# IMPLEMENTACIÓN Y CONFIGURACIÓN DE ENDIAN FIREWALL COMO SOLUCIÓN DE SEGURIDAD EN INFRAESTRUCTURAS LINUX

Christian Andrés Acero Ramírez
e-mail: caacerora@unadvirtual.edu.co
Elio Ramiro Diaz
e-mail: erdiaz@unadvirtual.edu.co
Rosemberg Arias Cortez
e-mail: rariasc@unadvirtual.edu.co
Tania Valentina Parrado Rojas
e-mail: tparrador@unadvirtual.edu.co

**RESUMEN:** *Este artículo presenta la implementación y configuración de Endian Firewall en un entorno virtualizado mediante VirtualBox, con el objetivo de establecer una infraestructura de red segura y segmentada en GNU/Linux. Se configuraron las zonas LAN, WAN y DMZ, permitiendo la organización del tráfico y la separación de servicios. Posteriormente, se implementaron reglas NAT para garantizar la comunicación entre redes y el acceso a Internet. Se habilitaron servicios como HTTP y FTP en la zona DMZ y se restringió el protocolo ICMP como medida de seguridad. Además, se definieron reglas de acceso interzona para controlar el tráfico y se implementó un proxy HTTP con autenticación y filtrado de contenido mediante listas negras. Los resultados evidencian un adecuado control de acceso, segmentación de red y fortalecimiento de la seguridad, demostrando la efectividad de Endian Firewall en entornos de red virtualizados.*

**ABSTRACT:** *This paper presents the implementation and configuration of Endian Firewall in a virtualized environment using VirtualBox, aiming to establish a secure and segmented network infrastructure based on GNU/Linux. The LAN, WAN, and DMZ zones were configured to organize traffic and isolate services. Network Address Translation (NAT) rules were implemented to enable communication between networks and provide Internet access. Services such as HTTP and FTP were deployed in the DMZ, while the ICMP protocol was restricted to enhance security. Additionally, inter-zone access rules were defined to control network traffic, and a non-transparent HTTP proxy with user authentication and content filtering through blacklists was implemented. The results demonstrate effective access control, network segmentation, and improved security, highlighting the efficiency of Endian Firewall in virtualized network environments.*

**PALABRAS CLAVE:** Endian Firewall, GNU/Linux, seguridad de red, segmentación de red.

## 1 INTRODUCCIÓN

El crecimiento de las redes informáticas y la necesidad de proteger la información han impulsado el uso de soluciones de seguridad que permitan controlar el acceso y gestionar el tráfico de manera eficiente. En este contexto, los firewalls basados en GNU/Linux se han convertido en herramientas fundamentales para la segmentación de redes y la protección de infraestructuras tecnológicas (Endian, s. f.).

El presente artículo tiene como objetivo implementar y configurar Endian Firewall en un entorno virtualizado mediante VirtualBox, con el fin de establecer una arquitectura de red segmentada en zonas LAN, WAN y DMZ (Endian, s. f.; Oracle, s. f.).

Durante el desarrollo del trabajo, se abordaron diferentes temáticas que incluyen la configuración inicial del sistema, la implementación de reglas NAT para la comunicación entre redes, la habilitación de servicios en la zona DMZ, la definición de políticas de acceso entre zonas y la implementación de un proxy HTTP con autenticación y filtrado de contenido.

Finalmente, se realizaron pruebas de conectividad y validación de las reglas configuradas, evidenciando el correcto funcionamiento de la infraestructura y demostrando la importancia de aplicar buenas prácticas de seguridad en entornos de red virtualizados.

## 2 DESARROLLO DE LAS ACTIVIDIDADES

El desarrollo de la actividad se estructuró en cinco temáticas principales orientadas a la implementación y configuración de un entorno seguro utilizando Endian Firewall. En primer lugar, se realizó la instalación del sistema en un entorno virtualizado mediante VirtualBox, configurando las interfaces de red correspondientes a las zonas LAN (GREEN), WAN (RED) y DMZ (ORANGE), con el fin de establecer una adecuada segmentación de la red.

Posteriormente, se implementaron reglas de traducción de direcciones de red (NAT) que permitieron la comunicación desde la red interna hacia Internet y desde la zona DMZ hacia la red externa, verificando el correcto funcionamiento mediante pruebas de conectividad.

En la tercera fase, se habilitaron servicios en la zona DMZ, específicamente HTTP y FTP, y se aplicaron restricciones al protocolo ICMP para impedir respuestas a solicitudes de ping, fortaleciendo así la seguridad de la red.

Luego, se definieron reglas de acceso entre las diferentes zonas para permitir o denegar el tráfico según los requerimientos establecidos, validando su funcionamiento mediante pruebas de navegación y acceso a servicios.

Finalmente, se implementó un proxy HTTP no transparente con autenticación de usuarios y políticas de filtrado, incluyendo listas negras para restringir el acceso a determinados sitios web desde la red interna.

## 2.1 CONFIGURACIÓN DE ENDIAN EN LA MÁQUINA VIRTUAL

Para la implementación de Endian Firewall, inicialmente se realizó la creación de una máquina virtual en VirtualBox, en la cual se configuraron tres adaptadores de red con el fin de establecer la segmentación correspondiente a las zonas WAN, LAN y DMZ (Oracle, s. f.).

En primer lugar, se configuró el adaptador 1 correspondiente a la zona WAN (red externa), el cual se habilitó y se estableció en modo NAT, permitiendo la conexión a Internet del firewall.

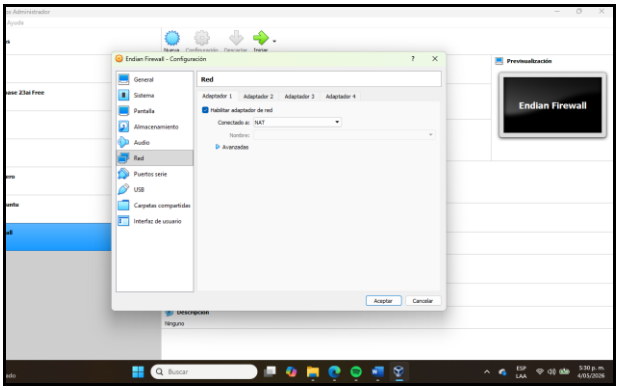


***Fig. 1.*** *Configuración del adaptador 1 en modo NAT (WAN).*

Posteriormente, se configuró el adaptador 2 correspondiente a la zona LAN (GREEN), el cual se habilitó y se estableció en modo de red interna, asignándole el nombre "LAN", permitiendo la comunicación dentro de la red local.

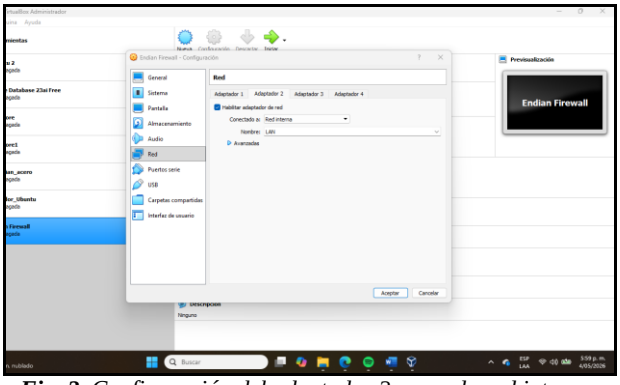


***Fig. 2.*** *Configuración del adaptador 2 en modo red interna (LAN).*

Finalmente, se configuró el adaptador 3 correspondiente a la zona DMZ (ORANGE), el cual se habilitó y se estableció en modo de red interna, asignándole el nombre "DMZ", con el propósito de alojar servicios accesibles desde otras redes manteniendo un nivel de aislamiento.

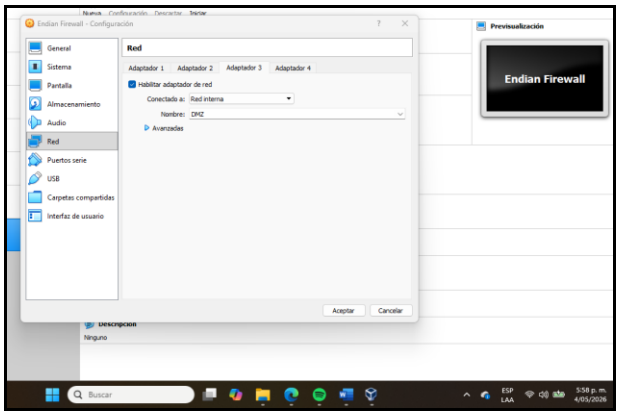


***Fig. 3.*** *Configuración del adaptador 3 en modo red interna (DMZ).*

Posteriormente, se realizó el montaje del archivo ISO de Endian en la máquina virtual, permitiendo iniciar el proceso de instalación del sistema operativo dentro del entorno configurado en VirtualBox.

