Implementación de seguridad perimetral en GNU/Linux mediante firewall Endian

Julio César Pedroza Aduén
jcpedrozaa@unadvirtual.edu.co
Margareth Sugeys Suarez Avila
mssuarezav@unadvirtual.edu.co
Ledo Rafael Pallares Navarro
lrpallaresn@unadvirtual.edu.co
Alex De Jesus Cera Viloria
adcerav@unadvirtual.edu.co
María Alejandra Castillo Figueroa
macastillofi@unadvirtual.edu.co

RESUMEN: *La seguridad perimetral es un elemento fundamental para proteger las redes y los sistemas informáticos contra el acceso no autorizado. Este artículo presenta la implementación de un esquema de seguridad perimetral basado en GNU/Linux, utilizando el cortafuegos Endian como componente central de control. La infraestructura se desarrolló en un entorno virtualizado mediante VirtualBox y se estructuró en tres zonas de red: LAN, DMZ y WAN. A través de un trabajo colaborativo, se abordaron temas relacionados con la instalación del cortafuegos, la configuración de la traducción de direcciones de red (NAT), la habilitación controlada de servicios en la DMZ, la definición de reglas de acceso entre zonas y la implementación de un proxy con mecanismos de autenticación. Los resultados obtenidos demuestran que Endian permite una gestión eficaz de la seguridad perimetral, garantizando una comunicación controlada y segura entre las diferentes zonas de red.*

PALABRAS CLAVE: DMZ, Endian Firewall, GNU/Linux, LAN, NAT, red, seguridad perimetral, WAN

ABSTRACT: *Perimeter security is a fundamental element in protecting computer networks and systems against unauthorized access. This article presents the implementation of a GNU/Linux-based perimeter security scheme, using the Endian firewall as the central control component. The infrastructure was developed in a virtualized environment using VirtualBox and was structured into three network zones: LAN, DMZ, and WAN. Through collaborative work, topics related to firewall installation, Network Address Translation (NAT) configuration, controlled service enablement in the DMZ, the definition of access rules between zones, and the implementation of a proxy with authentication mechanismswere addressed. The results obtained demonstrate that Endian enables effective management of perimeter security, ensuring controlled and secure communication between the different network zones.*

KEYWORDS: DMZ, Endian Firewall, GNU/Linux, LAN, NAT, Network, Perimeter Security, WAN

1 INTRODUCCIÓN

El crecimiento constante de las redes de datos y la interconexión de sistemas ha incrementado la exposición a amenazas informáticas, lo que hace indispensable la implementación de mecanismos de seguridad perimetral. Estos mecanismos permiten establecer controles entre redes internas y externas, reduciendo los riesgos asociados a accesos no autorizados y ataques provenientes de Internet.

En este contexto, el firewall Endian se presenta como una solución basada en GNU/Linux que facilita la segmentación de redes y el control del tráfico mediante políticas de seguridad. El presente artículo describe el desarrollo de la Etapa 7 del diplomado de profundización en administración de sistemas operativos Open Source, en la cual se implementó un entorno virtualizado de seguridad perimetral utilizando Endian Firewall, integrando diferentes temáticas que permiten evaluar su funcionamiento y efectividad.

2 DESARROLLO Y RESULTADOS

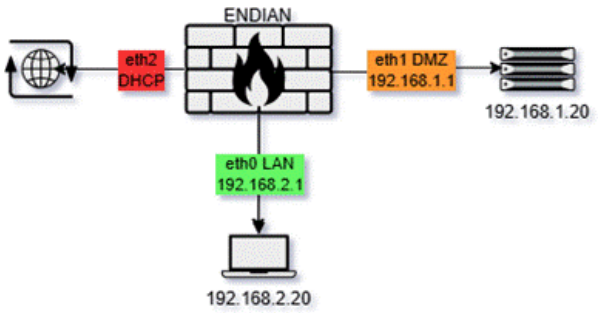
2.1 TEMÁTICA 1 – INFRAESTRUCTURA DE RED YCONFIGURACIÓN BASE

En esta etapa se implementó la infraestructura base de seguridad perimetral utilizando el firewall GNU/Linux Endian en un entorno virtualizado mediante VirtualBox. El objetivo principal fue diseñar una red segmentada que permitiera separar los distintos niveles de acceso y controlar el tráfico entre redes internas y externas.

Inicialmente, se diseñó una arquitectura compuesta por tres zonas principales: GREEN (LAN), ORANGE (DMZ) y RED (WAN), donde el firewall Endian actúa como elemento central de control y enrutamiento del tráfico. La Figura 1 muestra el diseño lógico de la arquitectura implementada, incluyendo la asignación de direcciones IP para cada segmento de red.

Figura 1.

Arquitectura de red segmentada implementada con Endian Firewall.

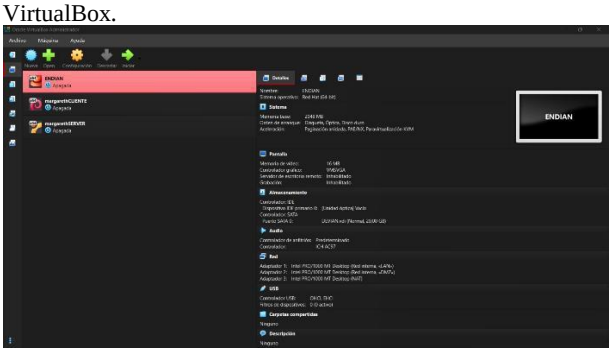


Fuente: Autoría Propia

Posteriormente, se procedió a la creación y configuración de las máquinas virtuales necesarias para el entorno de pruebas. Se implementaron tres sistemas virtualizados: un firewall Endian, un cliente Debian ubicado en la LAN y un servidor Ubuntu Server ubicado en la DMZ. Asimismo, se configuraron los adaptadores de red utilizando redes internas y NAT en VirtualBox para permitir la comunicación entre las distintas zonas y el acceso a Internet.

Figura 2.

Configuración de adaptadores de red y máquinas virtuales en VirtualBox.



Fuente: Autoría Propia

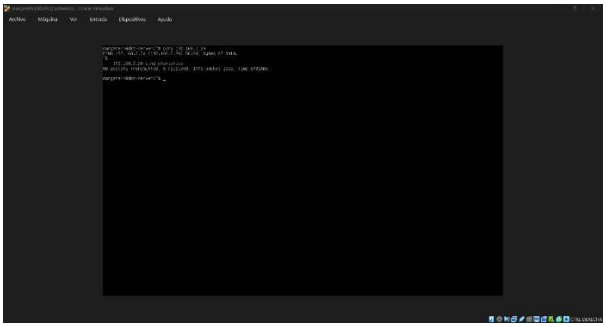
Una vez finalizada la instalación del firewall, se verificó el correcto funcionamiento de la interfaz web de administración de Endian. Desde esta consola se validaron las interfaces de red activas, el estado del sistema y el tráfico generado entre las diferentes zonas configuradas.

Posteriormente, se realizaron pruebas de conectividadpara validar el acceso a Internet desde la red LAN mediante el protocolo ICMP. Los resultados obtenidos evidenciaron que el firewall realizaba correctamente las funciones de enrutamiento y traducción de direcciones de red (NAT), permitiendo la comunicación hacia redes externas.

Finalmente, se realizó una prueba de aislamiento desde la DMZ hacia la LAN, donde no se obtuvo respuesta al intentar establecer comunicación con el cliente interno. Esto confirma que las políticas de seguridad implementadas en Endian restringen correctamente el acceso desde zonas con menor nivel de confianza hacia la red interna.

