Implementación de un Entorno Perimetral Seguro en GNU/Linux Usando Endian Firewall

Fabián Rojas Rivillas
Email: frojasri@unadvirtual.edu.co

Carol Tatiana Baena Hernández
Email: ctbaenah@unadvirtual.edu.co

Deibys Alejandro Cabeza Mendoza
Email: dacabezam@unadvirtual.edu.co

Julian Alzate Gonzalez
Email: jalzateg@unadvirtual.edu.co

Abstract This article presents the implementation of a perimeter security environment based on Endian Firewall (EFW) within a virtualized infrastructure using Oracle VirtualBox. The objective is to establish a secure and segmented network architecture that includes LAN, WAN, and DMZ zones, enabling traffic filtering, NAT configuration, HTTP proxy management, and user authentication. The unified deployment served as the foundation for multiple security-related tasks executed by the research team. This paper describes the installation process, network interface configuration, segmentation design, service publication in the DMZ, inter-zone traffic control using firewall rules, and the implementation of a non-transparent HTTP proxy with authentication. The results validate the correct operation of the configurations and demonstrate the applicability of EFW as a perimeter security solution.

PALABRAS CLAVE: DMZ, Endian Firewall, GNU/Linux, HTTP proxy.

1 INTRODUCCIÓN

La seguridad perimetral constituye uno de los pilares fundamentales en la protección de infraestructuras tecnológicas modernas. En entornos corporativos y académicos, garantizar la integridad, disponibilidad y confidencialidad de los servicios requiere mecanismos robustos capaces de filtrar, controlar y monitorear el tráfico entre redes internas y externas. En este contexto, la distribución Endian Firewall Community Edition (EFW) se presenta como una solución especializada para la implementación de firewalls, servidores proxy y sistemas de segmentación de red en plataformas GNU/Linux.

El presente artículo describe las fases iniciales del proceso de instalación y configuración de EFW en un entorno de virtualización, así como la arquitectura de red utilizada como base para las temáticas desarrolladas por cada integrante del grupo. Estas etapas constituyen el punto de partida necesario para la puesta en marcha de servicios de seguridad avanzados como NAT, filtrado de puertos, listas negras, políticas de autenticación y reglas de acceso interzona.

2 METODOLOGÍA

La implementación se llevó a cabo utilizando Oracle VirtualBox como plataforma de virtualización. Se creó una máquina virtual para alojar Endian Firewall y se configuraron múltiples adaptadores de red para simular las zonas perimetrales requeridas: zona verde (LAN), zona naranja (DMZ) y zona roja (WAN).

El proceso metodológico se dividió en tres etapas principales:

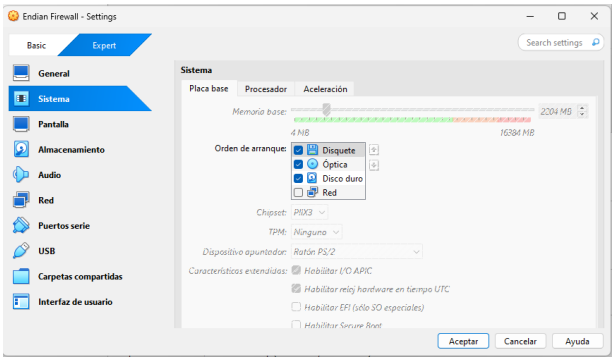
1. Instalación del sistema operativo Endian Firewall.
2. Configuración inicial de interfaces y servicios básicos.
3. Definición de la segmentación de red y asignación de direcciones IP.

Estas fases permiten asegurar un entorno funcional y replicable sobre el cual cada estudiante desarrolla su temática correspondiente.

INSTALACIÓN DE ENDIAN FIREWALL

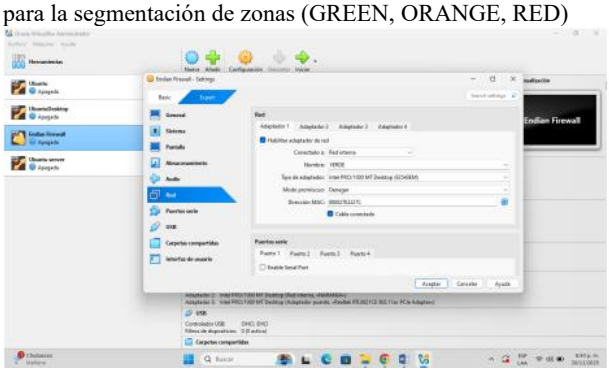
La instalación de Endian Firewall Community Edition (EFW 3.3.2) inicia con la creación de una máquina virtual con un disco virtual de 50 GB, 2 CPU y 2 GB de memoria RAM. Una vez iniciada la imagen ISO, el instalador advierte que el disco `/dev/sda` será particionado y todos los datos existentes se perderán. Tras la confirmación del usuario, el instalador procede a crear las particiones y sistemas de archivos necesarios para el sistema

Figura. 1. Configuración de recursos de hardware (CPU y RAM) para la máquina virtual de Endian Firewall



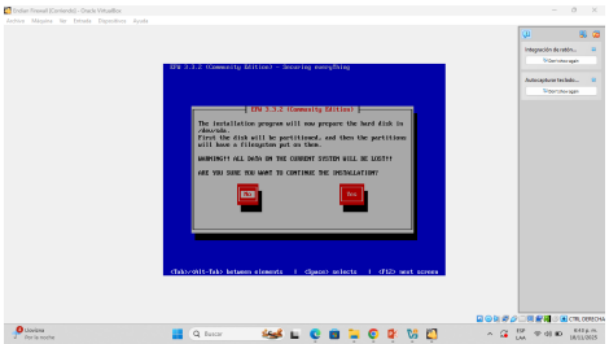
Fuente: Elaboración propia

Figura. 2. Asignación de adaptadores de red en VirtualBox para la segmentación de zonas (GREEN, ORANGE, RED)



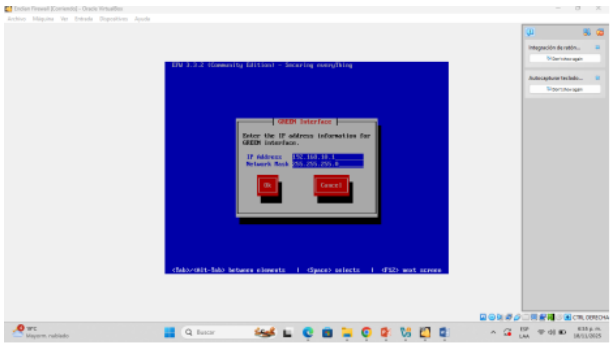
Fuente: Elaboración propia

Figura. 3. Advertencia de particionado de disco durante la fase de instalación del sistema operativo.



Fuente: Elaboración propia

Figura. 4. Configuración inicial de la dirección IP para la interfaz de gestión LAN (Zona VERDE).



Fuente: Elaboración propia

Finalizado el proceso, el asistente solicita la configuración de la interfaz GREEN, asignándole:

- **IP:** 192.168.10.1
- **Máscara:** 255.255.255.0

Completada la configuración básica, el sistema muestra un mensaje de instalación exitosa junto con las direcciones URL de acceso al panel web administrativo:

- `http://192.168.10.1`
- `https://192.168.10.1:10443`

Tras el primer reinicio, la máquina muestra el menú de administración por consola, confirmando que la interfaz GREEN está activa con la dirección configurada.

