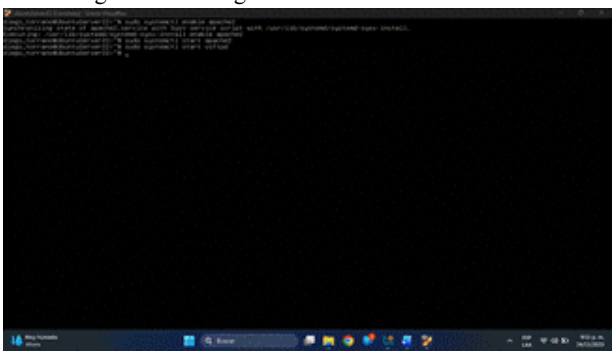
Figura 33. Instalación de apache y FTP en server.



Fuente: Autoría propia

Instalación de Apache y FTP en Ubuntu Server

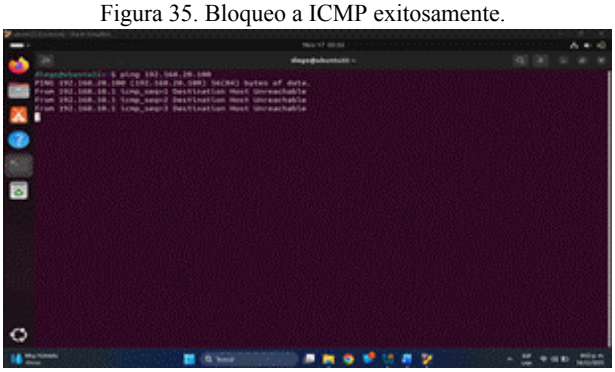
Figura 34. Configuración de servicios en server



Fuente: Autoría propia

Instalación de Apache y FTP en Ubuntu Server: Configuración de servicios HTTP y FTP.

Figura 35. Bloqueo a ICMP exitosamente.



Fuente: Autoría propia

El ping a la dirección IP de la red DMZ está siendo bloqueado, mostrando "Destination Host Unreachable", lo que indica que la regla para bloquear ICMP está funcionando correctamente.

2.4 TEMÁTICA 4 – REGLAS DE ACCESO PARA PERMITIR O DENEGAR TRÁFICO

La administración de tráfico entre zonas de seguridad constituye un componente esencial en el diseño de infraestructuras de red corporativas. La adecuada segmentación permite aislar recursos críticos, reducir la superficie de ataque y establecer controles granularmente definidos sobre los flujos permitidos. En este contexto, Endian Firewall Community se posiciona como una solución integral para la construcción de perímetros seguros, integrando funcionalidades como inspección de paquetes, gestión de interfaces, creación de zonas y establecimiento de políticas de comunicación.

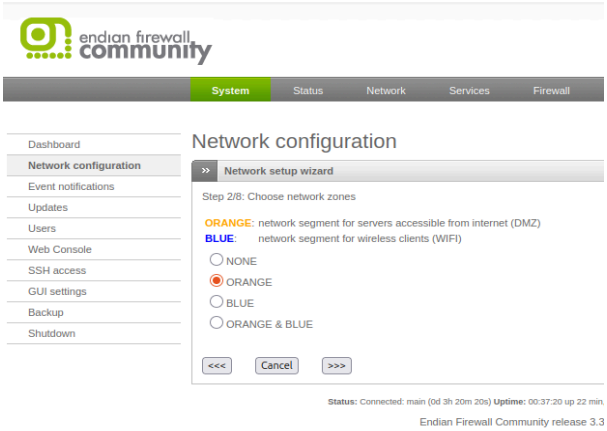
En la arquitectura tradicional, la zona Verde (LAN) se destina a los equipos internos de confianza; la zona Naranja (DMZ) alberga servicios expuestos; y la zona Roja (WAN) representa el entorno no confiable, usualmente asociado con Internet. El objetivo de la Temática 4 consiste en implementar reglas específicas que permitan, limiten o bloqueen el tráfico entre estas zonas, mediante protocolos HTTP y FTP, respetando los principios del mínimo privilegio y defensa en profundidad.

Cada interfaz fue verificada desde consola mediante el Network Configuration Wizard, asegurando que los roles fueran correctamente asociados y que las interfaces se encontraran en estado operativo (UP). A su vez, se configuraron los equipos cliente:

- Cliente LAN: 192.168.10.X → Gateway 192.168.10
- Servidor en DMZ (Ubuntu Server con Apache y FTP): 192.168.20.20 → Gateway 192.168.20.1