Figura 3.

Prueba de bloqueo de conectividad desde la DMZ hacia la LAN.



Fuente: Autoría Propia

Los resultados obtenidos permitieron validar la correcta segmentación de la red, el funcionamiento del firewall Endian y la aplicación de mecanismos básicos de seguridad perimetral en un entorno GNU/Linux virtualizado.

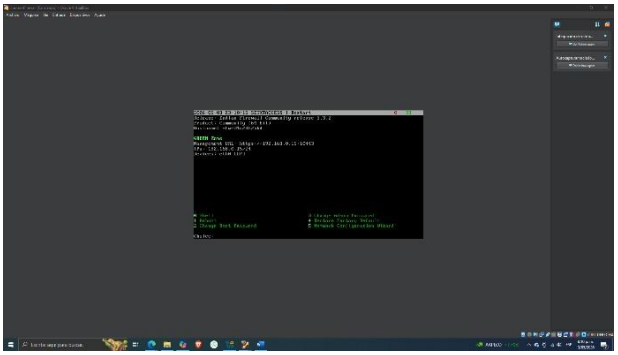
2.2 TEMÁTICA 2 – CONFIGURACIÓN DE NAT

En esta temática se validó la traducción de direcciones de red (NAT) en el firewall Endian, permitiendo la salida a Internet desde la red LAN y la zona DMZ. Mediante pruebas de conectividad se comprobó que el tráfico generado desde ambas zonas es correctamente traducido y enrutado hacia la WAN, garantizando la comunicación externa sin exponer las direcciones IP internas. Los resultados obtenidos demuestran el correcto funcionamiento del NAT como un mecanismo esencial para la seguridad perimetral.

2.2.1 REGISTRO DEL PROCESO

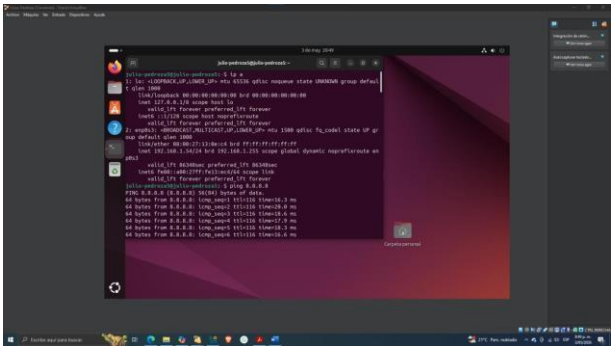
Figura 4.

Funcionamiento exitoso Endian.



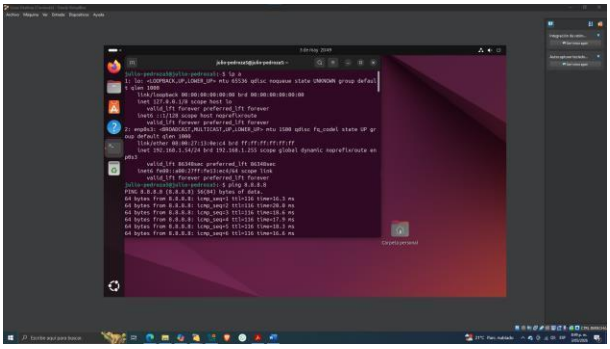
Fuente: Autoría Propia

Figura 5.
Prueba LAN → Internet.



Fuente: Autoría Propia

Figura 6.
Prueba DMZ → Internet.



Fuente: Autoría Propia

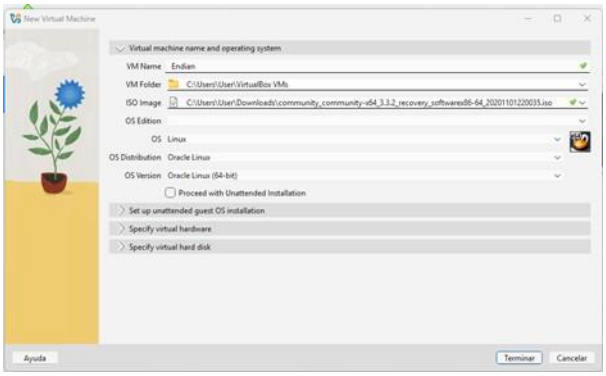
2.3 TEMÁTICA 3 – SERVICIOS EN LA DMZ

Se permitió el acceso a los servicios HTTP (Puerto 80) y FTP (Puerto 21) desde el servidor Web bajo Ubuntu Server. Denegar el protocolo ICMP (CMP Echo Request) para no permitir hacer ping en la red. Verificar mediante consola o terminal la no respuesta del comando ping hacia una IP de la red. Verificar en el tráfico de salida, la creación de las reglas.

2.4 DESARROLLO TEMÁTICA 3.

Se llevó a cabo la instalación y configuración de Endian Firewall en un entorno virtualizado. Para ello, se utilizó la versión 3.3.2, descargando la imagen ISO desde su sitio oficial en SourceForge (https://sourceforge.net/projects/efw). Posteriormente, se procedió a configurar la máquina virtual mediante la herramienta VirtualBox.Figura 7. Configuración máquina virtual Endian.

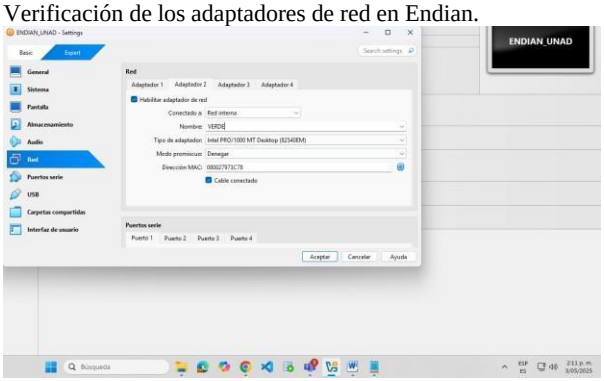
Figura 7.
Configuración de la máquina virtual de Endian



Fuente: Autoría Propia

Previo al proceso de instalación de la máquina, se configuraron los adaptadores de red que serían utilizados. Para ello, se consideraron las zonas roja, verde y naranja, las cuales fueron verificadas durante el proceso de instalación.

Figura 8.
Verificación de los adaptadores de red en Endian.



Fuente: Autoría Propia

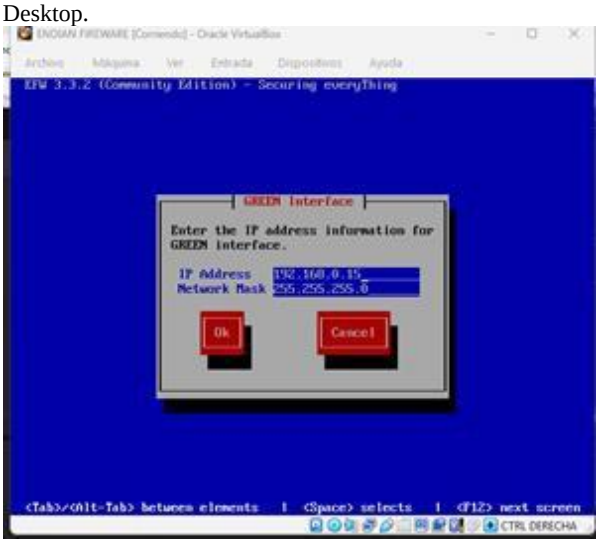
Una vez realizadas estas configuraciones, se continúa con la verificación del proceso de instalación de Endian. La instalación se lleva a cabo en idioma inglés y posteriormente se configuran las opciones necesarias, incluyendo las particiones del disco duro, procediendo finalmente a aceptar cada uno de estos pasos.