CONFIGURACIÓN DE LAS INTERFACES DE RED

Para simular correctamente las zonas de seguridad, se configuraron tres adaptadores de red en la máquina virtual de Endian Firewall:

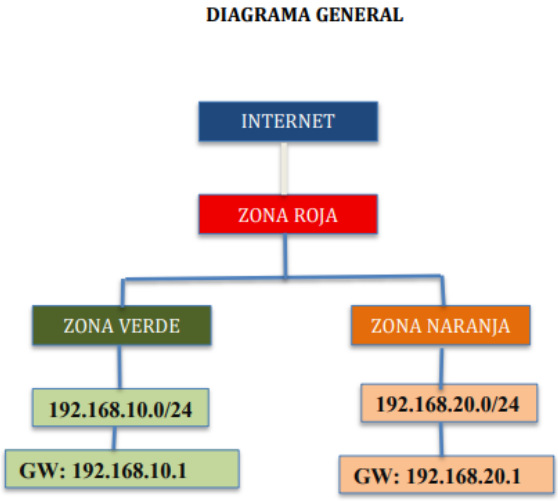
- **Adaptador 1 – GREEN (VERDE):** Red interna para la LAN.
- **Adaptador 2 – ORANGE (NARANJA):** Red interna para la DMZ.
- **Adaptador 3 – RED (WAN):** Conectado a NAT o Bridge para simular Internet.

Cada una de estas interfaces se enlaza posteriormente desde el asistente web, permitiendo asignar nombres, tipos de zonas y direcciones IP para cada segmento de red.

ARQUITECTURA Y SEGMENTACIÓN DE RED

El entorno perimetral se diseñó bajo un esquema de tres zonas, ampliamente utilizado en infraestructuras de seguridad:

Figura 4. *Diagrama general de segmentación de red por zonas (GREEN, RED y ORANGE)*



Nota. Diagrama que representa la arquitectura general de red con segmentación por zonas: RED (Internet/WAN), GREEN (LAN 192.168.10.0/24; GW 192.168.10.1) y ORANGE (DMZ 192.168.20.0/24; GW 192.168.20.1). Referencia: Endian Firewall (segmentación por zonas). Fuente: Elaboración propia.

Descripción de cada zona:

- **Zona Roja (RED):**
  Punto de entrada y salida hacia Internet. No confiable.
- **Zona Verde (GREEN):**
  Red interna, confiable, utilizada por estaciones de trabajo.
- **Zona Naranja (ORANGE / DMZ):**
  Segmento donde se ubican servidores accesibles desde la LAN o WAN, como servidores web o FTP.

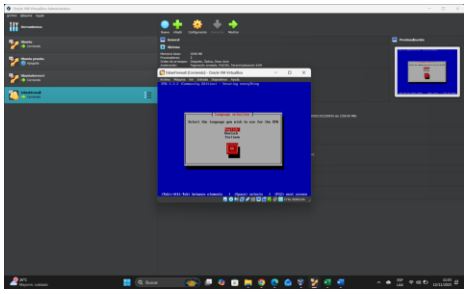
Esta segmentación permite aislar servicios críticos, minimizar el impacto ante intrusiones y aplicar reglas específicas de control de tráfico entre zonas.

3 IMPLEMENTACIÓN Y RESULTADOS

Esta temática se orienta a la instalación y configuración básica de un firewall perimetral GNU/Linux Edian (EFW) en un entorno virtualizado con Oracle VM Virtualbox, con el fin de implementar las tres zonas fundamentales de seguridad: GREEN (LAN internet), RED (acceso a internet/WAN) Y ORANGE (DMZ para servidores). Esta actividad responde a la necesidad de proteger los servidores y bases de datos de la organización mediante una arquitectura de red segmentada, en la que firewall actúa como punto de control y filtre entre la internet, extranet y la zona de servidores.

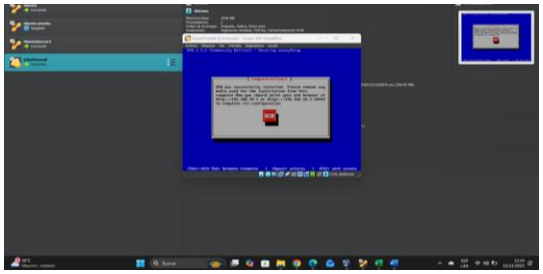
La Temática 1 se orienta a la instalación y configuración básica de un firewall perimetral GNU/Linux Endian (EFW) en un entorno virtualizado con Oracle VM VirtualBox, con el fin de implementar las tres zonas fundamentales de seguridad: GREEN (LAN interna), RED (acceso a Internet/WAN) y ORANGE (DMZ para servidores). Esta actividad responde a la necesidad de proteger los servidores y bases de datos de la organización mediante una arquitectura de red segmentada, en la que el firewall actúa como punto de control y filtro entre la intranet, la extranet y la zona de servidores.

Figura 5. *Ejecución del instalador de Endian Firewall en Oracle VM VirtualBox*



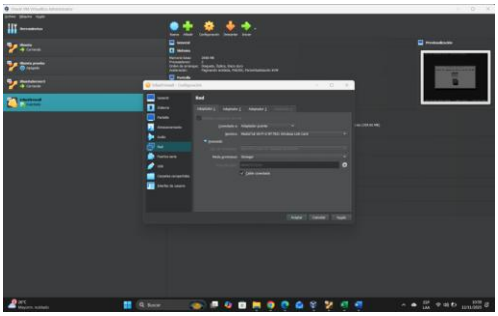
Nota. Captura de pantalla del entorno Oracle VM VirtualBox durante la ejecución del instalador de Endian Firewall. **Fuente:** Elaboración propia

Figura 6.*. Mensaje de advertencia durante la instalación de Endian Firewall en Oracle VM VirtualBox*



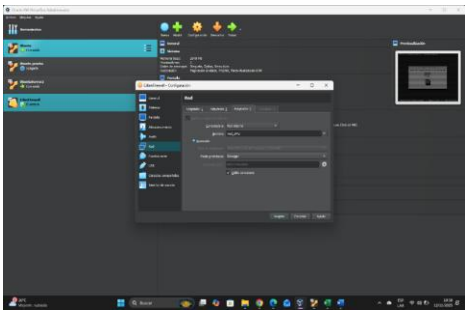
Nota. Captura de pantalla del instalador de Endian Firewall mostrando un mensaje de advertencia dentro de la máquina virtual ejecutada en Oracle VM VirtualBox. **Referencia:** Endian Firewall; Oracle VM VirtualBox. **Fuente:** Elaboración propia

Figura 7. *Configuración de red de la máquina virtual Endian Firewall en Oracle VM VirtualBox*



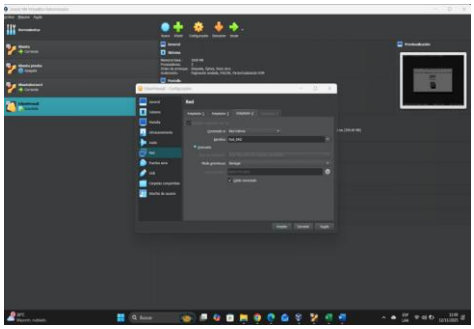
Nota. **Captura de pantalla de la sección Red en la configuración de la máquina virtual, donde se ajustan parámetros del adaptador de red para Endian Firewall en Oracle VM VirtualBox. Referencia: Oracle VM VirtualBox; Endian Firewall. Fuente: Elaboración propia**

Figura 8. *Parámetros del adaptador de red de la máquina virtual Endian Firewall en Oracle VM VirtualBox*



Nota. **Captura de pantalla de la sección Red en Oracle VM VirtualBox, donde se observan las opciones de configuración del adaptador de red asignado a la máquina virtual Endian Firewall (modo de conexión y nombre del adaptador). Referencia: Oracle VM VirtualBox; Endian Firewall. Fuente: Elaboración propia.**

Figura 9. *Configuración del Adaptador 1 de red en la máquina virtual Endian Firewall en Oracle VM VirtualBox*