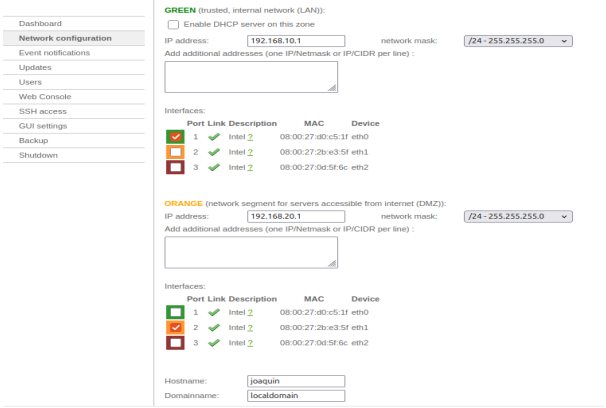
Esta disposición garantiza que el firewall se convierta en el único puente entre las zonas, centralizando todo el control del tráfico

Figura 36. Red estarán habilitadas; en este caso se selecciona ORANGE (DMZ)



Fuente: Autoría propia

Figura 37. Las zonas de red VERDE (LAN) y NARANJA (DMZ), asignando las direcciones



Fuente: Autoría propia

2.4.1 IMPLEMENTACIÓN DE REGLAS DE ACCESO ENTRE ZONAS (HTTP Y FTP)

La primera parte del ejercicio consistió en permitir el tráfico desde la zona Verde hacia la zona Naranja utilizando los protocolos HTTP (puerto 80/TCP) y FTP (puerto 21/TCP).

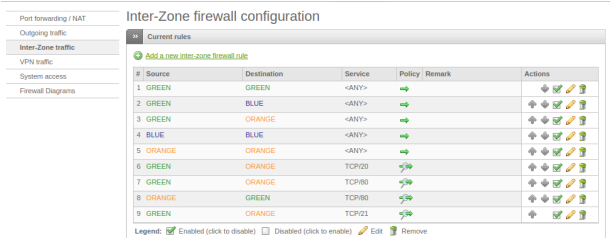
Para ello, se utilizó el módulo Tráfico entre Zonas dentro de la consola web de Endian.

La creación de cada regla implicó:

- Seleccionar VERDE como origen.
- Seleccionar NARANJA como destino.
- Definir el servicio (HTTP o FTP).
- Mantener la acción como Permitir con IP.
- Registrar el tráfico únicamente cuando fuera necesario.

Estas reglas permitieron habilitar el acceso desde los equipos de la LAN hacia los servicios alojados en la DMZ, manteniendo la DMZ aislada respecto a tráfico no autorizado.

Figura 38. Configuración del firewall Inter-Zona de Endian,



Fuente: Autoría propia

2.4.2 CONECTIVIDAD ENTRE LA WAN Y LA DMZ

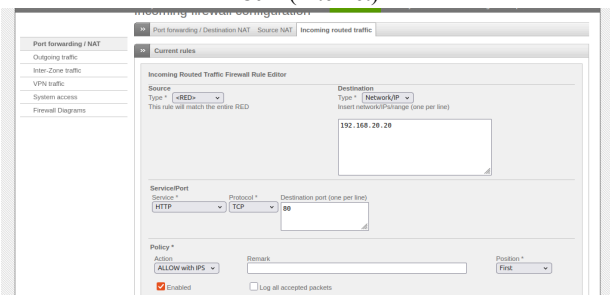
La segunda parte del objetivo consistió en permitir el tráfico proveniente de Internet hacia los servicios en la zona DMZ. Para ello se utilizaron las opciones de Tráfico enrutado de entrada (borde ROJO), ya que cualquier acceso externo debe filtrarse antes de ingresar a la red interna.

Las reglas creadas incluyeron:

- ROJO → 192.168.20.20 (HTTP/80)
- ROJO → 192.168.20.20 (FTP/21)

Estas reglas permiten el acceso controlado desde clientes externos, ideal para escenarios reales donde un servidor debe ser públicamente accesible.

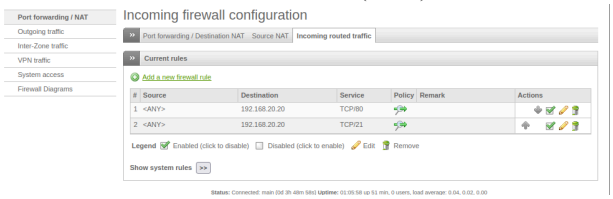
Figura 39. Tráfico HTTP (puerto 80) proveniente de la zona ROJA (Internet)



Fuente: Autoría propia

Las conexiones HTTP (TCP/80) y FTP (TCP/21) permiten que usuarios externos, ubicados en la zona roja (WAN), accedan a los servicios publicados en la zona naranja (DMZ). Esta configuración es esencial para que el servidor web o FTP pueda ofrecer contenido al público de forma controlada, sin exponer directamente la red interna.

Figura 40. Las conexiones HTTP (TCP/80) y FTP (TCP/21) en el tráfico entrante desde la ZONA ROJA (WAN) hacia la ZONA NARANJA (DMZ).