Figura 9.
Configuración de las particiones del disco en Endian.

Fuente: Autoría Propia

Se configuran los parámetros de la dirección IP para la zona verde, la cual corresponde a la máquina cliente (Desktop). A esta se le asigna la dirección IP 192.168.0.15/24, con una máscara de red 255.255.255.0. De esta manera, se establece la primera zona necesaria para el funcionamiento de Endian.

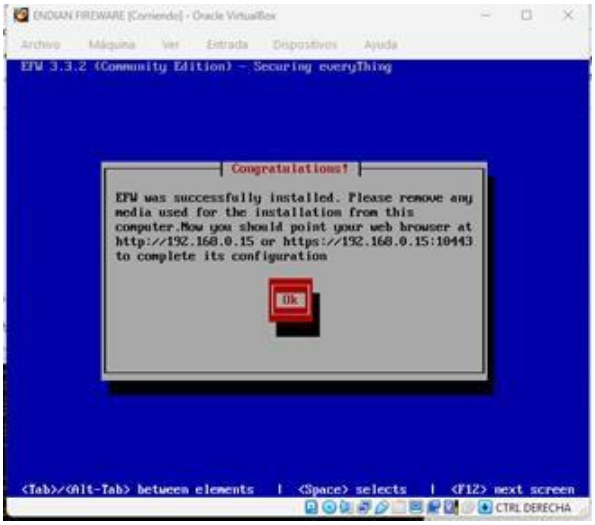
Figura 10.
Verificación de la dirección IP de la zona verde en el equipo Desktop.



Fuente: Autoría Propia

De esta manera, se obtiene la URL de acceso a la interfaz gráfica de configuración de Endian, quedando establecida como https://192.168.0.15:10443. Esta dirección corresponde a la zona verde previamente configurada. Posteriormente, se selecciona la opción “Ok” para confirmar los ajustes realizados y continuar con el proceso de configuración y uso del servicio Endian.

Figura 11.
Verificación de la URL de acceso a Endian.



Fuente: Autoría Propia

A través de este proceso inicial, se obtienen las configuraciones correspondientes a las zonas GREEN y RED. En este caso, la dirección IP de la zona roja se asigna automáticamente mediante DHCP, quedando establecida como 10.0.2.15/24.

Figura 12.
Ajustes de las zonas GREEN y RED.

Fuente: Autoría Propia

Se accede a la URL asignada desde el equipo Desktop, el cual está configurado mediante el adaptador de la zona verde previamente validado en la máquina de Endian. Este equipo cuenta con la dirección IP 192.168.0.15, desde la cual se ingresa a través del navegador web. De esta forma, se obtiene una respuesta satisfactoria, permitiendo realizar las configuraciones necesarias desde la interfaz gráfica.

Figura 13.
Ajustes iniciales del proceso de Endian

Fuente: Autoría Propia

Una vez finalizado el proceso de configuraciones iniciales, se procede a validar los ajustes de red, los cuales quedan establecidos mediante enrutamiento a través de una conexión DHCP. Posteriormente, se selecciona la opción "Siguiente" y se continúa con la configuración del adaptador de red faltante, correspondiente a la zona naranja. Esta zona cumple la función de servidor DMZ y se configura con la dirección IP 192.168.1.1/24 y una máscara de red 255.255.255.0. Asimismo, se pueden visualizar las tarjetas de red asociadas a cada uno de los adaptadores previamente configurados.

Figura 14.
Configuración de la zona naranja (servidor).

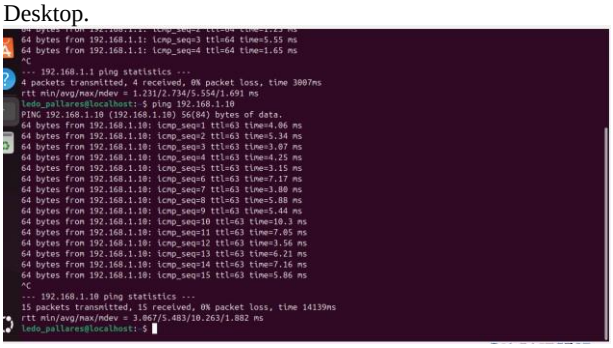
Fuente: Autoría Propia

De esta forma se permitirá visualizar cada una de las configuraciones de adaptadores de red la zona roja es la conexión a internet esto validado mediante el tipo NAT. Se aceptan las configuraciones necesarias y se permitirá acceder de manera exitosa a las configuraciones del Endian en el cual podemos observar las previas configuraciones de las diferentes zonas de red.

Cada una de las validaciones realizadas permite garantizar el acceso correcto a las máquinas configuradas, en este caso el Desktop y el servidor, los cuales forman parte del proceso. Para ello, se efectúan pruebas previas de conectividad, como el acceso y el comando ping en cada equipo, con el fin de verificar que cada uno esté utilizando su dirección IP correspondiente. Asimismo, se realizan configuraciones adicionales relacionadas con los servidores DNS, incorporando en este caso los de Google para asegurar la resolución de nombres.

Finalmente, se define el nombre del host como *svr-firewall* y el dominio como *localdomain*, lo que permite visualizar correctamente los tres adaptadores de red configurados.

Figura 15.
Comprobación de conectividad (ping) desde el equipo Desktop.



Fuente: Autoría Propia

Figura 16.
Verificación de conectividad (ping) desde el servidor DMZ.

Fuente: Autoría Propia

Se procede a validar el acceso a los servicios HTTP y FTP, utilizando los puertos 80 y 21 respectivamente, a través del servidor web. Estas configuraciones se realizan desde la opción de Firewall, específicamente en el apartado de tráfico entre zonas.

Para ello, se crea una nueva regla en la que se establece como origen la zona naranja y como destino la zona verde. En el caso del servicio HTTP, se define el protocolo TCP y el puerto 80, permitiendo así el acceso correspondiente conforme a la configuración establecida.

Figura 17.
Ingreso de la regla para el servicio HTTP en el puerto 80.

Fuente: Autoría Propia

Para habilitar el servicio FTP, se configura una regla que permite el tráfico bajo el protocolo TCP a través del puerto 21. En esta configuración, se establece la zona naranja como origen y la zona verde como destino, autorizando así la comunicación correspondiente entre dichas zonas.

Figura 18.
Creación de la regla para el servicio FTP en el puerto 21.

Fuente: Autoría Propia

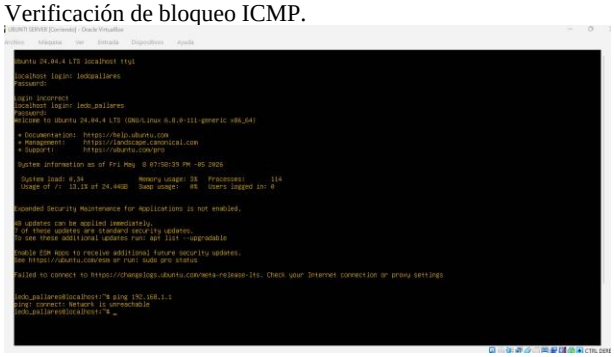
Se configura una regla para denegar el tráfico ICMP, evitando así la realización de pruebas de conectividad (ping). Para ello, se crea una nueva regla en la que se establece como origen la zona verde y como destino la zona naranja, aplicando la denegación de este protocolo.

De esta manera, al intentar hacer ping desde el equipo Desktop hacia la dirección IP 192.168.2.10, no se obtiene respuesta, bloqueando cualquier solicitud de este tipo. Finalmente, es necesario aplicar los cambios realizados para que las reglas configuradas surtan efecto.

