Forjando un muro Digital: Un Viaje desde Cero con Endian Firewall

José Ignacio Galindo Florez jigalindof@unadvirtual.edu.co
Eliana Sofía Guerrero Rincón esguerreror@unadvirtual.edu.co
Edson Andrés Ruiz Linares: earuiz@unadvirtual.edu.co
Juan Sebastian Quintero Motato: jsquinteromo@unadvirtual.edu.co
Jose Luis Forero Rey: jlforero@unadvirtual.edu.co

RESUMEN— Este artículo presenta la implementación integral de un sistema de seguridad perimetral utilizando GNU/Linux Endian Firewall dentro de un entorno virtualizado en Oracle VirtualBox. El trabajo se estructura en cinco temáticas que abarcan desde la instalación de la plataforma, la segmentación de la red en zonas Verde (LAN), Roja (WAN) y Naranja (DMZ), hasta la configuración de políticas de seguridad basadas en NAT, filtrado de tráfico, control de servicios y autenticación en proxy HTTP. A partir de máquinas virtuales Ubuntu Desktop y Ubuntu Server, se validan las reglas de acceso entre zonas, el funcionamiento de servicios HTTP y FTP, la restricción del protocolo ICMP, y la correcta aplicación de perfiles de navegación. Los resultados demuestran la capacidad de Endian para gestionar de manera centralizada funciones críticas como traducción de direcciones, inspección de tráfico y control de contenidos, permitiendo establecer una arquitectura segura, modular y adaptable a escenarios educativos y administrativos. Este proceso evidencia la importancia de una segmentación adecuada y la aplicación de políticas explícitas para garantizar la integridad y disponibilidad de los servicios en una red perimetral.

Abstract— This paper presents the implementation of a perimeter security architecture using the GNU/Linux-based Endian Firewall platform deployed in a virtualized environment under Oracle VirtualBox. The study is structured into five thematic components that address the installation of the security gateway, the segmentation of the network into Green (LAN), Red (WAN), and Orange (DMZ) zones, and the configuration of NAT rules, inter-zone traffic policies, and controlled exposure of network services. Using Ubuntu Desktop and Ubuntu Server as endpoint and service hosts, detailed tests were conducted to validate access permissions for HTTP and FTP services, enforce ICMP blocking, and apply user-based authentication through a non-transparent HTTP proxy. The results confirm that Endian Firewall provides a robust and centralized mechanism for traffic control, service filtering, and secure communication across network zones. Furthermore, the implementation highlights the relevance of network segmentation and policy-driven security as essential practices for ensuring integrity, confidentiality, and controlled access in academic and enterprise infrastructures.

PALABRAS CLAVE: DMZ, Endian Firewall, Linux, NAT, Seguridad Perimetral

I. INTRODUCCIÓN

La protección del perímetro de red es un componente esencial en la administración de sistemas GNU/Linux, especialmente cuando se requiere controlar el acceso entre segmentos internos y externos. En este trabajo se implementa Endian Firewall en un entorno virtualizado con VirtualBox, configurando una arquitectura compuesta por tres zonas: verde (LAN), naranja (DMZ) y roja (WAN).

A través de esta estructura se desarrollan tareas relacionadas con la traducción de direcciones (NAT), la habilitación y restricción de servicios, el control de protocolos y la aplicación de políticas de seguridad orientadas al tráfico entre zonas. Para validar el funcionamiento se emplean máquinas virtuales Ubuntu Desktop y Ubuntu Server, permitiendo comprobar el comportamiento de las reglas configuradas y la respuesta del firewall ante distintos escenarios.

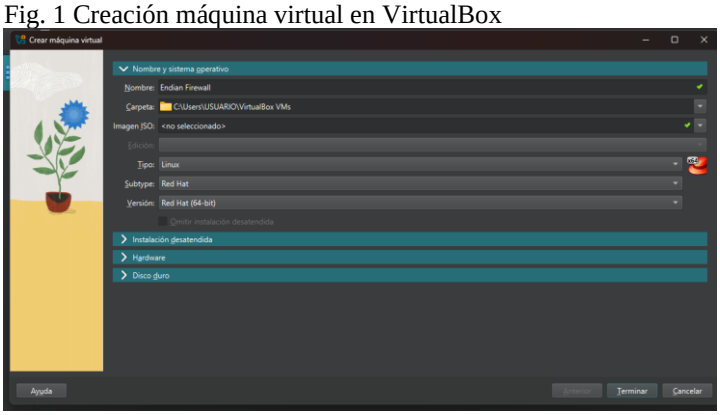
El proceso evidencia la importancia de la segmentación y del establecimiento de políticas explícitas como mecanismos efectivos para fortalecer la seguridad perimetral en infraestructuras educativas y administrativas.

I. TEMÁTICA 1

El objetivo de esta temática es la implementación de GNU/Linux Endian con las zonas verde, roja y naranja, para comenzar se descarga la imagen de disco del siguiente enlace: https://www.endian.com/en/community/
Después de hacer descarga, se debe instalar en virtual Box, para comenzar, se asigna un nombre, es importante tener presente que la versión de sistema operativo corresponde a RedHat

I.I Desarrollo de la temática 1

Fig. 1 Creación máquina virtual en VirtualBox



Fuente: Autoría propia

Fig. 1 Asignación memoria base

Fuente: Autoría propia

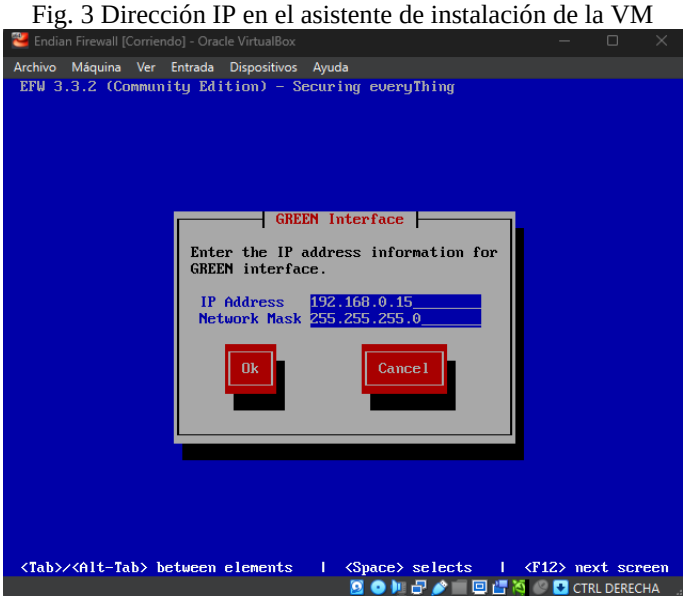
Ahora se requiere asignar la imagen de disco que se descargó, para tal fin se ingresa a la configuración de la máquina virtual que a partir de ahora se va a denominar como VM (virtual Machine) y en la sección de almacenamiento se agrega

Fig. 2 asignación unidad óptica

Fuente: Autoría propia

Con respecto a las configuraciones de red se requiere que el adaptador 1 sea de tipo NAT y el 2 y 3 de tipo red interna de tal manera cuando se inicia la VM se puede observar el asistente de instalación, es importante asignar una dirección IP como se observa a continuación

Fig. 3 Dirección IP en el asistente de instalación de la VM



Fuente: Autoría propia

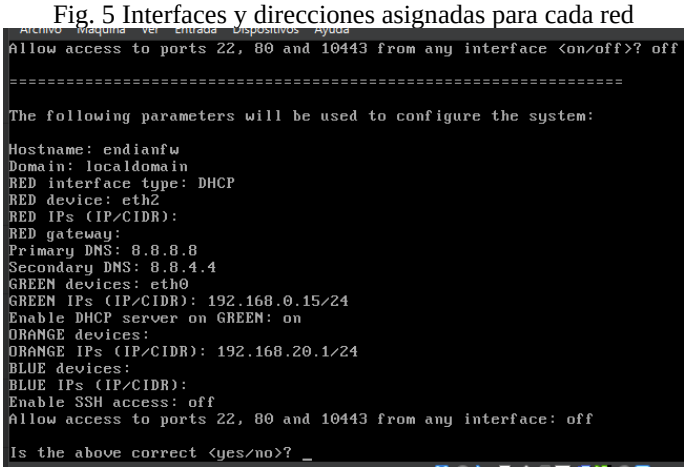
Una vez finalizado el proceso de instalación, se puede observar el inicio de la configuración a realizar, por lo tanto, se cuenta con las siguientes opciones

