IMPLEMENTACIÓN DE SEGURIDAD EN GNU/LINUX USANDO ENDIAN FIREWALL PARA LA PROTECCIÓN LAN/DMZ/WAN

Karen Dayana Sanabria Duran
kdsanabriad@unadvirtual.ecu.co

RESUMEN: *Este artículo expone el desarrollo e implementación de un entorno de seguridad en redes basadas en GNU/Linux, empleando Endian Firewall como núcleo de protección. El proyecto se llevó a cabo en un contexto educativo colaborativo, con énfasis en la separación lógica de redes mediante la creación de zonas LAN, DMZ y WAN dentro de un laboratorio virtualizado. Se realizaron tareas como el diseño de reglas de traducción de direcciones (NAT), la activación y supervisión de servicios de red, la restricción de protocolos no deseados y la integración de mecanismos de control de navegación mediante proxy con autenticación. Las configuraciones fueron aplicadas y verificadas a través de comandos en consola, asegurando trazabilidad y transparencia en cada etapa. Los hallazgos evidencian la utilidad de EFW como solución práctica y adaptable para reforzar la infraestructura de red, destacando la importancia del aislamiento de servicios críticos y el control de tráfico como pilares para una defensa efectiva ante amenazas externas*.

PALABRAS CLAVE: Seguridad Perimetral, Endian Firewall, GNU/Linux, Segmentación de Red, NAT y Proxy.

ABSTRACT: *This article presents the development and implementation of a network security environment based on GNU/Linux, using Endian Firewall as the core protection platform. The project was conducted in a collaborative educational setting, focusing on the logical segmentation of networks through the creation of LAN, DMZ, and WAN zones within a virtualized lab environment. Key tasks included the design of Network Address Translation (NAT) rules, the activation and monitoring of network services, the restriction of undesired protocols, and the integration of proxy-based access control with authentication. Configurations were applied and validated via command-line interface, ensuring traceability and transparency throughout the process. The findings highlight the effectiveness of EFW as a practical and adaptable solution for strengthening network infrastructure, emphasizing the importance of isolating critical services and managing traffic as essential strategies for mitigating external threats.*.

KEYWORDS: Perimeter Security, Endian Firewall, GNU/Linux, Network Segmentation, NAT and Proxy.

1 INTRODUCCIÓN

En el ámbito tecnológico contemporáneo, la protección cibernética desempeña un rol crítico para salvaguardar la integridad, disponibilidad y confidencialidad de los sistemas informáticos. En este documento se expone el diseño, implementación y análisis de una infraestructura de seguridad basada en una zona desmilitarizada (DMZ) configurada mediante Endian Firewall Community sobre sistemas GNU/Linux. El estudio se desarrolló en un entorno virtualizado, donde se configuraron y segregaron las redes LAN, WAN y DMZ, aplicando reglas de traducción de direcciones de red (NAT) y políticas de filtrado de tráfico a nivel de firewall. Se gestionaron servicios expuestos en la DMZ, incluyendo servidores web y FTP, complementados con la integración de un proxy HTTP autenticado con listas negras para controlar y restringir el acceso a recursos web. La implementación combinó el uso de la consola gráfica de administración web de Endian con comandos directos en la interfaz de línea de comandos (CLI), permitiendo la verificación empírica de la efectividad y robustez de los controles de seguridad aplicados..

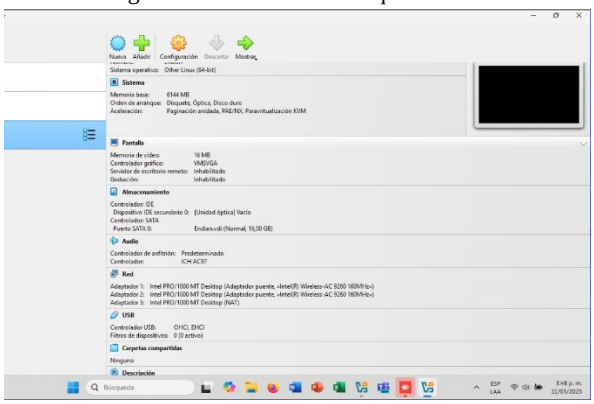
2 INSTALACIÓN DE ENDIAN

Inicialmente, se procede a la obtención de la ultims versión de Endian Firewall Community desde su sitio web oficial. Posteriormente, la instalación del sistema se realiza en un entorno virtualizado, empleando para ello la plataforma Oracle VM VirtualBox.

2.1 REQUISITOS PREVIOS

- Hipervisor: Oracle VM VirtualBox
- Sistema: Endian Firewall Community
- Memoria: 2048 MB de RAM
- Disco duro virtual: 20 GB

Figura 1. Creación de la máquina virtual.