Figura 19.
Configuración de una regla para bloquear el protocolo ICMP.

Fuente: Autoría Propia

Figura 20.
Verificación de bloqueo ICMP.

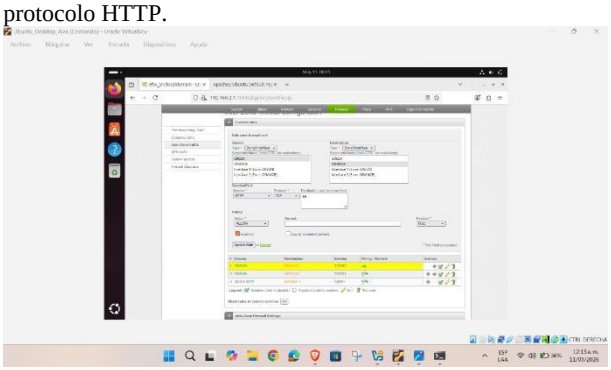


Fuente: Autoría Propia

2.5 TEMÁTICA 4 – REGLAS DE ACCESO ENTRE ZONAS

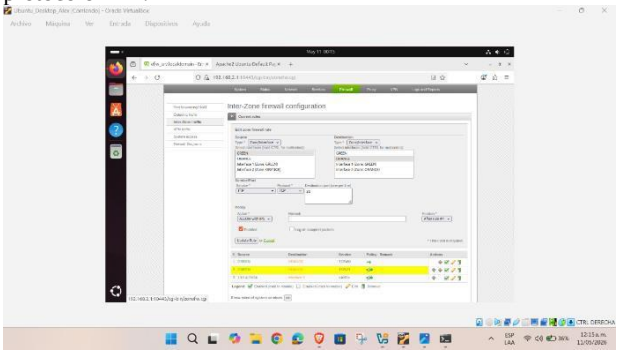
La temática 4 consistió en la definición de las reglas o políticas de acceso (ACLs) que regulan el tráfico entre zonas. Las políticas se configuraron siguiendo el principio de mínimo privilegio, denegando todo el tráfico por defecto y permitiendo únicamente lo requerido.

Figura 21.
Comunicación entre la zona verde y la zona naranja – protocolo HTTP.



Fuente: Autoría Propia

Figura 22.
Comunicación entre la zona verde y la zona naranja – protocolo FTP.



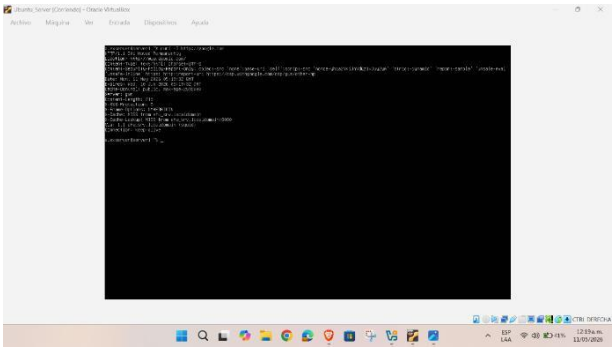
Fuente: Autoría Propia

Flujo entre zona verde a naranja (LAN a DMZ): Se habilitaron reglas para permitir el tráfico HTTP (TCP puerto 80) y FTP (TCP puerto 21) desde la Zona Verde hacia la Zona

Naranja. Esto permite a los administradores de la red interna acceder a los servicios públicos desplegados en la DMZ.

Flujo Rojo a Naranja (WAN a DMZ): Se configuraron reglas de acceso restringidas para permitir solo el tráfico necesario hacia los servicios expuestos en la DMZ (HTTP/HTTPS para servidores web). Esta es la única zona donde se permite el acceso de entrada desde Internet, aplicando seguridad a la red interna (Zona Verde) de accesos directos. La configuración permitió que el servidor web en la DMZ fuera visible desde la WAN.

Figura 23.
Comprobación comunicación zona naranja con zona roja - HTTP.



Fuente: Autoría Propia

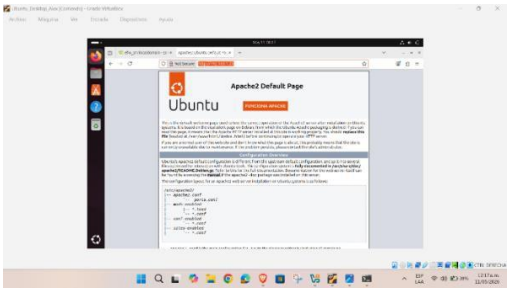
Flujo Naranja a Roja (DMZ a WAN): Se habilitó la salida desde la DMZ hacia Internet para permitir que los servicios accedan a recursos externos, asegurando la operatividad de los servidores públicos.

Es importante mencionar que el desarrollo de esta temática tomó en cuenta previamente lo establecido en la temática 1 y 2 donde se implementaron reglas de Network Address Translation (NAT) dinámicas (Masquerading) para permitir que los dispositivos de la Zona Verde y la Zona Naranja accedan a la Zona Roja compartiendo la IP pública de la interfaz WAN.

2.5.1 VALIDACIÓN DE LA CONECTIVIDAD

Para verificar la eficacia de la configuración y el cumplimiento de las reglas de seguridad, se ejecutaron un conjunto de pruebas de conectividad utilizando herramientas de línea de comandos y navegadores web.

Figura 24.
Comprobación comunicación zona verde con zona naranja - HTTP.

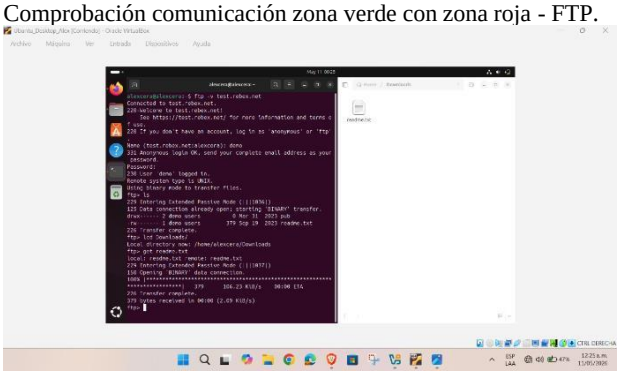


Fuente: Autoría Propia

Desde la Zona Verde, se accedió exitosamente al servidor web Apache alojado en la Zona Naranja mediante el navegador, confirmando que la regla de entrada hacia la DMZ desde la LAN es operativa.

Desde la Zona Roja (simulada mediante la terminal del firewall), se realizó una prueba con el comando curl -I http://<IP_DMZ> para verificar la respuesta HTTP del servidor web en la DMZ, validando la exposición controlada desde Internet.

Figura 25.
Comprobación comunicación zona verde con zona roja - FTP.



Fuente: Autoría Propia

Se comprobó la conectividad FTP desde la Zona Verde hacia un servidor de prueba en la Zona Roja utilizando el comando “ftp -v test.rebex.net”. La conexión exitosa demostró que las reglas de salida hacia Internet y las políticas de estado del firewall permiten el tráfico de datos de sesión FTP correctamente.

2.5.2 VALIDACIÓN DE AISLAMIENTO Y SEGURIDAD.

Las pruebas confirmaron que el tráfico no autorizado entre zonas (ej. acceso directo de la Zona Roja a la Zona Verde) fue denegado por el firewall, demostrando la efectividad de la segmentación.