Fig. 4 Opciones de configuración

Fuente: Autoría propia

Seleccionando la opción 2 y 3 se puede asignar contraseñas para los usuarios admin y Root, una vez hecho esto se selecciona la opción 5 que permite configurar la red, por lo que se asignan tipos de direccionamiento y las Ip para cada red como se muestra a continuación

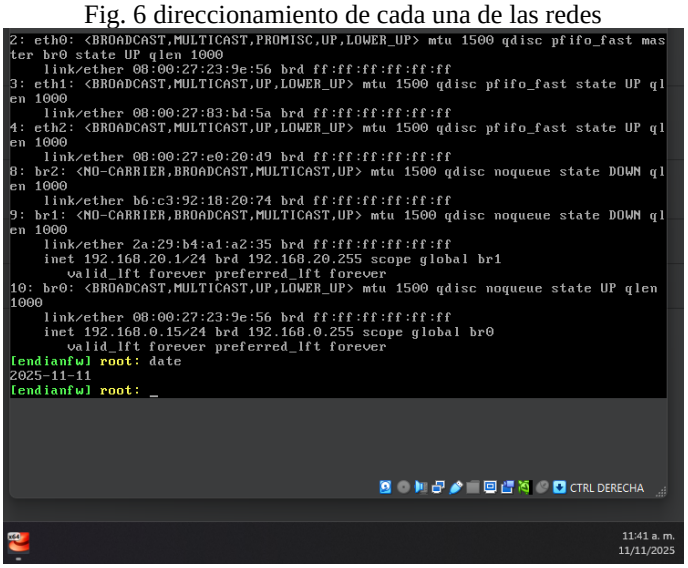
Fig. 5 Interfaces y direcciones asignadas para cada red



Fuente: Autoría propia

Una vez realizada estas asignaciones, se procede a generar evidencias que muestren que todo fue correcto, para tal fin, la Fig.7 muestra la hora, fecha y la correcta implementación de las redes y las direcciones IP

Fig. 6 direccionamiento de cada una de las redes



Fuente: Autoría propia

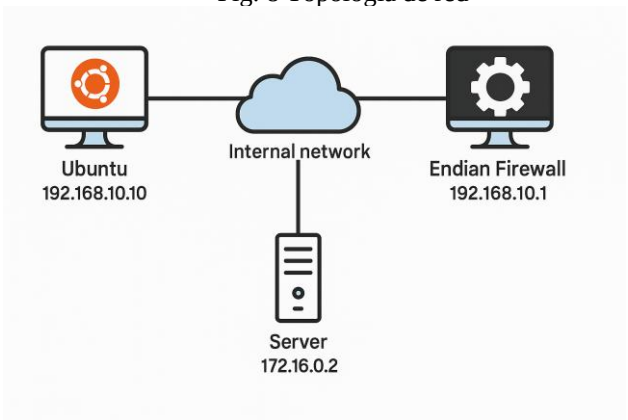
Esto demuestra que se realiza el proceso de manera correcta, donde las redes tiene su propia interfaz.

II. TEMÁTICA 2

El objetivo de esta temática es implementar y validar reglas de Traducción de Direcciones de Red (NAT) en la plataforma Endian Firewall, con el fin de habilitar la comunicación y el acceso a Internet tanto desde la red interna (LAN – zona verde) como desde la red perimetral de servidores (DMZ – zona naranja) hacia la WAN (zona roja). Asimismo, se busca verificar el correcto funcionamiento de dichas reglas mediante pruebas de conectividad y la revisión del registro generado en el módulo de NAT del sistema.

II.I Desarrollo de la temática 2

Fig. 8 Topología de red

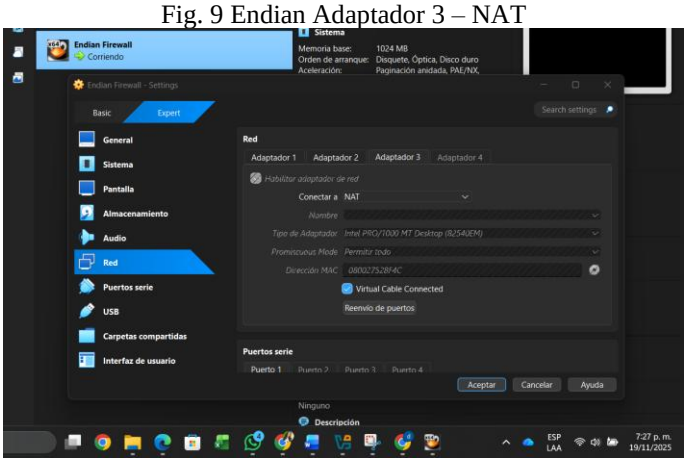


Fuente: Autoría propia

Configuración de los adaptadores de red:

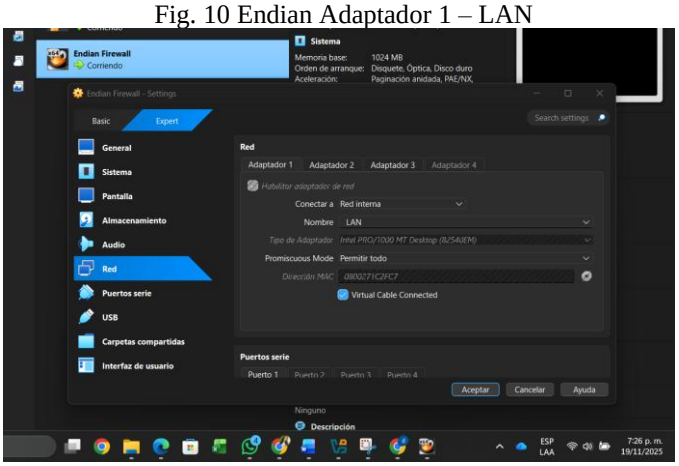
La interfaz RED (WAN) del firewall fue configurada en VirtualBox como **NAT**, permitiendo que Endian obtenga Internet a través del NAT de VirtualBox. Esto habilita la salida a Internet desde las zonas LAN y DMZ.

Fig. 9 Endian Adaptador 3 – NAT



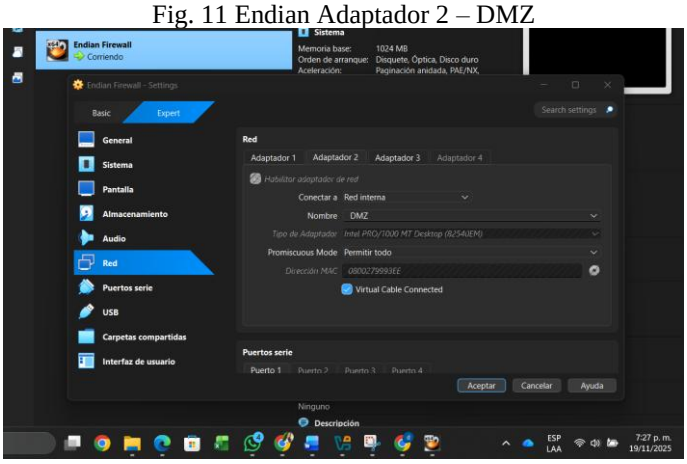
Fuente: Autoría propia

Fig. 10 Endian Adaptador 1 – LAN



Fuente: Autoría propia

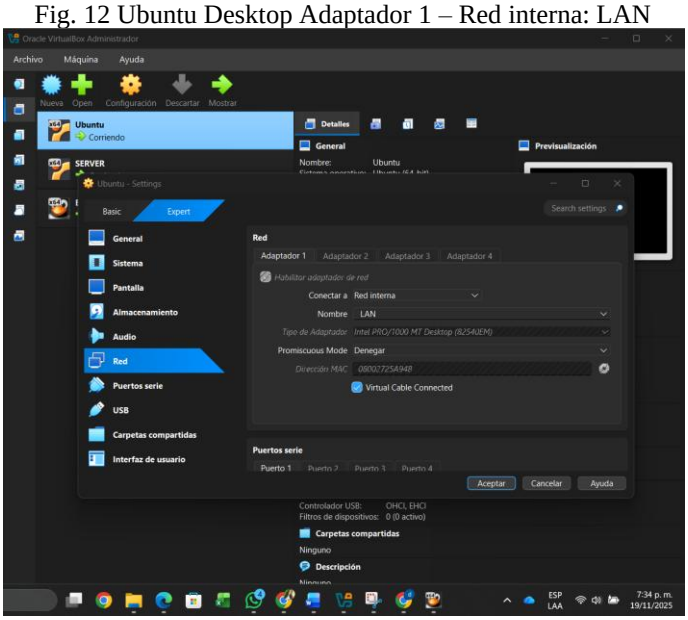
Fig. 11 Endian Adaptador 2 – DMZ



Fuente: Autoría propia

Adaptadores del Ubuntu Desktop (LAN):
El Ubuntu Desktop fue configurado en la red interna **LAN**, asociada a la zona GREEN del firewall. Esta red opera en el rango 192.168.10.0/24.