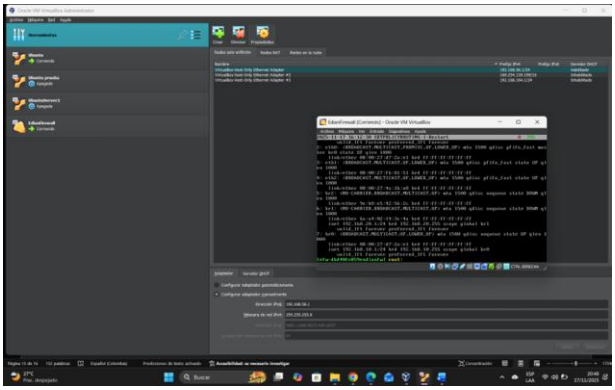


Nota. Captura de pantalla de la sección ***Red (Adaptador 1)*** *en Oracle VM VirtualBox, donde se configura el adaptador de red asignado a la máquina virtual* ***Endian Firewall*** *(habilitación del adaptador, modo de conexión y estado del cable).* ***Referencia:*** *Oracle VM VirtualBox; Endian Firewall.* ***Fuente:*** *Elaboración propia*

Posteriormente, se procedió a la configuración de las tarjetas de red de la máquina Endian en VirtualBox, asignando a cada adaptador el rol correspondiente a cada zona: un adaptador para la zona RED (WAN), conectado hacia el exterior; un segundo adaptador para la zona GREEN (LAN interna), configurado como red interna o host-only; y un tercer adaptador para la zona ORANGE (DMZ), destinado a futuros servidores bajo GNU/Linux. Esta definición de interfaces permitió reflejar de forma práctica el modelo de segmentación de la red que se busca implementar en la solución de seguridad perimetral.

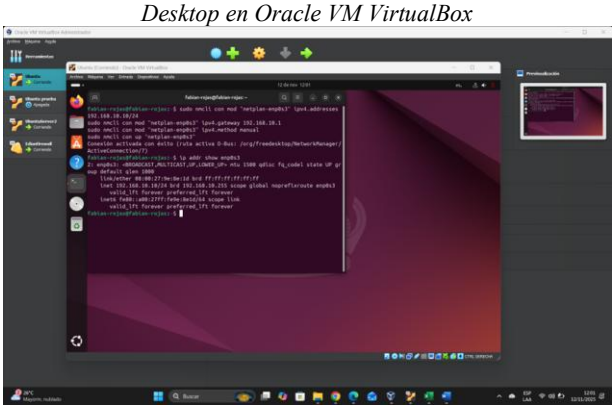
Una vez instaladas las interfaces en Endian, se configuraron las direcciones IP de cada zona. En particular, para la zona GREEN se asignó al firewall la dirección 192.168.10.1, mientras que al equipo cliente Ubuntu Desktop se le asignó la dirección 192.168.10.10/24 sobre la interfaz de red correspondiente. Esta configuración se verificó mediante los comandos de red habituales, comprobando que ambos equipos compartían correctamente el mismo segmento de red y que el firewall quedaba definido como puerta de enlace de la LAN interna.

Figura 10 .*Prueba de conectividad (ping) desde Endian Firewall en Oracle VM VirtualBox*



Nota. **Captura de pantalla de la consola de Endian Firewall ejecutándose en una máquina virtual, donde se realiza un comando ping para verificar la conectividad de red con otro equipo de la topología. Referencia: Oracle VM VirtualBox; Endian Firewall. Fuente: Elaboración propia**

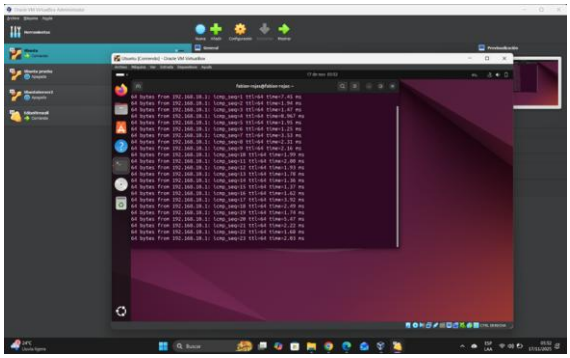
Figura 11. *Verificación de la configuración de red en Ubuntu Desktop en Oracle VM VirtualBox*



Nota. Captura de pantalla de la terminal de **Ubuntu Desktop** ejecutándose en Oracle VM VirtualBox, donde se utiliza el comando ip a para verificar la interfaz de red (por ejemplo, enp0s3), su dirección IP asignada y el estado de conectividad. **Referencia:** Ubuntu Desktop; Oracle VM VirtualBox. **Fuente:** Elaboración propia

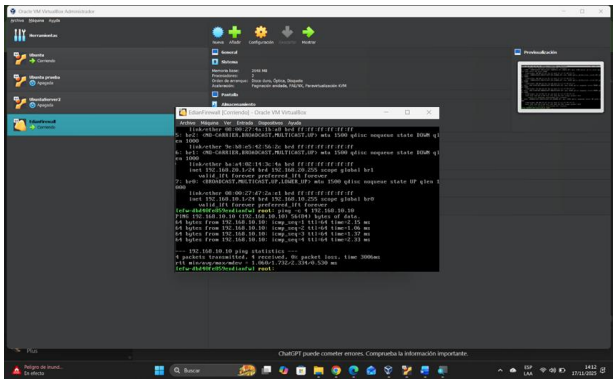
A continuación, se realizaron pruebas de conectividad para validar el correcto funcionamiento de la infraestructura. Desde Ubuntu Desktop se ejecutó un ping a la dirección IP 192.168.10.1 del firewall, obteniendo respuestas satisfactorias que demostraron que la zona GREEN estaba operativa y que el tráfico llegaba hasta Endian. De forma complementaria, desde la consola de Endian se ejecutó un ping hacia la dirección 192.168.10.10 de Ubuntu, verificando así la comunicación bidireccional entre el firewall y el cliente. Estas evidencias consolidan que la topología planteada es funcional y que Endian desempeña efectivamente el rol de gateway de la red interna.

Figura 12. *Prueba de conectividad (ping) desde Ubuntu Desktop en Oracle VM VirtualBox*



Nota. Captura de pantalla de la terminal de Ubuntu Desktop en Oracle VM VirtualBox, donde se ejecuta el comando ping para comprobar la conectividad con el equipo Endian Firewall (respuestas “64 bytes from …” con tiempos de latencia). Referencia: Ubuntu Desktop; Oracle VM VirtualBox. Fuente: Elaboración propia

Figura 13 .*Resultados de prueba de conectividad en Endian Firewall en Oracle VM VirtualBox*



Nota. Captura de pantalla de la consola de **Endian Firewall** ejecutándose en Oracle VM VirtualBox, donde se evidencian comandos y resultados de verificación de conectividad de red (por ejemplo, **ping** y estadísticas de paquetes). **Referencia:** Endian Firewall; Oracle VM VirtualBox. **Fuente:** Elaboración propia.

Durante todo el proceso se registraron capturas de pantalla de la configuración de las zonas RED, GREEN y ORANGE, de la asignación de direcciones IP y de las pruebas de ping, las cuales fueron organizadas y rotuladas como figuras siguiendo las normas APA (título y nota explicativa). Este registro visual no solo deja evidencia del trabajo realizado, sino

que también facilita la comprensión del procedimiento para futuras referencias, auditorías o ampliación del proyecto hacia temáticas más avanzadas como NAT, publicación de servicios en la DMZ y definición de políticas de filtrado.