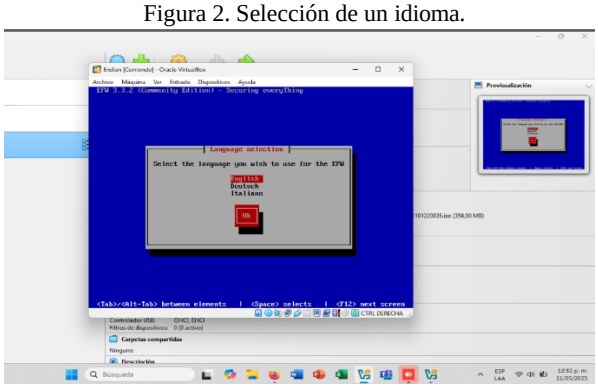


Fuente: Autoría Propia.

Antes de iniciar el proceso de instalación, se prepara el entorno de hardware (ver Figura 1).

2.2 PROCESO DE INSTALACIÓN

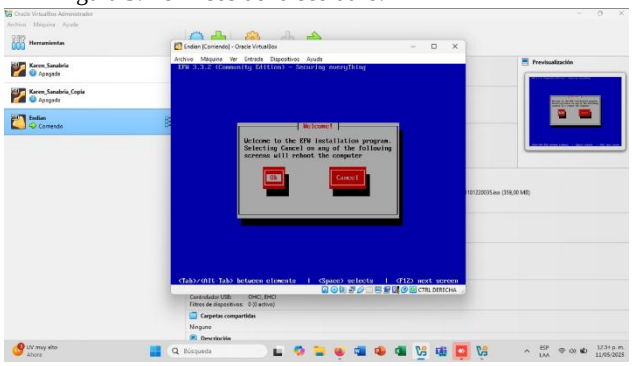
Figura 2. Selección de un idioma.



Fuente: Autoría Propia.

Al iniciar el medio de instalación, se presenta una interfaz para la selección del idioma del entorno (ver Figura 2).

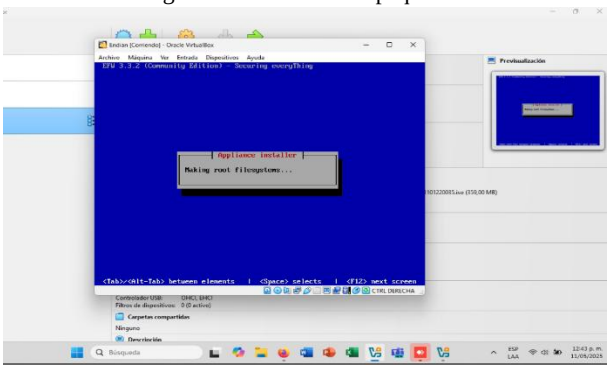
Figura 3. Permisos del disco duro.



Fuente: Autoría Propia.

Se procede con la creación de la partición y del sistemas de archivos en el disco duro seleccionado. En este proceso, se eliminan todos los datos previamente almacenados (ver Figura 3).

Figura 4. Instalación de paquetes.

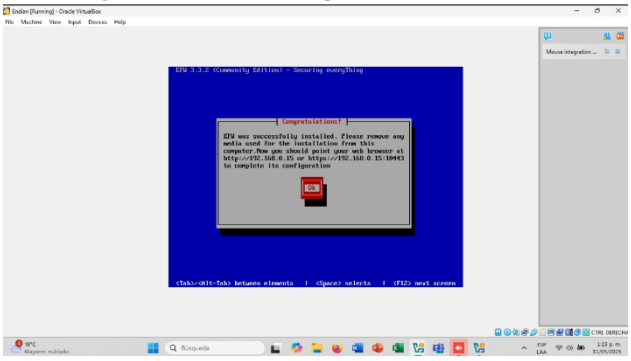


Fuente: Autoría Propia.

Se ejecuta la replicación y extracción de los paquetes fundamentales del sistema, que comprenden los módulos de red, el subsistema de administración web y los servicios críticos, tales como proxy HTTP, firewall, antivirus y filtrado de contenido, entre otros (ver Figura 4).

Figura 5. Configuración de la ip red Green.

Figura 6. Instalación completada exitosamente.



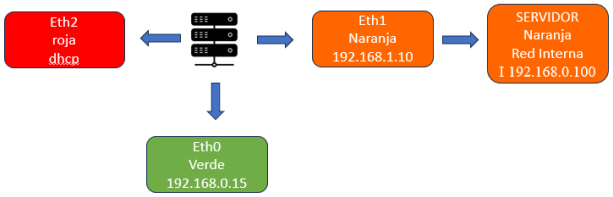
Fuente: Autoría Propia.

Tras finalizar la instalación de los paquetes, se presenta la dirección IP asignada, a través de la cual es posible acceder al sistema mediante los protocolos HTTP o HTTPS para completar la configuración de Endian desde un dispositivo conectado a la misma red. (ver Figura 5), (ver Figura 6).