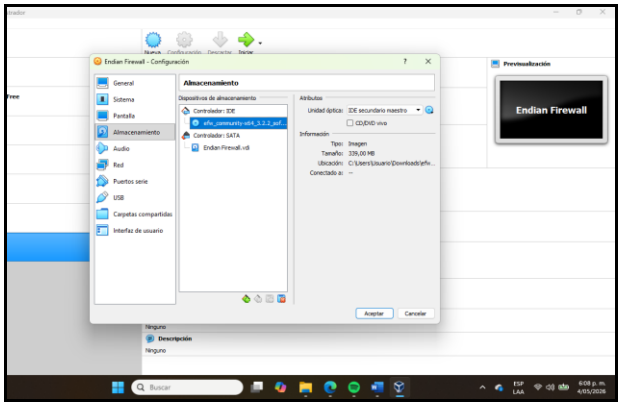


***Fig. 4.*** *Montaje del archivo ISO de Endian en la máquina virtual.*

## 2.2 INSTALACIÓN Y CONFIGURACIÓN INICIAL DE ENDIAN FIREWALL

Una vez montado el archivo ISO, se inició el proceso de instalación de Endian Firewall en la máquina virtual. Durante esta fase inicial, se realizó la selección del idioma del sistema, lo cual permite definir el entorno de configuración y facilitar la interacción con el sistema operativo. La elección del idioma es un paso fundamental, ya que influye en la correcta interpretación de las opciones y parámetros durante el proceso de instalación.

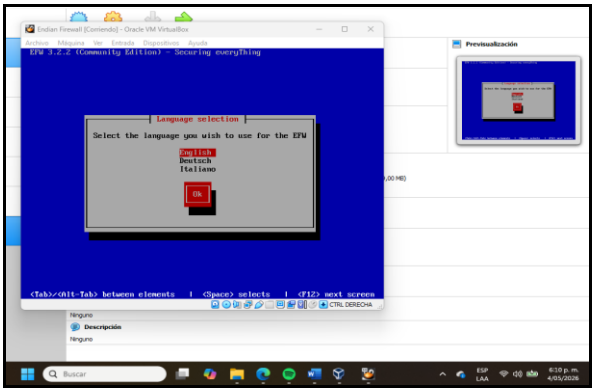


***Fig. 5.*** *Selección del idioma durante la instalación.*

Durante el proceso de instalación, se realizó la configuración de la interfaz de red GREEN, correspondiente a la red interna (LAN). En esta etapa, se asignó una dirección IP estática junto con su respectiva máscara de red, permitiendo establecer la comunicación dentro de la red local y garantizando la correcta conectividad entre los dispositivos internos.

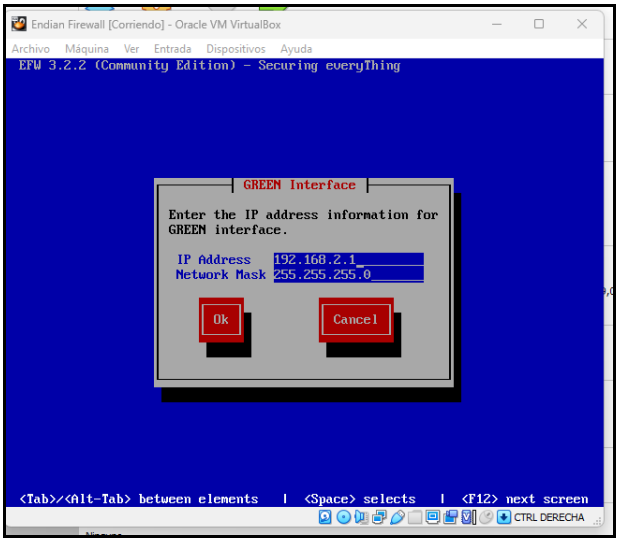


***Fig. 6.*** *Configuración de la dirección IP en la interfaz GREEN.*

Durante la fase final de instalación, el sistema muestra el menú de configuración denominado Network Wizard, el cual permite realizar ajustes adicionales sobre la red y los parámetros administrativos del firewall. En este punto, se visualiza la dirección IP asignada a la interfaz GREEN, así como el estado de los dispositivos de red, lo que confirma la correcta configuración inicial del sistema.

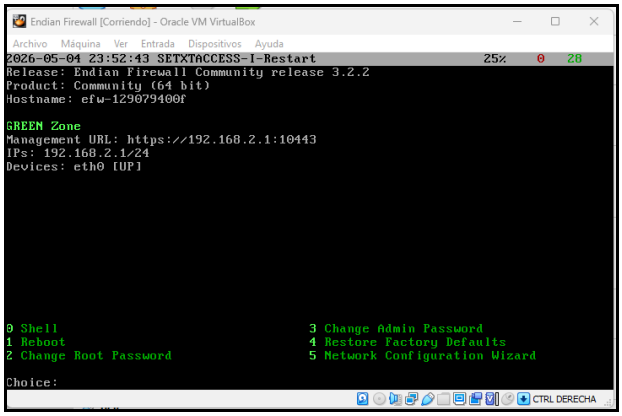


***Fig. 7.*** *Visualización del Network Wizard y parámetros de red en Endian Firewall.*

## 2.3 VALIDACIÓN DE CONECTIVIDAD DESDE LA MÁQUINA CLIENTE

Para la validación de la conectividad en la red interna, se configuró la máquina cliente con el fin de establecer comunicación dentro de la zona LAN (GREEN). En esta etapa, se verificó la correcta asignación de la interfaz de red en modo interno, lo que permite la interacción directa con el firewall Endian desde la red local.

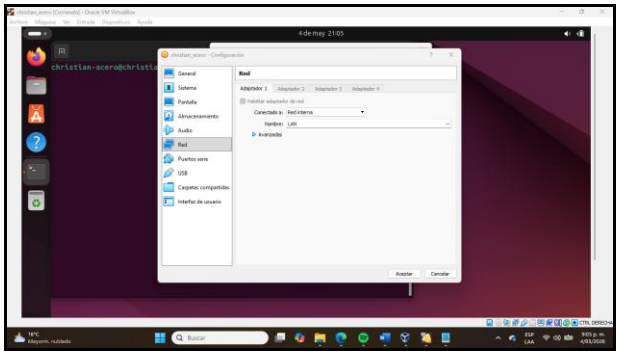

***Fig. 8.*** *Configuración de la interfaz de red en la máquina cliente para acceso a la zona LAN (GREEN).*

Posteriormente, se realizó la configuración manual de la dirección IP en la máquina cliente, debido a la ausencia de un servidor DHCP en la red. Para ello, se definieron parámetros como la dirección IP, la máscara de red, la puerta de enlace y los servidores DNS, garantizando así la conectividad con el firewall Endian y el acceso a servicios de red.

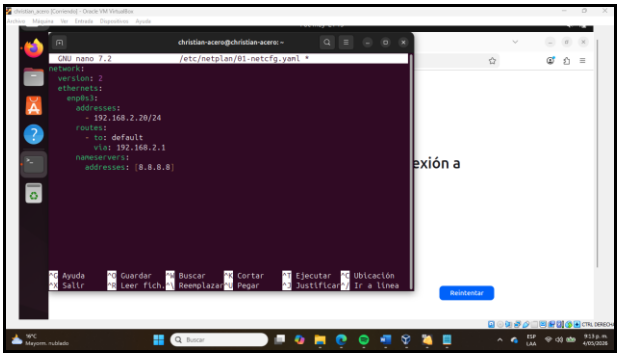

***Fig. 9.*** *Configuración manual de la dirección IP en la máquina cliente.*

Adicionalmente, se verificó el estado de la interfaz de red mediante el uso de comandos de diagnóstico, con el fin de confirmar que la dirección IP configurada se encuentra activa y operativa. Esta comprobación permitió evidenciar que la máquina cliente cuenta con conectividad dentro de la red definida.