Se utilizó el comando curl -I http://google.com desde la terminal de la Zona Naranja para validar el acceso a Internet desde la DMZ, asegurando que los servicios públicos puedan operar sin comprometer la seguridad de la red interna.

El estado de las comunicaciones inter-zona se cumple con la topología implementada que tomó en cuenta los requisitos de seguridad perimetral: la red interna queda protegida, los servicios públicos son accesibles desde Internet con control, y la comunicación entre zonas se rige estrictamente por las políticas definidas.

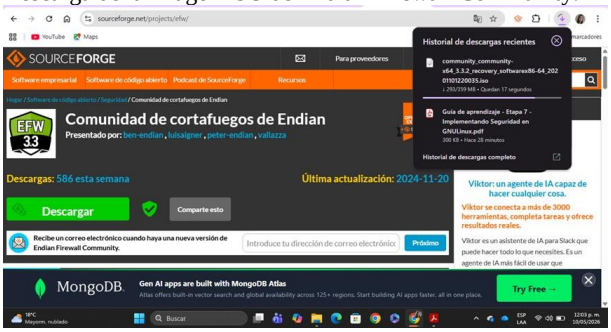
2.5.3 RESULTADOS

La configuración de reglas de NAT y filtrado de paquetes garantizan que solo el tráfico legítimo fuera permitido, reduciendo significativamente el acceso no autorizado.

Es fundamental destacar que la correcta asignación de interfaces y la ordenación de las reglas de firewall son críticas; un error en la prioridad de las reglas podría vulnerar y exponer la red interna.

2.6 TEMÁTICA 5 – PROXY Y AUTENTICACIÓN

Figura 26.
Descarga de la imagen ISO de Endian Firewall Community.



Fuente: Autoría Propia

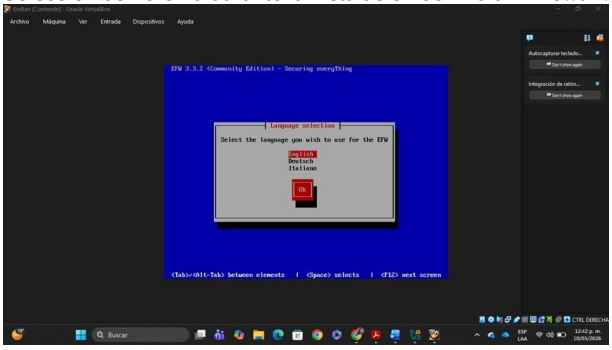
Se realizó la descarga de la imagen ISO de Endian Firewall Community desde el sitio oficial con el objetivo de implementar un firewall de seguridad perimetral en un entorno virtualizado. Esta distribución GNU/Linux fue utilizada como plataforma principal para la configuración del proxy HTTP, las políticas de autenticación y el filtrado de navegación web dentro de la red LAN.

Figura 27.
Carga de la imagen ISO de Endian Firewall en VirtualBox.

Fuente: Autoría Propia

Se realizó la carga y montaje de la imagen ISO de Endian Firewall Community en la máquina virtual creada en VirtualBox, permitiendo iniciar el proceso de instalación y configuración del firewall dentro del entorno virtualizado. Esta configuración permitió implementar posteriormente las zonas de red GREEN, RED y ORANGE utilizadas en la práctica de seguridad perimetral.

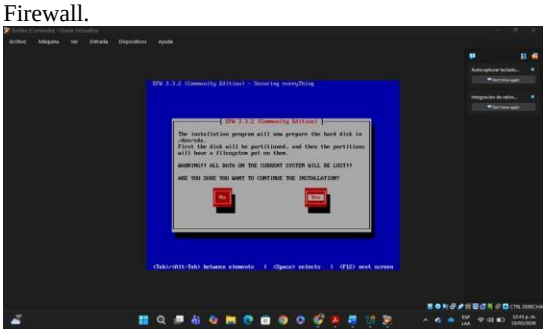
Figura 28.
Selección del idioma durante la instalación de Endian Firewall.



Fuente: Autoría Propia

Durante el proceso de instalación de Endian Firewall se seleccionó el idioma inglés como idioma predeterminado del sistema. Esta configuración permitió continuar con la instalación inicial y la configuración de los servicios de seguridad perimetral requeridos en la actividad.

Figura 29.
Confirmación del proceso de instalación del sistema Endian Firewall.



Fuente: Autoría Propia

El instalador de Endian Firewall mostró la confirmación del proceso de instalación y la ubicación donde serían almacenados los archivos del sistema operativo dentro de la máquina virtual creada en VirtualBox. Esta instalación corresponde a la plataforma encargada de administrar la comunicación entre las zonas GREEN, RED y ORANGE.

Figura 30.
Configuración de la dirección IP de la interfaz GREEN.

Fuente: Autoría Propia

Se configuró la interfaz GREEN correspondiente a la red LAN interna con la dirección IP 192.168.2.1 y máscara de red

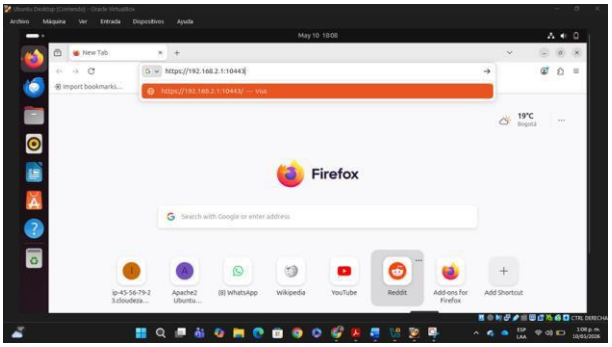
255.255.255.0. Esta interfaz representa la zona verde del firewall, utilizada para la comunicación de los usuarios finales dentro de la red interna.

Figura 31.
Finalización de la instalación de Endian Firewall Community.

Fuente: Autoría Propia

El sistema indicó la finalización correcta de la instalación de Endian Firewall Community, permitiendo continuar con la configuración administrativa desde la interfaz web mediante el protocolo HTTPS.

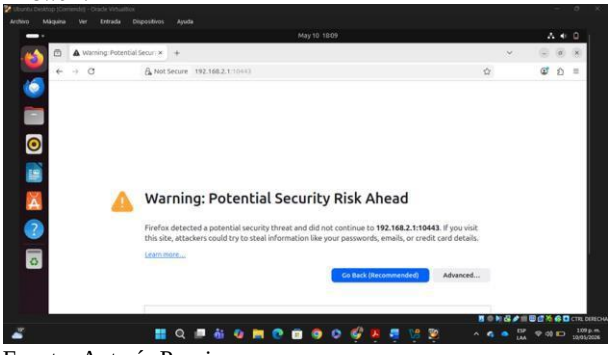
Figura 32.
Acceso a la interfaz administrativa web de Endian Firewall.



Fuente: Autoría Propia

Se realizó el acceso a la interfaz administrativa de Endian Firewall utilizando el protocolo HTTPS mediante la dirección IP 192.168.2.1 y el puerto 10443. Esta interfaz permite administrar las configuraciones de red, autenticación, filtrado web y políticas de seguridad del firewall.

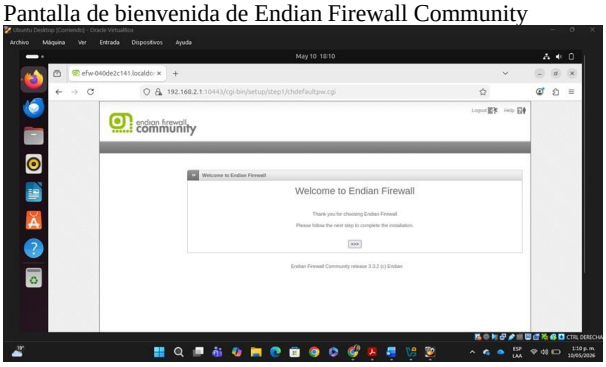
Figura 33.
Advertencia de seguridad del certificado HTTPS en Endian Firewall.