3 TEMÁTICA 1 CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN

Se procede a configurar el segundo adaptador de red en Endian en modo 'red interna', destinado a la zona NARANJA (DMZ) (ver Figura 9).

Figura 7. Diagrama de la red.

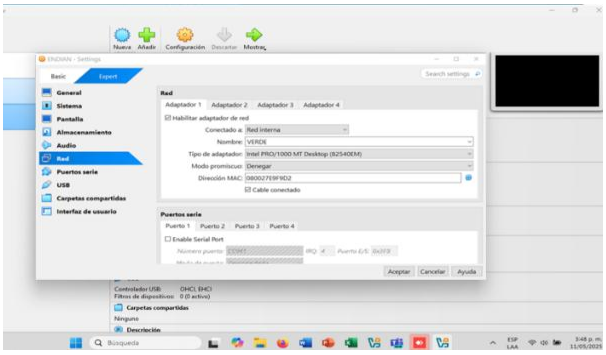


Fuente: Autoría Propia.

Se define el diagrama de direccionamiento IP de toda la red, el cual servirá de base para su configuración y operación (ver Figura 7).

3.1 CONFIGURACIÓN DE ADAPTADORES DE RED EN ENDIAN

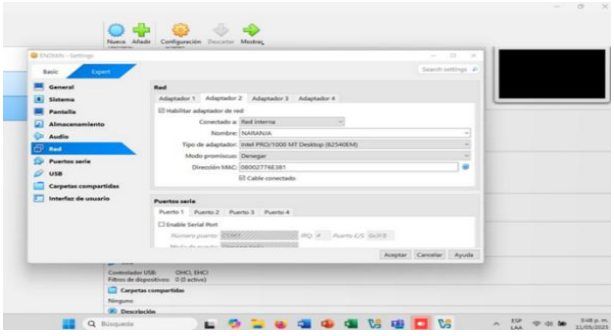
Figura 8. Primer adaptador de red Endian.



Fuente: Autoría Propia.

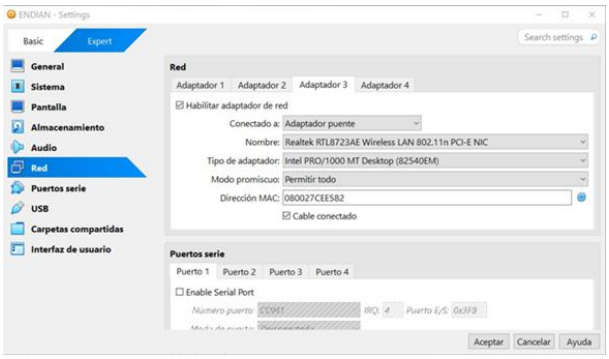
Se configura en Endian el primer adaptador de red como red interna y se utiliza para establecer la zona VERDE (LAN) (ver Figura 8).

Figura 9. Segundo adaptador de red Endian.



Fuente: Autoría Propia.

Figura 10. Tercer adaptador de red Endian.

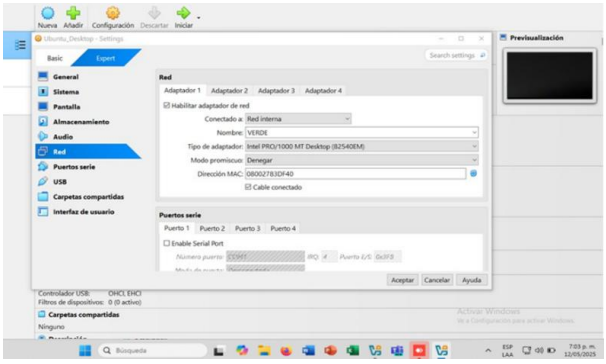


Fuente: Autoría Propia.

El tercer adaptador de red en Endian se configura como adaptador puente (ZONA ROJA) (ver Figura 10).

3.2 CONFIGURACIÓN DE ADAPTADOR DE RED EN UBUNTU DESKTOP

Figura 11. Adaptador de red Ubuntu.



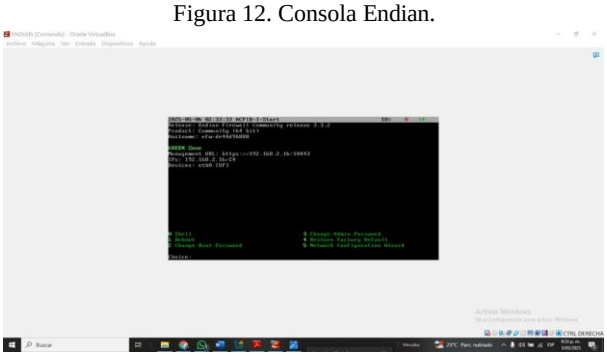
Fuente: Autoría Propia.

