FORTALECIENDO LA SEGURIDAD DE REDES: IMPLEMENTACIÓN DE VIRTUALBOX EN EL FIREWALL GNU/LINUX ENDIAN

Esteban Lozano Pulido
elozanop@unadvirtual.edu.co
Karen Natalia Bravo Giraldo
knbravog@unadvirtual.edu.co
Johan Sebastian Alvarez Rodriguez
jsalvarezro@unadvirtual.edu.co
David Santiago Ospina Piratoba
dsospinap@unadvirtual.edu.co
Luis Alejandro Delgadillo Garcia
ladelgadillog@unadvirtual.edu.co

RESUMEN: *Mediante una exploración exhaustiva de VirtualBox, un entorno de virtualización, podemos encontrar fácilmente su aplicación en el firewall GNU/Linux Endian 3.X. Cuanto más profundizamos, más apreciamos la libertad ilimitada que aporta a la realidad bajo una guía teórica. Al comparar dos infraestructuras subyacentes completamente diferentes, revelamos en profundidad las diferencias entre ellas, proporcionando así una base más sólida para la posterior selección de arquitecturas seguras y fiables. Mediante una planificación y configuración meticulosas, dividimos la red en tres áreas principales: una red de área local (LAN) interna, una red de banda ancha (WAN) externa y una zona DMZ relativamente independiente. Esto permite tanto la apertura externa como el aislamiento interno. Las solicitudes ICMP externas están bloqueadas, lo que proporciona un cierto grado de seguridad. También habilitamos servicios HTTP y FTP externos dentro de la DMZ, con nuestros servidores HTTP y FTP internos gestionando las solicitudes externas, manteniendo así la apertura externa. Definimos reglas de acceso apropiadas tanto para el acceso entre zonas externo como interno. Finalmente, todas las solicitudes HTTP salientes se enrutan mediante proxy con autenticación de usuario y no son transparentes. Este modelo de gestión, práctico y eficiente no solo simplifica enormemente la gestión de la seguridad de la red empresarial, sino que también proporciona una plataforma fiable para la defensa de la seguridad de la red.*

PALABRAS CLAVE: Firewall, Endian, Redes y Seguridad perimetral.

ABSTRACT: *Through an exhaustive exploration of VirtualBox, a virtualization environment, we can easily find its application in the GNU/Linux Endian 3.X firewall. The deeper we delve, the more we appreciate the unlimited freedom it brings to reality under a theoretical guide. By comparing two completely different underlying infrastructures, we reveal in depth the differences between them, thus providing a stronger foundation for the subsequent selection of secure and reliable architectures. Through meticulous planning and configuration, we divided the network into three main areas: an internal local area network (LAN), an external wide area network (WAN), and a relatively independent DMZ zone. This allows for both external openness and internal isolation. External ICMP requests are blocked, providing a certain degree of security. We also enabled external HTTP and FTP services within the DMZ, with our internal HTTP and FTP servers managing external requests, thereby maintaining external openness. We defined appropriate access rules for both external and internal zone access. Finally, all outgoing HTTP requests are routed through a proxy with user authentication and are non-transparent. This practical and efficient management model not only greatly simplifies the management of enterprise network security but also provides a reliable platform for network security defense.*

KEYWORDS: Firewall, Endian, Networks, and Perimeter Security.

1 INTRODUCCIÓN

Como soporte fundamental para las empresas, la seguridad del perímetro de la red es primordial, lo que la convierte en un requisito esencial para las soluciones de gestión de GNU/Linux. Con la creciente prevalencia de las redes y la continua revalorización de los activos digitales, la urgente necesidad de protegerlos ha impulsado el rápido desarrollo de soluciones de firewall de código abierto. Estas soluciones integran numerosas funciones de firewall, NAT, proxy y VPN en una única interfaz, mejorando significativamente la eficiencia y desempeñando un papel crucial en la gestión de redes de tamaño pequeño a mediano. En particular, admiten el flujo de tráfico basado en temas, lo que permite categorizar el tráfico de red en diferentes flujos según los temas. Esto facilita la obtención de estadísticas, la monitorización y el control de los diferentes flujos de tráfico, y permite tratarlos de forma diferente, lo que resulta muy útil para la gestión de grandes redes. Una de las características más destacadas es su compatibilidad con el flujo de tráfico basado en temas, que permite segmentar el tráfico de red en diferentes flujos según los temas. Esto facilita la obtención de estadísticas, la monitorización y el control del tráfico en los diferentes flujos, y permite un tratamiento diferente del tráfico dentro de cada flujo, lo que resulta fundamental para la gestión de grandes redes. Mediante un control preciso del tráfico en diferentes zonas de red (como el aislamiento verde, naranja y rojo), los valiosos recursos internos se protegen eficazmente de redes externas maliciosas.

El presente artículo documenta la implementación colaborativa de cinco componentes de seguridad perimetral

sobre Endian Firewall en un entorno virtualizado, los cuales conformen a Tomala y Argoti (2024) permiten con VirtualBox: la instalación y configuración inicial de zonas de red, la configuración de NAT, la habilitación de servicios en la DMZ, la definición de reglas de acceso inter-zona, y la implementación de un proxy HTTP con autenticación. Cada componente fue desarrollado de forma individual por los integrantes del grupo y consolidado en este artículo como resultado grupal.

2 TEMATICA 1: INSTALACIÓN Y CONFIGURACIÓN DE LA DISTRIBUCIÓN ENDIAN

2.1 INSTALACIÓN ENDIAN

En esta sección de este artículo se relata el proceso realizado para descargar, configurar e instalar Endian, el cual según Escobar et, al. (2023) es una herramienta de distribución Open Source basada en Linux, diseñada no solo para funcionar como un cortafuegos, sino también como una solución integral para proteger su red de amenazas externas. Ofrece la mayoría de los servicios que proporciona un UTM (Gestión Unificada de Amenazas), siendo fácil de usar e instalar. Su función ha permitido la segmentación de redes en zonas específicas, lo que contribuyó a una gestión más eficiente y segura de los recursos informáticos.

El primer paso consistió en la descarga del software. Se accedió al sitio web oficial de Endian, donde se encontraba disponible la última versión de Endian UTM. Se seleccionó la versión adecuada en formato ISO, asegurándose de que se tratara de la más reciente y segura.

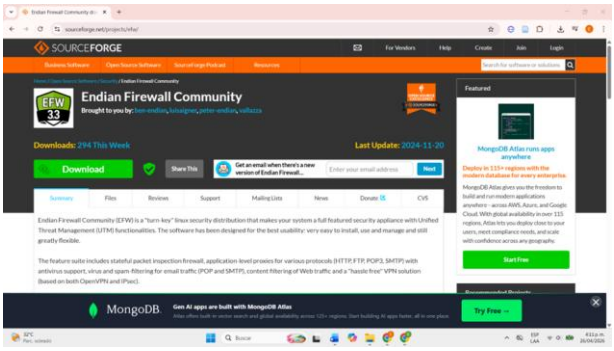

Figura 1. Descarga Endian. Fuente: de autoría propia.

Con el archivo ISO preparado, se procedió a la configuración de la máquina virtual en un entorno como VirtualBox. Se inició VirtualBox y se creó una nueva máquina virtual, a la que se le asignó un nombre representativo, como "Endian". Durante esta etapa, se seleccionó el tipo de sistema operativo adecuado y se asignó una cantidad de memoria RAM suficiente para el correcto funcionamiento del firewall. Posteriormente, se creó un disco duro virtual, configurando el almacenamiento de manera que se adaptara a las necesidades de la instalación.

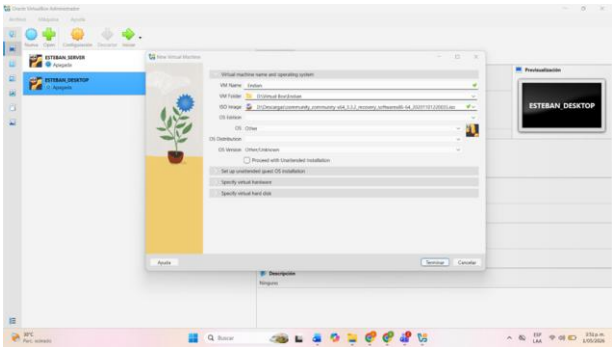

Figura 2. Configuración Virtual Box. Fuente: de autoría propia.