En síntesis, la Temática 1 permitió pasar de la teoría de la arquitectura de sistemas Linux y de los conceptos de firewall perimetral, a una implementación práctica concreta sobre VirtualBox con Endian Firewall. El resultado es una infraestructura básica pero funcional, que establece las bases para continuar con la configuración de reglas de seguridad, traducción de direcciones y exposición controlada de servicios en la DMZ, manteniendo protegida la red interna y sus recursos críticos.

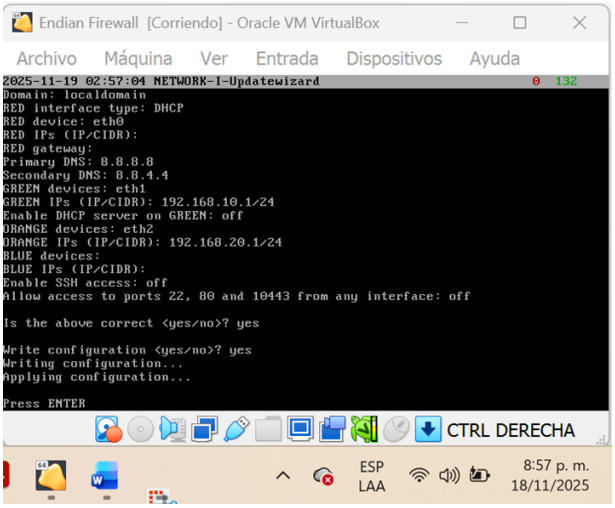
PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

Se describen los procedimientos realizados para configurar los servicios en la zona DMZ mediante el firewall Endian, con el fin de controlar y asegurar el acceso a los recursos publicados. Se habilitan los servicios HTTP (puerto 80) y FTP (puerto 21) desde un servidor Ubuntu Server, y se implementa el bloqueo del protocolo ICMP para impedir respuestas al comando *ping*. Finalmente, se verifica el funcionamiento de las reglas creadas mediante pruebas y capturas de pantalla.

Este proceso permite establecer una separación clara entre la red interna y los servicios expuestos, garantizando que solo el tráfico autorizado llegue al servidor en la DMZ. Además, refuerza la seguridad al limitar la información que los dispositivos pueden obtener mediante ICMP y al asegurar que los servicios publicados estén controlados por reglas específicas del firewall, reduciendo riesgos y mejorando la administración del acceso.

Primero se configuró el firewall Endian, encargado de administrar y controlar el tráfico entre la red interna y la DMZ. Desde esta máquina se gestionan las reglas de seguridad y la publicación de los servicios.

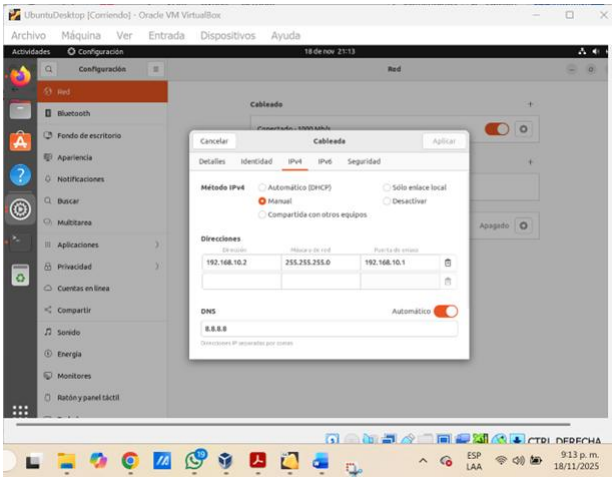
Figura 14. *Configuración del firewall Endian*



Fuente: Elaboración propia

Luego se configuró la máquina Desktop, que actúa como cliente dentro de la red interna. A esta máquina se le asignó manualmente su red desde Ubuntu Desktop, definiendo su dirección, máscara y puerta de enlace para permitir las pruebas de conectividad y acceso a los servicios.

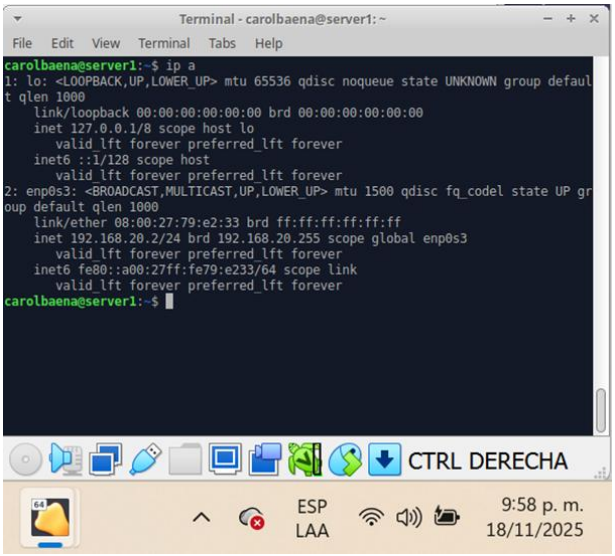
Figura 15. *Configuración del cliente Desktop dentro de la red interna.*



Fuente: Elaboración propia

Finalmente se configuró el servidor Ubuntu, ubicado en la zona DMZ. Del mismo modo, a este servidor se le asignó manualmente su configuración de red, necesaria para ejecutar los servicios publicados (HTTP y FTP) que serán gestionados por el firewall.

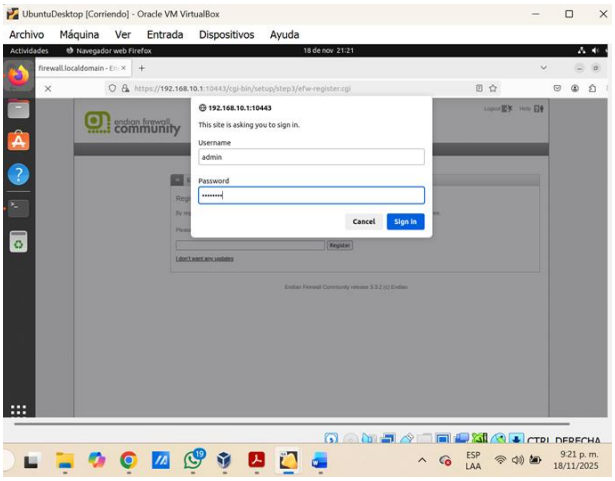
Figura 16. *Asignación manual de parámetros de red en el servidor Ubuntu.*



Fuente: Elaboración propia

Para continuar la configuración, se accede a la interfaz web de Endian Firewall desde la máquina Desktop mediante la dirección https://192.168.10.1:10443, verificando el acceso al panel principal

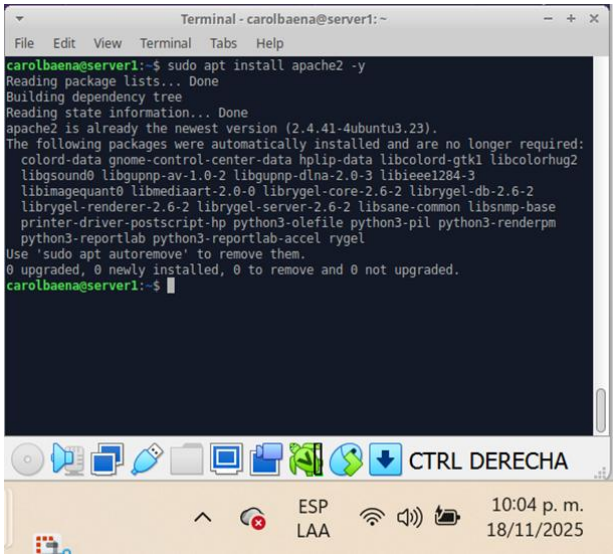
Figura 17. *Verificación del acceso al panel principal de Endian Firewall.*



Fuente: Elaboración propia

En el servidor Ubuntu se instaló Apache desde la terminal utilizando el comando de instalación correspondiente.