Se configura en Ubuntu un adaptador de red, el cual se conecta a la red interna en la zona VERDE (LAN) (ver Figura 11).

Luego, se accede a Ubuntu y, desde la terminal, se modifica el archivo de configuración de red para asignar la dirección IP 192.168.0.15, correspondiente a la zona VERDE (LAN), con una puerta de enlace 192.168.0.1 la cual está conectada al firewall Endian

3.3 CONFIGURACIÓN DE ENDIAN

Figura 12. Consola Endian.

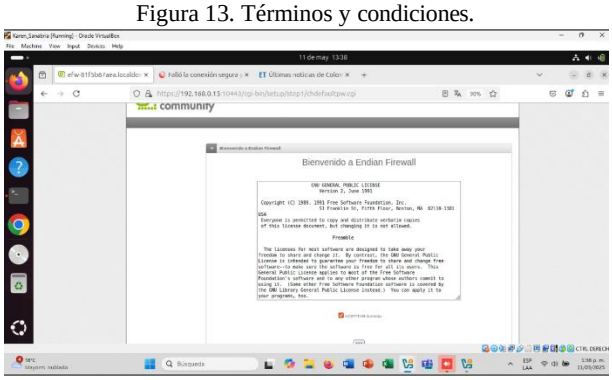


Fuente: Autoría Propia.

El sistema Endian se ejecuta por defecto en modo consola (ver Figura 12), aunque también permite su administración a través de una interfaz gráfica web, accesible desde cualquier dispositivo conectado a la red mediante la dirección IP asignada durante la instalación.

Con el sistema Endian en ejecución, se procede con la configuración inicial accediendo a la dirección web https:// https://192.168.0.15:10443. En esta etapa, se selecciona el idioma de la interfaz gráfica

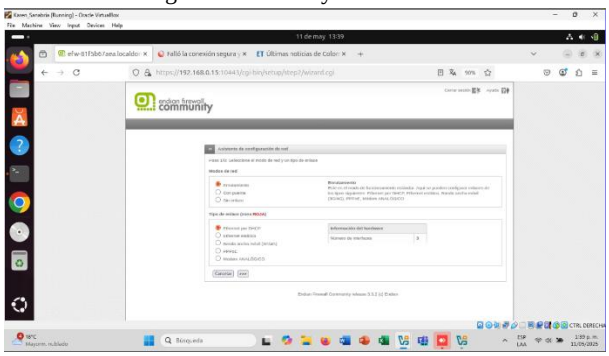
Figura 13. Términos y condiciones.



Fuente: Autoría Propia.

Se aceptan los términos y condiciones de la licencia ofrecidos por Endian (ver Figura 13).

Figura 14. Enlace y modo de red.



Fuente: Autoría Propia.

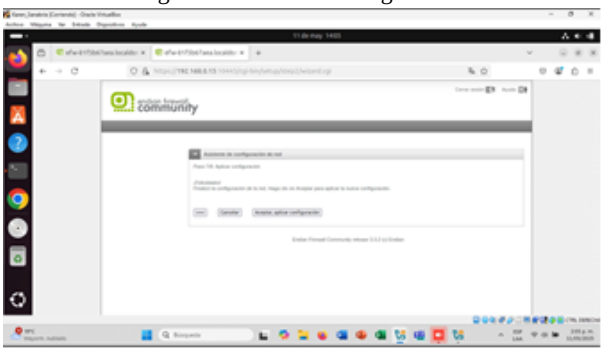
Se selecciona el modo de red Enrutamiento, que corresponde al modo de funcionamiento estándar del firewall. Para la zona ROJA, la conexión se configura mediante asignación dinámica de direcciones IP (DHCP) (ver Figura 14).

Figura 15. Preferencias de red.

Fuente: Autoría Propia.

En el siguiente paso, dentro del apartado de preferencias de red, se configuran las zonas VERDE (LAN) y NARANJA (DMZ), asignando a cada una dirección IP, una máscara de red y su interfaz correspondiente. A la zona VERDE se le asigna la dirección IP 192.168.0.15, y a la zona NARANJA, la dirección IP 192.168.1.10. (ver Figura 15).

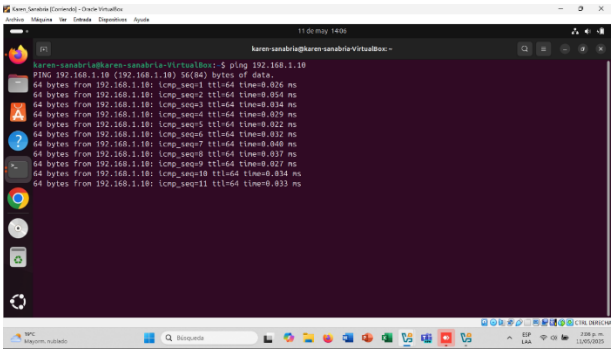
Figura 16. Fin de la configuración.