Una parte esencial de la configuración de Endian fue la segmentación de la red en diferentes zonas, este proceso conforme a Villareal (2024) el diseño de la red permite establecer un mapa de conexión útil para la arquitectura de red. Para ello, se configuraron adaptadores de red dentro de la máquina virtual. El primer adaptador se estableció como "Adaptador puente", permitiendo la conexión a la red externa y formando así la Zona roja (WAN). El segundo adaptador se configuró como "Red interna", creando la Zona verde (LAN), que era esencial para la comunicación interna. Si el diseño de la red lo requería, se activó un tercer adaptador para la Zona naranja (DMZ), que albergaría servidores que necesitaban acceso externo. La configuración se presenta a continuación.

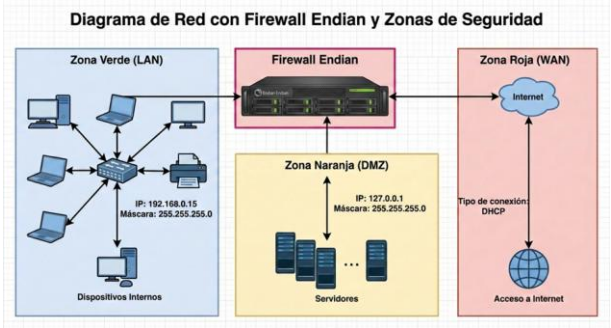

Figura 3. Estructura de zonas de red. Fuente: de autoría propia.

Una vez que la máquina virtual estuvo configurada y los adaptadores de red fueron correctamente establecidos, se inició la máquina virtual de Endian. Durante el arranque, se seleccionó el archivo ISO previamente descargado, permitiendo que el instalador de Endian se ejecutara. El proceso de instalación resultó ser intuitivo; se siguió el asistente, eligiendo el idioma y aceptando los términos de la licencia. La instalación se realizó de manera automática, aunque se tuvo la opción de ajustar las particiones según las necesidades específicas.

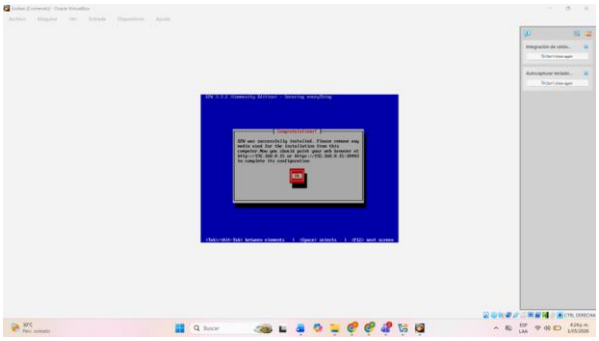

Figura 4. Instalación Endian en máquina virtual. Fuente: de autoría propia.

Tras completar la instalación, se reinició la máquina virtual, asegurándose de que se iniciara desde el disco duro virtual. En este punto, se accedió a la interfaz de gestión de Endian a través de un navegador web, introduciendo la dirección IP asignada al firewall. Las credenciales predeterminadas permitieron el acceso inicial, y desde allí, se procedió a realizar la configuración de las zonas de red. La Zona verde se estableció con una dirección IP específica, mientras que la Zona roja se configuró para permitir el acceso a Internet. La Zona naranja, si fue necesaria, se ajustó para garantizar que los servidores tuvieran la conectividad requerida.

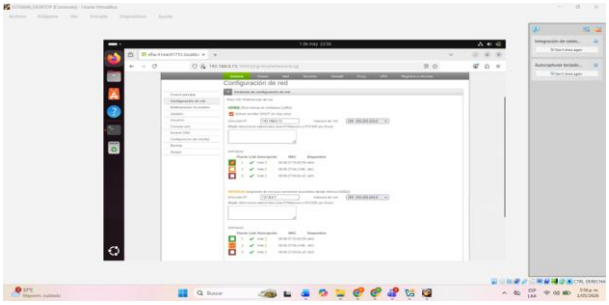

Figura 5. Configuración y verificación de adaptadores de red Fuente: de autoría propia.

Seguido, se llevó a cabo una verificación de la conectividad de la red. Desde la máquina Endian, se realizaron pruebas de ping a diversas direcciones IP, tanto internas como externas, para confirmar que la configuración era correcta y que todos los dispositivos podían comunicarse adecuadamente. Este proceso de verificación respalda lo planteado por Perdigon (2022) expresando que Endian brinda un conjunto de funcionalidades que contribuye a elevar la seguridad en la red de datos, ya que en este caso no solo aseguró que el sistema estuviera operativo, sino que también proporcionó una mayor confianza en la seguridad de la red.

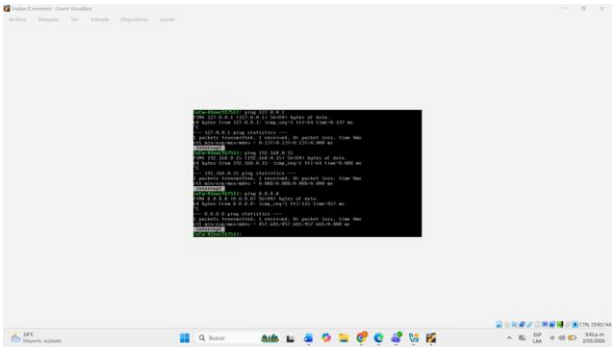

Figura 6. Evidencia de conexión activa. Fuente: de autoría propia.

3 TEMÁTICA 2: CONFIGURACIÓN NAT

En esta práctica se configuró Endian Firewall para aplicar reglas de NAT y Port Forwarding. Estas reglas permiten traducir las direcciones IP privadas de las zonas internas (LAN y DMZ) hacia la IP pública asignada a la interfaz WAN del firewall. De esta manera, según Sanabria (2025) múltiples equipos dentro de la red local pueden compartir una única dirección pública para acceder a Internet, mientras que los servicios alojados en la DMZ pueden ser publicados externamente mediante redirección de puertos

3.1 INSTALACIÓN Y VALIDACIÓN DE ENDIAN FIREWALL

En la Figura 7 se observa el correcto funcionamiento del firewall luego de su instalación. El sistema se encuentra operativo y listo para administrar el tráfico de red

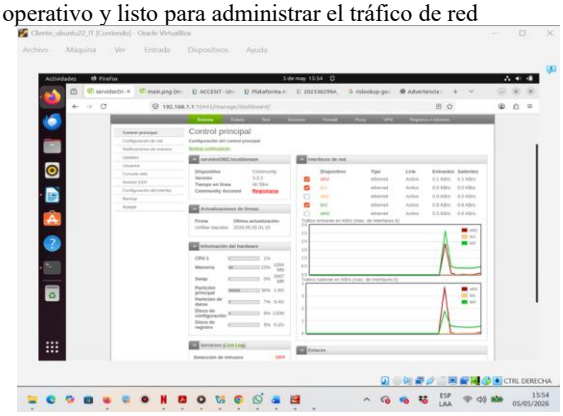

Figura 7. Funcionamiento correcto de Endian Firewall Fuente: Autoría Propia

3.1.1 VALIDACIÓN DE INTERFACES

En la Figura 8 se muestran las interfaces activas configuradas en el firewall:

- GREEN: Red LAN interna.
- ORANGE: Zona DMZ.
- RED: Conexión WAN/Internet.

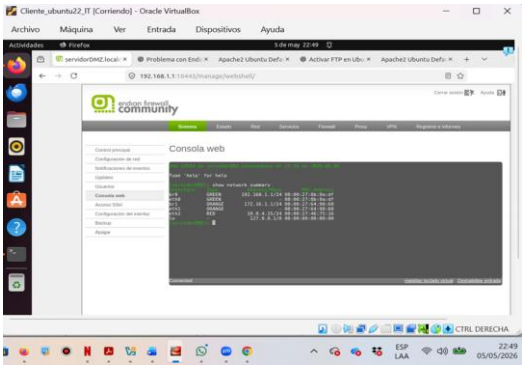

Figura 8. Interfaces activas del firewall. Fuente: Autoría Propia

3.1.2 VALIDACIÓN DE CONECTIVIDAD

En esta fase de la práctica se realizaron pruebas de conectividad entre las interfaces orange (DMZ) y green (LAN) utilizando el comando ping hacia sus respectivas puertas de enlace configuradas en Endian. Desde un cliente en la zona verde se verificó la comunicación con la dirección 192.168.1.1, mientras que desde la zona naranja se comprobó la respuesta de la dirección 192.16.1.1. Es conveniente validar la conexión, en palabras de Quijano et, al. (2025)Estas validaciones iniciales permiten confirmar la correcta interacción entre las zonas de red y constituyen la base para aplicar posteriormente las configuraciones necesarias dentro del laboratorio.