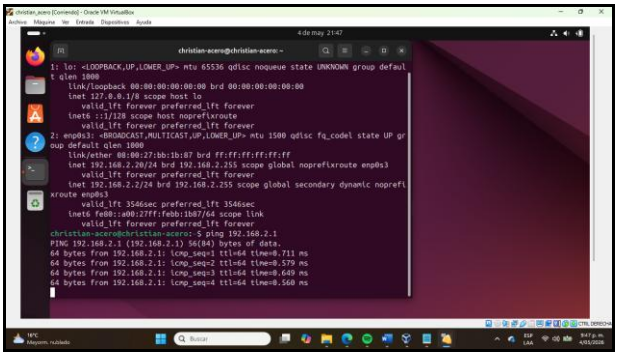

***Fig. 10.*** *Estado de la interfaz de red y verificación de la dirección IP en la máquina cliente.*

Finalmente, se verificó el acceso al entorno de administración de Endian Firewall desde la máquina cliente mediante un navegador web. Esta prueba permitió confirmar la conectividad entre el cliente y el firewall, así como la disponibilidad del servicio web de administración dentro de la red interna.

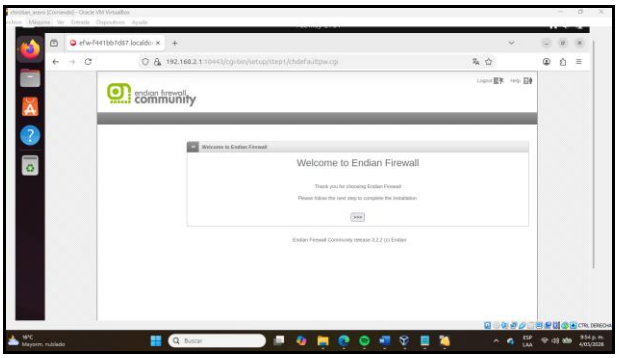


***Fig. 11.*** *Acceso al entorno web de administración de Endian Firewall desde la máquina cliente.*

Posteriormente, se inició la configuración de las zonas de red en Endian Firewall, específicamente las zonas ORANGE (DMZ) y RED (WAN). En esta etapa, se definieron los modos de red y las interfaces correspondientes, permitiendo establecer la segmentación del tráfico y la correcta asignación de funciones dentro de la infraestructura de red.

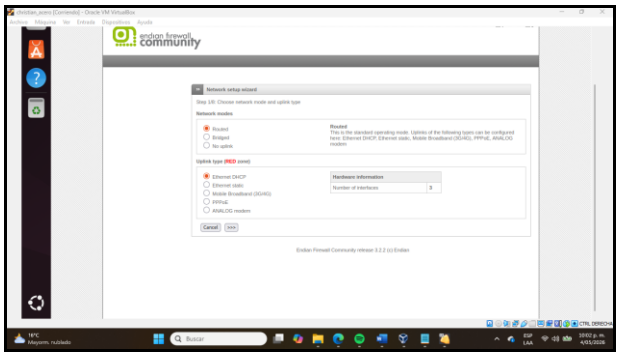

***Fig. 12.*** *Configuración inicial de las zonas ORANGE (DMZ) y RED (WAN) en Endian Firewall.*

A continuación, se realizó la configuración de la zona ORANGE (DMZ), asignando una dirección IP dentro de un segmento de red definido. En este caso, se estableció la dirección 192.168.1.1 junto con su respectiva máscara de red, vinculando la interfaz correspondiente (eth1) para permitir la conexión de servicios ubicados en la zona desmilitarizada.

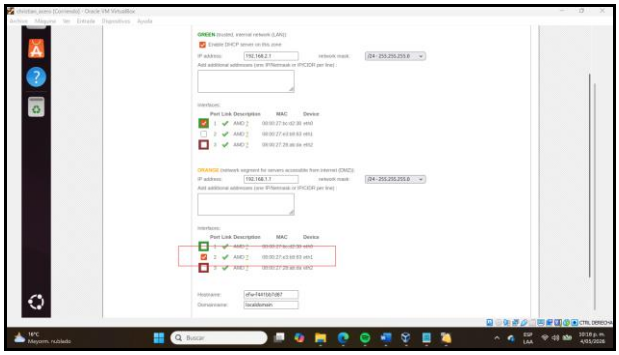

***Fig. 13.*** *Configuración de la zona ORANGE (DMZ) con dirección IP y asignación de interfaz.*

Finalmente, se realizó la configuración de la zona RED (WAN), asignando la interfaz correspondiente para el acceso a la red externa. En esta etapa, se definió la interfaz eth2 como la encargada de gestionar la conectividad hacia Internet, permitiendo al firewall establecer comunicación con redes externas.

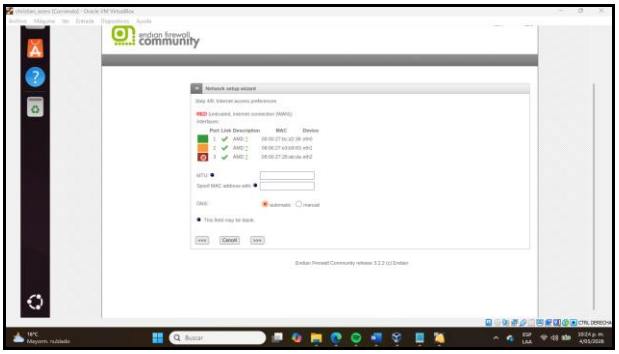

***Fig. 14.*** *Configuración de la zona RED (WAN) y asignación de la interfaz eth2.*

## 2.4 CONFIGURACIÓN DEL SERVIDOR EN LA ZONA DMZ Y ACCESO A ENDIAN

Se configuró la interfaz de red del servidor con el propósito de integrarlo a la zona ORANGE (DMZ), donde se alojaron servicios sobre Ubuntu Server para su posterior validación dentro de la infraestructura (Canonical, s. f.). Para ello, se habilitó el adaptador correspondiente en modo de red interna, asignando el nombre de la red DMZ, lo que permite ubicar el servidor dentro de una zona aislada destinada a la prestación de servicios controlados.

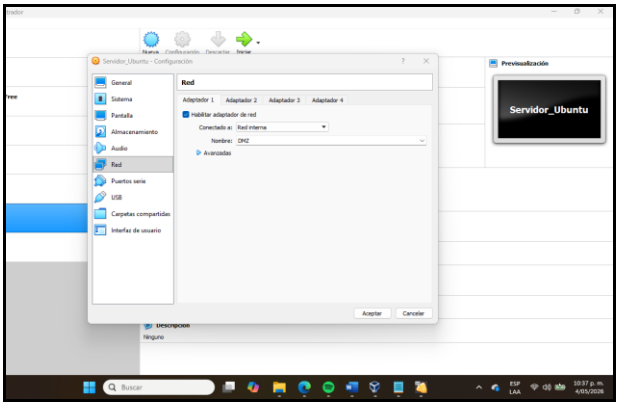


***Fig. 15.*** *Configuración de la interfaz de red del servidor en la zona ORANGE (DMZ).*

Posteriormente, se realizó una prueba de conectividad desde la máquina servidor ubicada en la zona ORANGE (DMZ) hacia el firewall Endian, utilizando herramientas de diagnóstico de red. Esta validación permitió confirmar la correcta comunicación entre el servidor y el firewall dentro de la infraestructura configurada.

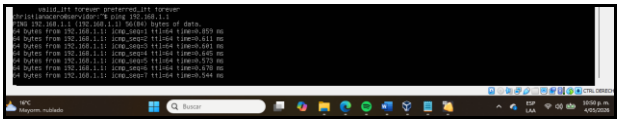

***Fig. 16.*** *Prueba de conectividad desde el servidor en la zona ORANGE (DMZ) hacia el firewall Endian.*

Finalmente, se accedió al panel de administración de Endian Firewall, donde se visualizaron las métricas y el estado general del sistema. Este entorno permite monitorear el rendimiento del firewall, el estado de las interfaces de red y el tráfico generado, proporcionando información clave para la gestión y control de la infraestructura.