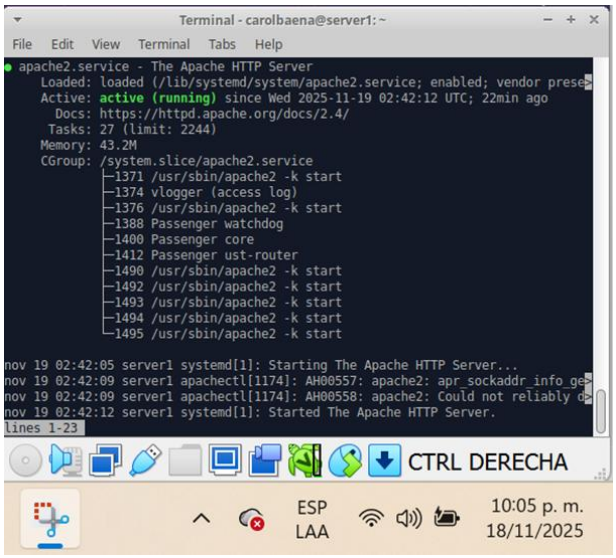
Figura 18. *Instalación de Apache en servidor Ubuntu*



Fuente: Elaboración propia

Luego, se verificó que el servicio estuviera activo y en ejecución mediante el estado del servicio, confirmando que el servidor web estaba funcionando correctamente.

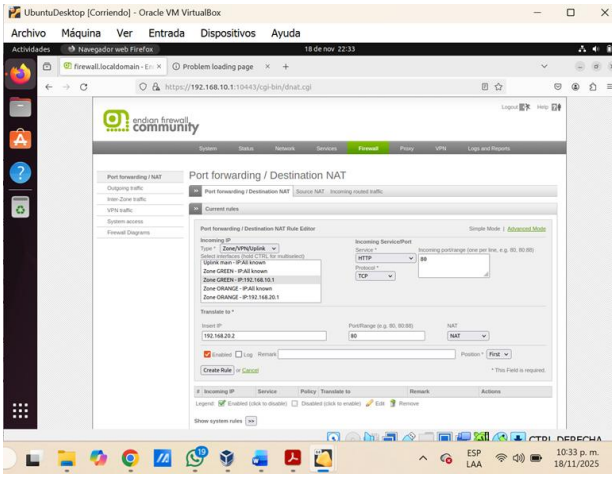
Figura 19. *Estado del servicio Apache en ejecución*



Fuente: Elaboración propia

Se procede a permitir el servicio HTTP creando una regla de port forwarding que redirige el puerto 80 hacia la IP del servidor Ubuntu ubicado en la DMZ.

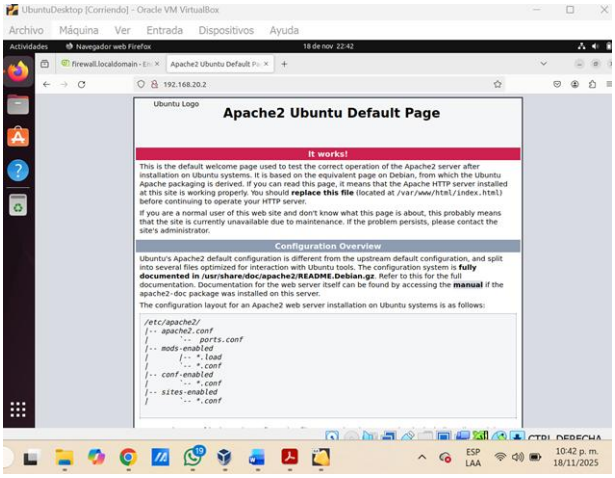
Figura 20. *Configuración de port forwarding para HTTP*



Fuente: Elaboración propia

Se prueba el acceso al sitio web desde un cliente interno para confirmar su funcionamiento.

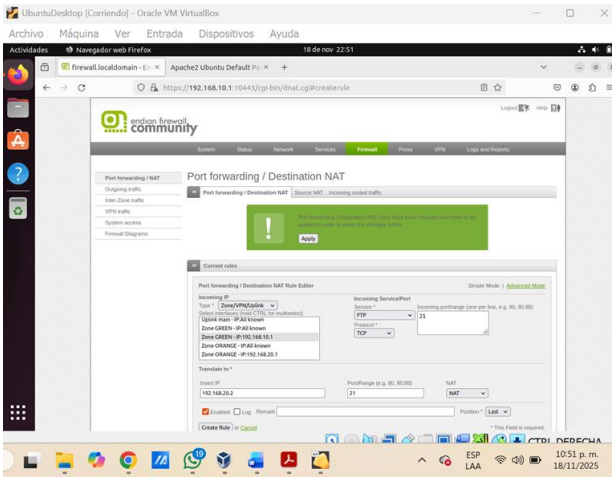
Figura 21. *Validación del funcionamiento del sitio web*



Fuente: Elaboración propia

Se habilita el servicio FTP mediante una nueva regla de port forwarding que redirige el puerto 21 hacia el mismo servidor en la DMZ.

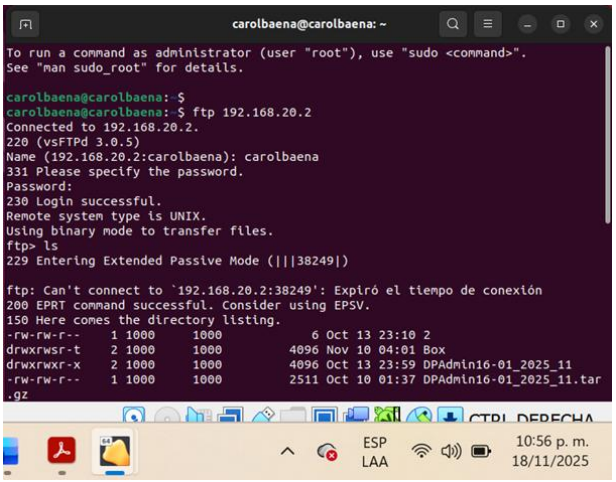
Figura 22. *Habilitación del servicio FTP*



Fuente: Elaboración propia

Se valida conectándose al servicio FTP desde la red interna.

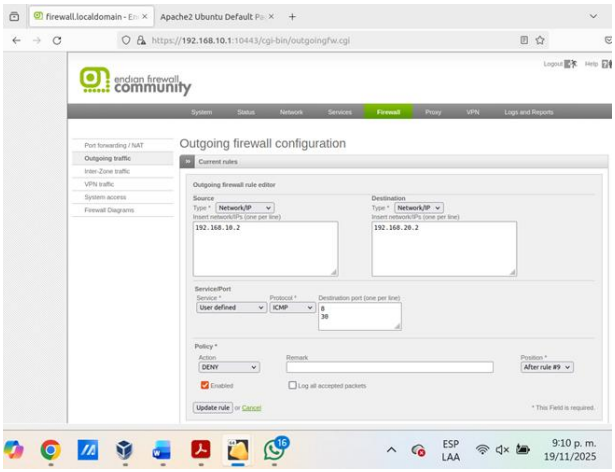
Figura 23. *Prueba de conexión al servicio FTP*



Fuente: Elaboración propia

Posteriormente, se bloquea el protocolo ICMP creando reglas de filtrado que descartan las solicitudes de eco, lo cual impide obtener respuestas al comando ping.