En la Figura 9 se validó la conectividad entre las interfaces mediante pruebas de puerta de enlace utilizando comandos de red.

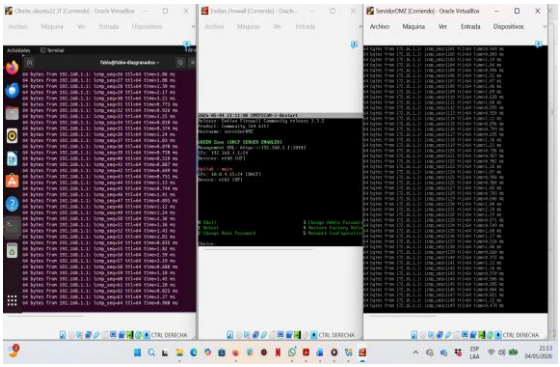

Figura 9. Validación de conectividad entre interfaces . Fuente: Autoría Propia

3.1.3 CONFIGURACIÓN NAT PARA LA RED LAN (GREEN → WAN)

La traducción de direcciones de red (NAT) posibilita que varios equipos dentro de una red privada puedan acceder a Internet utilizando una sola dirección IP pública. De esta forma, se optimiza el uso de direcciones y se facilita la comunicación externa de múltiples dispositivos a través de un único identificador público.

3.1.4 CONFIGURACIÓN DE REGLAS NAT

En este procedimiento se configuraron reglas de NAT dentro de Endian Community para permitir que las redes internas GREEN (LAN) y ORANGE (DMZ) accedieran a Internet mediante SNAT/MASQUERADE. Además, se implementaron reglas de DNAT (Port Forwarding) con el fin de publicar servicios como HTTP y FTP alojados en un servidor de la zona DMZ, asegurando tanto la conectividad hacia el exterior como la disponibilidad de servicios internos para usuarios externos.

En la Figura 10 se muestra la configuración inicial de NAT para las redes GREEN y ORANGE.

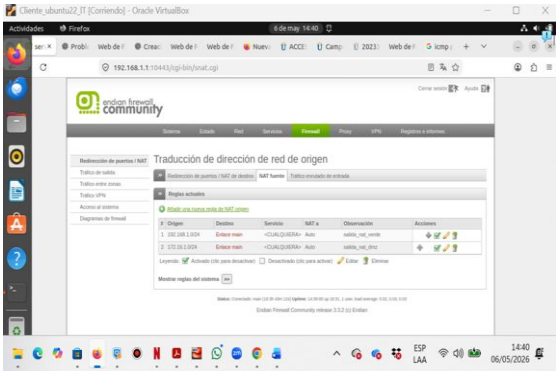

Figura 10. Configuración NAT para GREEN y ORANGE Fuente: de autoría propia**.**

3.1.5 ASIGNACIÓN DE DIRECCIONES IP

En la Figura 11 se observa la configuración específica de la red GREEN junto con las direcciones IP correspondientes.

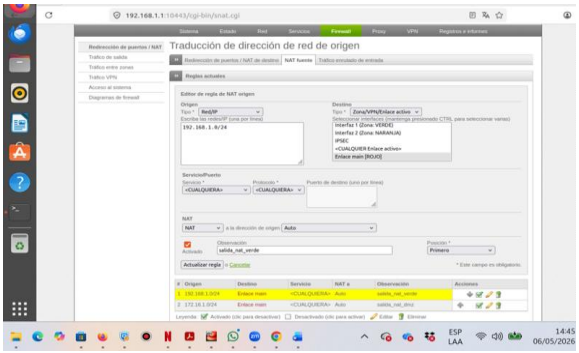

Figura 11. Configuración IP de la red GREEN. Fuente: de autoría propia.

3.1.6 CONFIGURACIÓN NAT PARA LA DMZ (ORANGE → WAN)

La zona ORANGE fue configurada como DMZ para alojar servicios accesibles desde el exterior manteniendo aislamiento respecto de la red interna.

En la Figura 12 se muestra la configuración NAT aplicada a la red ORANGE.

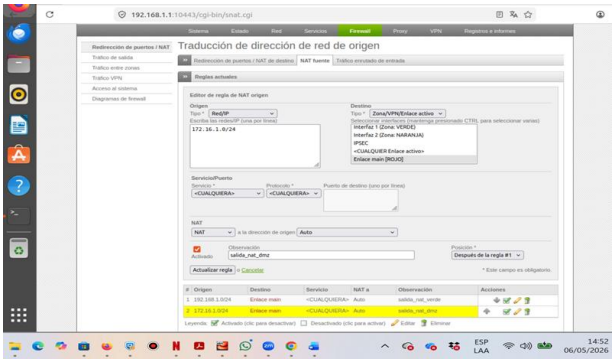

Figura 12. Configuración NAT para la DMZ. Fuente: de autoría propia.

3.1.7 CONFIGURACIÓN DE PORT FORWARDING / DNAT

El Port Forwarding permite redirigir tráfico externo hacia servicios específicos alojados en la DMZ.

3.1.8 CONFIGURACIÓN DE PUERTOS

En las Figuras 13 y 14 se configuró la redirección de los puertos:

- Puerto 80 (HTTP)
- Puerto 21 (FTP)

Estas reglas permiten el acceso externo a los servicios web y FTP del servidor DMZ.

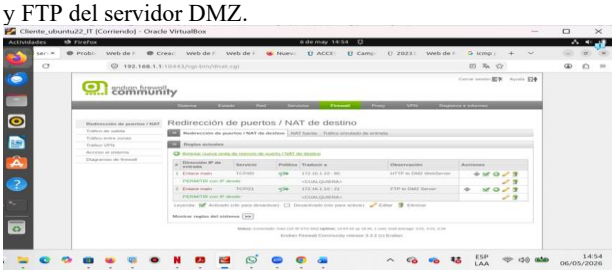

Figura 13. Configuración del puerto 80 y 21Autoría propia.

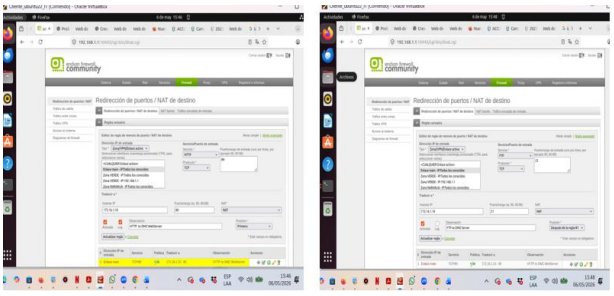

Figura 14. Reglas DNAT configuradas. Fuente: de autoría propia.

3.1.9 VALIDACIÓN DE TRÁFICO DE ENTRADA

La Figura 15 muestra las reglas NAT aplicadas al tráfico entrante.

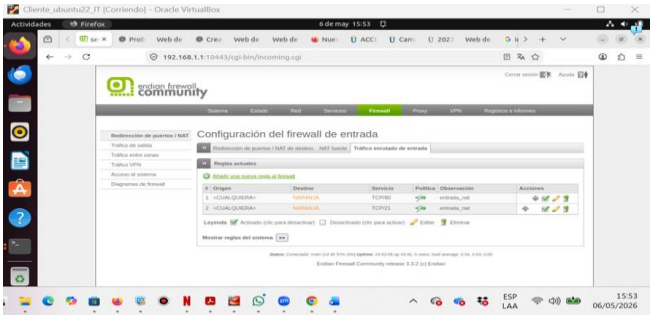

Figura 15. Validación del tráfico de entrada NAT. Fuente: de autoría propia.