Fuente: Autoría propia

2.4.3 PRUEBAS FUNCIONALES Y VALIDACIÓN DEL TRÁFICO

Luego de crear las reglas, se realizaron pruebas desde:

- Navegadores en la LAN.
- Navegadores en la DMZ.

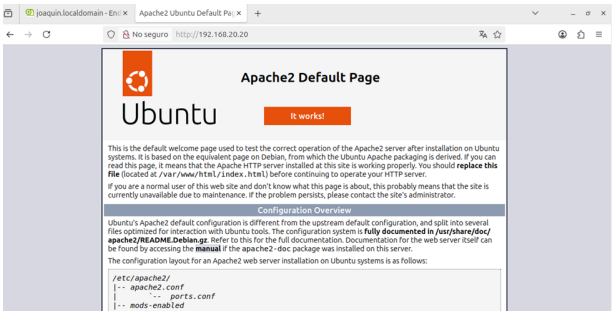
Conexiones simuladas desde la WAN (mediante red virtual). Se verificó:

- Acceso HTTP LAN → DMZ
- Acceso HTTP LAN → WAN
- Acceso HTTP DMZ → WAN
- Acceso FTP LAN → WAN
- Acceso FTP WAN → DMZ

Las pruebas mostraron que:

- El ping (ICMP) respondía adecuadamente entre zonas permitidas.
- Apache estaba activo escuchando en los puertos 80 y 443.
- Vsftpd respondía en el puerto 21.
- Las denegaciones producidas corresponden solo a reglas no definidas.

Figura 41. La regla HTTP desde LAN → DMZ funciona correctamente



Fuente: Autoría propia

Figura 42. El ping exitoso desde el servidor ubicado en la DMZ hacia la IP de la zona ROJA (192.168.20.1).

Fuente: Autoría propia

2.5 TEMÁTICA 5 – IMPLEMENTACIÓN DE UN PROXY HTTP CON AUTENTICACIÓN

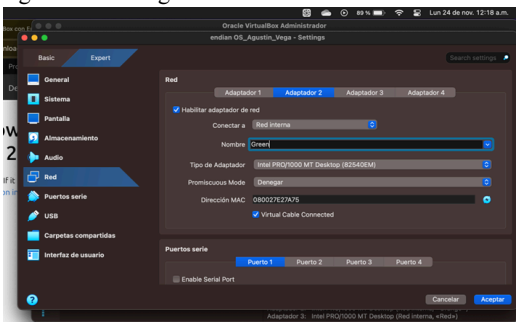
El objetivo de este laboratorio fue configurar un servidor proxy HTTP no transparente utilizando la plataforma Endian Firewall Community, permitiendo centralizar el control del tráfico de navegación web en una red corporativa mediante políticas de autenticación de usuarios y listas de control de acceso (ACL) basadas en categorías de sitios web.

2.5.1 PREPARACIÓN DEL ENTORNO VIRTUALIZADO

Antes de iniciar la configuración del proxy, se procedió a establecer la infraestructura necesaria en VirtualBox. Se descargó la imagen ISO de Endian Firewall desde su repositorio oficial y se creó una máquina virtual con tres interfaces de red configuradas de la siguiente manera:

- Interfaz 1 (GREEN): Red interna segura (192.168.10.0/24) destinada para clientes internos.
- Interfaz 2 (ORANGE): DMZ semitrusted (192.168.20.0/24) para servidores expuestos (opcional en este escenario).
- Interfaz 3 (RED): Conexión a Internet mediante DHCP desde la red NAT de VirtualBox.

Figura 43. Configuración de Red Green en virtual box



Fuente: Autoría Propia

La instalación de Endian Firewall siguió el asistente de configuración inicial (Network Setup Wizard), permitiendo seleccionar el modo de operación "Routed" y la configuración automática del DNS mediante revolvedores públicos (8.8.8.8). Esta arquitectura de tres zonas implementa el modelo de defensa en profundidad, separando el tráfico según su nivel de confianza.

Figura 44. Creación de Máquina virtual para Endian.

Fuente: Autoría Propia

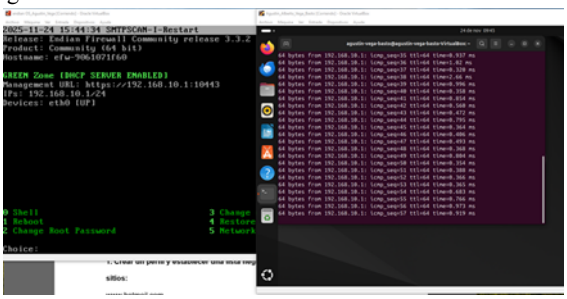
2.5.2 CONFIGURACIÓN DE LA RED GREEN Y VERIFICACIÓN DE CONECTIVIDAD

Una vez instalado Endian, se configuró el servidor DHCP en la zona GREEN para asignar direcciones IP automáticamente a los clientes (rango 192.168.10.100-192.168.10.200). Se creó una máquina virtual Ubuntu Desktop con interfaz de red configurada en la red interna GREEN, asignando manualmente IP 192.168.10.20.