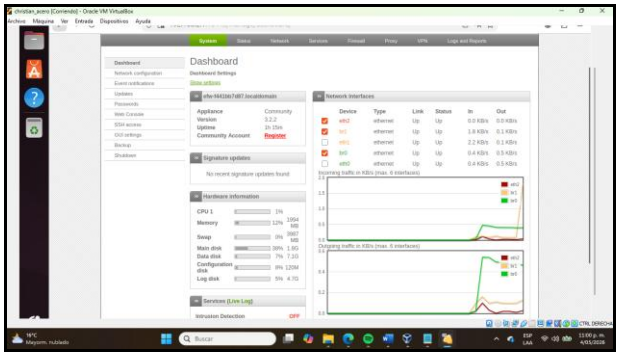


***Fig. 17.*** *Visualización del panel de administración (dashboard) de Endian Firewall.*

Como resultado de la actividad desarrollada, se cumplió con el producto esperado, logrando la implementación funcional de Endian Firewall con la configuración de las zonas GREEN (LAN), RED (WAN) y ORANGE (DMZ). Asimismo, se verificó la conectividad entre los distintos elementos de la red y el acceso al sistema de administración, demostrando la correcta operación de la infraestructura configurada.

## 2.5 CONFIGURACIÓN NAT

La figura presenta el proceso de configuración de una regla de NAT fuente en Endian Firewall, aplicada a la red de origen 192.168.2.0/24, correspondiente a la zona GREEN (LAN). La traducción de direcciones permite modificar la dirección origen o destino del tráfico para facilitar la comunicación entre redes internas y externas (Netfilter, s. f.).

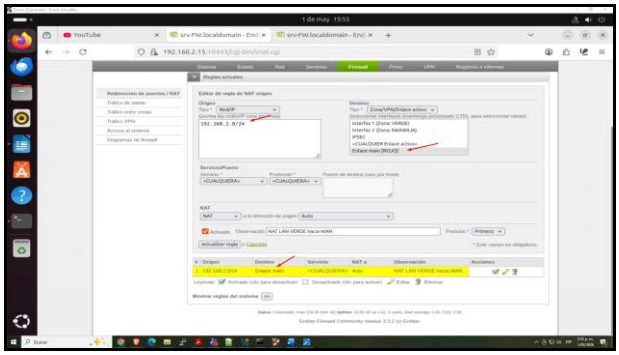

***Fig. 18.*** *Configuración de NAT fuente para la zona LAN en Endian Firewall.*

La figura presenta el proceso de configuración de una regla de NAT fuente en Endian Firewall, aplicada a la red de origen 192.168.1.0/24, correspondiente a la zona ORANGE (DMZ). En esta regla, el tráfico saliente de la DMZ se direcciona hacia la interfaz principal RED/WAN, permitiendo que el firewall realice la traducción de direcciones IP para la salida hacia la red externa. Esta configuración hace parte de la

habilitación de conectividad controlada de los servidores ubicados en la DMZ hacia Internet.

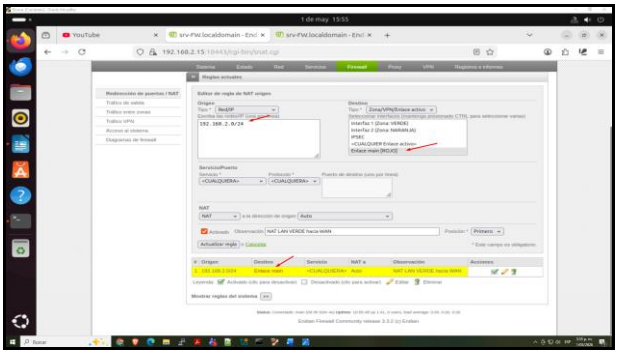

***Fig. 19.*** *Configuración de NAT fuente para la zona DMZ en Endian Firewall.*

La figura presenta el listado de reglas de NAT fuente configuradas en Endian Firewall, donde se identifican las redes de origen 192.168.2.0/24, correspondiente a la zona GREEN (LAN), y 192.168.1.0/24, asociada a la zona ORANGE (DMZ). Ambas reglas direccionan el tráfico hacia la interfaz principal RED/WAN y aplican traducción automática de direcciones IP, permitiendo la salida controlada de la LAN y la DMZ hacia la red externa.

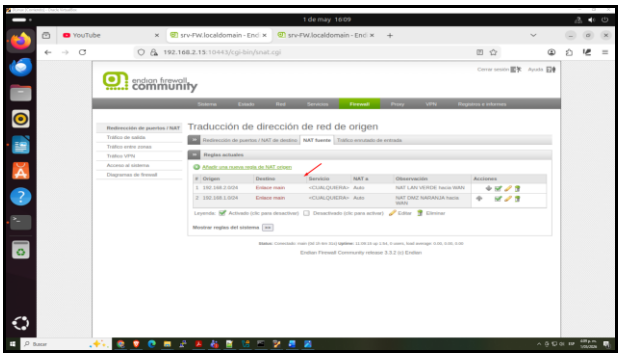

***Fig. 20.*** *Visualización de reglas NAT fuente configuradas en Endian Firewall.*

La figura presenta el listado de reglas de redirección de puertos / NAT de destino configuradas en Endian Firewall. Se evidencian reglas activas desde Enlace ANY hacia el servidor 192.168.1.20, ubicado en la zona ORANGE (DMZ), permitiendo la publicación de servicios como FTP por el puerto 21, HTTP por el puerto 80, HTTPS por el puerto 443 y un servicio adicional asociado al puerto 8080. Esta configuración permite que las solicitudes provenientes de la red externa sean traducidas y dirigidas hacia el servidor de la DMZ, habilitando el acceso controlado a los servicios publicados.

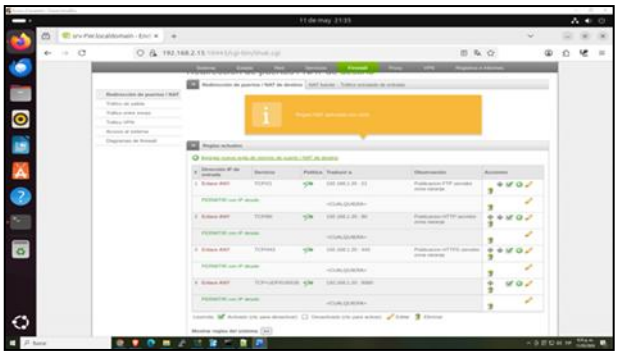

***Fig. 21.*** *Configuración de reglas de redirección de puertos hacia el servidor en la zona ORANGE/DMZ.*

La figura presenta la salida del comando iptables ejecutado desde la consola de Endian Firewall, donde se evidencian las reglas de traducción de direcciones configuradas en el sistema. En la sección POSTPORTFW se observan reglas DNAT, utilizadas para redirigir tráfico entrante hacia direcciones internas, mientras que en la sección SOURCENAT se identifican reglas SNAT aplicadas a las redes 192.168.1.0/24 y 192.168.2.0/24. Esta validación confirma que las reglas de NAT fuente y NAT de destino configuradas desde la interfaz web fueron aplicadas correctamente a nivel del firewall.

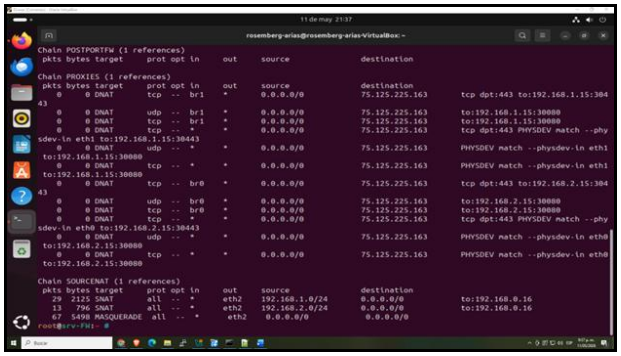

***Fig. 22.*** *Verificación de reglas NAT mediante iptables en Endian Firewall.*

La figura presenta el listado de reglas activas del firewall de salida en Endian Firewall, donde se evidencian las reglas que permiten el tráfico desde las redes internas hacia la zona ROJO/WAN. En particular, se observan las reglas asociadas a la red 192.168.2.0/24, correspondiente a la zona GREEN (LAN), y a la red 192.168.1.0/24, correspondiente a la zona ORANGE (DMZ). Ambas reglas permiten cualquier servicio hacia la WAN, lo que habilita la salida controlada del tráfico de la LAN y la DMZ hacia la red externa, complementando el funcionamiento de las reglas de NAT fuente configuradas previamente.