3.1.10 VALIDACIÓN DE TRÁFICO DE SALIDA

En esta sección de configuración se gestionó la salida de puertos habilitados en las reglas NAT correspondientes a la zona naranja (DMZ), tal como lo requería el laboratorio. Es conveniente la implementación de medidas de seguridad, según Saboya et, al. (2025) dado que esta zona está destinada a los servidores, resulta necesario aplicar mayores restricciones para garantizar un nivel adecuado de seguridad.

En la Figura 16 se observa la configuración aplicada al tráfico de salida. Las reglas predeterminadas fueron ajustadas, permitiendo el acceso general desde la zona verde (LAN) y únicamente las conexiones necesarias desde la zona naranja (DMZ). Estas políticas pueden modificarse posteriormente según las necesidades específicas de cada entorno.

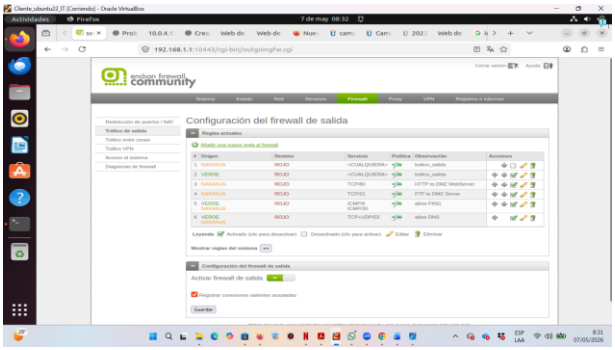

Figura 16. Configuración del tráfico de salida. Fuente: de autoría propia.

3.1.11 VALIDACIÓN DE REGLAS NAT

Para verificar las reglas configuradas se utilizó el comando: iptables -t nat -L -n -v en el endian. La salida permitió visualizar las reglas MASQUERADE y DNAT configuradas en el sistema. En particular, las reglas MASQUERADE permiten que las redes privadas salgan hacia Internet mediante traducción de direcciones.

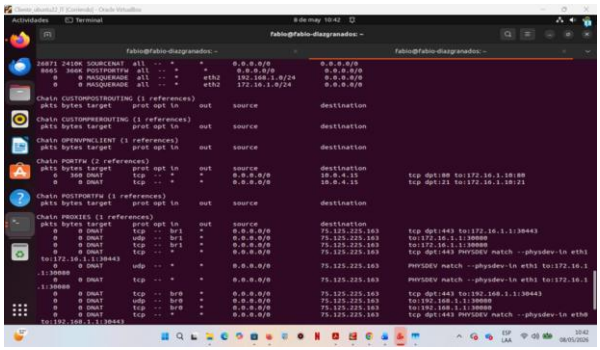

Figura 17. Validación de reglas NAT mediante IPTables. Fuente: de autoría propia.

3.1.12 PRUEBAS DE CONECTIVIDAD

Por medio de la consola del cliente en este caso ubuntu 22 realizamos pruebas de conectividad a través de comandos esto con el fin de evaluar el servicio HTTP. En la Figura 18 se validó el acceso desde la red LAN hacia Internet mediante tráfico HTTP.

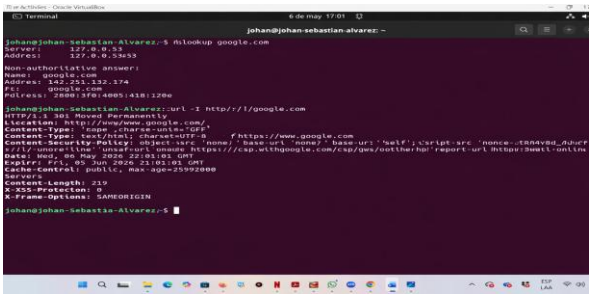

Figura 18. Validación de acceso HTTP desde LAN. Fuente: de autoría propia.

3.1.13 VERIFICACIÓN DMZ → INTERNET

En la Figura 19 se comprobó la salida hacia Internet NAT por el puerto HTTP desde el servidor ubicado en la DMZ utilizado un comando para validar la conectividad mediante acceso a Google.

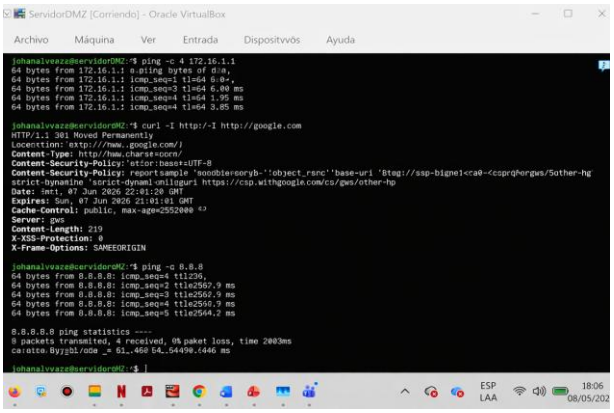

Figura 19. Validación de acceso desde DMZ hacia Internet Fuente: de autoría propia.

4 TEMÁTICA 3: GESTIÓN DE SEGURIDAD PERIMETRAL Y PUBLICACIÓN DE SERVICIOS EN DMZ

En esta sección se detalla el procedimiento técnico para la implementación de políticas de seguridad y la exposición controlada de servicios en una Zona Desmilitarizada (DMZ). El desarrollo se fundamenta conforme a Castaño (2025) en el principio de "menor privilegio", permitiendo únicamente el tráfico estrictamente necesario para la operatividad del servidor.

En cuanto a la arquitectura de Red y Segmentación Lógica, para el desarrollo de la temática, se segmentó la infraestructura en tres zonas de seguridad claramente definidas en el Firewall Endian:

1. Zona Verde (LAN): Red interna confiable donde reside el cliente Debian (192.168.10.16).
2. Zona Naranja (DMZ): Segmento aislado para el servidor Ubuntu (192.168.20.10).
3. Zona Roja (WAN): Interfaz conectada a la red externa.

Esta segmentación es crítica, ya que el firewall actúa como puerta de enlace (*Gateway*) denegando por defecto cualquier tráfico entre zonas que no haya sido autorizado explícitamente.

Respecto al procedimiento y configuración de reglas perimetrales, la administración del tráfico se centralizó en el módulo de cortafuegos de Endian UTM, aplicando políticas específicas para el control de flujo entre la red LAN (Green) y la DMZ (Orange). A continuación, se describen los procedimientos técnicos aplicados para cada regla configurada:

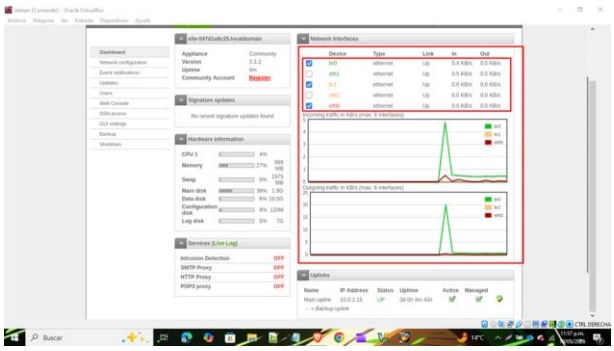

Figura 20. Validación de conectividad exitosa al servicio FTP desde el cliente Debian hacia el servidor Ubuntu en la zona DMZ. Fuente: de autoría propia.

4.1 Regla de Acceso para el Servicio HTTP (Puerto 80):

Para la publicación del servidor Web, se creó una regla de tráfico inter-zona permitiendo el protocolo TCP. En la configuración se definió como origen la interfaz de la zona Verde y como destino la dirección IP estática del servidor Ubuntu (192.168.20.10) en la zona Naranja. Esta regla garantiza que las estaciones de trabajo internas puedan consumir las

aplicaciones y bases de datos alojadas en el servidor sin exponer el segmento LAN a la zona DMZ.

Figura 21. Configuración de la política de tráfico inter-zona en Endian Firewall para permitir el acceso al servicio HTTP (Puerto 80) desde la Zona Verde hacia la DMZ.
Fuente: de autoría propia.