Fuente: Autoría Propia.

Para finalizar, se aceptan y aplican las configuraciones realizadas (ver Figura 16).

Figura 17. Verificación de conexión.

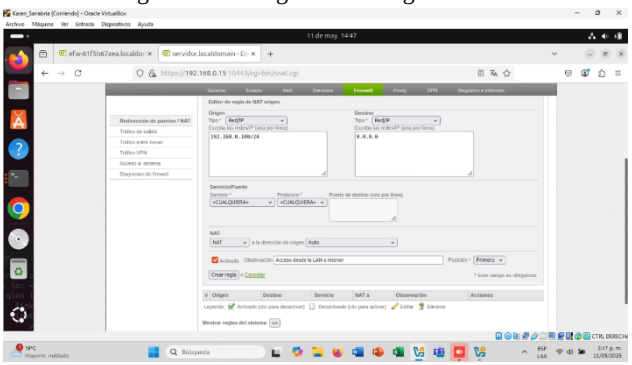


Fuente: Autoría propia.

Se verifica que toda la red esté correctamente configurada y funcionando (ver Figura 17).

4 TEMÁTICA 2 CONFIGURACIÓN NAT

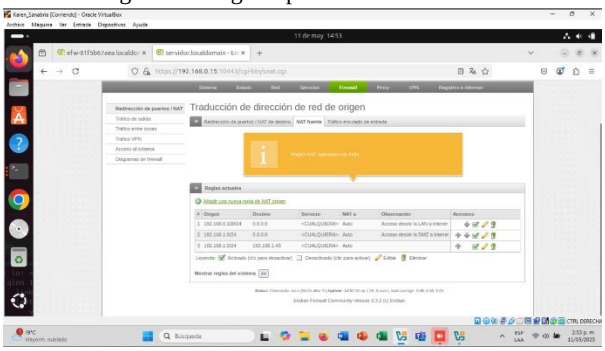
Figura 18. Configurando la regla NAT.



Fuente: Autoría Propia.

Se configura la red NAT de origen accediendo a la interfaz web de Endian. Desde la pestaña 'Firewall', se selecciona la opción 'NAT fuente' y, posteriormente, se elige 'Añadir una nueva regla'. (ver Figura 18).

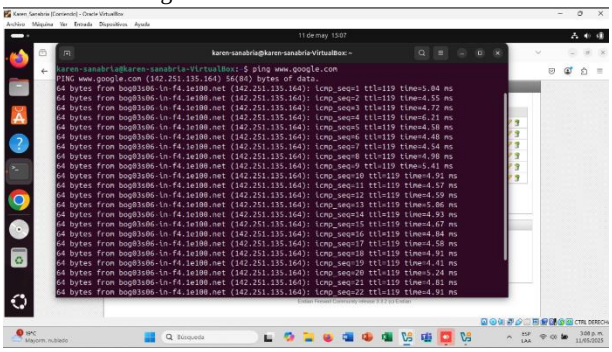
Figura 19. Reglas aplicadas correctamente.



Fuente: Autoría Propia.

se ha aplicado correctamente y ahora aparecen las reglas creadas (ver Figura 19).

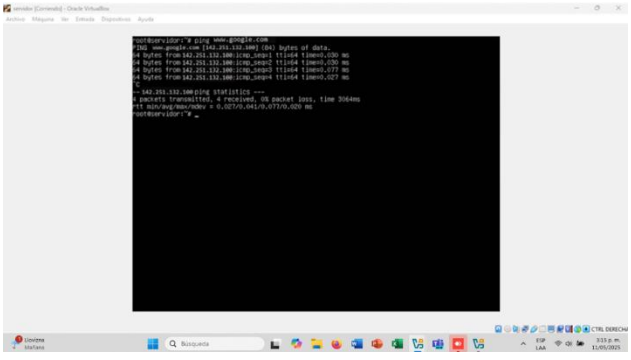
Figura 20. Verificando conexión.



Fuente: Autoría Propia.

Ahora se verifica la conectividad desde la terminal de Ubuntu Server (DMZ) hacia la red roja WAN para probar que el tráfico originado puede alcanzar la red externa; para esto, se ingresa la orden ping www.google.com (ver Figura 20).

Figura 21. Comprobación de salida de internet .