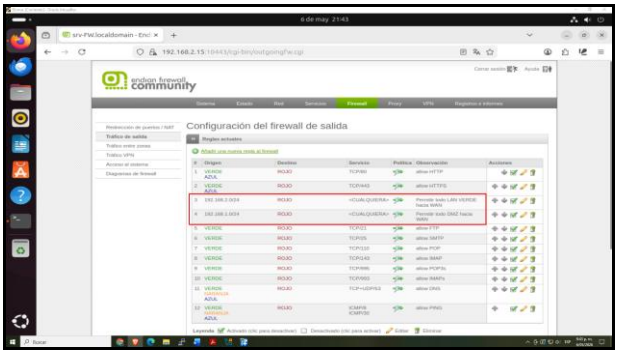

***Fig. 23.*** *Configuración de reglas del firewall de salida en Endian Firewall.*

La figura presenta la configuración de red de la máquina virtual cliente en Oracle VirtualBox, donde el adaptador de red se encuentra asociado a una red interna correspondiente a la zona GREEN (LAN). Esta configuración permite que el equipo cliente forme parte de la red interna administrada por Endian Firewall, estableciendo comunicación con la interfaz GREEN del firewall para validar la conectividad, el enrutamiento y la salida controlada hacia la red externa mediante las reglas NAT configuradas.

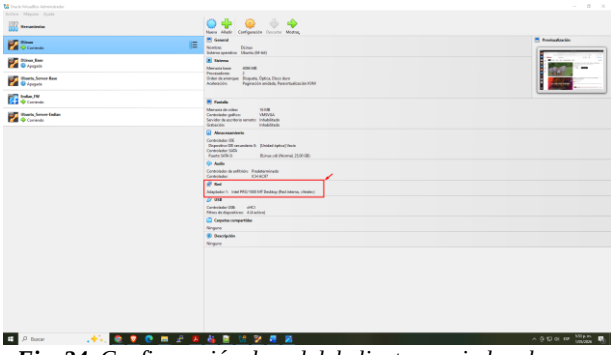

***Fig. 24.*** *Configuración de red del cliente asociado a la zona GREEN/LAN.*

La figura presenta la prueba de conectividad realizada desde el cliente ubicado en la zona GREEN (LAN) hacia la interfaz interna del firewall Endian, identificada con la dirección IP 192.168.2.15. Mediante la ejecución del comando ping, se evidencia respuesta satisfactoria desde dicha interfaz, lo cual confirma la comunicación entre el equipo cliente y el firewall dentro de la red LAN. Esta validación permite comprobar que la configuración de red del cliente y la conexión con la zona GREEN se encuentran operativas como paso previo a la verificación de salida hacia la red externa mediante NAT fuente.

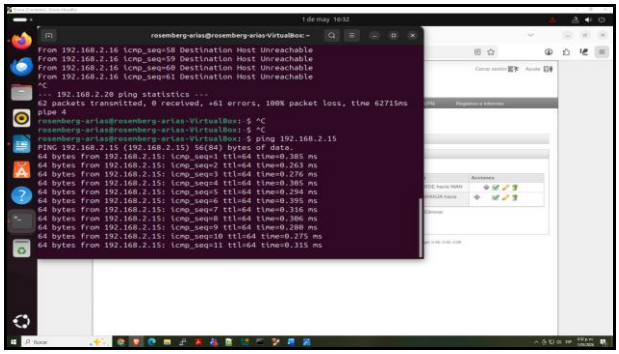

***Fig. 25.*** *Verificación de conectividad desde la LAN GREEN hacia la interfaz del firewall.*

La figura presenta la ejecución del comando ping google.com desde el equipo cliente ubicado en la zona GREEN (LAN). La respuesta satisfactoria desde el dominio externo evidencia que el cliente cuenta con resolución DNS y conectividad hacia Internet. Este resultado permite validar que el tráfico saliente de la red LAN está siendo encaminado correctamente a través de Endian Firewall mediante la regla de NAT fuente configurada hacia la interfaz RED/WAN.

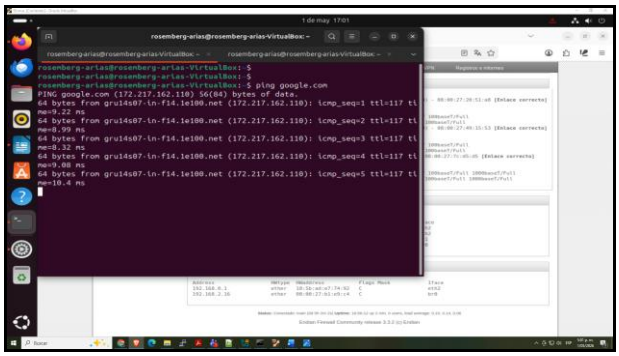

***Fig. 26.*** *Prueba de conectividad hacia Internet desde el cliente de la zona GREEN/LAN.*

La figura presenta la ejecución del comando traceroute google.com desde el equipo cliente Ubuntu, con el objetivo de validar la ruta seguida por el tráfico hacia Internet. En el primer salto se evidencia la dirección IP 192.168.2.15, correspondiente al firewall Endian en la zona GREEN (LAN). Esto confirma que el tráfico saliente del cliente es enviado inicialmente hacia el firewall, el cual actúa como puerta de enlace predeterminada y aplica las reglas de enrutamiento y NAT fuente para permitir la salida hacia la interfaz RED/WAN. Posteriormente, la traza continúa hacia la red externa hasta alcanzar el destino asociado a Google, validando la conectividad hacia Internet.

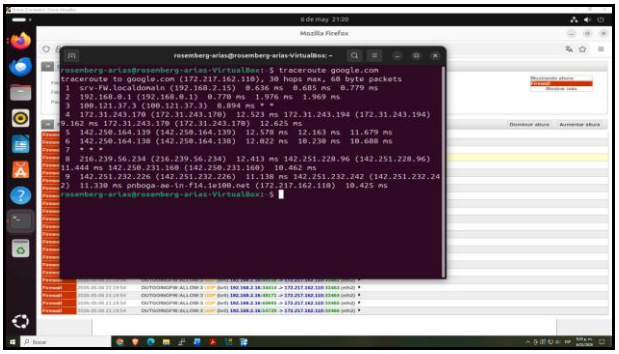

***Fig. 27.*** *Verificación de la ruta de salida hacia Internet mediante traceroute.*

La figura presenta la configuración de red de la máquina virtual servidor en Oracle VirtualBox, donde el adaptador de red se encuentra asociado a una red interna correspondiente a la zona ORANGE (DMZ). Esta configuración permite que el servidor forme parte de la red desmilitarizada administrada por Endian Firewall, estableciendo comunicación con la interfaz ORANGE del firewall para validar el aislamiento de la DMZ, el enrutamiento y la salida controlada hacia la red externa mediante las reglas de NAT fuente configuradas.

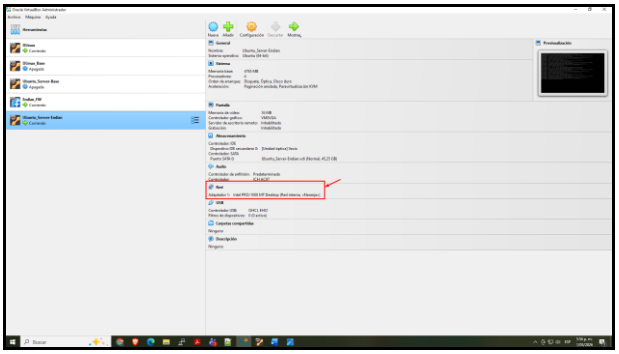

***Fig. 28.*** *Configuración de red del servidor asociado a la zona ORANGE/DMZ.*

La figura presenta la ejecución de los comandos ip route, ping 192.168.1.15, ping 8.8.8.8 y ping google.com desde el servidor ubicado en la zona ORANGE (DMZ). En la salida del comando ip route se evidencia que la puerta de enlace predeterminada corresponde a la dirección 192.168.1.15, asociada al firewall Endian en la zona DMZ. Posteriormente, las pruebas de conectividad muestran respuesta satisfactoria hacia la puerta de enlace, hacia la dirección pública 8.8.8.8 y hacia el dominio google.com, lo cual confirma el correcto enrutamiento, la resolución DNS y la salida controlada hacia Internet mediante la regla de NAT fuente configurada para la zona ORANGE/DMZ.