Fuente: Autoría Propia

El navegador web mostró una advertencia de seguridad debido al uso de un certificado digital autofirmado por parte de Endian Firewall. Se permitió continuar con el acceso seguro para realizar la configuración del sistema.

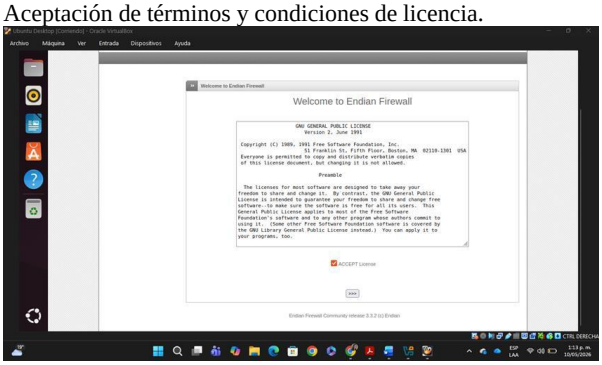
Figura 34.
Pantalla de bienvenida de Endian Firewall Community



Fuente: Autoría Propia

La plataforma Endian Firewall Community presentó la pantalla de bienvenida correspondiente al inicio de la configuración administrativa del firewall y de los servicios de seguridad implementados en la red.

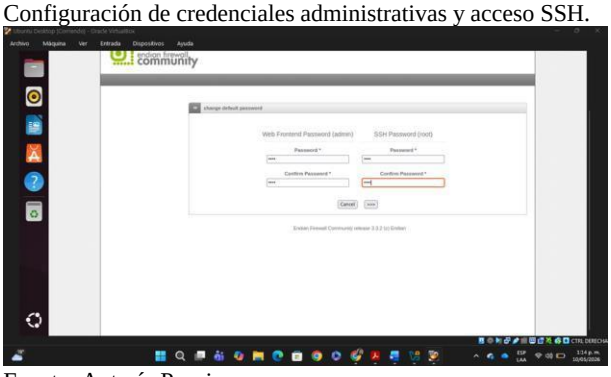
Figura 35.
Aceptación de términos y condiciones de licencia.



Fuente: Autoría Propia

Se aceptaron los términos de licencia y condiciones de uso de Endian Firewall Community necesarios para continuar con el proceso de configuración del firewall y los servicios de red.

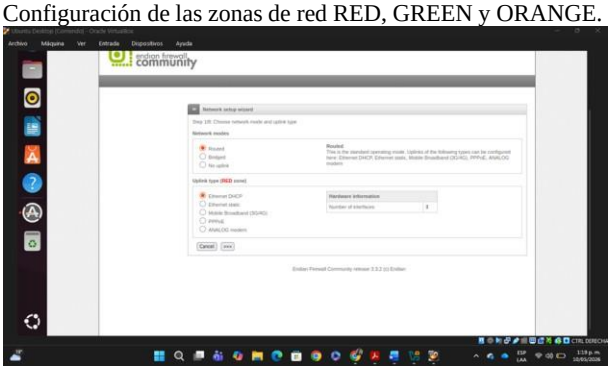
Figura 36.
Configuración de credenciales administrativas y acceso SSH.



Fuente: Autoría Propia

Se configuraron las credenciales administrativas del firewall, asignando una contraseña al usuario administrador y una contraseña al servicio SSH del usuario root, permitiendo así la administración segura del sistema.

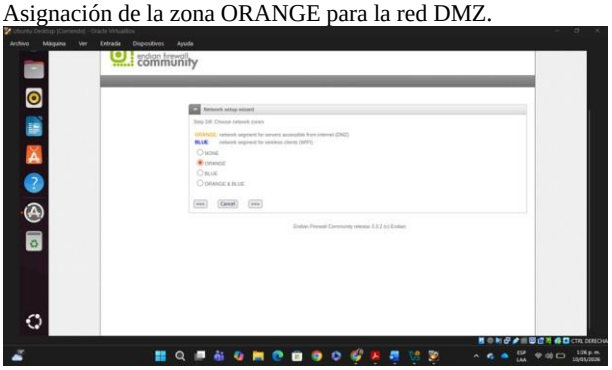
Figura 37.
Configuración de las zonas de red RED, GREEN y ORANGE.



Fuente: Autoría Propia

Se realizó la configuración de las interfaces de red del firewall asignando la zona RED para la conexión WAN hacia Internet mediante DHCP, la zona GREEN para la red LAN interna de usuarios y la zona ORANGE para la red DMZ destinada a servidores.

Figura 38.
Asignación de la zona ORANGE para la red DMZ.



Fuente: Autoría Propia

Se configuró la interfaz ORANGE correspondiente a la zona DMZ, utilizada para alojar servicios y servidores accesibles desde otras redes manteniendo el aislamiento y la seguridad respecto a la red LAN interna.

Figura 39.
Configuración de la dirección IP de la zona ORANGE.

Fuente: Autoría Propia

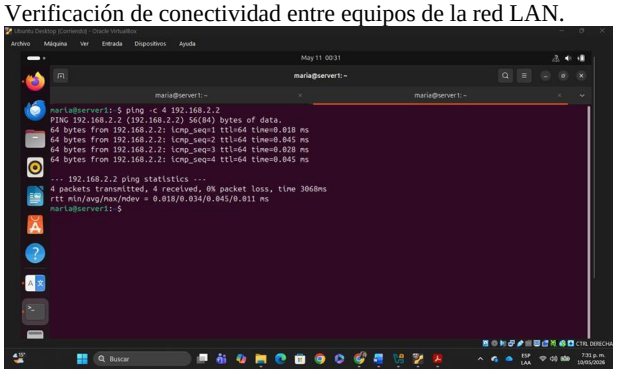
Se asignó la dirección IP 192.168.1.1 a la interfaz ORANGE correspondiente a la red DMZ. Esta configuración permitió establecer la comunicación entre el firewall Endian y el servidor Ubuntu Server ubicado en la zona desmilitarizada.

Figura 40.
Implementación de las máquinas virtuales en VirtualBox

Fuente: Autoría Propia

Se configuraron tres máquinas virtuales dentro de VirtualBox: Ubuntu Desktop como cliente de la red GREEN con dirección IP 192.168.2.20, Ubuntu Server como servidor de la zona ORANGE con dirección IP 192.168.1.20 y Endian Firewall como firewall encargado de controlar la comunicación entre las diferentes zonas de red.

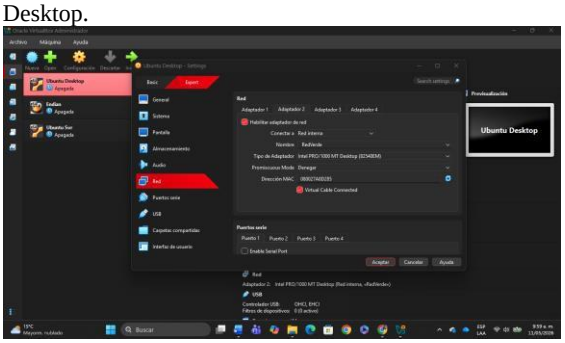
Figura 41.
Verificación de conectividad entre equipos de la red LAN.