Se realizaron pruebas básicas de conectividad:

- ping -c 3 192.168.10.1 (gateway Endian)
- ping -c 3 8.8.8.8 (prueba de salida a Internet)

Figura 45. Prueba de comunicación en consola Ubuntu Sever.



Fuente: Autoría Propia

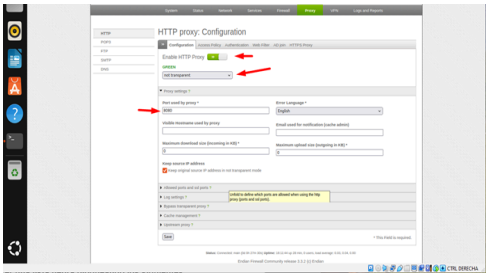
Ambas pruebas respondieron satisfactoriamente, confirmando que la topología de red estaba correctamente establecida y que Endian tenía acceso a Internet a través de su interfaz RED.

2.5.3 ACCESO A LA INTERFAZ WEB DE ENDIAN Y CONFIGURACIÓN PRELIMINAR

Desde el navegador Firefox en Ubuntu Desktop, se navegó a la dirección IP de Endian (192.168.10.1) para acceder al panel de administración web. Se autenticó con las credenciales por defecto (admin/password) y se procedió a explorar el módulo de System > Network configuration para verificar que:

- El DNS estaba configurado como 8.8.8.8 (solucionando el problema inicial de resolución de nombres).
- Las tres interfaces estaban activas y correctamente mapeadas.
- El enrutamiento dinámico y la salida a Internet estaban funcionales.

Figura 46. Prueba de comunicación en consola Ubuntu Sever.



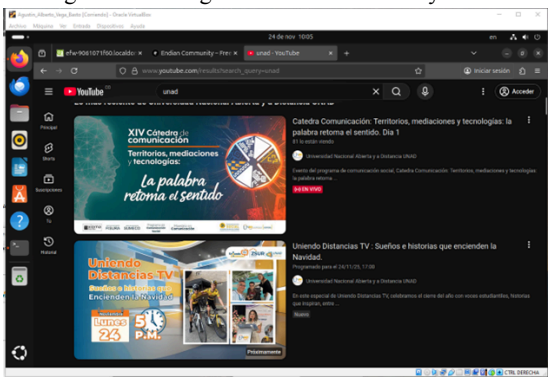
Fuente: Autoría Propia

2.5.4 PRUEBAS DE NAVEGACIÓN INICIAL (LÍNEA BASE)

Antes de configurar las restricciones, se realizaron pruebas navegando sin proxy hacia los sitios web que posteriormente formarían la lista negra:

- www.youtube.com → Navegación exitosa
- www.hotmail.com → Navegación exitosa
- www.elnuevodia.com.co → Navegación exitosa

Figura 47. Navegación exitosa en la url youtube



Fuente: Autoría Propia

Figura 48. Navegación exitosa en la url hotmail.

Fuente: Autoría Propia

Figura 49. Navegación exitosa en la url El nuevo día

Fuente: Autoría Propia

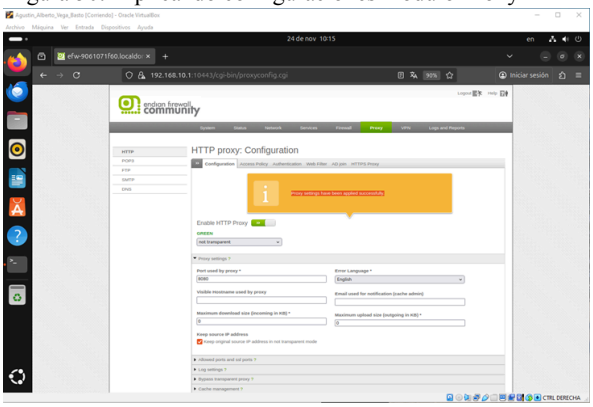
Este procedimiento estableció una línea base, demostrando que, en ausencia de políticas restrictivas, el cliente podía acceder a cualquier sitio web sin limitaciones.