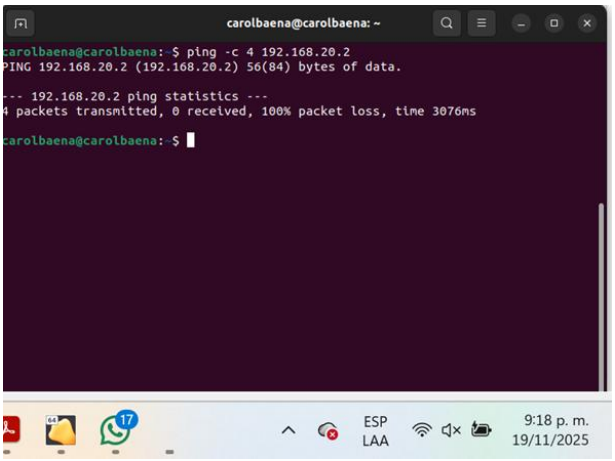
Figura 24. *Bloqueo para tráfico ICMP*



Fuente: Elaboración propia

Las pruebas realizadas desde la Desktop muestran pérdida total de paquetes, confirmando el bloqueo.

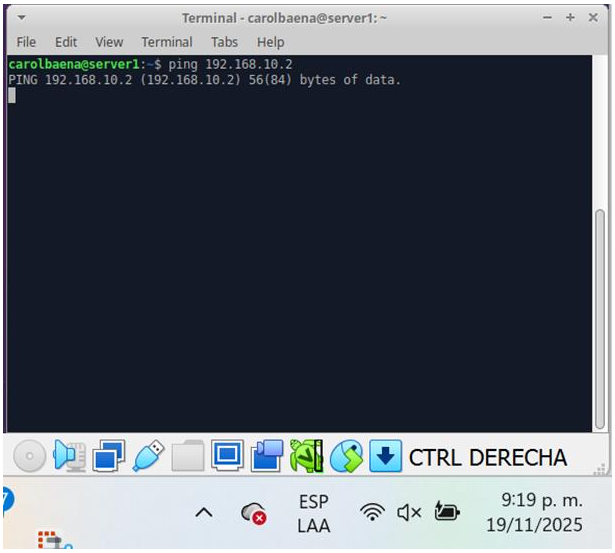
Figura 25. *Verificación del bloqueo de ICMP desde la estación de trabajo*



Fuente: Elaboración propia

La prueba se ejecutó igualmente desde el servidor; sin embargo, no se obtuvo ninguna respuesta.

Figura 26. *Verificación del bloqueo de ICMP en el servidor*

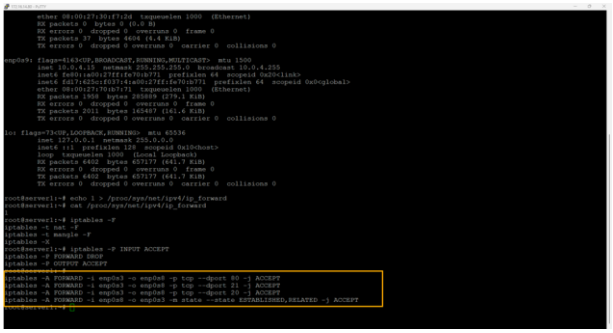


Fuente: Elaboración propia

Reglas de acceso para permitir o denegar el tráfico. Producto esperado

1. Comunicar la zona Verde con la zona Naranja con el protocolo HTTP y FTP con sus respectivos puertos.
Con estas directivas de iptables comunicamos las interfaces

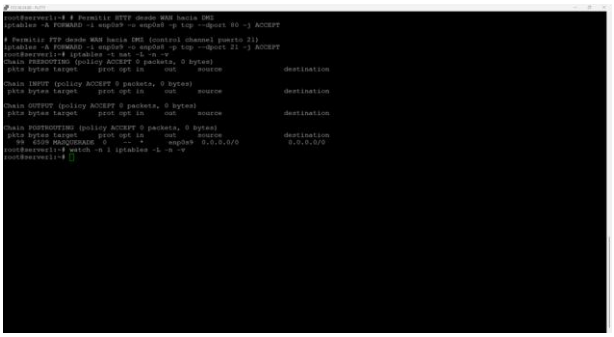
Figura 27. Comunicar la zona Verde con la zona Naranja con el protocolo HTTP y FTP con sus respectivos puertos.



Fuente: Elaboración propia

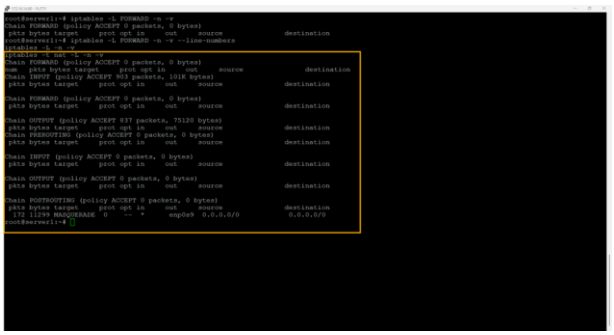
Figura 28. Comunicar la zona Internet con la zona DMZ.

Consiste en permitir que usuarios externos accedan únicamente a los servicios autorizados que se encuentran en la DMZ, como HTTP o FTP. Esto se realiza mediante reglas de firewall que controlan qué puertos y protocolos pueden pasar.



Fuente: Elaboración propia

Figura 29. Verificar en el tráfico Inter - Zona, la creación de las reglas.



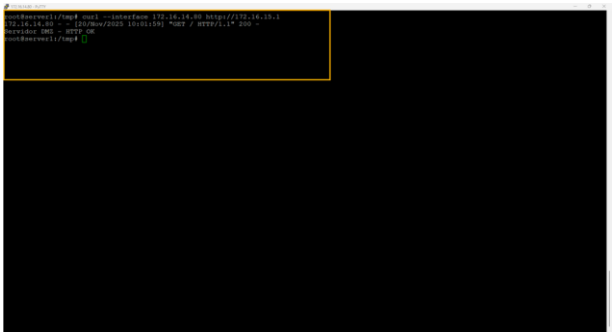
Fuente: Elaboración propia

Figura 30. Probar desde un navegador Web, las siguientes directivas

Probar desde un navegador web estas directivas consiste en verificar que las reglas del firewall funcionan correctamente permitiendo acceso HTTP según cada caso. Desde la LAN, se prueba que los usuarios puedan ingresar al servidor web ubicado en la DMZ, y también que puedan acceder a servicios web en la WAN (Internet). Estas pruebas confirman que el tráfico autorizado fluye de manera correcta entre cada zona y que la configuración de seguridad es efectiva.

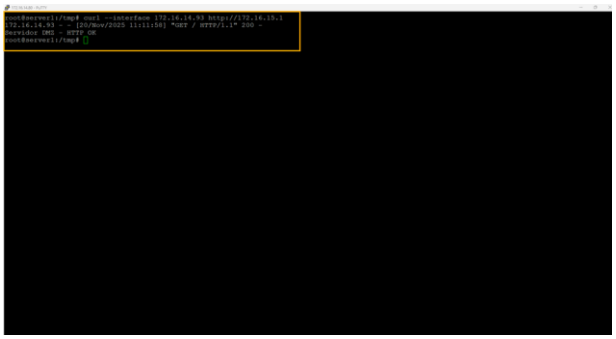
El ingreso del servicio HTTP desde la LAN hacia la zona DMZ. El ingreso del servicio HTTP desde la LAN hacia la WAN.

Figura 31. El ingreso del servicio HTTP desde la zona DMZ hacia la WAN.



Fuente: Elaboración propia

Figura 32. El ingreso del servicio HTTP desde la WAN hacia la zona DMZ.