Fuente: Autoría Propia

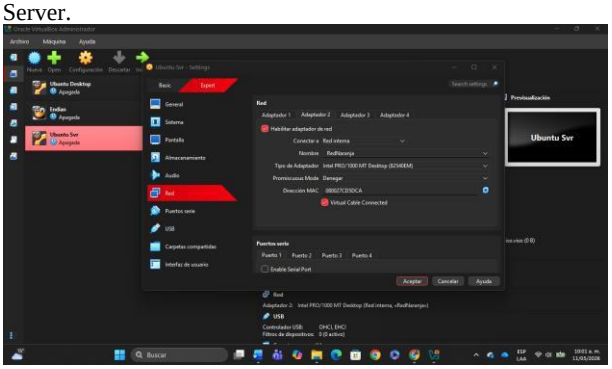
Se realizó una prueba de conectividad mediante el comando ping entre los equipos de la red LAN para verificar la correcta comunicación y funcionamiento de la configuración de red implementada en Endian Firewall.

Figura 42.
Configuración de redes virtuales en VirtualBox – Ubuntu Desktop.



Fuente: Autoría Propia

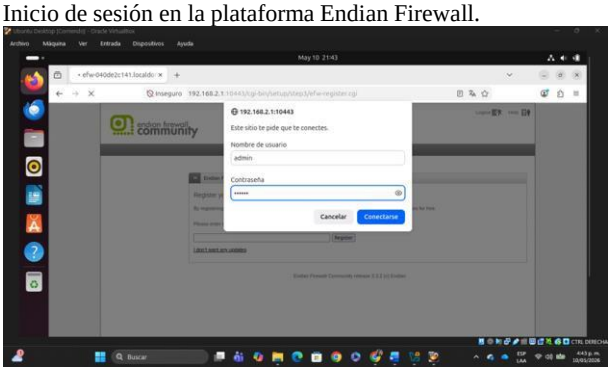
Figura 43.
Configuración de redes virtuales en VirtualBox – Ubuntu Server.



Fuente: Autoría Propia

Se configuraron las interfaces de red virtuales utilizando redes internas y NAT. La máquina Ubuntu Desktop fue conectada a la red interna GREEN, Ubuntu Server fue conectado a la red interna ORANGE y Endian Firewall fue configurado con tres interfaces de red para permitir la comunicación entre la LAN, la DMZ y la WAN.

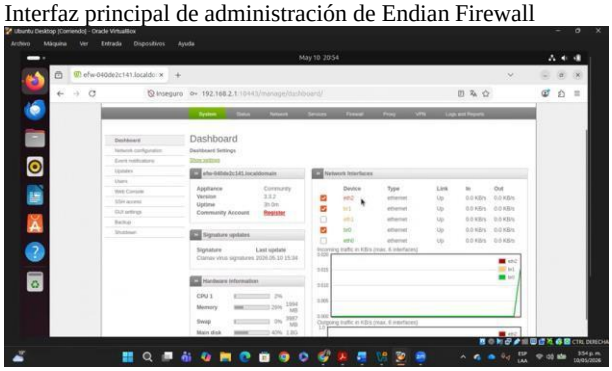
Figura 44.
Inicio de sesión en la plataforma Endian Firewall.



Fuente: Autoría Propia

Se realizó el acceso a la plataforma administrativa de Endian Firewall utilizando las credenciales previamente configuradas para administrar las políticas de seguridad y navegación web.

Figura 45.
Interfaz principal de administración de Endian Firewall



Fuente: Autoría Propia

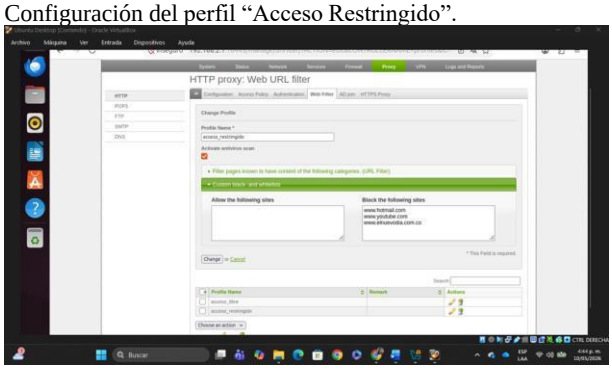
La interfaz principal de Endian Firewall permitió visualizar y administrar las configuraciones relacionadas con autenticación, proxy HTTP, filtrado web, reglas de acceso y monitoreo de la red.

Figura 46.
Creación de perfiles de navegación web

Fuente: Autoría Propia

Se crearon perfiles de navegación web dentro del módulo Proxy → Web Filter con el fin de establecer políticas diferenciadas de acceso para usuarios con navegación libre y restringida.

Figura 47.
Configuración del perfil “Acceso Restringido”.

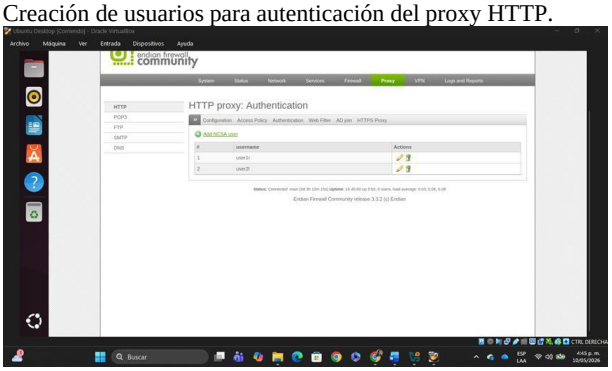


Fuente: Autoría Propia

Se configuró el perfil denominado “Acceso Restringido” agregando a la lista negra los dominios www.hotmail.com,

www.youtube.com y www.elnuevodia.com, con el propósitode bloquear el acceso a dichos sitios web desde la red LAN.

Figura 48.
Creación de usuarios para autenticación del proxy HTTP.



Fuente: Autoría Propia

Se crearon usuarios locales dentro de Endian Firewall para implementar autenticación en el servicio proxy HTTP. Los usuarios fueron utilizados para aplicar políticas diferenciadas de navegación web.

Figura 49.
Creación de grupos de usuarios con políticas de acceso.

Fuente: Autoría Propia

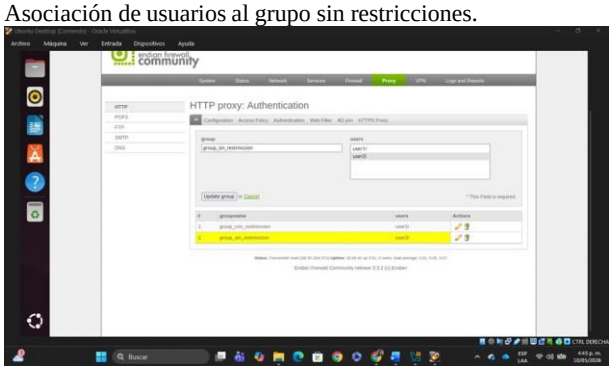
Se configuraron grupos de usuarios denominados “Grupo con Restricción” y “Grupo sin Restricción” con el fin de asociar políticas específicas de filtrado web y autenticación.

Figura 50.
Asociación de usuarios a grupos de autenticación.

Fuente: Autoría Propia

Los usuarios creados previamente fueron asociados a sus respectivos grupos de autenticación para aplicar las políticas de navegación correspondientes dentro del proxy HTTP implementado en Endian Firewall.

Figura 51.
Asociación de usuarios al grupo sin restricciones.