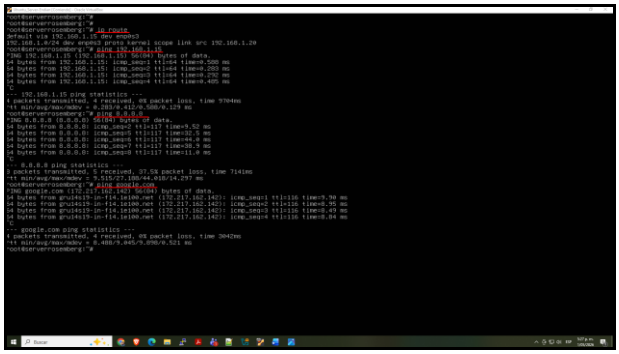

***Fig. 29.*** *Validación de conectividad del servidor ubicado en la zona ORANGE/DMZ.*

La figura presenta la ejecución del comando traceroute google.com desde el servidor ubicado en la zona ORANGE (DMZ), con el objetivo de validar la ruta seguida por el tráfico hacia Internet. En el primer salto se evidencia la dirección IP 192.168.1.15, correspondiente al firewall Endian en la zona DMZ, lo que confirma que el tráfico saliente del servidor es enviado inicialmente hacia el firewall. Posteriormente, la traza continúa hacia redes externas hasta alcanzar el destino asociado a Google, validando el correcto enrutamiento y la operación de la regla de NAT fuente configurada para permitir la salida controlada de la DMZ hacia la interfaz RED/WAN.

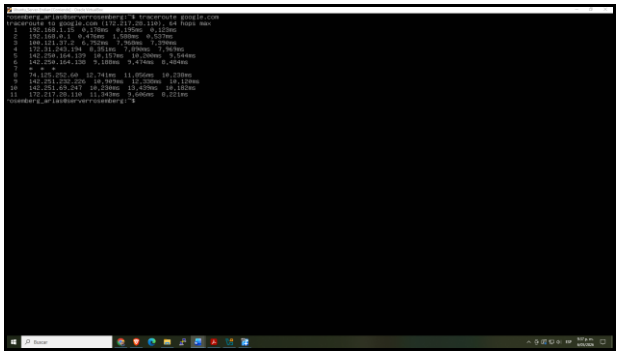

***Fig. 30.*** *Verificación de la ruta de salida hacia Internet desde la zona ORANGE/DMZ.*

La figura presenta la ejecución de pruebas de conectividad mediante el comando ping hacia diferentes plataformas externas, entre ellas www.youtube.com y www.unad.edu.co, desde el servidor ubicado en la zona ORANGE (DMZ). Las respuestas satisfactorias obtenidas evidencian que el servidor cuenta con conectividad hacia Internet y resolución DNS funcional. Este resultado confirma que el tráfico saliente de la DMZ es encaminado correctamente a través de Endian Firewall, mediante la regla de NAT fuente configurada hacia la interfaz RED/WAN.

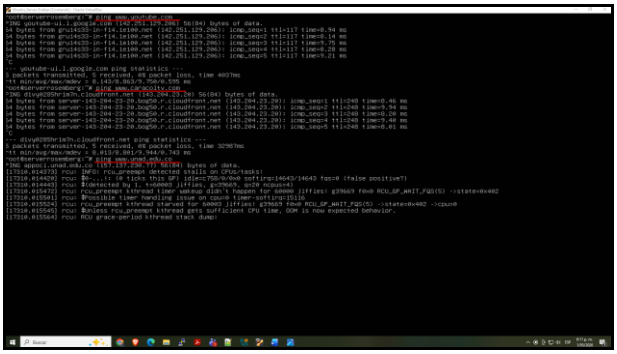

***Fig. 31.*** *Validación de conectividad hacia plataformas externas desde la zona ORANGE/DMZ.*

La figura presenta la validación del acceso al servidor web publicado detrás de Endian Firewall desde el equipo físico. Para esta prueba, se ingresa en el navegador a la dirección IP 192.168.0.16, correspondiente a la interfaz de publicación configurada en el firewall. Como resultado, se visualiza la página predeterminada de Apache2 del servidor Ubuntu ubicado en la zona ORANGE (DMZ), lo cual confirma que la regla de NAT de destino y la redirección del puerto HTTP se encuentran funcionando correctamente, permitiendo el acceso controlado al servicio web desde la red externa.

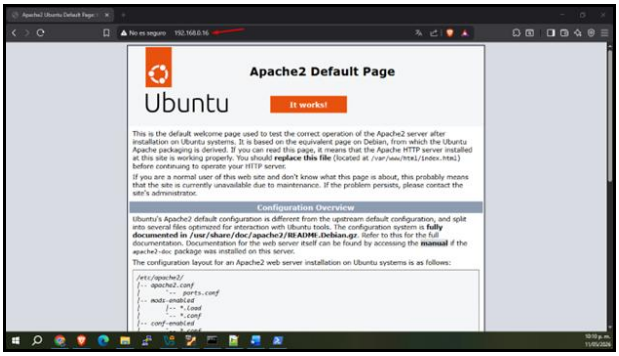


***Fig. 32.*** *Validación del acceso al servidor web Apache publicado en la zona DMZ.*

La figura presenta los registros en tiempo real del módulo de firewall en Endian Firewall, donde se evidencia el tráfico generado desde las redes internas hacia la interfaz de salida RED/WAN. En los eventos registrados se observan conexiones permitidas mediante reglas OUTGOINGFW: ALLOW, asociadas a direcciones internas como 192.168.1.20 y 192.168.2.16, con destino a diferentes direcciones externas a través de protocolos TCP y UDP. Esta evidencia permite verificar que el tráfico de las zonas ORANGE (DMZ) y GREEN (LAN) está siendo procesado por el firewall y encaminado hacia la red externa conforme a las reglas de salida y NAT fuente configuradas.

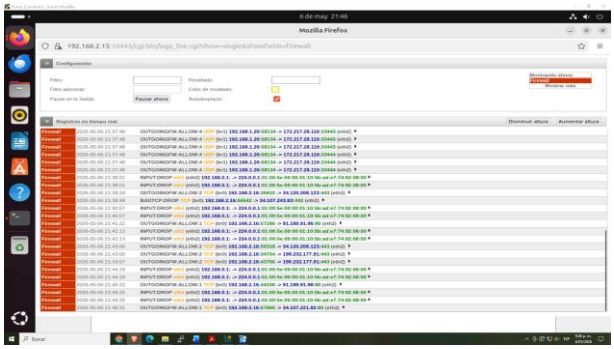

***Fig. 33.*** *Visualización de registros en tiempo real del firewall Endian.*

## 2.6 IMPLEMENTACIÓN DE PROXY HTTP Y FILTRADO DE CONTENIDO

La infraestructura organizacional requiere la implementación de un intermediario que regule las peticiones entre la red interna (ZONA GREEN) y la red pública (ZONA RED). En este contexto, se procedió con la activación del servicio HTTP Proxy en el Endian Firewall, configurándolo inicialmente en modo transparente para facilitar la administración de los dispositivos finales sin requerir ajustes manuales en cada cliente (Endian, s. f.). Esta configuración permite capturar el tráfico saliente por los puertos estándar y someterlo a las políticas de seguridad corporativas, optimizando el uso del ancho de banda y estableciendo una primera barrera de defensa contra sitios potencialmente maliciosos o no permitidos.

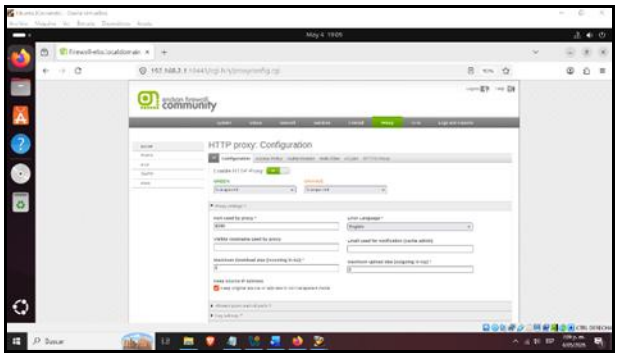


***Fig. 34.*** *Activación del servicio HTTP Proxy y definición de parámetros operativos en la interfaz de gestión.*

Para gestionar restricciones, se diseñó el perfil granular 'Filtro_Elio', integrando protección antivirus para mitigar malware (Endian, s. f.). En la configuración de Blacklists, se añadieron dominios como facebook.com y youtube.com. Este método genera una base de datos de consulta rápida que intercepta peticiones de clientes Ubuntu antes de conectar con el destino, bloqueando autónomamente el tráfico no autorizado (Canonical, s. f.).