Fuente: Elaboración propia

Figura 33. El ingreso del servicio FTP desde la LAN hacia la WAN. Con esto validamos el tráfico de ftp

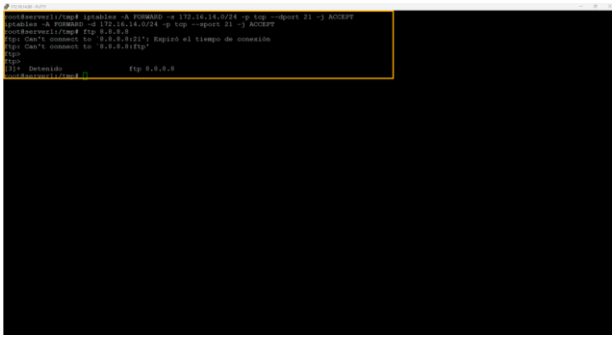
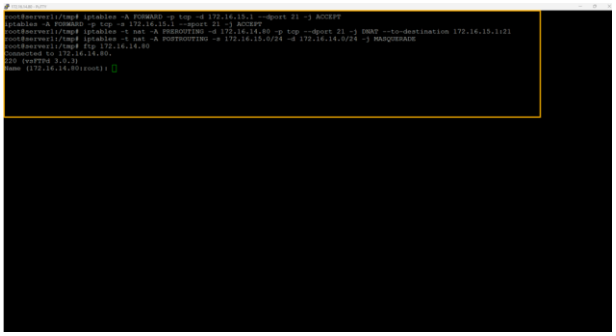


Figura 34. El ingreso del servicio FTP desde la WAN hacia la zona DMZ.



Fuente: Elaboración propia

PROXY HTTP NO TRANSPARENTE CON AUTENTICACIÓN

La implementación del Proxy HTTP no transparente en Endian Firewall permite controlar la navegación web mediante políticas de filtrado, autenticación y listas de control. Este módulo constituye un componente fundamental en la seguridad perimetral, dado que permite monitorear y restringir el tráfico HTTP y HTTPS que atraviesa la red interna hacia Internet.

En esta sección se detalla el procedimiento técnico realizado para habilitar el proxy, configurar perfiles de filtrado, activar la autenticación de usuarios y establecer una lista negra de sitios web, siguiendo estrictamente los lineamientos de la guía de aprendizaje.

Activación del Proxy HTTP No Transparente

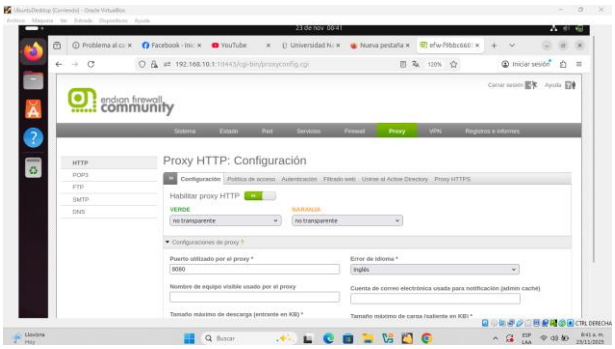
El proceso inició accediendo al panel web administrativo mediante la URL segura:

https://192.168.10.1:10443

Dentro del menú Proxy HTTP, se habilitó el servicio seleccionando el modo No Transparente, lo que implica que los clientes deben configurar manualmente el uso del proxy en su navegador o sistema operativo. Esta configuración se aplicó para las zonas GREEN y ORANGE, estableciendo el puerto por defecto:

Puerto del proxy: 8080

Figura. 35. Panel de configuración del Proxy HTTP en modo no transparente sobre el puerto 8080.



Fuente: Elaboración propia

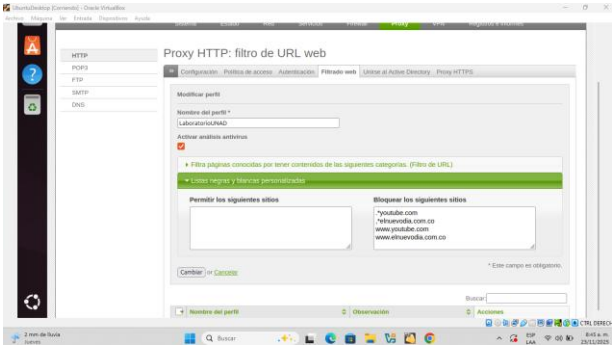
Esta habilitación garantiza que el tráfico web pase obligatoriamente por el filtro de seguridad, permitiendo aplicar políticas de control sobre los usuarios y destinos.

Configuración del Filtro Web y Perfil de Seguridad

Endian permite la creación de perfiles personalizados para gestionar el acceso a contenidos web. Para este trabajo se creó el perfil:

Nombre del perfil: LaboratorioUNAD

Fig. 36. Creación del perfil de filtrado "LaboratorioUNAD" y definición de lista negra de dominios.



Fuente: Elaboración propia

Dentro del perfil se configuraron los siguientes parámetros:

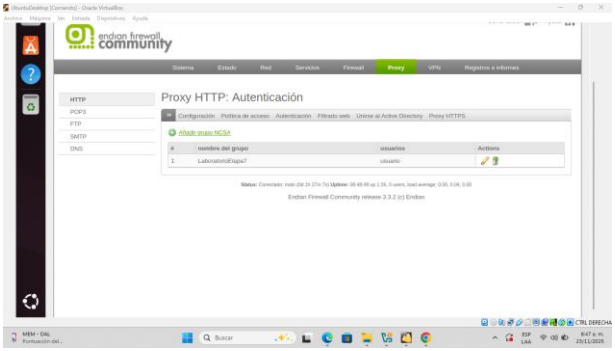
1. Activación de análisis antivirus, permitiendo detectar contenido malicioso en descargas.
2. Frecuencia de actualización del filtro, establecida de manera mensual.
3. Lista negra personalizada, donde se añadieron los siguientes sitios a bloquear:
    - www.youtube.com
    - www.elnuevodia.com.co

Estos sitios cumplen con el requisito de la guía y representan portales frecuentemente bloqueados en entornos laborales o académicos para evitar pérdida de tiempo o riesgos de seguridad.

Implementación de la Autenticación por Usuario

El proxy fue configurado para exigir autenticación a los usuarios antes de permitir el acceso. Para ello, se utilizó el sistema NCSA (National Center for Supercomputing Applications), que permite crear usuarios locales almacenados en el firewall.

Fig. 37. Configuración de grupos y usuarios (NCSA) para la autenticación en el proxy.



Fuente: Elaboración propia

Se crearon:

- Grupo: LaboratorioEtapa7
- Usuario asociado: credencial configurada para acceso mediante proxy

El usuario creado se vinculó al perfil del proxy previamente configurado, garantizando que únicamente quienes posean credenciales autorizadas puedan acceder a Internet.

Esta medida fortalece la seguridad al proporcionar trazabilidad y evitar navegación anónima desde la red.

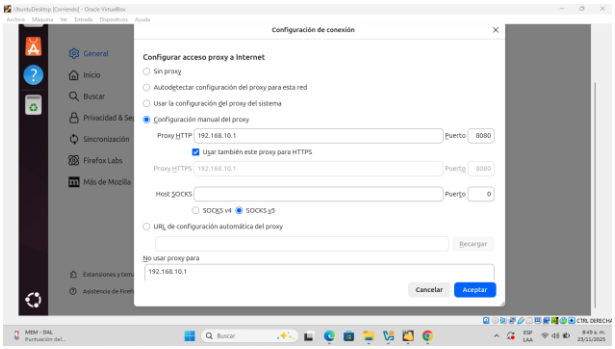
Configuración del Navegador para el Uso del Proxy

En la estación cliente (ubicada en la red GREEN), se ajustó la configuración manual del proxy en el navegador Firefox:

- Proxy para HTTP: 192.168.10.1
- Puerto: 8080
- Proxy para HTTPS: 192.168.10.1
- Puerto: 8080

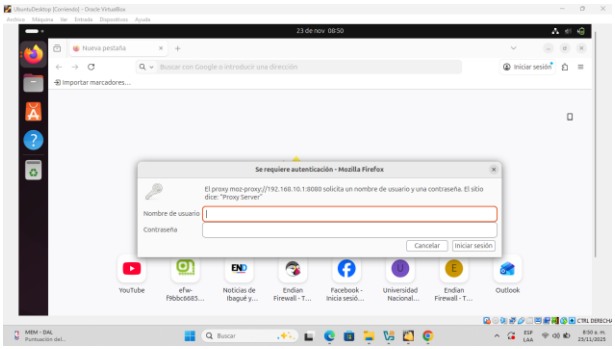
Tras aplicar estos parámetros, al intentar acceder a cualquier sitio web, se despliega un cuadro de diálogo solicitando usuario y contraseña. Esta ventana confirma que la autenticación del proxy está funcionando correctamente.