Fig. 12 Ubuntu Desktop Adaptador 1 – Red interna: LAN



Fuente: Autoría propia

Adaptadores del Ubuntu Server (DMZ):
El servidor Ubuntu se conectó a la red interna **DMZ**, asociada a la zona ORANGE del firewall. Este segmento usa el rango 172.16.0.0/24.

Fig. 13 Ubuntu Server Adaptador 1 – Red interna: DMZ

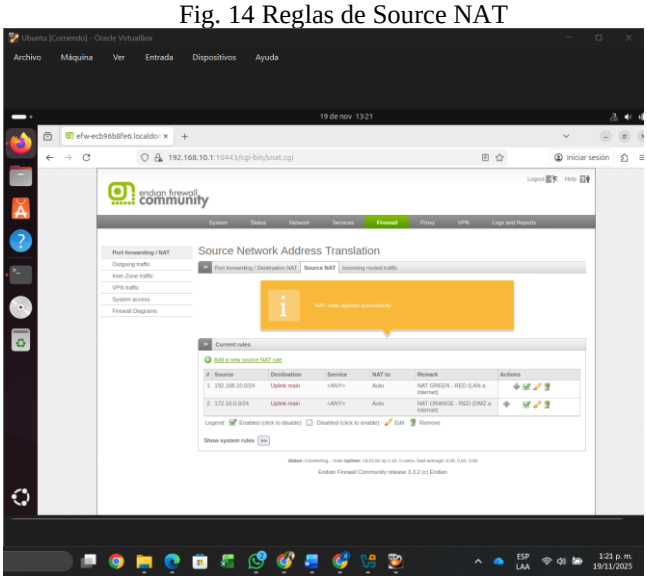
Fuente: Autoría propia

Configuración de reglas NAT en Endian:
En la sección **Firewall → Source NAT**, se crearon dos reglas:

- NAT desde LAN (192.168.10.0/24) hacia la WAN (RED).
- NAT desde DMZ (172.16.0.0/24) hacia la WAN (RED).

Ambas reglas permiten que los dos segmentos internos salgan a Internet mediante la IP pública asignada a la interfaz RED.

Fig. 14 Reglas de Source NAT



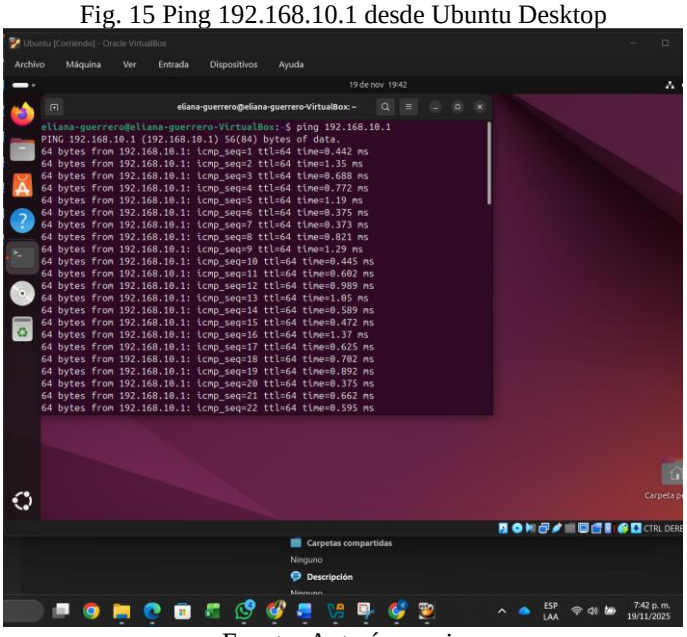
Fuente: Autoría propia

Verificación de conectividad LAN → WAN:
Desde el equipo en la zona LAN se realizaron pruebas de conectividad hacia:

- La interfaz GREEN del firewall (192.168.10.1)
- Un host en Internet (8.8.8.8)
- Un dominio público (google.com)

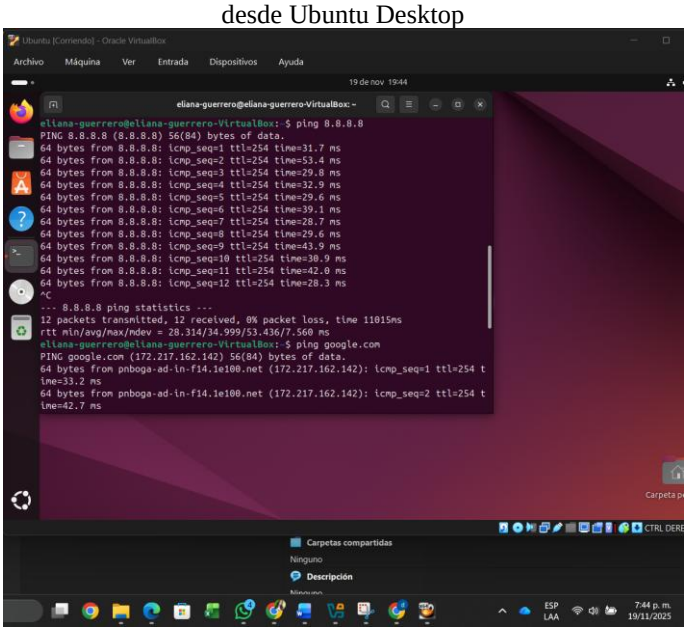
Los resultados demuestran que la LAN tiene acceso correcto hacia Internet mediante NAT.

Fig. 15 Ping 192.168.10.1 desde Ubuntu Desktop



Fuente: Autoría propia

Fig. 16 Ping 8.8.8.8 desde Ubuntu Desktop y Ping google.com desde Ubuntu Desktop



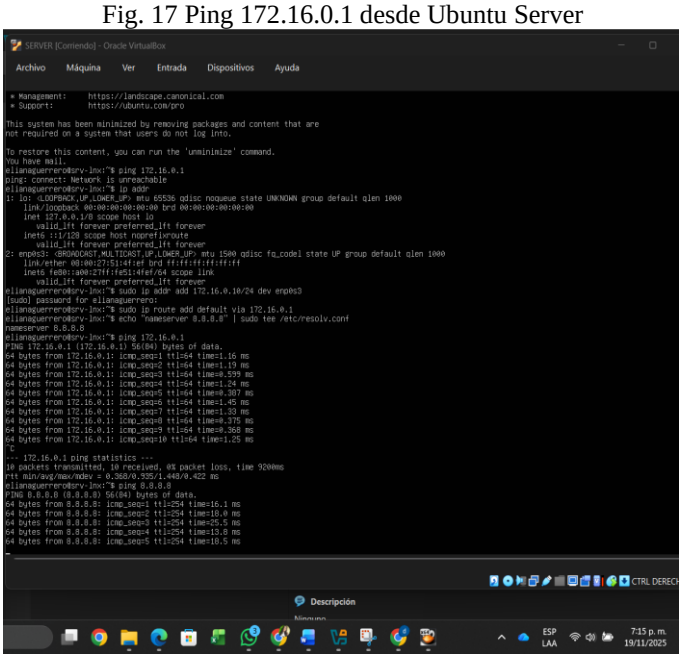
Fuente: Autoría propia

Verificación de conectividad DMZ → WAN:
Desde el Ubuntu Server ubicado en la DMZ se probó conectividad hacia:

- La interfaz ORANGE del firewall (172.16.0.1)
- El servidor DNS público 8.8.8.8
- El dominio google.com

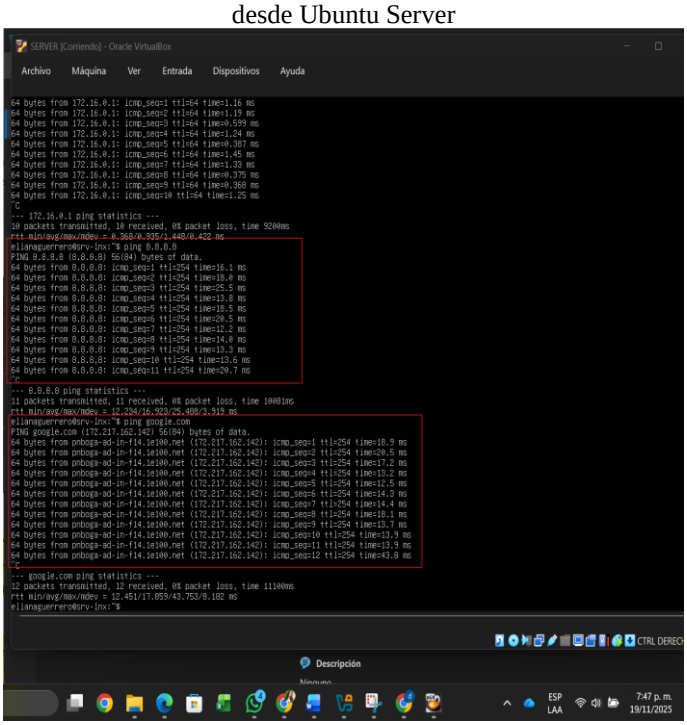
Las respuestas positivas confirman que la DMZ también tiene salida exitosa a Internet a través del NAT configurado en Endian Firewall.

Fig. 17 Ping 172.16.0.1 desde Ubuntu Server



Fuente: Autoría propia

Fig. 18 Ping 8.8.8.8 desde Ubuntu Server y Ping google.com desde Ubuntu Server



Fuente: Autoría propia

La configuración de NAT en Endian Firewall permitió habilitar con éxito la salida a Internet tanto para la red LAN como para la red DMZ. Las pruebas de conectividad demostraron que los equipos de ambos segmentos pueden comunicarse con sus respectivas interfaces del firewall y, posteriormente, alcanzar recursos externos mediante la interfaz RED. Las reglas de Source NAT funcionaron correctamente, permitiendo la traducción de direcciones privada-a-pública y confirmando el flujo adecuado del tráfico. Con esto se cumple completamente el objetivo de la Temática 2, dejando lista la infraestructura para continuar con las políticas de acceso y filtrado correspondientes a la siguiente temática.

III. TEMATICA 3

Permitir el uso de servicios HTTP (Puerto 80) y FTP (Puerto 21) desde el servidor Web en Ubuntu Server. Bloquear el protocolo ICMP (Puerto 8 y puerto 30) para impedir que se realicen pings en la red. Comprobar mediante una consola o terminal la falta de respuesta del comando ping a una dirección IP de la red. Revisar en el tráfico saliente la configuración de las reglas.

III.I Desarrollo de la temática 3

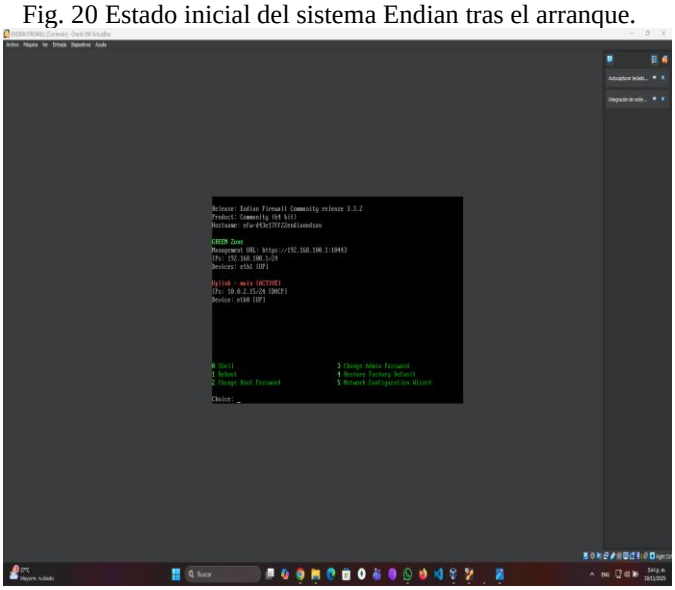
Para iniciar la implementación de la temática, se verificó la configuración base de la máquina virtual Endian en VirtualBox. En esta etapa se definieron los adaptadores de red que representarán las zonas Verde, Roja y Naranja, asegurando que el firewall pueda gestionar correctamente el tráfico entre los diferentes segmentos.

Fig. 19 Configuración inicial de Endian en VirtualBox.

Fuente: Autoría propia.

Una vez que se ha iniciado la máquina virtual, se comprueba la correcta carga del sistema Endian y el estado de sus interfaces. En esta pantalla se verifica que la zona GREEN y la conexión Uplink están habilitadas, además de que se encuentran accesibles las herramientas de gestión requeridas para proseguir con la configuración del firewall.

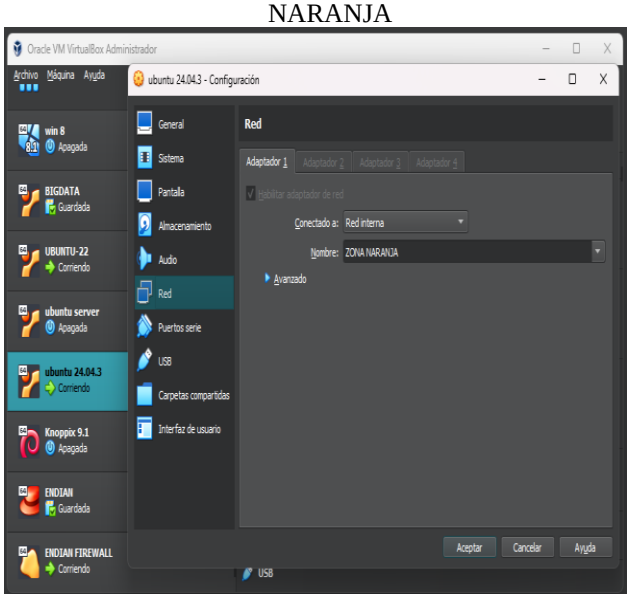
Fig. 20 Estado inicial del sistema Endian tras el arranque.



Fuente: Autoría propia.

En esta disposición, se asigna el adaptador principal de la máquina Ubuntu 24. 04. 3 a la red interna nombrada “ZONA NARANJA”, lo que facilita su integración en el segmento adecuado para las pruebas de control de tráfico utilizando Endian Firewall.

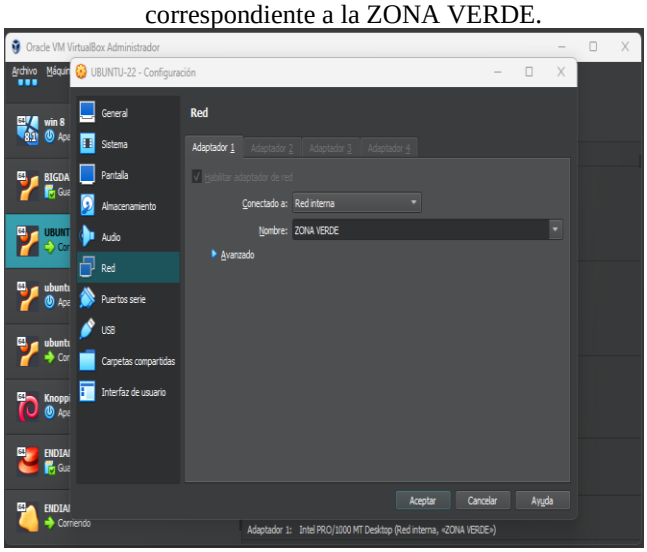
Fig. 21 Ubuntu 24.04.3 – Adaptador conectado a ZONA NARANJA



Fuente: Autoría propia

En esta fase se confirma que la máquina Ubuntu 22 esté conectada a la ZONA VERDE, que representa la parte segura dentro de la estructura establecida para el Firewall Endian. Esta colaboración es esencial para facilitar más tarde la verificación del acceso a los servicios disponibles y la implementación de las normas de tráfico establecidas en esa área.