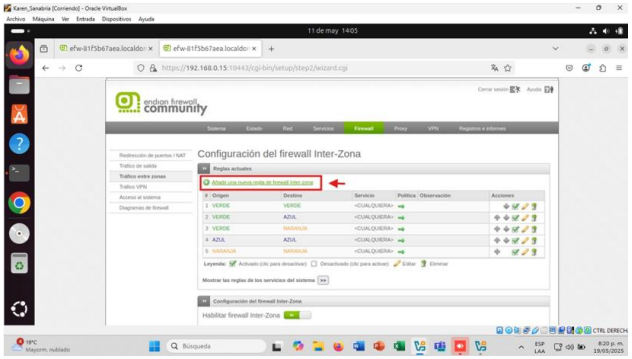


Fuente: Autoría Propia.

Se hace ping desde la terminal del Server Ubuntu en la red Naranja (DMZ) a la red Roja (WAN) para comprobar la conexión a internet a través del DNS de Google 8.8.8.8 (ver Figura 39).

5 TEMÁTICA 3 PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

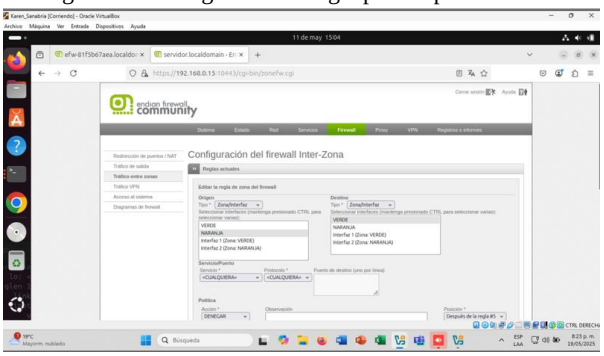
Figura 22. Creación de la regla para el puerto 80.



Fuente: Autoría Propia.

Se configura la primera regla para el puerto 80, ingresando a la interfaz de Endian, desde la pestaña “Firewall” se elige la opción “ Tráfico entre zonas”, luego se selecciona la opción “Añadir una nueva regla” (ver Figura 22).

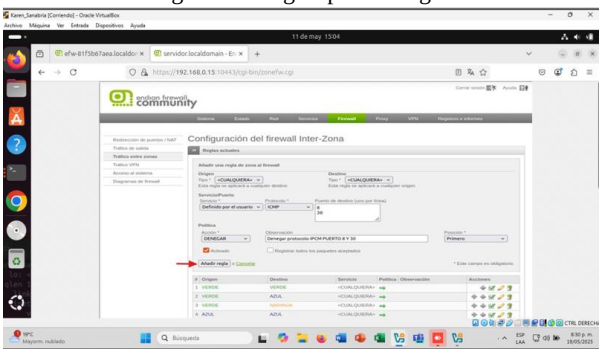
Figura 23. Configurando la regla para el puerto 80.



Fuente: Autoría Propia.

Configuración de reglas de Port Forwarding para permitir el tráfico HTTP (puerto 80) desde la zona LAN hacia la DMZ en el firewall Endian. Al finalizar la configuración, se selecciona la opción 'Crear regla'. (ver Figura 23).

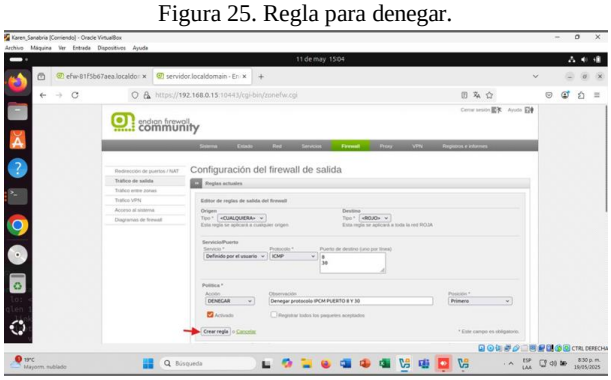
Figura 24. Reglas para denegar.



Fuente: Autoría Propia.

Se configura una nueva regla para denegar el acceso a los puertos 8 y 30. Al finalizar se selecciona la opción “Crear Regla” (ver Figura 24).

Figura 25. Regla para denegar.



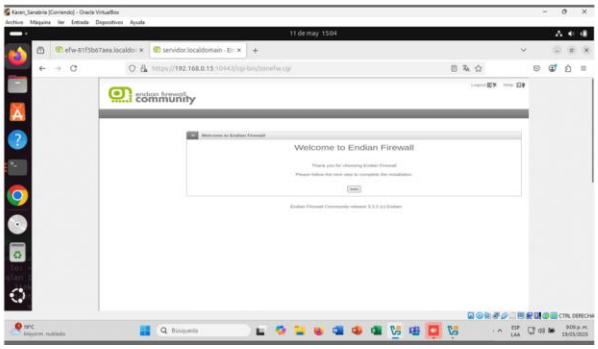
Fuente: Autoría Propia.

Se configura una nueva regla para bloquear el tráfico de salida hacia los puertos 8 y 30, impidiendo así cualquier conexión saliente a través de dichos puertos (ver Figura 25).