Fig. 38. Configuración manual del proxy en el navegador Firefox del cliente



Fuente: Elaboración propia

Fig. 39. Ventana de autenticación solicitando credenciales de usuario para permitir la navegación.



Fuente: Elaboración propia

Prueba de la Lista Negra y Bloqueo de Sitios

Después de aplicar la configuración del filtro web, se procedió a validar el bloqueo de sitios incluidos en la lista negra. Al intentar ingresar, por ejemplo, a:

www.elnuevodia.com.co

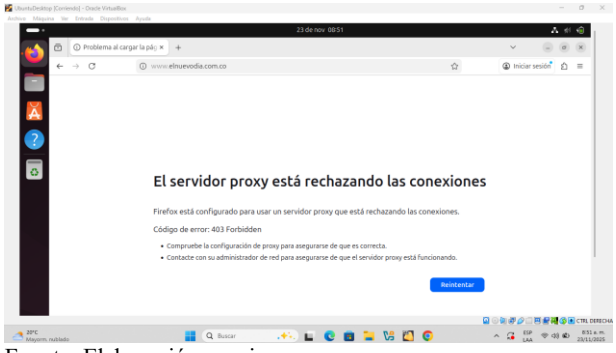
El navegador respondió con:

Este comportamiento confirma que:

1. El proxy está procesando correctamente el tráfico.
2. La lista negra está activa.
3. El perfil asignado al usuario fue aplicado adecuadamente.

Las pruebas se replicaron con los otros sitios definidos en la lista negra, obteniendo consistentemente el mismo resultado.

Fig. 40. Restricción de acceso (Error 403) desplegada al intentar ingresar a un sitio web bloqueado por la lista negra.



Fuente: Elaboración propia

RESULTADOS OBTENIDOS

Los resultados obtenidos durante la implementación del proxy HTTP permiten verificar el correcto funcionamiento del mecanismo de seguridad. Entre los principales hallazgos se encuentran:

- La autenticación mediante NCSA obliga al usuario a identificarse antes de navegar.
- La lista negra bloquea efectivamente el acceso a sitios no permitidos.
- El proxy no transparente permite aplicar políticas diferenciadas por usuario o grupo.
- El firewall registra el tráfico autenticado, facilitando auditorías futuras.
- La integración con antivirus refuerza la protección contra contenido malicioso.

En conjunto, estos resultados evidencian que el Proxy HTTP de Endian Firewall constituye una herramienta eficaz para la administración del tráfico web en entornos organizacionales.

ANÁLISIS

Durante las pruebas se comprobó que la autenticación y el filtrado del proxy operan únicamente cuando los clientes configuran correctamente el puerto 8080 en sus navegadores, lo cual es una característica inherente del modo no transparente. Esto implica que, en redes de mayor tamaño, es recomendable acompañar esta modalidad con políticas de despliegue centralizado (por ejemplo, mediante GPO o scripts de arranque).

En cuanto al rendimiento, la implementación sobre VirtualBox resultó suficiente para entornos de prueba. Sin embargo, en escenarios reales, el análisis antivirus y el filtrado profundo pueden requerir hardware con mayor capacidad de procesamiento.

El uso de listas negras personalizadas demostró ser flexible y fácil de administrar, permitiendo ajustar el control de navegación según las necesidades de la organización.

4 Conclusiones.

La implementación de la segmentación perimetral permitió evidenciar, de manera práctica, la importancia de implementar un firewall perimetral basado en GNU/Linux Endian para segmentar la red en zonas GREEN, RED y ORANGE. A través de la instalación en VirtualBox, la configuración de interfaces de red, el direccionamiento IP y las pruebas de conectividad, se consolidó una infraestructura básica pero funcional que protege la red interna y sienta las bases para futuras configuraciones de NAT, publicación de servicios en la DMZ y aplicación de políticas de seguridad más avanzadas.

Se configuró la red con DMZ y se definieron las reglas necesarias en el firewall para asegurar y controlar el acceso. Se habilitó correctamente el servicio HTTP y el servicio FTP, verificando que ambos pudieran ser accedidos desde la red permitida. Con esto se garantiza un acceso seguro y funcional.

La implementación de reglas de acceso por medio de iptables es fundamental para controlar el tráfico entre diferentes zonas de red y fortalecer la seguridad del sistema operativo GNU/Linux.

Las pruebas realizadas entre LAN, DMZ y WAN demostraron que una correcta configuración permite habilitar únicamente los servicios necesarios, evitando accesos no autorizados y reduciendo la superficie de ataque.

Validar las reglas mediante tráfico real (HTTP y FTP) permite asegurar que la política de seguridad se aplique de forma efectiva, garantizando que la infraestructura cumpla con los requisitos de disponibilidad y protección definidos en el proyecto.

La implementación del Proxy HTTP no transparente en Endian Firewall permitió establecer un control efectivo sobre la navegación web en la red interna. La autenticación mediante NCSA garantizó que solo usuarios autorizados pudieran acceder a Internet, fortaleciendo la trazabilidad y el manejo de permisos. Asimismo, la configuración del perfil de filtrado y la lista negra demostró un bloqueo preciso de los sitios definidos, confirmando la correcta aplicación de las políticas de seguridad. En conjunto, los resultados evidencian que Endian Firewall ofrece una solución robusta, eficiente y fácilmente replicable para gestionar el tráfico web y reforzar la seguridad perimetral en entornos GNU/Linux.

5 REFERENCIAS

[1] A. Belmar, *Seguridad GNU/Linux: Curso práctico*, Ediciones de la U, n.d. [Online]. Available: https://edicionesdelau.com/producto/seguridad-gnu-linux-curso-practico/

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

[3] E. A. Hoyos Pantoja, C. A. Hoyos Pantoja, J. A. Montealegre Aquite, and C. R. Gómez Aguirre, "Endian firewall como solución de seguridad en redes en un entorno virtualizado," Universidad Nacional Abierta y a Distancia – UNAD, 2025. [Online]. Available: https://repository.unad.edu.co/handle/10596/68800

[4] Endian S.r.l., *Endian Firewall Reference Manual (r. 2.2.1.9) – The Proxy Menu*, 2008. [Online]. Available: https://docs.endian.com/archive/2.2/efw.proxy.html

[5] Endian S.r.l., *Endian UTM 5.1: Reference Manual*, 2019. [Online]. Available: https://docs.endian.com/5.1/utm/index.html

[6] Linux Professional Institute, *LPIC-1 Exam 101 (101-500) Learning Materials*, n.d. [Online]. Available: https://learning.lpi.org/es/learning-materials/101-500/

[7] Oracle Corporation, *Oracle VM VirtualBox: User Guide for Release 7.0 (F43655-13)*, 2024. [Online]. Available: https://docs.oracle.com/en/virtualization/virtualbox/7.0/user/index.html