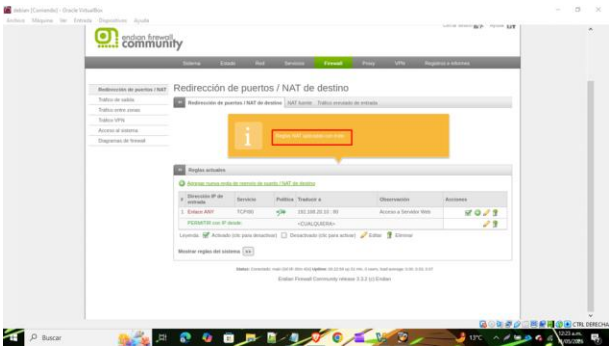

Figura 22. Confirmación de la aplicación exitosa de la Regla 1 para el servicio HTTP en la tabla de políticas de Endian.
Fuente: de autoría propia.

4.2 Regla de Acceso para el Servicio FTP (Puerto 21):

Similar al servicio web, se habilitó el puerto 21 para permitir la transferencia de archivos. Dado que el protocolo FTP requiere el establecimiento de canales de control, se aseguró que el Firewall gestionara el seguimiento de conexiones (Connection Tracking) para permitir el intercambio de datos seguro entre Debian y Ubuntu. Esta configuración es vital para las tareas de actualización de contenido en el servidor desde la red administrativa.

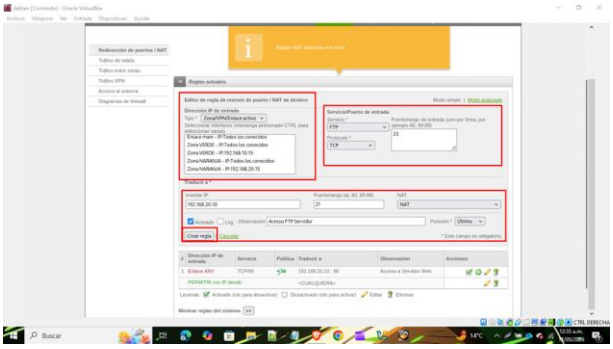

Figura 23. Configuración de la Regla 2 en Endian Firewall para habilitar el servicio de transferencia de archivos FTP (Puerto 21) hacia la Zona Naranja. Fuente: de autoría propia

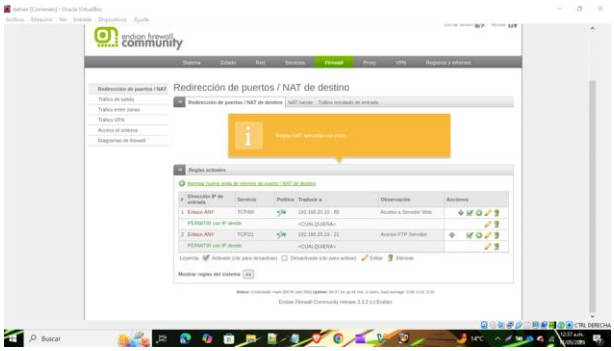

Figura 24. Visualización de la Regla 2 habilitada en la tabla de redirección de puertos, garantizando la persistencia del servicio FTP hacia la DMZ. Fuente: de autoría propia

Política de Denegación de Tráfico ICMP (Puertos 8 y 30): Con el fin de elevar el nivel de seguridad y aplicar técnicas de Hardening, se implementó una regla de bloqueo absoluto para el protocolo ICMP.

Configuración Técnica: Se seleccionó la acción DROP (descartar) para los tipos de mensaje Echo Request (ping) y paquetes de trazado de ruta.

Jerarquía: Esta regla se posicionó en la parte superior de la tabla de políticas. En seguridad perimetral, el orden es crítico: al procesarse primero, el firewall descarta cualquier intento de descubrimiento de red antes de evaluar permisos de aplicaciones, evitando que atacantes potenciales obtengan información sobre la topología de la DMZ.

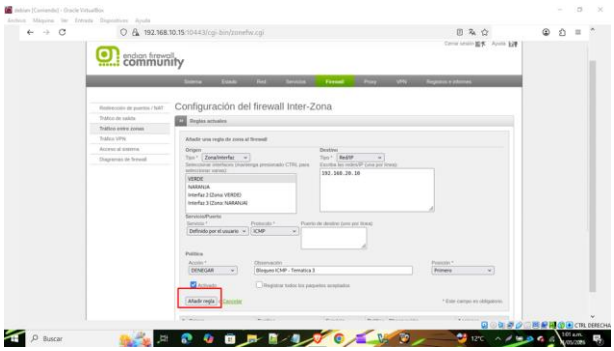

Figura 25. Configuración de la Regla 3 para el bloqueo del protocolo ICMP (Ping), estableciendo la acción de descarte (DROP) para mejorar la seguridad perimetral.
Fuente: de autoría propia

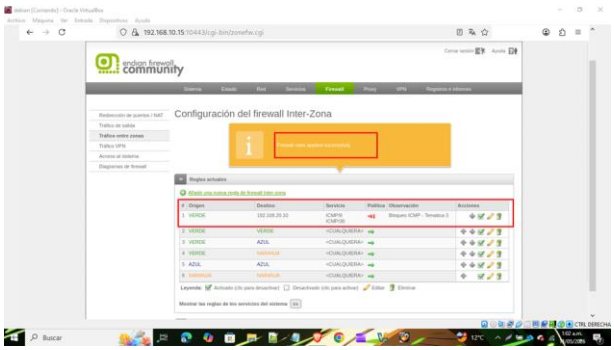

Figura 26. Validación de la aplicación exitosa de la Regla 3 en la tabla de tráfico Inter-Zona, denegando paquetes ICMP/8 e ICMP/30 hacia el servidor en la DMZ Fuente: de autoría propia

4.3 EVIDENCIAS DE VALIDACIÓN Y PRUEBAS DE CAMPO

En esta sección se presentan las pruebas de funcionamiento realizadas desde el cliente Debian (Zona Verde), validando la efectividad de las políticas de seguridad y la disponibilidad de los servicios en el servidor Ubuntu (Zona Naranja).

4.3.1 Validación de Conectividad y Acceso Web

La figura 27 muestra la terminal de la estación de trabajo Debian (Cliente) realizando una consulta de encabezados HTTP hacia el servidor Ubuntu (Servidor DMZ).

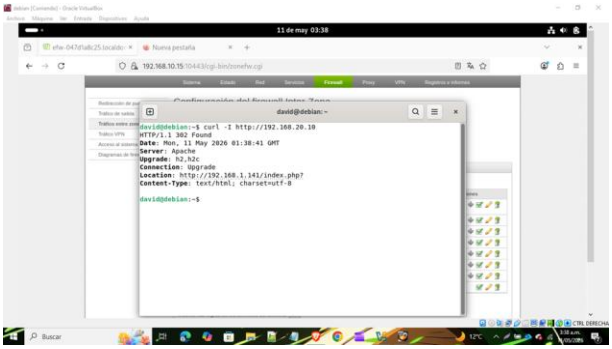

Figura 27. Validación de disponibilidad del servicio HTTP mediante la terminal de Debian, evidenciando la respuesta satisfactoria del servidor Apache alojado en la DMZ.Fuente: de autoría propia

4.3.2 Análisis del Comando Ejecutado:

El comando curl -I http://192.168.20.10 se utiliza para solicitar únicamente la información del servidor y el estado de la página sin descargar todo el contenido. El éxito de este comando prueba lo siguiente:

- Enrutamiento Exitoso: El paquete logró viajar desde la red 192.168.10.0 (Verde) hacia la red 192.168.20.0 (Naranja). Esto confirma que la ruta estática y el "gateway" en el Firewall Endian están operando correctamente.

- Permiso de Firewall: La regla de tráfico inter-zona "LAN - DMZ" permitió el paso del tráfico en el puerto 80, validando que el cortafuegos no está bloqueando las peticiones legítimas.

4.3.3 Análisis de la Respuesta del Servidor:

La respuesta recibida contiene datos técnicos fundamentales:

- HTTP/1.1 302 Found: Este código indica que el servidor web está activo. Aunque es una redirección, confirma que el servicio Apache recibió la petición y procesó una respuesta lógica.

- Server: Apache: Identifica claramente que quien responde es el servicio web configurado en el servidor Ubuntu, descartando que la respuesta venga de otro dispositivo.

- Location: http://192.168.1.141/index.php?: Muestra que el servidor intenta dirigir al cliente hacia una página específica, lo cual es el comportamiento normal de una aplicación web funcional.