Se verifica el funcionamiento del puerto HTTP desde del Desktop ingresando la IP del servidor http://192.168.0.15 comprobando que hay conexión.Se prueba el funcionamiento desde la terminal de Ubuntu ejecutando el comando ping 8.8.8.8 que es la DNS de Google.

6 TEMÁTICA 4 REGLAS DE ACCESO

Figura 26. Verificar en el tráfico Inter-zona, la creación de las reglas.

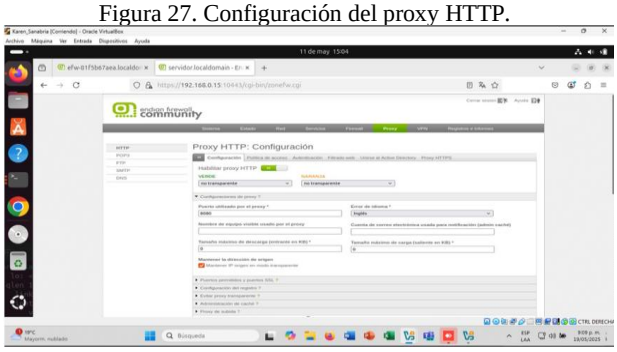


Fuente: Autoría Propia.

En este paso, se realiza la verificación de las reglas de tráfico para asegurar que la red funcione conforme a lo esperado (ver Figura 26).

6.1 CONFIGURACIÓN HTTP

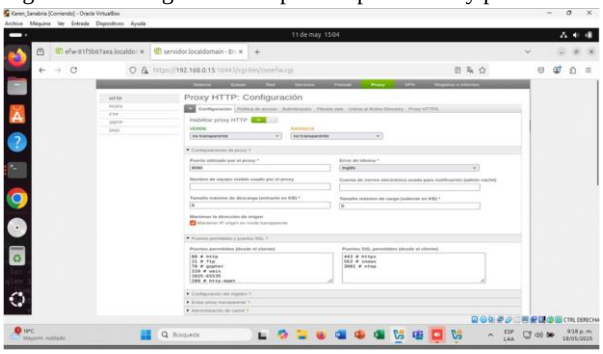
Figura 27. Configuración del proxy HTTP.



Fuente: Autoría Propia.

En esta etapa, se realiza la configuración del proxy, el cual actúa como intermediario entre el cliente y el servidor web. (ver Figura 27).

Figura 28. Configuración de puertos permitidos y puertos SSL.



Fuente: Autoría Propia.

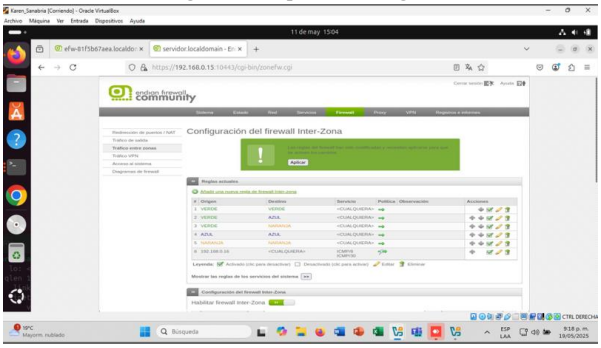
Como se observa en la imagen anterior (ver Figura 28), este procedimiento se realiza con el propósito de controlar el tráfico de red.

Figura 29. Creación de una nueva regla para el firewall de protocolo ICMP.

Fuente: Autoría Propia.

Se configura regla de firewall para permitir o bloquear el tráfico ICMP (ver Figura 29).

Figura 30. Aplicar las reglas.



Fuente: Autoría Propia.

Se procede a aplicar la configuración para activar las reglas de acceso recientemente creadas. (ver Figura 30).

Se configura una regla que permite el acceso al servicio FTP en la zona DMZ, redirigiendo el tráfico desde la WAN hacia la dirección IP interna correspondiente, bajo el control del firewall.

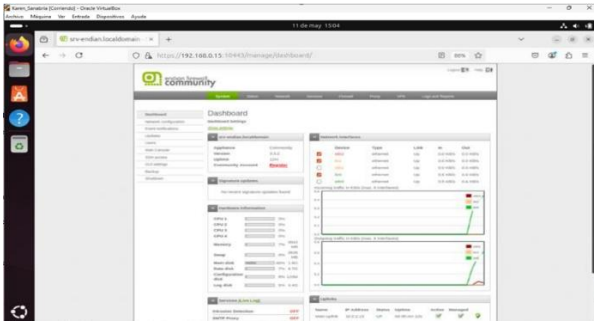
7 TEMÁTICA 5 IMPLEMENTACIÓN DE PROXY HTTP

Un proxy HTTP no transparente requiere que los navegadores de los usuarios estén configurados manualmente para su utilización, ya que no intercepta el tráfico de forma automática. A diferencia del proxy transparente, este tipo ofrece mayores posibilidades de control, como la autenticación de usuarios y la aplicación de políticas avanzadas de acceso.