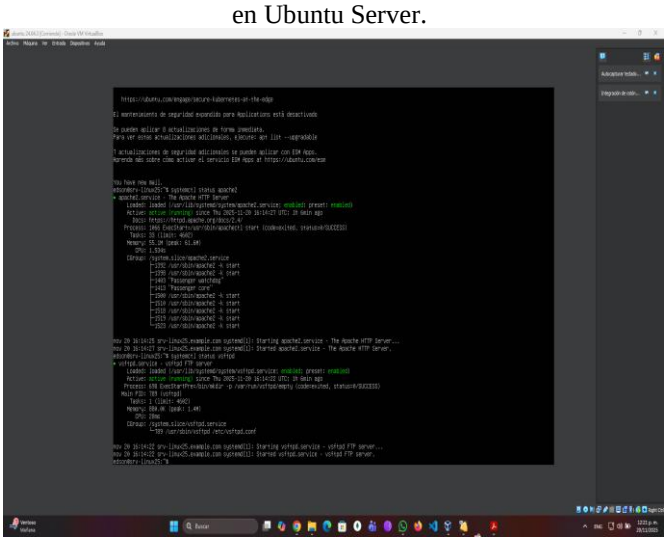
Figura 22. Asignación de Ubuntu 22 a la red interna correspondiente a la ZONA VERDE.



Fuente: Autoría propia

En esta etapa se verifica la operatividad de los servicios Apache2 y VSFTPD en el servidor Ubuntu, garantizando que ambos estén en funcionamiento antes de implementar las normas de gestión de tráfico en Endian Firewall. Esta verificación es esencial para confirmar más adelante la eficacia de las limitaciones y autorizaciones establecidas para las áreas internas.

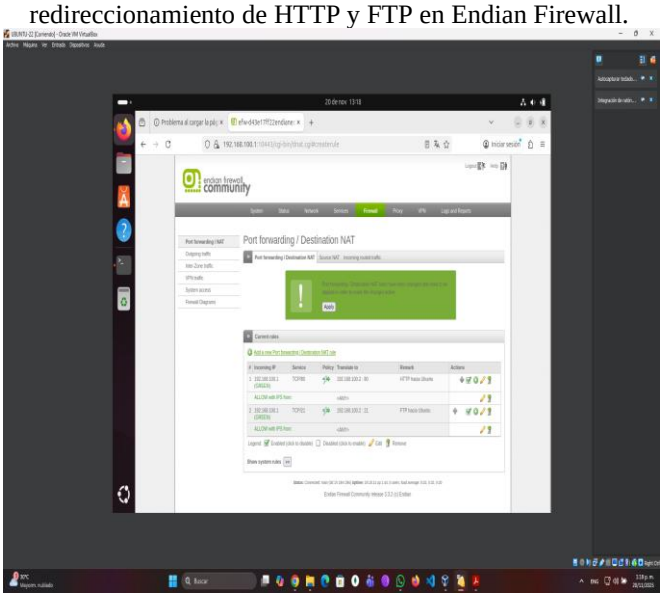
Fig. 23 Verificación del estado de los servicios HTTP y FTP en Ubuntu Server.



Fuente: Autoría propia

La sección de Redirección de Puertos en el cortafuegos Endian permite conectar los servicios proporcionados por el servidor Ubuntu a las zonas internas a través de normas de modificación de direcciones. En esta fase se observan las políticas activas que redirigen el tráfico HTTP y FTP hacia el servidor establecido, lo cual es un paso necesario para analizar el funcionamiento de los servicios una vez que se implementen las limitaciones de acceso estipuladas en la arquitectura de seguridad.

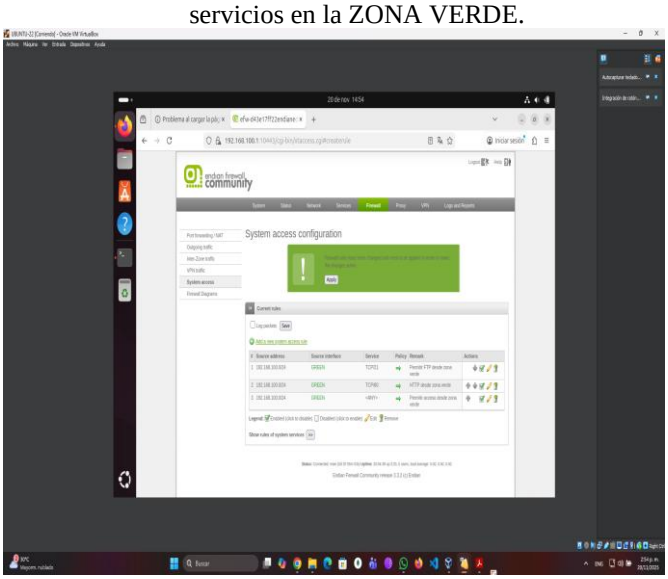
Fig. 24 Configuración de reglas NAT para el redireccionamiento de HTTP y FTP en Endian Firewall.



Fuente: Autoría propia

En la sección de Acceso al Sistema se pueden ver las normas establecidas para permitir el ingreso a los servicios disponibles en el servidor Ubuntu desde la ZONA VERDE. Estas normas añaden a la configuración de NAT que se había establecido anteriormente, facilitando el uso controlado de HTTP y FTP dentro de la zona segura, antes de aplicar la limitación del protocolo ICMP conforme a las necesidades del tema.

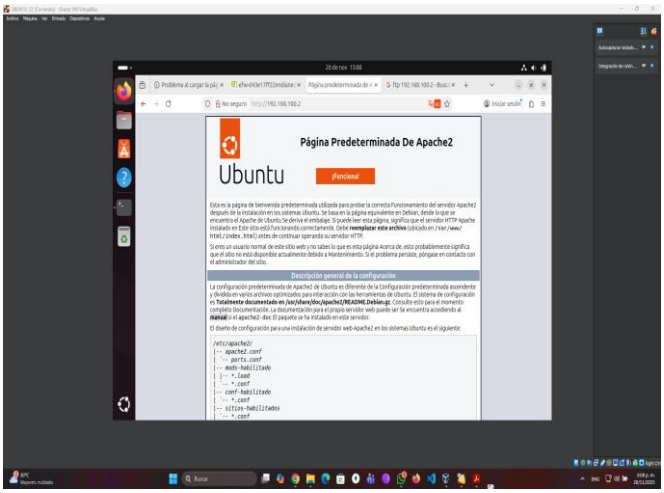
Fig. 25 Reglas de acceso configuradas para permitir servicios en la ZONA VERDE.



Fuente: Autoría propia

En el proceso de verificación de las normas NAT y de acceso establecidas en Endian Firewall, se comprueba el correcto funcionamiento del servicio HTTP accediendo a la página predeterminada de Apache2 desde un dispositivo situado en la ZONA VERDE. La respuesta apropiada del servidor verifica que el tráfico permitido mediante la política TCP/80 se está gestionando sin limitaciones en el segmento autorizado.

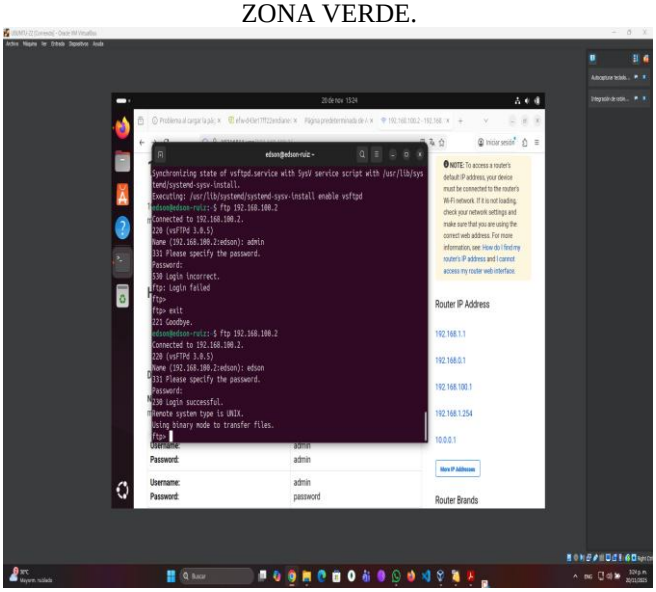
Fig. 26 Comprobación del acceso HTTP al servidor Ubuntu desde la ZONA VERDE.