4.3.4 Éxito en la Configuración de Red y Seguridad

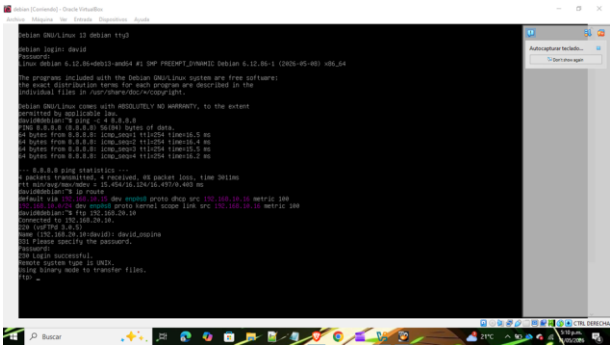

Figura 28. Verificación de la salida a Internet (WAN) y validación de la puerta de enlace predeterminada en el host Debian. Fuente: de autoría propia.

La captura de pantalla realizada en la terminal de Debian (Zona Verde) es la evidencia definitiva de que el enrutamiento, las reglas del firewall y los servicios del servidor están operando en perfecta sincronía.

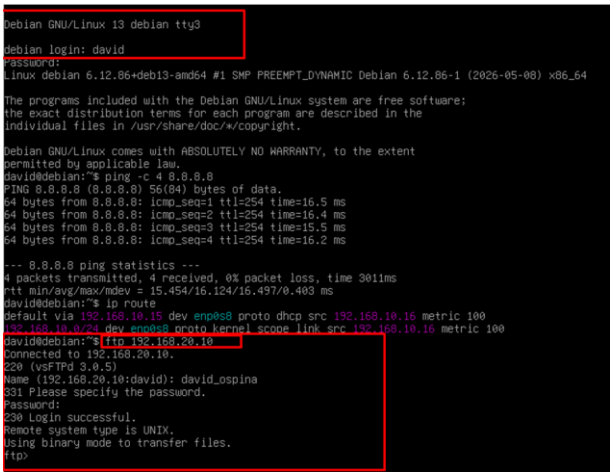

Figura 29. Prueba de autenticación exitosa en el servidor remoto vsftpd mediante el puerto de control 21 desde el segmento LAN. Fuente: de autoría propia.

4.3.5 Validación de Conectividad WAN (Salida a Internet)

- Prueba: Ejecución de ping -c 4 8.8.8.8.
- Resultado: 0% de pérdida de paquetes.
- Análisis: Esto demuestra que el cliente en la red interna tiene salida a través del Firewall Endian hacia la red Roja (Internet). La regla de NAT y las políticas de salida están correctamente aplicadas.

4.3.6 Validación de Enrutamiento y Gateway

- Prueba: Comando ip route.
- Resultado: default via 192.168.10.15.
- Análisis: Se confirma que la puerta de enlace predeterminada es la interfaz Verde del Firewall. Esto es lo que permite que el tráfico pueda saltar de una red a otra de forma controlada.

4.3.7 Validación de Acceso a Servicios (Capa de Aplicación)

- Prueba: Conexión mediante ftp 192.168.20.10.
- Resultado: 230 Login successful.
- Análisis: Esta es la prueba más contundente del ejercicio. Para que este mensaje aparezca, ocurrieron tres cosas exitosas simultáneamente:
    - Firewall Inter-Zona: La regla "LAN - DMZ" permitió el tráfico del puerto 21.
    - Segmentación Correcta: El tráfico logró cruzar de la red .10.x a la .20.x.
    - Servicio Activo: El servidor Ubuntu recibió las credenciales y autenticó al usuario, confirmando que el servicio vsftpd está bien configurado.

4.3.8 Validación de Seguridad Perimetral y Segmentación de Red

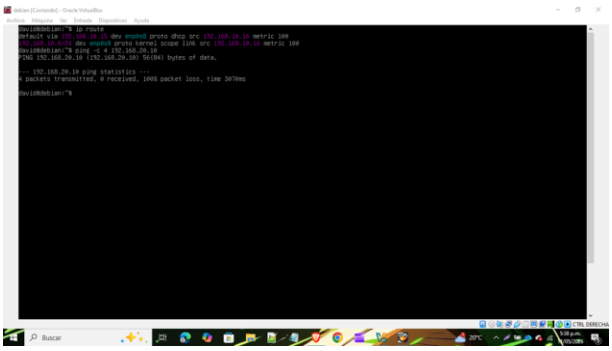

Figura 30. Validación de la tabla de enrutamiento en el host cliente para el direccionamiento de tráfico inter-zona. Fuente: de autoría propia.

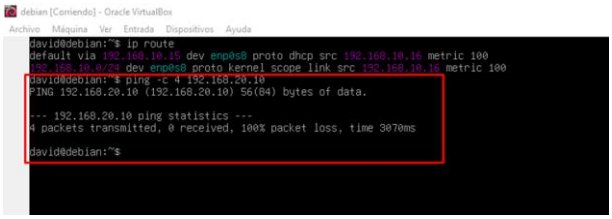

Figura 31. Evidencia de Hardening de red: bloqueo efectivo del protocolo ICMP hacia la DMZ con un 100% de pérdida de paquetes. Fuente: de autoría propia.

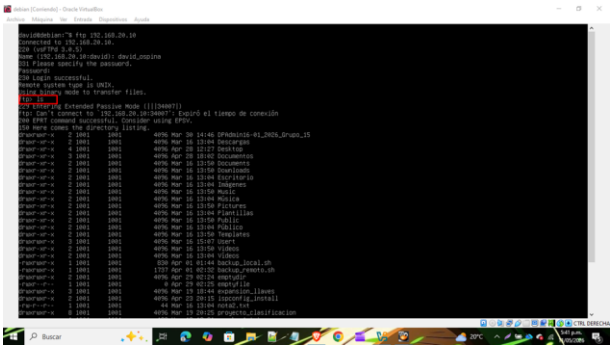

Figura 32. Ejecución exitosa del comando de listado de directorios (ls) mediante el protocolo FTP, validando la transferencia de datos hacia la zona DMZ. Fuente: de autoría propia.

Las evidencias enviadas demuestran el cumplimiento total de los objetivos de seguridad perimetral, segmentación de red y publicación de servicios. El ejercicio funciona porque se ha logrado pasar de un estado de aislamiento total a uno de acceso controlado y seguro.

4.3.9 Cumplimiento del Bloqueo ICMP (Seguridad)

- Evidencia: El comando ping -c 4 192.168.20.10 resulta en 100% packet loss.
- Explicación: Esto prueba que la Regla de Firewall Inter-Zona en la Posición #1 está operando correctamente. Al denegar los puertos 8 y 30 de ICMP, el servidor en la DMZ se vuelve "invisible" ante intentos de rastreo o diagnóstico desde la red Verde, cumpliendo con el estándar de endurecimiento (hardening) de red solicitado.

4.3.10 Cumplimiento de Publicación de Servicios (Operatividad)

- Evidencia: Conexión exitosa vía FTP y ejecución del comando ls con respuesta 226 Directory send OK.
- Explicación: Funciona gracias a la combinación de dos configuraciones:
- DNAT (Redirección de Puertos): El Firewall traduce la petición externa hacia la IP privada del servidor.
- Regla de Acceso LAN-DMZ: El Firewall permite el tráfico de datos, demostrando que la seguridad no impide la operatividad del negocio. Ver el listado de archivos confirma que el canal de datos está abierto y el servidor Ubuntu responde correctamente.

4.3.11 Cumplimiento de Enrutamiento y Salida WAN

- Evidencia: El comando ip route y el acceso previo a internet.
- Explicación: El ejercicio cumple con el objetivo de permitir que la DMZ sea una zona funcional que

puede actualizarse (salida a la red Roja) mientras permanece protegida de accesos no autorizados.

5 TEMATICA 4 REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO

5.1 COMUNICACIÓN ZONA VERDE (LAN) CON ZONA NARANJA (DMZ)

Para permitir la comunicación entre los equipos de la red LAN y el servidor ubicado en la DMZ, fue necesario configurar reglas de acceso en la sección Firewall → Inter-Zone Traffic de Endian. En esta parte se creó una regla para permitir el tráfico HTTP por el puerto 80 y otra para permitir el servicio FTP por el puerto 21, ambas desde la zona GREEN hacia la zona ORANGE con la acción ALLOW. Después de aplicar los cambios, el sistema mostró el mensaje "Firewall rules applied successfully", confirmando que las reglas fueron configuradas correctamente.