2.5.5 CONFIGURACIÓN DEL PROXY HTTP NO TRANSPARENTE

Se accedió al módulo Proxy > HTTP > Configuration en la interfaz web de Endian. Se habilitó el servidor proxy HTTP en el puerto 8080 con las siguientes características:

- Transparente: Deshabilitado (garantiza que Firefox deba configurarse explícitamente).
- Listening Port: 8080
- Max connections: 5000
- Chaining proxy: Deshabilitado

Figura 50. Aplicando configuraciones módulo Proxy HTTP



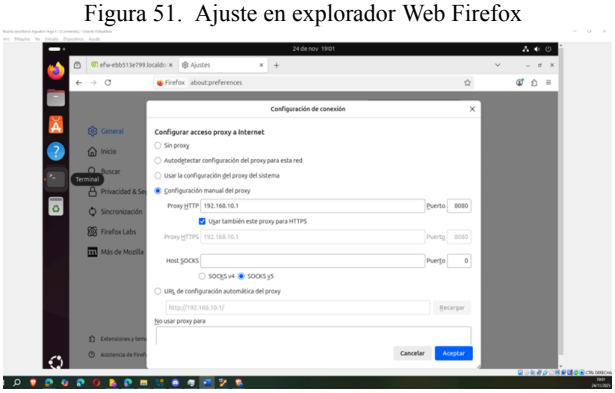
Fuente: Autoría Propia

En el navegador Firefox del cliente Ubuntu, se navegó a Preferences > Network > Settings y se configuró:

- HTTP Proxy: 192.168.10.1
- Puerto: 8080

Usar el mismo proxy para HTTPS: Habilitado

Figura 51. Ajuste en explorador Web Firefox



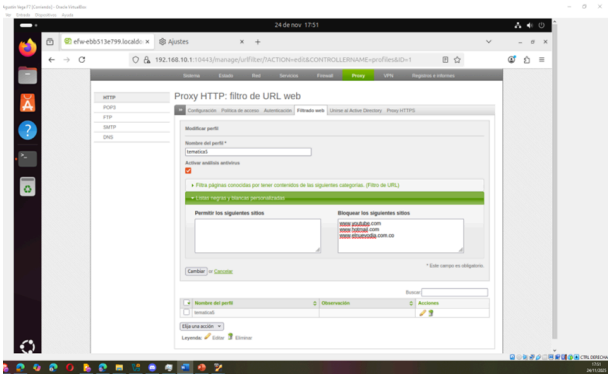
Fuente: Autoría Propia

2.5.6 CREACIÓN DE PERFIL WEB FILTER Y LISTA NEGRA

Se accedió a Proxy > HTTP > Web Filter y se creó un nuevo perfil denominado "temática 5" con las siguientes categorías bloqueadas:

- www.youtube.com
- www.hotmail.com
- www.elnuevodia.com.co

Figura 52. Configuración de Lista Negra



Fuente: Autoría Propia

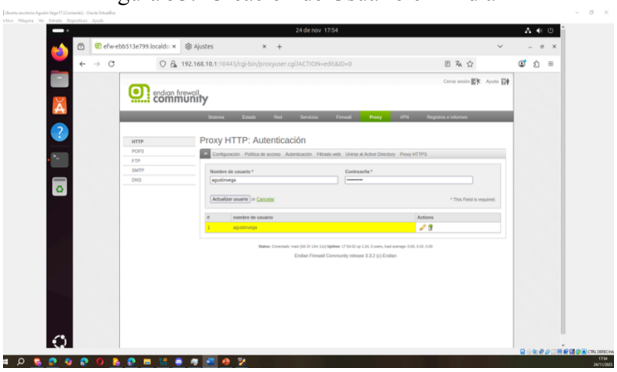
Se añadieron estos dominios manualmente a la lista negra del perfil, definiendo que cualquier intento de acceso hacia estas URLs resultaría en una página de error 403 Forbidden.

2.5.7 CONFIGURACIÓN DE AUTENTICACIÓN Y POLÍTICAS DE ACCESO

En Proxy > HTTP > Authentication, se configuró la autenticación mediante:

1. Creación de usuario: "agustinvega" con contraseña de 9 dígitos (cumpliendo requisitos de seguridad).

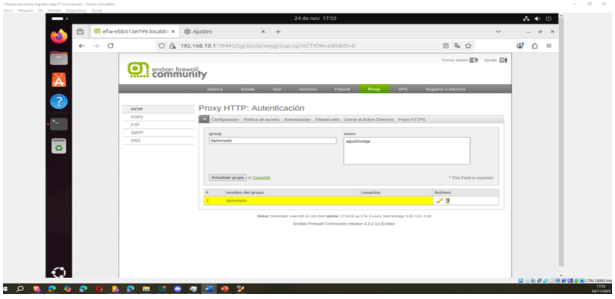
Figura 53. Creación de Usuario en Endian