Fuente: Autoría propia

En esta prueba se examina la conexión FTP hacia el servidor Ubuntu situado en la red interna, asegurando que la política de acceso establecida en Endian Firewall permite la autenticación y el intercambio de datos a través del puerto TCP/21. La conexión exitosa confirma que las reglas establecidas para este servicio están funcionando antes de implementar más limitaciones sobre el tráfico ICMP.

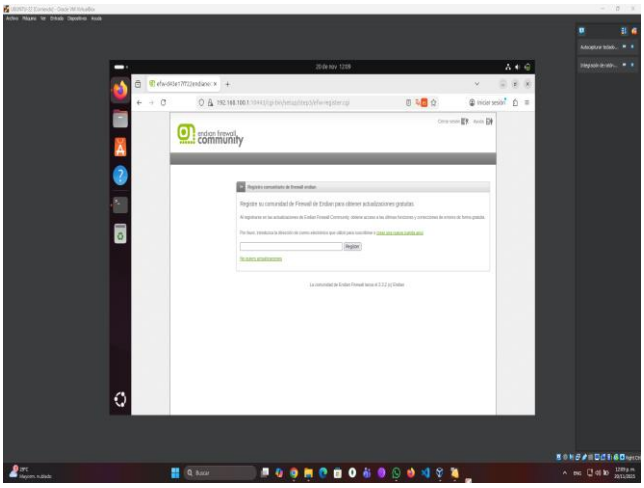
Fig. 27 Verificación del acceso FTP al servidor desde la ZONA VERDE.



Fuente: Autoría propia

La interfaz de gestión en línea de Endian Firewall incluye un panel de registro que tiene como propósito conectar la instalación con la comunidad del proyecto. Si bien este paso no es necesario para que las funciones de red operen, su aparición asegura el acceso correcto a la consola de administración a través de la dirección asignada a la ZONA VERDE, lo que confirma la integración adecuada del firewall en el entorno virtual configurado.

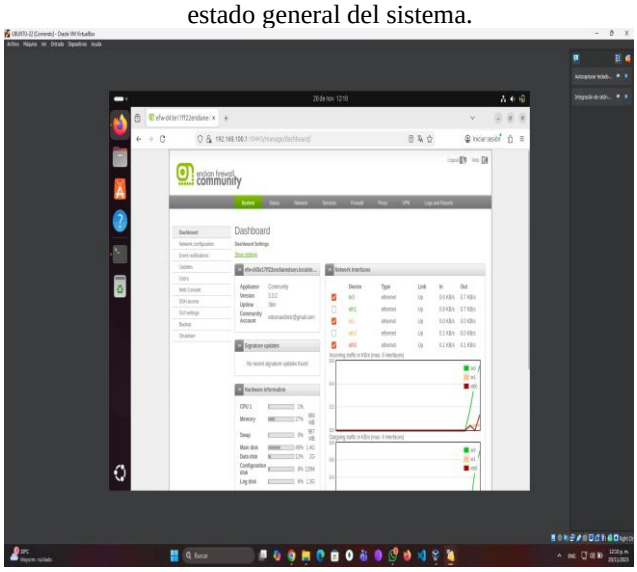
Fig. 28 Interfaz inicial de registro comunitario en la consola web de Endian Firewall.



Fuente: Autoría propia

La visualización del panel de control facilita la verificación del estado de funcionamiento de los diversos elementos de Endian Firewall, abarcando las interfaces de red, el uso de recursos y los servicios internos. Esta revisión asegura que el sistema del firewall está operativo tras implementar las normas de acceso y redireccionamiento, lo cual proporciona un entorno firme para las pruebas de tráfico y limitaciones establecidas en el tema.

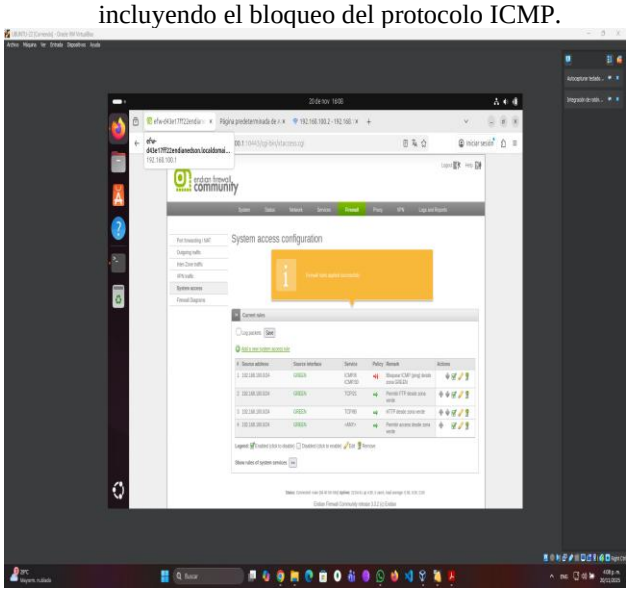
Fig. 29 Panel de control principal de Endian Firewall con el estado general del sistema.



Fuente: Autoría propia

En esta parte se presenta la aplicación definitiva de las reglas de acceso, en la cual se incluye la política diseñada para impedir el tráfico ICMP que proviene de la ZONA VERDE, además de los permisos que ya se habían establecido para HTTP y FTP. La adecuada implementación de estas normativas asegura que el firewall ejecute y active cada política establecida, un requisito esencial para avanzar con la verificación práctica del bloqueo de ping y de la limitación del protocolo ICMP mencionado en el tema.

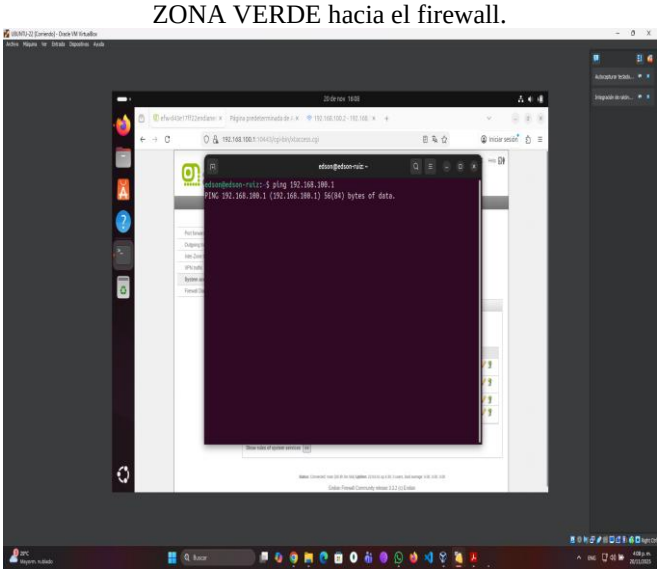
Fig. 30 Aplicación de reglas de acceso en Endian Firewall, incluyendo el bloqueo del protocolo ICMP.



Fuente: Autoría propia

Luego de implementar la norma diseñada para prevenir el tráfico ICMP, se lleva a cabo una solicitud de ping desde un dispositivo en la ZONA VERDE hacia la dirección del cortafuegos. La falta de respuestas indica que la política de rechazo se ha implementado de manera adecuada, demostrando así que el control de tráfico establecido para este asunto funciona de manera efectiva.

Fig. 31 Prueba de bloqueo del protocolo ICMP desde la ZONA VERDE hacia el firewall.