Para comprobar el funcionamiento de las reglas, desde el equipo Ubuntu Desktop de la LAN se ingresó en Firefox a la dirección http://192.168.20.10, mostrando la página predeterminada de Apache2 con el mensaje "¡Funciona!", lo que confirmó la conectividad HTTP entre la LAN y la DMZ. De igual manera, se realizó la prueba del servicio FTP desde la terminal utilizando el comando ftp 192.168.20.10, logrando iniciar sesión correctamente y obteniendo el mensaje "230 Login successful".

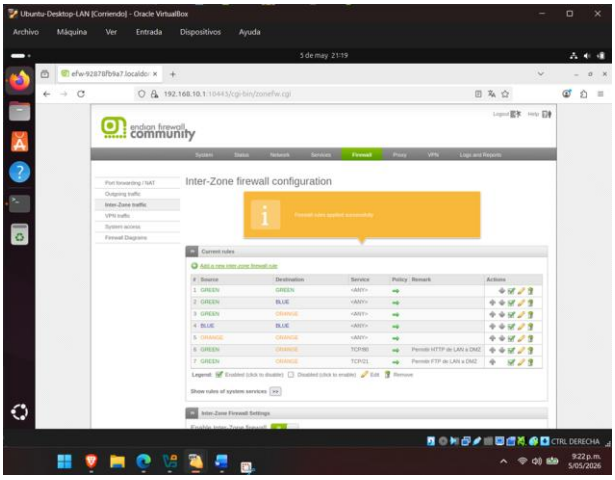

Figura 33. Reglas inter-zona configuradas: GREEN→ORANGE HTTP (TCP/80) y FTP (TCP/21. Fuente: de autoría propia.

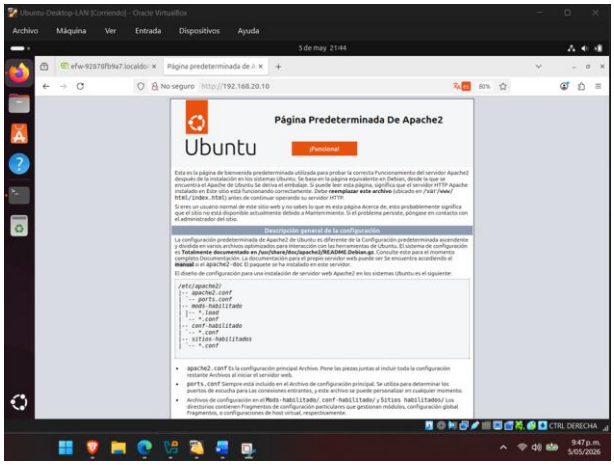

Figura 34. Prueba exitosa HTTP desde LAN hacia DMZ — página de Apache2. Fuente: de autoría propia.

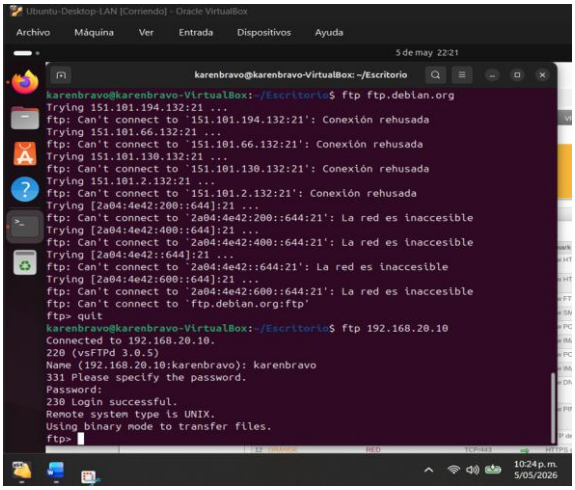

Figura 35. Prueba exitosa FTP desde LAN hacia DMZ — login exitoso con vsftpd. Fuente: de autoría propia.

5.2 COMUNICACIÓN ZONA WAN CON ZONA DMZ

Para permitir el acceso desde internet (zona WAN/Roja) hacia el servidor web en la DMZ, se configuró una regla de Port Forwarding / Destination NAT en Endian. Esta regla según Acero et, al. (2025) redirige el tráfico HTTP entrante desde la interfaz Uplink main (WAN) hacia la dirección IP del servidor en la DMZ (192.168.20.10) en el puerto 80.

La verificación se realizó accediendo desde el navegador a la dirección IP de la interfaz WAN de Endian (10.0.2.15), simulando un acceso externo desde internet. La página predeterminada de Apache2 se cargó correctamente, confirmando que el Port Forwarding NAT funciona y que el tráfico HTTP desde la WAN es correctamente redirigido al servidor en la DMZ.

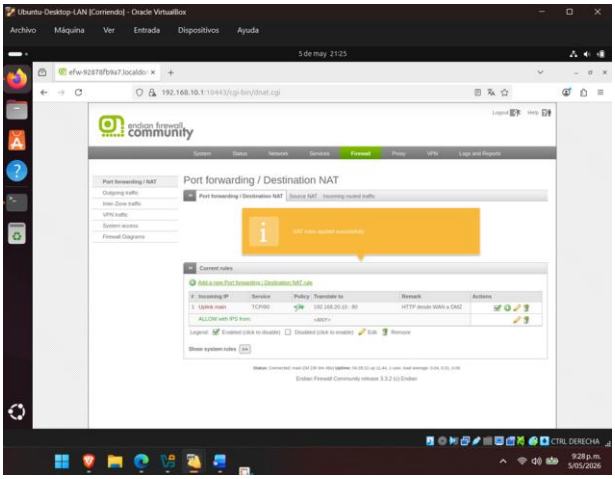

Figura 36. Regla de Port Forwarding NAT configurada: WAN → DMZ TCP/80. Fuente: de autoría propia.

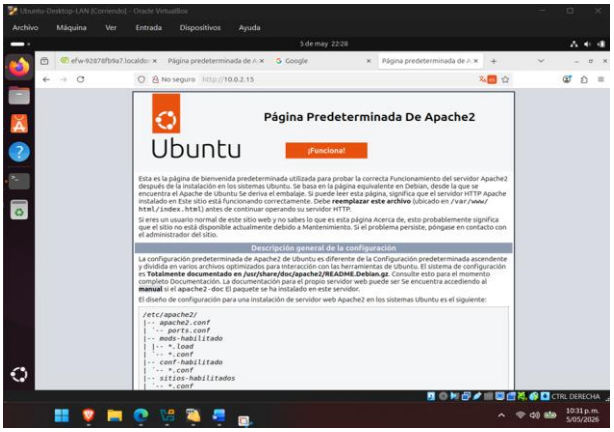

Figura 37. Prueba exitosa de HTTP desde WAN hacia DMZ mediante Port Forwarding. Fuente: de autoría propia.

6 Temática 5: Implementar un Proxy HTTP (No transparente) con políticas de autenticación para navegación en Internet.

Para esta sección, se realiza la asignación de usuario y contraseña para permitir el acceso a usuarios o el bloqueo según corresponda

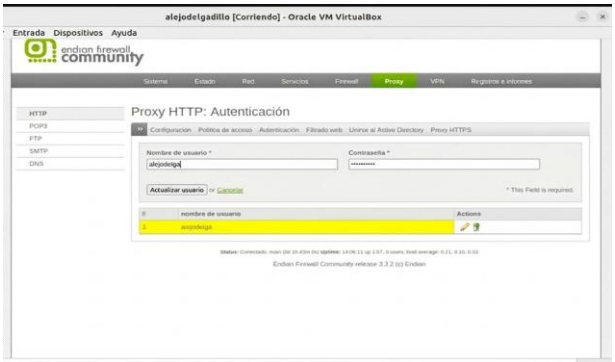

Figura 38. Asignación de credenciales. Fuente: de autoría propia.

En la configuración de Endian se ingresa a la configuración de Proxy, la cual conforme a Carrasco et, al. (2025) permite establecer un bloqueo de acceso a sitios web, en este caso Hotmail, Facebook, Youtube y nuevo dia.

Figura 39. Configuración de Bloqueos. Fuente: de autoría propia.

Seguido se realiza la configuración de Proxy HTTP para conceder acceso a usuarios permitidos o su respectivo bloqueo.