Fuente: Autoría Propia

2. Creación de grupo: "diplomado", asociando al usuario "agustinvega" como miembro.

Figura 54. Creación de grupo para incluir el nuevo usuario

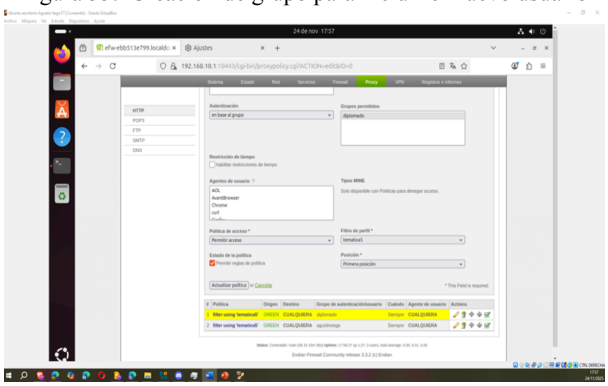


Fuente: Autoría Propia

3. Política de acceso (Access Policy):

- Source Zone: GREEN
- Source group: diplomado
- Authentication: Local (NCSA)
- Access policy: Allow access
- Filter profile: temática 5
- Prioridad: 1 (aplicar primero)

Figura 55. Creación de grupo para incluir el nuevo usuario



Fuente: Autoría Propia

Se aplicaron los cambios (System > Apply Changes) para que las configuraciones tomarán efecto en el demonio Squid del proxy.

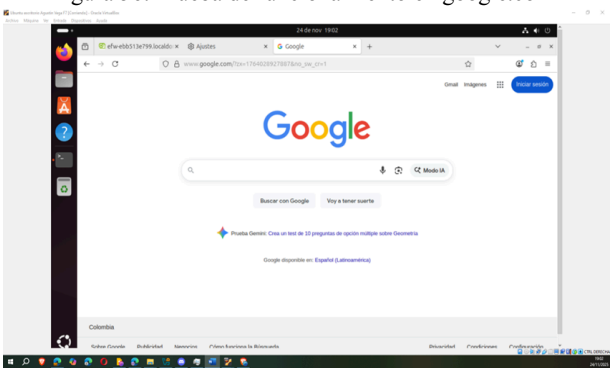
La configuración de autenticación y políticas de acceso es fundamental para asegurar que solo los usuarios autorizados puedan utilizar los servicios de red. Mediante este mecanismo, el firewall controla quién puede navegar, qué recursos puede usar y bajo qué condiciones, fortaleciendo el modelo de seguridad perimetral. Además, permite registrar y auditar las conexiones, facilitando la detección de comportamientos irregulares y garantizando un uso responsable y seguro de la infraestructura.

2.5.8 PRUEBAS DE FUNCIONAMIENTO CON PROXY ACTIVADO

Navegación a sitios permitidos (sin restricciones en la lista negra):

- www.google.com → Cargó correctamente

Figura 56. Prueba de funcionamiento en google.com



Fuente: Autoría Propia

- www.unad.edu.co → Cargó correctamente

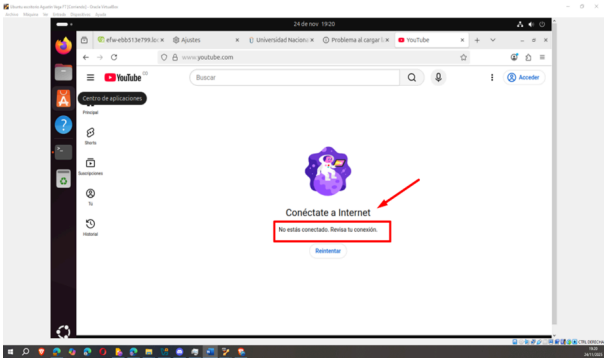
Figura 57. Prueba de funcionamiento en unad.edu.co

Fuente: Autoría Propia

Navegación a sitios bloqueados (en la lista negra):

- www.youtube.com → Error 403 Forbidden (Acceso denegado por policy)

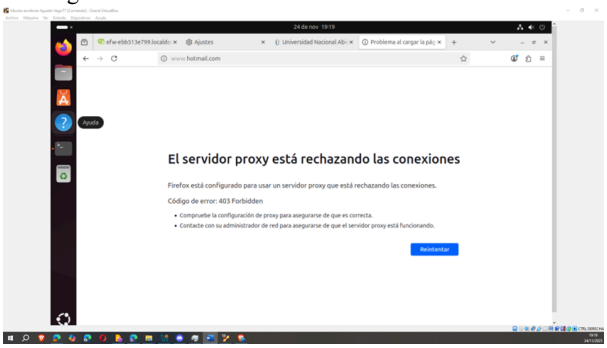
Figura 58. Prueba de funcionamiento en youtobe



Fuente: Autoría Propia

- www.hotmail.com → Error 403 Forbidden (Acceso denegado por policy)

Figura 59. Prueba de funcionamiento en hotmail.com

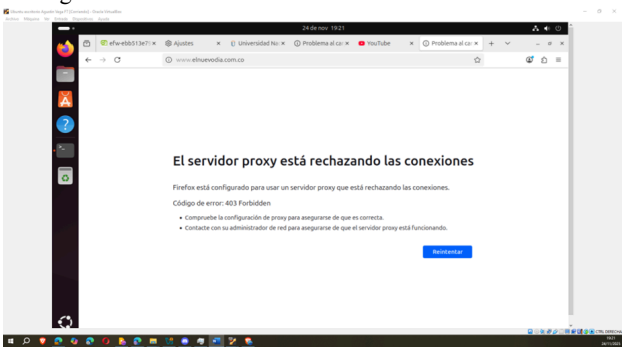


Fuente: Autoría Propia

El mensaje de error mostrado en Firefox especificaba que "El servidor proxy está rechazando las conexiones", confirmando que la política de filtrado estaba siendo aplicada correctamente.