***Fig. 35.*** *Configuración de perfiles de filtrado y gestión de listas negras para la restricción de dominios.*

Una vez robustecido el perfil, se creó una Access Policy (Política de Acceso) que actúa como el puente entre la configuración lógica y el tráfico real de la red. En esta regla se definió que todo el tráfico proveniente de la zona GREEN debe ser procesado obligatoriamente por el perfil de seguridad "Filtro_Elio" (Endian, s. f.). Para garantizar la ejecución de las restricciones, la política se ubicó estratégicamente en la primera posición de la tabla de reglas. Al guardar los cambios, el sistema confirmó la aplicación exitosa de los parámetros mediante un mensaje informativo, activando formalmente la protección y el filtrado de contenidos para todos los usuarios de la red local.

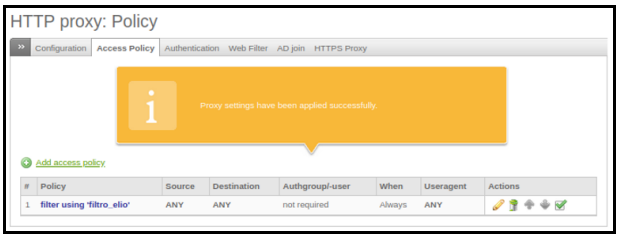


***Fig. 36.*** *Jerarquización de reglas y confirmación de la aplicación de políticas de acceso en el firewall.*

Dado que la mayor parte del tráfico web actual se encuentra cifrado, se habilitó el módulo HTTPS Proxy utilizando el modo de operación "Decrypt and scan" (Endian, s. f.). Esta técnica de inspección profunda permite al firewall interceptar el tráfico seguro para validar el destino real de la petición, asegurando que el filtrado de dominios como Facebook sea efectivo incluso bajo protocolos SSL/TLS. La validación técnica se ejecutó desde el cliente Ubuntu, donde el navegador Firefox reportó una advertencia de seguridad al intentar acceder a los sitios restringidos, confirmando que el firewall intercepta la comunicación y cumple con la política de bloqueo establecida (Endian, s. f.).

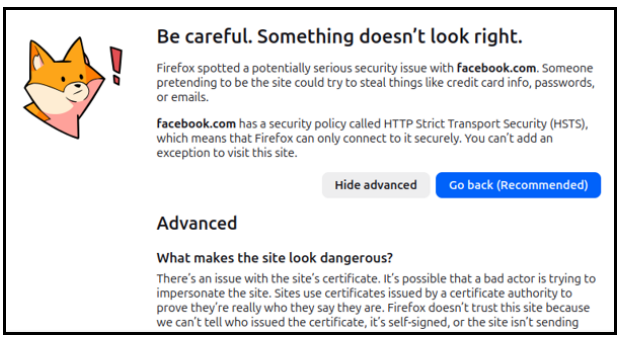


***Fig. 37.*** *Prueba de campo evidenciando el bloqueo efectivo de la red social bajo protocolos de seguridad cifrados.*

Como fase final de la implementación, se utilizó la herramienta de auditoría Live Logs para verificar el comportamiento del sistema desde la perspectiva de los registros de actividad (Endian, s. f.). En esta interfaz se pudo observar el flujo de paquetes en paralelo con el navegador del cliente, destacando las entradas en color rojo con el estado DROP. Estas líneas de registro proveen información detallada sobre el origen y destino del tráfico, evidenciando cómo el firewall intercepta y rechaza las peticiones hacia los servidores de las redes sociales bloqueadas, lo que constituye una evidencia técnica de la operatividad del sistema de seguridad perimetral implementado (Endian, s. f.).

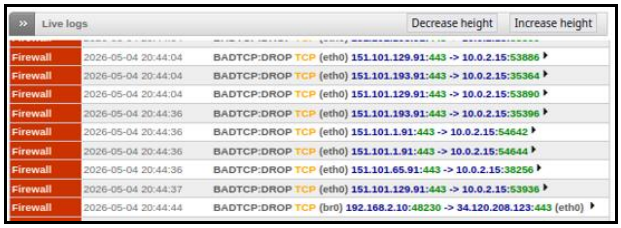


***Fig. 38.*** *Auditoría de tráfico en tiempo real mediante registros de actividad y validación de políticas.*

## 2.7 REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO

En esta primera parte se configuró la comunicación entre la zona GREEN, que corresponde a la LAN, y la zona ORANGE, que corresponde a la DMZ, donde se encontraba ubicado el servidor Ubuntu Server. El objetivo de esta configuración fue permitir que desde la red interna se pudiera acceder a los servicios publicados en el servidor de la DMZ, específicamente HTTP por el puerto 80 y FTP por el puerto 21, ya que estos servicios hacen parte de los requerimientos del laboratorio.

Estas evidencias muestran básicamente el momento en que se habilita la comunicación entre la red interna y la DMZ. En otras palabras, aquí se dejó listo el camino para que desde la LAN se pudiera consultar el servidor web alojado en la zona ORANGE y, de igual forma, intentar el acceso al servicio FTP configurado en esa misma máquina.

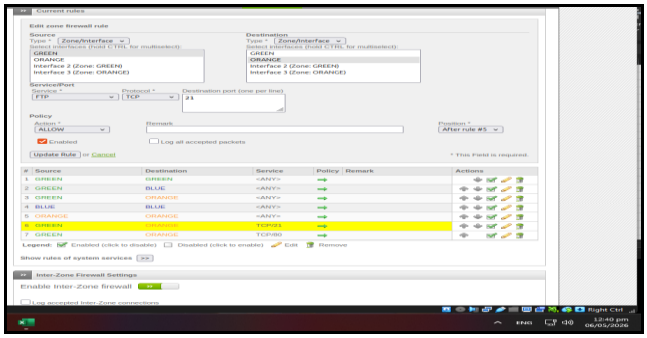

***Fig. 39.*** *Comunicación entre la zona GREEN y la zona ORANGE mediante los protocolos HTTP y FTP, utilizando sus respectivos puertos.*

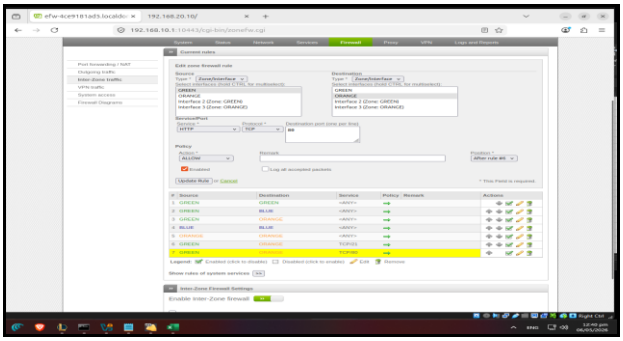

***Fig. 40.*** *Habilitación de la comunicación entre la red interna y la zona desmilitarizada (DMZ).*

En la segunda parte del laboratorio se trabajó la comunicación entre la zona Internet, representada por la WAN, y la zona DMZ. Para esto fue necesario configurar reglas de Port Forwarding / Destination NAT dentro de Endian, ya que el servidor de la DMZ se encontraba protegido detrás del firewall y no era accesible directamente desde el exterior.

Lo que se hizo en esta etapa fue publicar los servicios del servidor DMZ para que pudieran ser alcanzados desde la WAN. En este caso, se configuró el reenvío del tráfico entrante hacia la dirección IP del servidor en la zona ORANGE, es decir, hacia 192.168.1.20, permitiendo el acceso al puerto 80 para HTTP y al puerto 21 para FTP.

Estas capturas evidencian la creación de las reglas NAT necesarias para que el tráfico proveniente de Internet no terminara en el firewall, sino que fuera redirigido correctamente al servidor ubicado en la DMZ. Gracias a esta parte de la configuración fue posible, posteriormente, realizar pruebas de acceso desde el host hacia los servicios publicados en la zona ORANGE.