Fuente: Autoría propia

IV. TEMÁTICA 4

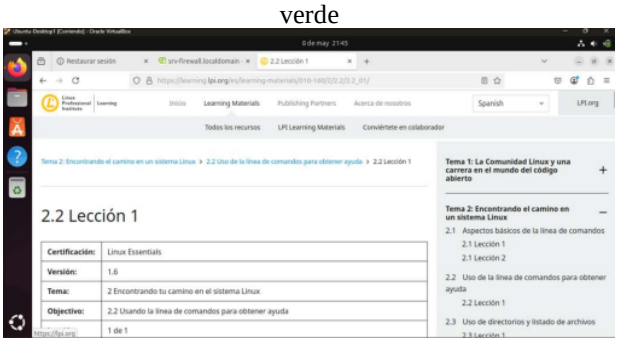
Con el objetivo de establecer una arquitectura de red segura y funcional, se definieron reglas específicas de comunicación entre zonas dentro del entorno de pruebas basado en Endian Firewall. Las reglas se diseñaron conforme a principios de segmentación de red y control de acceso por servicio, permitiendo únicamente el tráfico necesario para los servicios definidos y reduciendo la superficie de ataque. Se definieron las siguientes reglas de acceso en el firewall para cumplir con los requisitos de comunicación:

Comunicación de la Zona Verde a la Zona Naranja: A. Permitir tráfico HTTP (puerto 80) desde la Zona Verde a la Zona Naranja B. Permitir tráfico FTP (puertos 21) desde la Zona Verde a la Zona Naranja Esta configuración permite a los usuarios internos acceder a servidores web y servicios de transferencia de archivos

Fig. 32 Ajustes de acceso a Internet desde la zona roja

Fuente: Autoría propia

Fig. 33 Comprobación de acceso a Internet desde la zona verde



Fuente: Autoría propia

Fig. 34 Verificación de acceso a Internet desde un equipo en la zona naranja

Fuente: Autoría propia

Una vez que se haya establecido correctamente el acceso a Internet desde las áreas Verde (LAN) y Naranja (DMZ), se puede comenzar a ajustar la comunicación interna entre ambas. En este escenario, se facilitará el tráfico únicamente para los servicios HTTP (puerto 80) y FTP (puerto 21). Esta configuración resulta esencial cuando los dispositivos de la LAN requieren conectarse a aplicaciones o servicios que se encuentran en la DMZ, como sitios web internos o servidores para la transferencia de archivos.

Antes de implementar las reglas que permiten la comunicación entre las diferentes zonas, es fundamental asegurarse de que tanto la zona Verde como la Naranja tienen una salida operativa hacia la red externa (zona Roja - WAN). Para verificar esto, se deben revisar los siguientes aspectos:

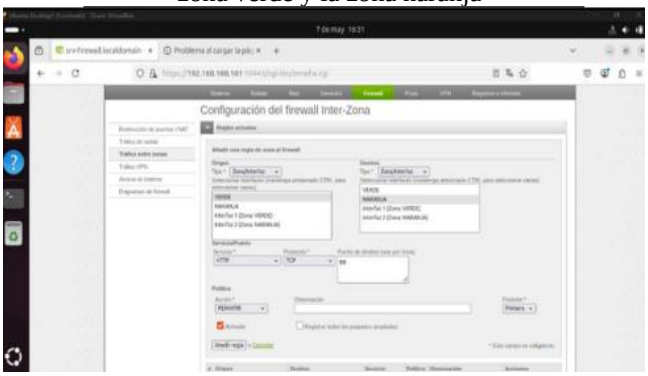
Es necesario confirmar que las reglas que permiten la conexión a Internet desde ambas zonas estén activadas y operativas.

El firewall debe estar aplicando adecuadamente las reglas de NAT para traducir y enrutar el tráfico correctamente.

Desde ambas zonas, se debe poder realizar un ping a direcciones públicas.

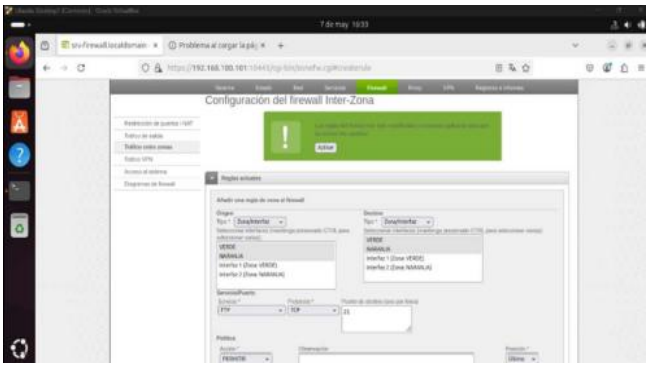
Este proceso garantiza que los dispositivos de la LAN y los de la DMZ no solamente operen en su red interna, sino que también puedan acceder y mantenerse conectados al exterior. E sta capacidad es crucial en contextos donde se integran tanto servicios internos como externos, o
en situaciones que demandan actualizaciones a distancia y comunicación con recursos externos.

Fig. 35 Intercambio de archivos mediante FTP entre la zona verde y la zona naranja



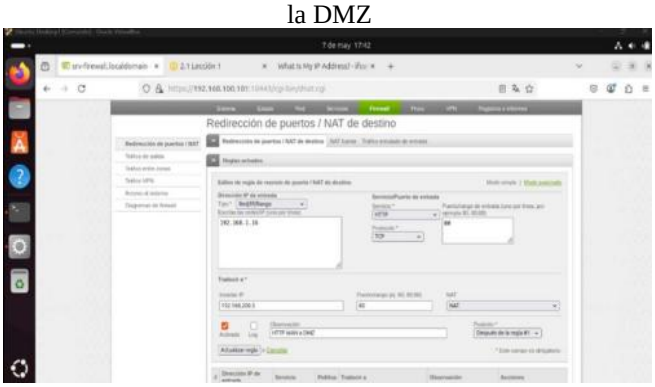
Fuente: Autoría propia

Fig. 36 Intercambio de tráfico HTTP entre la zona roja y la DMZ



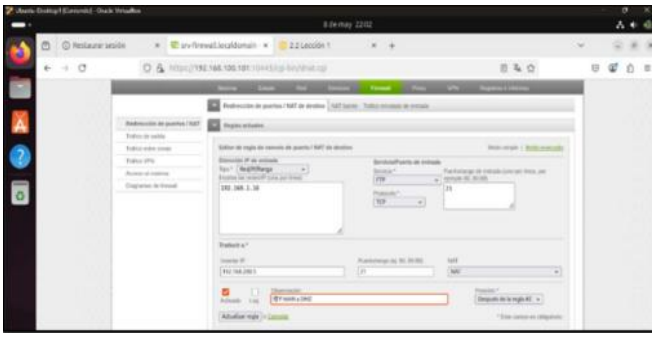
Fuente: Autoría propia

Fig. 37 Transferencia de datos vía FTP entre la zona roja y la DMZ



Fuente: Autoría propia

Fig. 38 Tráfico HTTP establecido entre la zona roja y la DMZ



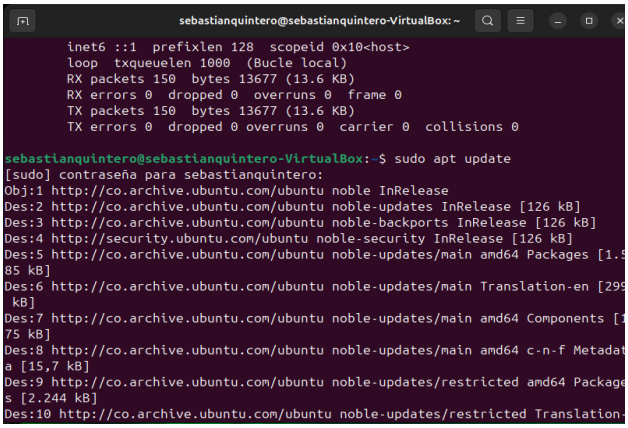
Fuente: Autoría propia

La reenvío de puertos HTTP y FTP desde la zona expuesta (Internet) hacia la DMZ en Endian facilita la publicación de servicios dirigidos al público, como un servidor web o un servidor FTP, sin poner en riesgo la red interna de manera directa.Esta configuración permite que el cortafuegos gestione las conexiones entrantes desde Internet a puertos determinados, como el 80 para HTTP y el 21 para FTP, redirigiéndolas a los servidores ubicados en la DMZ, que actúa como una red intermedia aislada.Este sistema asegura que los servicios disponibles sean accesibles para usuarios externos, al tiempo que se preserva la seguridad de la infraestructura interna y de los recursos más críticos de la organización.