- www.elnuevodia.com.co → Error 403 Forbidden (Acceso denegado por policy)

Figura 60. Prueba de funcionamiento en nuevodia.com



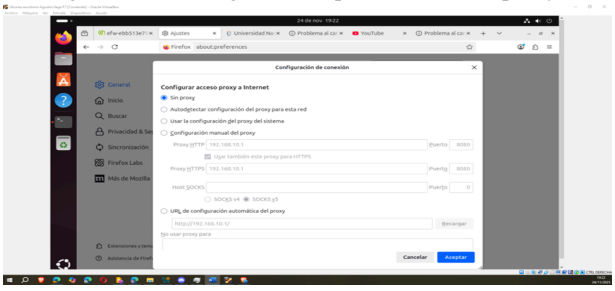
Fuente: Autoría Propia

2.5.9 VERIFICACIÓN SIN PROXY (COMPROBACIÓN COMPARATIVA)

Se deshabilitó la configuración del proxy en Firefox (Network Settings: No proxy) y se volvieron a acceder a los mismos sitios previamente bloqueados:

- www.youtube.com → Cargó correctamente
- www.hotmail.com → Cargó correctamente
- www.elnuevodia.com.co → Cargó correctamente

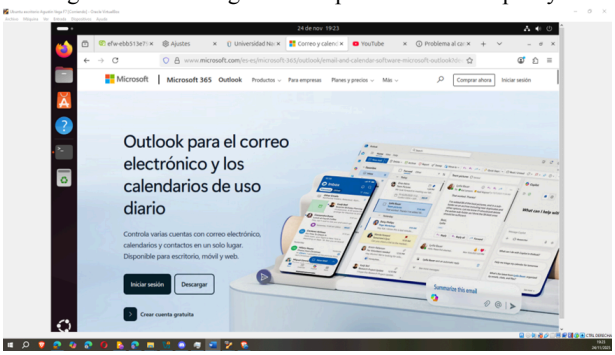
Figura 61. Reconfigurando explorador web sin proxy



Fuente: Autoría Propia

Este resultado demostró que el bloqueo era causado exclusivamente por las políticas de Endian, no por restricciones de red o DNS, validando que el proxy estaba funcionando como control centralizado del tráfico web.

Figura 62. Reconfigurando explorador web sin proxy



Fuente: Autoría Propia

2.5.10 ANÁLISIS DE LOGS Y VALIDACIÓN

Se consultaron los registros de proxy en Proxy > Logs and Reports para verificar que:

- Las conexiones bloqueadas fueron registradas con timestamp, usuario autenticado y URL solicitada.
- El perfil "temática 5" fue aplicado correctamente a cada solicitud.
- No hubo conexiones fallidas por autenticación (indicador de que la política fue correctamente vinculada al usuario).

3. CONCLUSIONES

3.1 TEMÁTICA 1

La configuración inicial de Endian Firewall en VirtualBox permitió establecer la base estructural del entorno de seguridad perimetral. La correcta asignación de las tarjetas de red y la instalación del sistema garantizaron que el firewall reconociera cada zona (verde, naranja y roja) con sus respectivas funciones. Este proceso fue esencial para habilitar la segmentación de la red, la administración del tráfico y la posterior implementación de reglas y servicios de seguridad. En conjunto, la temática 1 demostró la importancia de una instalación precisa para asegurar el funcionamiento adecuado del firewall y de todas las temáticas desarrolladas posteriormente.

3.2 TEMÁTICA 2

La configuración de NAT en Endian Firewall demostró ser un componente clave para garantizar la conectividad y la seguridad dentro del entorno perimetral implementado. A través del enmascaramiento de direcciones fue posible permitir que los equipos de la LAN accedieron a la WAN sin comprometer su identidad interna, fortaleciendo la protección del sistema y asegurando el flujo adecuado del tráfico. Las pruebas de conectividad confirmaron la operatividad del esquema NAT y su correcta integración con las demás zonas de seguridad, contribuyendo de manera directa al cumplimiento del propósito general de la actividad y al fortalecimiento de las competencias en administración de redes y sistemas GNU/Linux.