Fuente: Autoría Propia

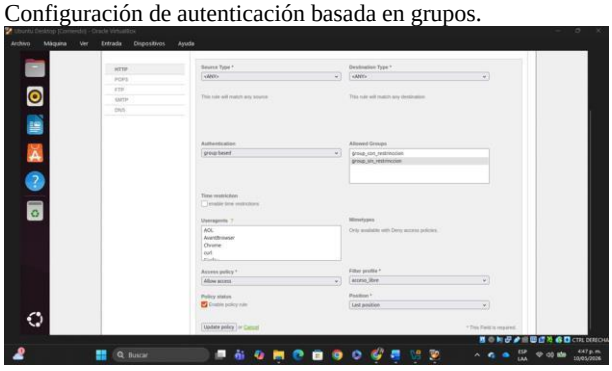
El usuario sin restricciones fue asociado al grupo sin restricciones

Figura 52.
Asociación de usuarios al grupo con restricciones.

Fuente: Autoría Propia

El usuario con restricciones fue asociado al grupo encargado de aplicar políticas de filtrado y bloqueo de contenido web

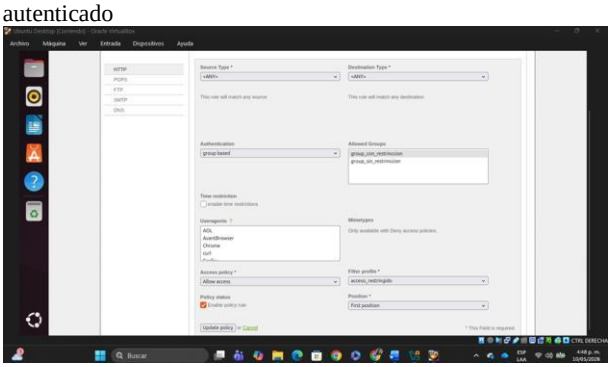
Figura 53.
Configuración de autenticación basada en grupos.



Fuente: Autoría Propia

Se configuró el sistema de autenticación del proxy HTTP utilizando políticas basadas en grupos, permitiendo aplicar perfiles de navegación específicos dependiendo del tipo de usuario autenticado.

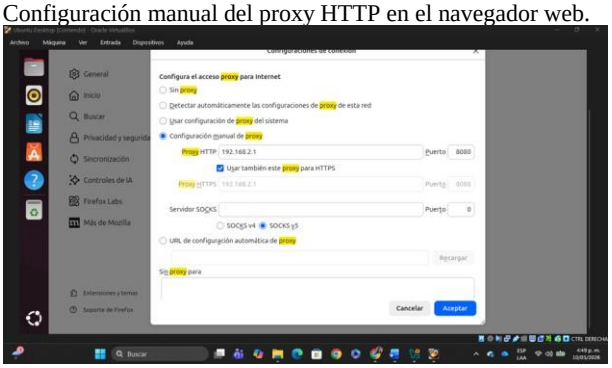
Figura 54.
Asignación del perfil “Acceso Restringido” al grupo autenticado



Fuente: Autoría Propia

Se aplicó el perfil “Acceso Restringido” al grupo de usuarios restringidos para bloquear automáticamente el acceso a los sitios web configurados en la lista negra.

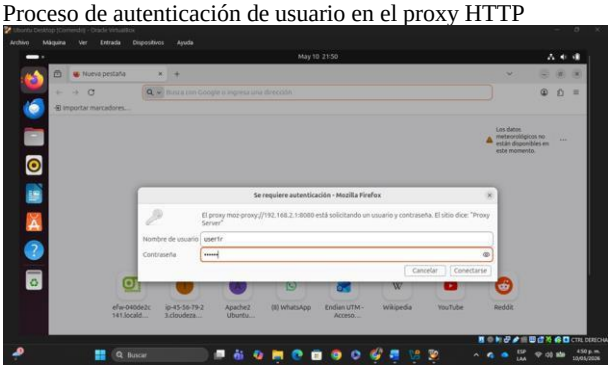
Figura 55.
Configuración manual del proxy HTTP en el navegador web.



Fuente: Autoría Propia

Se configuró manualmente el proxy HTTP en el navegador Firefox utilizando la dirección IP 192.168.2.1 correspondiente a la interfaz GREEN del firewall y el puerto 8080 para controlar la navegación web de los usuarios autenticados.

Figura 56.
Proceso de autenticación de usuario en el proxy HTTP



Fuente: Autoría Propia

El navegador solicitó autenticación mediante usuario y contraseña antes de permitir el acceso a Internet, validando las políticas de autenticación configuradas en Endian Firewall.

Figura 57.
Validación del bloqueo de sitios web mediante lista negra

Fuente: Autoría Propia

Se verificó el correcto funcionamiento de las políticas de filtrado web evidenciando el bloqueo del sitio www.elnuevodia.com.co desde la red LAN. El sistema mostró el mensaje “Access Denied – Custom Blacklist”, confirmando que el dominio fue restringido correctamente mediante la lista negra configurada en el proxy HTTP.

3 CONCLUSIONES

La implementación de la infraestructura base permitió establecer una arquitectura de red segmentada en zonas con distintos niveles de confianza, lo cual constituye un principio fundamental en la seguridad perimetral para entornos GNU/Linux.

La configuración de la traducción de direcciones de red (NAT) a través del firewall Endian demostró ser un mecanismo eficaz para permitir la salida a Internet desde la LAN y la DMZ sin exponer las direcciones IP internas.

La habilitación controlada de servicios en la zona DMZ permitió ofrecer servicios específicos minimizando el riesgo de acceso no autorizado a la red interna, fortaleciendo el aislamiento entre zonas.

La definición de reglas de acceso entre la LAN, la DMZ y la WAN permitió aplicar el principio de mínimo privilegio, garantizando que el tráfico de red se gestione conforme a políticas de seguridad preestablecidas.

La implementación de un proxy con mecanismos de autenticación permitió mejorar el control del acceso a Internet, aportando un nivel adicional de seguridad y supervisión sobre la navegación de los usuarios.

Finalmente, el desarrollo colaborativo de la actividad fortaleció las competencias prácticas en administración de sistemas GNU/Linux y evidenció la importancia de integrar múltiples mecanismos de seguridad en un entorno perimetral coherente.

4 REFERENCIAS

[1] Learning materials. Recuperado el 11 de mayo de 2026 de https://learning.lpi.org/en/learning-materials/010-160/

[2] Endian. (s. f.). Endian firewall community documentation. Recuperado el 11 de mayo de 2026 de https://www.endian.com/community/

[3] Oracle Corporation. (s. f.). Oracle VM VirtualBox user manual. Recuperado el 11 de mayo de 2026 de https://www.virtualbox.org/manual/

[4] Canonical Ltd. (s. f.). Ubuntu Server documentation. Recuperado el 11 de mayo de 2026 de https://ubuntu.com/server/docs

[5] Debian Project. (s. f.). Debian administrator's handbook. Recuperado el 11 de mayo de 2026 de https://www.debian.org/doc/manuals/debian-reference/

[6] IEEE. (s. f.). IEEE author guidelines for conference papers. Recuperado el 11 de mayo de 2026 de https://www.ieee.org/conferences/publishing/templates.html

[7] Oppliger, R. (2000). Security technologies for the World Wide Web (2nd ed.). Artech House.

[8] Northcutt, S., & Novak, J. (2002). Network intrusion detection (3rd ed.). New Riders Publishing.

[9] Srisuresh, P., & Egevang, K. (2001, enero). Traditional IP network address translator (Traditional NAT) (RFC 3022). https://datatracker.ietf.org/doc/html/rfc3022

[10] Stallings, W. (2017). Network security essentials: Applications and standards (6th ed.). Pearson.