V. TEMÁTICA 5

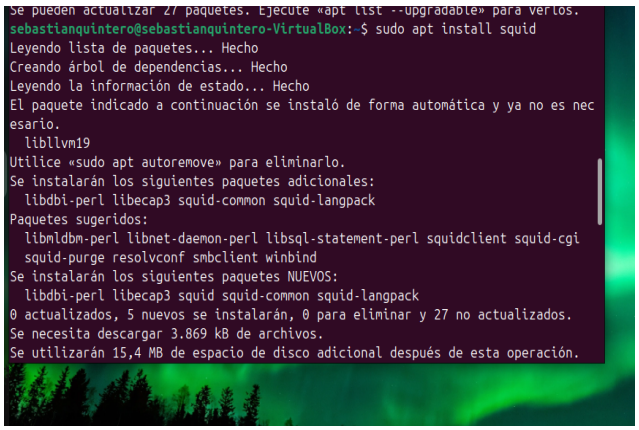
Implementar un Proxy HTTP (No transparente) con políticas de autenticación para navegación en Internet.

Fig. 39 actualiza la base de datos de paquetes, asegurando que tu sistema sepa cuáles son las versiones más recientes disponibles



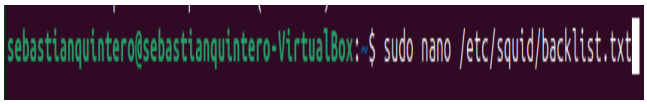
Fuente: Autoría propia

Fig. 40 Con Squid instalado, procedemos a crear la lista negra, en la que se especifican los nombres de las páginas web que se desea bloquear para restringir su acceso desde la red.



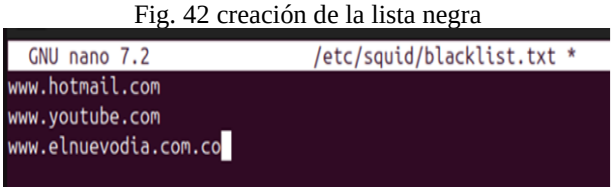
Fuente: Autoría propia

Fig. 41 con este comando creamos el listado de sitios que queremos restringir su acceso directo



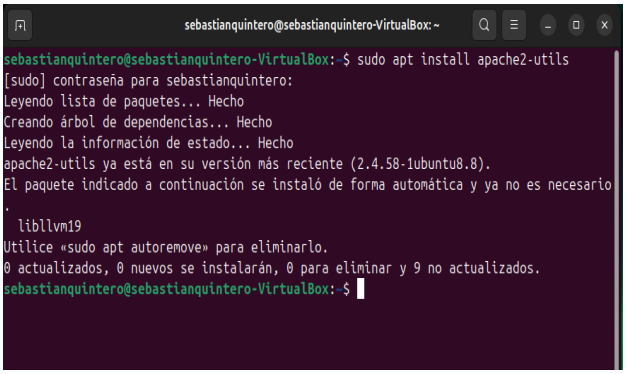
Fuente: Autoría propia

Fig. 42 creación de la lista negra



Fuente: Autoría propia

Fig. 43 El paquete apache2-utils en sistemas basados en Debian (como Ubuntu) contiene varias herramientas útiles para la administración y configuración de servidores Apache.



Fuente: Autoría propia

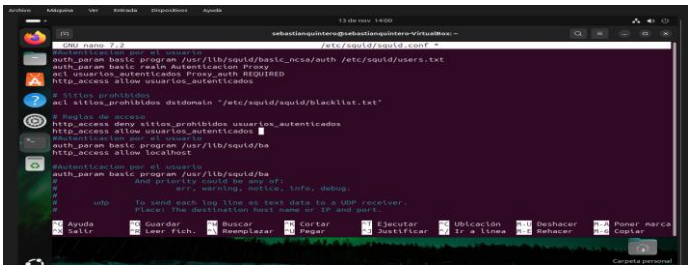
Fig. 44 Se utiliza para crear y actualizar archivos de contraseñas para la autenticación básica HTTP. Este archivo es utilizado para proteger áreas de un servidor web mediante usuario y contraseña.

Fuente: Autoría propia

Fig. 45 Este comando sirve para abrir y editar el archivo principal de configuración de Squid usando el editor nano, con permisos de administrador.

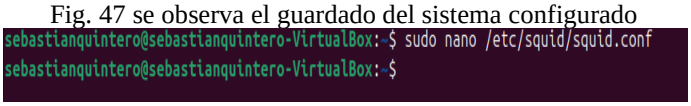
Fuente: Autoría propia

Fig. 46 se configura el squid y se agrega estos comandos dentro de este para que cumpla con la función



Fuente: Autoría propia

Fig. 47 se observa el guardado del sistema configurado

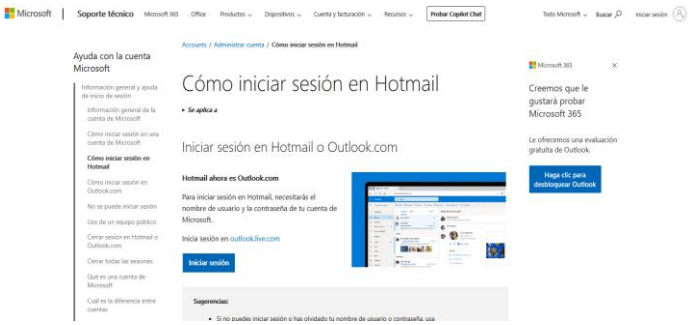


Fuente: Autoría propia

Fig. 48 se efectúa el nombre y contraseña de para poder usar los sitios nombrados en las listas con http

Fuente: Autoría propia

Fig. 49 se inicia correctamente la página de http



Fuente: Autoría propia

VI. CONCLUSIONES

La adopción de Endian Firewall en un entorno virtualizado facilitó la comprensión práctica de cómo se establece una arquitectura de seguridad perimetral fundamentada en la segmentación de red, el control del tráfico y la gestión centralizada de servicios. A través de los cinco temas, se observó que dividir la red en áreas Verde (LAN), Naranja (DMZ) y Roja (WAN) permite implementar políticas distintas, lo que disminuye los riesgos y optimiza la administración del flujo de información.

La adecuada configuración de NAT mostró que tanto la LAN como la DMZ son capaces de comunicarse con el exterior a través del firewall, asegurando un control riguroso sobre los servicios que se autorizan o se impiden. De igual manera, la activación específica de HTTP y FTP, junto con la restricción del protocolo ICMP, permitió comprobar el efecto directo que las normas del cortafuegos tienen en la disponibilidad y seguridad de los servicios internos.

Además, la creación del proxy HTTP con autenticación destacó la relevancia de establecer políticas de control de navegación fundamentadas en los usuarios, lo que permite limitar el acceso a determinados contenidos y supervisar el uso de Internet. Estos mecanismos son fundamentales en contextos académicos y administrativos donde es necesario asegurar un uso responsable y seguro de los recursos.

En resumen, el proyecto demuestra que las herramientas de seguridad que funcionan con GNU/Linux, como Endian Firewall y Squid, proporcionan una solución sólida, modular y flexible para salvaguardar las infraestructuras de red. La experiencia práctica obtenida representa una contribución importante en la educación profesional en administración de sistemas y en ciberseguridad.

VII. REFERENCIAS

[1] Endian. (2025). Endian Firewall Community. https://www.endian.com/en/community/

[2] Ubuntu. (2025). Documentación oficial de Ubuntu Server y Ubuntu Desktop. https://ubuntu.com/server/docs

[3] VirtualBox. (2025). Oracle VM VirtualBox User Manual. Oracle Corporation. https://www.virtualbox.org/manual/

[4] Squid-Cache. (2025). Squid: Optimising Web Delivery. http://www.squid-cache.org/

[5] The Apache Software Foundation. (2025). Apache HTTP Server Documentation. https://httpd.apache.org/docs/

[6] vsftpd Project. (2025). Very Secure FTP Daemon Documentation. https://security.appspot.com/vsftpd.html