3.3 TEMÁTICA 3

La realización de este trabajo permitió consolidar de manera clara los conocimientos sobre la instalación, configuración y administración del sistema Endian. A lo largo del proceso se evidenció la importancia de comprender la estructura de las zonas de red GREEN, ORANGE, WAN y DMZ y cómo cada uno cumple un rol fundamental en la seguridad y el funcionamiento de la infraestructura. Asimismo, la creación y verificación de reglas en el firewall, como la habilitación de los puertos 80 y 21 para los servicios HTTP y FTP, y el bloqueo del protocolo ICMP, permitió aplicar conceptos prácticos de control de tráfico y protección de la red.

Esta actividad fortaleció mi capacidad para gestionar entornos seguros, interpretar configuraciones técnicas y asegurar que los servicios funcionen adecuadamente dentro de un esquema organizado y protegido.

3.4 TEMÁTICA 4

La implementación de reglas de acceso en el firewall Endian permitió evidenciar la importancia de una adecuada administración del tráfico entre zonas con distintos niveles de confianza. A través de la configuración y verificación de políticas para los protocolos HTTP y FTP, se comprobó que la segmentación en zonas Verde (LAN), Naranja (DMZ) y Roja (WAN) constituye un mecanismo efectivo para controlar la superficie de exposición y fortalecer la seguridad perimetral. La creación de reglas específicas facilitó el tránsito autorizado de servicios entre segmentos críticos, al tiempo que bloqueó conexiones no permitidas, garantizando así el principio del mínimo privilegio.

Asimismo, las pruebas realizadas desde diferentes puntos de la arquitectura confirmaron que la DMZ opera como un espacio intermedio seguro, donde los servicios expuestos hacia la WAN pueden mantenerse disponibles sin comprometer la red interna. La plataforma Endian demostró ser una solución robusta para gestionar flujos diferenciados, permitiendo monitorear, registrar y validar el comportamiento del tráfico según las políticas definidas.

En conjunto, la práctica permitió comprender de manera aplicada cómo un firewall perimetral, correctamente configurado, contribuye a la defensa en profundidad, asegurando la continuidad del servicio y la protección de los activos tecnológicos. La experiencia evidenció que la correcta creación, ordenamiento y prueba de reglas es esencial para garantizar un funcionamiento adecuado en entornos reales donde la segregación de redes y el acceso seguro son fundamentales.

3.5 TEMÁTICA 5

La implementación exitosa de un proxy HTTP no transparente con Endian Firewall Community demostró cómo centralizar la administración de acceso a Internet mediante autenticación de usuarios, perfiles de filtrado web y listas negras, implementando un control granular del tráfico de red basado en políticas y categorías de contenido.

4. REFERENCIAS

[1] G. Obregón-Pulido, B. Castillo-Toledo and A. Loukianov, *"A globally convergent estimator for n frequencies"*, IEEE Trans. On Aut. Control. Vol. 47. No 5. pp 857-863. May 2002.

[2] H. Khalil, *"Nonlinear Systems"*, 2nd. ed., Prentice Hall, NJ, pp. 50-56, 1996.

[3] Francis. B. A. and W. M. Wonham, *"The internal model principle of control theory"*, Automatica. Vol. 12. pp. 457-465. 1976.

[4] E. H. Miller, *"A note on reflector arrays"*, IEEE Trans. Antennas Propagat., Aceptado para su publicación.

[5] Sanabria Duran, K. D. *Implementación de seguridad en GNU/LINUX usando Endian firewall para la protección LAN/DMZ/WAN.* https://repository.unad.edu.co/handle/10596/68794

[6] Gómez Rojas, G. V., Goyeneche Goyeneche, A. L., Moreno Guaidia, N. J., & Tibocha Coronado, Y. *Seguridad perimetral con*

Endian firewall. https://repository.unad.edu.co/handle/10596/69074

[7] Gomes, J. R. D. F. (2023). *Segurança de redes de computadores: um estudo sobre o Endian Firewall*. https://repositorio.pucgoias.edu.br/jspui/handle/123456789/6739

[8] López, J. G., & Navarro, R. B. (2006). *Seguridad en sistemas operativos Windows y Linux*. Ra-Ma.

[9] López, J. G. (2022). *Administración de sistemas GNU/LINUX®*. Ediciones de la U.

[10] Jorba Esteve, J., Suppi Boldrito, R., Megías Jiménez, D., & Mas, J. (2004). *Administración avanzada de GNU-Linux: Software libre*. Barcelona, Fundació per a la Universitat Oberta de Catalunya. 2012.

[11] Desnoyers, M., & Dagenais, M. R. (2006, July). *The lttng tracer: A low impact performance and behavior monitor for gnu/linux. In OLS* (Ottawa Linux Symposium) (Vol. 2006, pp. 209-224). Citeseer.

[12] García, J. Á. (2008). *GNU/LINUX Endian: Endian Firewall Security Appliance. Mundo Linux: Sólo programadores Linux*, (103), 34-40.