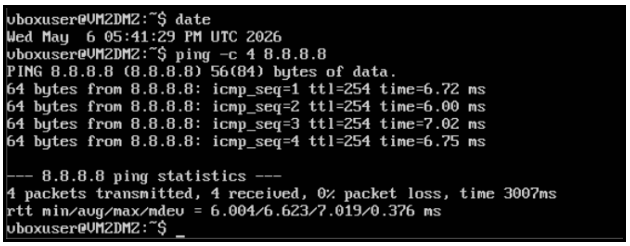


***Fig. 41.*** *Establecimiento de comunicación entre la red de Internet y la zona desmilitarizada (DMZ).*

En esta sección se hizo la validación de las reglas creadas dentro del módulo Inter-Zone traffic del firewall Endian. Esta parte fue importante porque no bastaba con crear reglas, sino que también era necesario comprobar que sí hubieran quedado aplicadas correctamente entre las diferentes zonas definidas en el escenario: GREEN, ORANGE y RED.

Las evidencias de esta hoja muestran el listado de políticas configuradas en el firewall, donde se puede observar el origen, el destino, el servicio permitido y la acción aplicada. Esto permitió verificar que la comunicación entre la LAN y la DMZ estaba habilitada bajo los protocolos requeridos, y que la estructura general de acceso entre zonas estaba coherente con lo solicitado en la actividad.

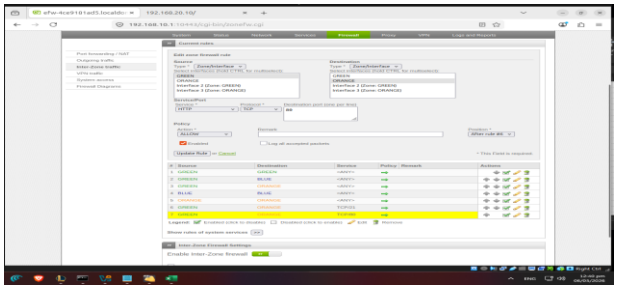

***Fig. 42.*** *Validación del tráfico interzona para la comprobación de la creación de reglas.*

En la última parte se realizaron las pruebas funcionales para comprobar que las reglas configuradas sí estaban dando resultado en el entorno del laboratorio. Aquí se validó el acceso al servicio HTTP desde la LAN hacia la DMZ, desde la LAN hacia la WAN, desde la DMZ hacia la WAN y también desde la WAN hacia la DMZ, que eran varios de los requerimientos principales planteados en la temática 4.

Estas evidencias reflejan ya la parte más práctica del laboratorio, porque es donde se comprueba si toda la configuración previa realmente funcionó. En otras palabras, aquí se demuestra que las reglas creadas en Endian sí permitieron el paso del tráfico esperado y que el escenario LAN–WAN–DMZ quedó operando de acuerdo con lo pedido en la guía.

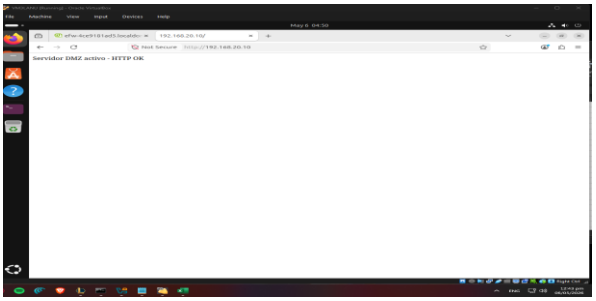


***Fig. 43.*** *Acceso al servicio HTTP desde la red LAN hacia la zona desmilitarizada (DMZ).*

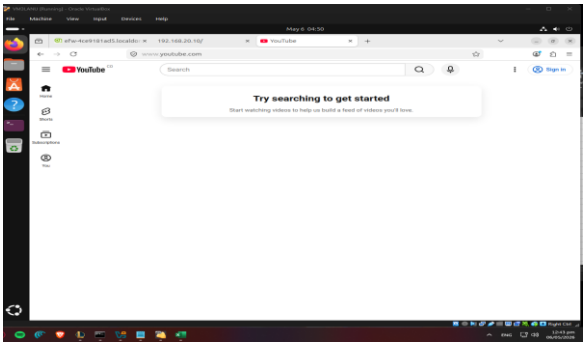


***Fig. 44.*** *Acceso al servicio HTTP desde la red LAN hacia la red WAN.*


***Fig. 45.*** *Acceso al servicio HTTP desde la zona desmilitarizada (DMZ) hacia la red WAN.*

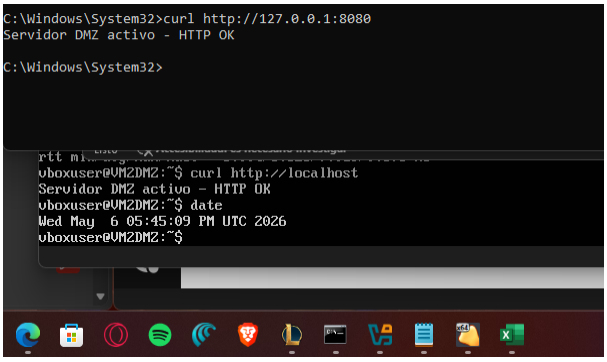


***Fig. 46.*** *Acceso al servicio HTTP desde la red WAN hacia la zona desmilitarizada (DMZ).*

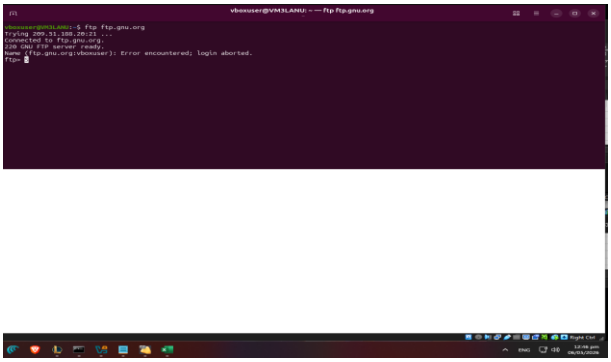

***Fig. 47.*** *Acceso al servicio FTP desde la red LAN hacia la red WAN.*

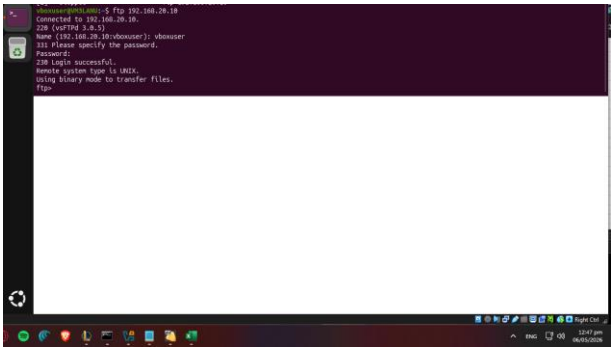

***Fig. 48.*** *Acceso al servicio FTP desde la red WAN hacia la zona desmilitarizada (DMZ).*

Las pruebas finales permitieron validar el acceso a los servicios HTTP y FTP desde diferentes zonas de red, confirmando que las reglas de acceso, NAT y redirección de puertos fueron aplicadas correctamente. Estas evidencias demuestran que la comunicación entre LAN, WAN y DMZ quedó configurada de acuerdo con los requerimientos establecidos en la actividad.

# 3 CONCLUSIONES

La implementación de Endian Firewall en un entorno virtualizado permitió establecer una infraestructura de red segmentada mediante las zonas GREEN (LAN), RED (WAN) y ORANGE (DMZ), garantizando un adecuado control del tráfico y una mejor organización de los servicios dentro de la red.

La configuración de reglas NAT y políticas de acceso posibilitó la comunicación entre las diferentes zonas de red y el acceso controlado a Internet, evidenciando el correcto funcionamiento de las interfaces y de los mecanismos de traducción de direcciones implementados.

La habilitación de servicios HTTP y FTP en la zona DMZ, junto con la restricción del protocolo ICMP y el uso de reglas de filtrado, permitió fortalecer la seguridad de la infraestructura, limitando accesos no autorizados y controlando el tráfico entre redes.

La implementación de un proxy HTTP con autenticación de usuarios y políticas de filtrado demostró la capacidad de Endian Firewall para gestionar el acceso a contenidos web, aplicando restricciones mediante listas negras y mejorando el control de navegación dentro de la red.

# 4 REFERENCIAS

Canonical. (s. f.). Ubuntu Server documentation. https://ubuntu.com/server/docs

Endian. (s. f.). Endian Firewall community documentation. https://docs.endian.com

Netfilter. (s. f.). Netfilter and iptables documentation. https://netfilter.org/documentation/

Oracle. (s. f.). *Oracle VM VirtualBox user manual.* https://www.virtualbox.org/wiki/Documentation