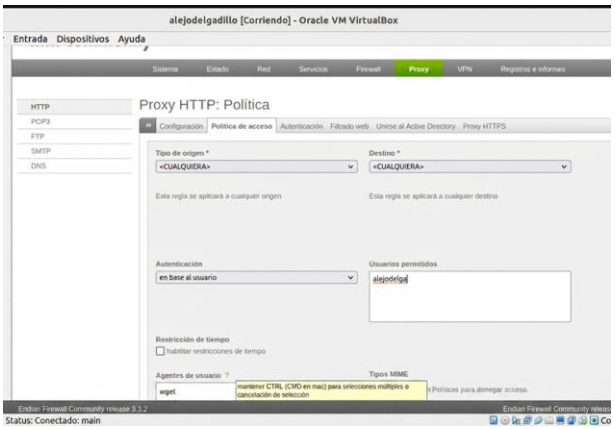

Figura 40. Política HTTP. Fuente: de autoría propia.

Con la configuración establecida, al intentar ingresar al sitio web, no se permite el ingreso como se evidencia en la figura 41.

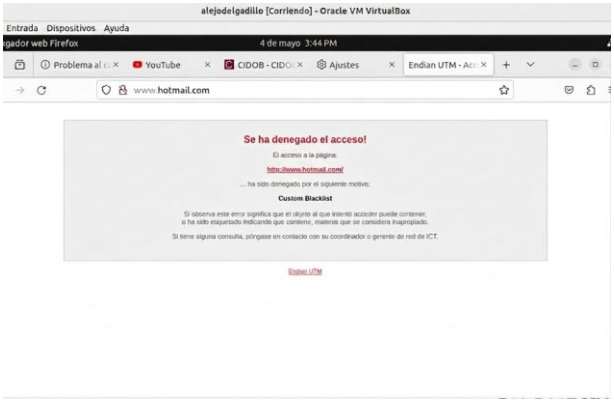

Figura 41. Acceso Denegado. Fuente: de autoría propia.

7 CONCLUSIONES

7.1 TEMÁTICA 1

La instalación y configuración del firewall Endian ha demostrado ser un ejercicio valioso, ya que ha proporcionado una comprensión práctica de la segmentación de redes y la importancia de establecer un entorno seguro. A través de la creación de zonas diferenciadas (LAN, WAN y DMZ), se ha podido observar cómo una adecuada configuración de red contribuye a la protección de los recursos y servicios.

7.2 TEMÁTICA 2

La Temática 2 permitió comprobar la importancia de la correcta configuración de reglas NAT y Port Forwarding en Endian Firewall para garantizar tanto la salida segura de las redes internas hacia Internet como la publicación controlada de servicios en la DMZ. La validación de interfaces y pruebas de conectividad confirmaron la interacción adecuada entre las zonas LAN, WAN y DMZ, mientras que la aplicación de reglas MASQUERADE y DNAT optimizó el uso de direcciones IP y habilitó el acceso externo a servicios HTTP y FTP. En conjunto, se logró un entorno funcional, seguro y administrado, fortaleciendo la seguridad perimetral y la gestión de tráfico en la infraestructura virtualizada.

7.3 TEMÁTICA 3

La implementación técnica permitió validar la eficacia de Endian Firewall en la segmentación de redes mediante el uso de zonas de seguridad diferenciadas (Verde, Naranja y Roja). Se concluye que la configuración de una zona DMZ (Naranja) es fundamental para garantizar la disponibilidad de servicios críticos como HTTP y FTP sin comprometer la integridad de la red interna (LAN). Asimismo, la aplicación de reglas de hardening mediante el bloqueo absoluto del protocolo ICMP demostró ser una medida proactiva eficiente para mitigar el reconocimiento de red, logrando que el servidor sea "invisible" ante intentos de diagnóstico externos. Finalmente, la gestión exitosa de servicios mediante systemctl y el filtrado granular de paquetes confirman que una administración robusta de sistemas GNU/Linux permite equilibrar la operatividad del negocio con los más altos estándares de seguridad perimetral.

7.4 TEMÁTICA 4

Configurar las reglas de acceso inter-zona en Endian fue una experiencia muy práctica para entender cómo funciona realmente el control del tráfico en una red segmentada. Ver cómo al habilitar únicamente los puertos necesarios (HTTP y FTP) la comunicación entre la LAN, la DMZ y la WAN funcionó correctamente, dejó claro que una buena política de firewall no tiene que ser compleja para ser efectiva. Las pruebas de conectividad fueron la mejor evidencia de que las reglas configuradas estaban bien aplicadas.

7.5 TEMATICA 5

El uso de Endian Firewall con GNU/Linux permite una gestión centralizada del tráfico HTTP saliente desde una red LAN y facilita la aplicación de ciertas directivas de seguridad como parte de las normas de seguridad perimetral de la red. Se ha implementado una solución de seguridad no transparente con nuestro firewall para impedir el acceso a webs no deseadas mediante listas negras, y restringir el acceso al resto de webs mediante autenticación por usuario. Se demuestra de forma didáctica el uso de GNU/Linux dentro de sistemas que gestionan el tráfico HTTP saliente de una red corporativa.

8 REFERENCIAS

[1] Acero Arevalo, A. B., Rodriguez Camargo, A. M., Villa Duque, F. S., & Mendez Hernandez, L. M. (2025) Implementando seguridad en GNU/LINUX.

[2] Carrasco Cocinero, D. R., Bolaños Delgado, S. M., Cháves Montánchez, D. T., Pacichaná Domínguez, L. A., & Mosquera Delgado, L. C. (2025) Implementación de Seguridad Perimetral en GNU/Linux con Endian Firewall (EFW).

[3] Castaño, L. D. B. (2025). Implementación protocolos de seguridad gnu/linux mediante endian.

[4] Endian Team. (2024). *Endian Firewall Community Edition Documentation.* Endian.com. [Online]. Available: https://help.endian.com/

[5] Escobar, D. E. Z., Tangarife, I. L. G., Munera, J. D. A., Ibarra, C. H. O., & Arango, D. A. G. (2023). Implementación de un sistema de control y seguridad Informático ENDIAN FIREWALL. *Ingeniería: ciencia, tecnología e innovación*, *10*(1), 98-115.

[6] LPI Linux Professional Institute, "Tema 4: El sistema operativo Linux," *Linux Essentials (010-160)*, 2022. [En línea]. Disponible: https://learning.lpi.org/es/learning-materials/010-160/4/

[7] Perdigón, R. (2022). Evaluación del rendimiento de cortafuegos basados en software libre . Novasinergia, ISSN 2631-2654, 5(1), 31–42. https://doi.org/10.37135/ns.01.09.03

[8] P. F. Hernández y J. Sánchez, "Monitoreo y administración de sistemas Linux," *Objeto Virtual de Información (OVI)*, Repositorio Institucional UNAD, 2022. [En línea]. Disponible: https://repository.unad.edu.co/handle/10596/53211

[9] Quijano Carantón, M. C., Ocampo Cardenas, L. F., & Angel Cogollo, J. J. (2025) Arquitectura de Seguridad Perimetral GNU/Linux Basada en la Virtualización de Endian Firewall para la Delimitación de Redes.

[10] Saboya Jimenez, J. D., Gonzalez Fuentes, F. A., Vallejo Colmenares, Y. M., & Garcia Corredor, K. S. (2025) Implementación del Firewall Endian en entorno virtualizado como estrategia de segmentación de red en GNU/Linux.

[11] Sanabria Duran, K. D. (2025) Implementación de seguridad en GNU/LINUX usando Endian firewall para la protección LAN/DMZ/WAN.

[12] Tomalá Parra, E. R., & Argoti Caiza, J. D. (2024). *Diseño de una máquina virtual y análisis de sus vulnerabilidades con fines prácticos: servidor de correo electrónico, servidor de aplicaciones, desbordamiento de búffer e inyección de comandos* (Master's thesis).

[13] Villarreal Brito, G. (2024). Diseño de red y publicación de servicio web a internet sin una IP homologada. *Cuadernos Técnicos Universitarios De La DGTIC*, *2*(1). https://doi.org/10.22201/dgtic.ctud.2024.2.1.33 (Original work published 13 de febrero de 2024)