En esta sección se explica cómo implementar este tipo de proxy en Endian Firewall Community, permitiendo gestionar el acceso a Internet por usuario y restringir dominios específicos.

7.1 FILTRADO WEB

Figura 31. Accediendo al dashboard.



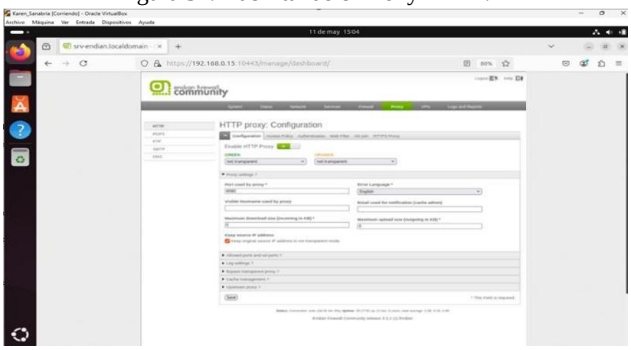
Fuente: Autoría Propia.

Al acceder al dashboard del sistema Endian Firewall Community desde un navegador web mediante la dirección IP local 192.168.0.15, se muestra una visión general del estado del sistema. En esta interfaz se pueden observar estadísticas de tráfico de red, uso de CPU y memoria, eventos de seguridad recientes, así como información del sistema y del estado de los servicios. Esta vista centralizada permite al administrador monitorear y gestionar de manera eficiente el comportamiento del firewall y la red en tiempo real. (Ver Figura 31).

7.2 POLÍTICAS DE ACCESO

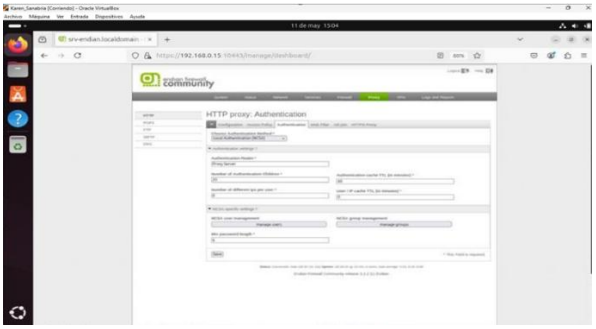
El servidor proxy actúa como un filtro que aplica políticas de acceso, sólo permite navegar a usuarios que cumplen ciertos requisitos como el autenticarse con usuario y contraseña o tener permisos para el acceso a determinados sitios web.

Figura 32. Habilitando el Proxy HTTP.



Fuente: Autoría Propia.

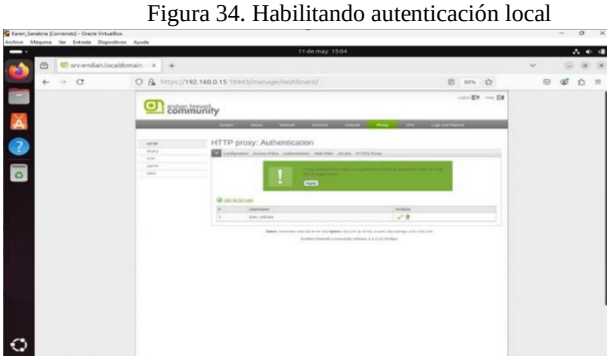
Figura 33. Habilitando el Proxy HTTP.



Fuente: Autoría Propia.

Desde la interfaz web de Endian Firewall, se habilita el proxy HTTP en la sección de autenticación, permitiendo controlar el acceso a Internet mediante usuarios autenticados. (ver Figura 33)

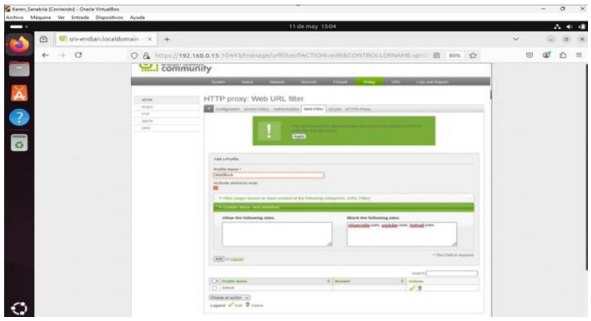
Figura 34. Habilitando autenticación local



Fuente: Autoría Propia.

Se habilita la autenticación local en el proxy HTTP de Endian Firewall, lo que permite controlar el acceso a Internet solicitando usuario y contraseña guardados en el sistema. (ver Figura 34).

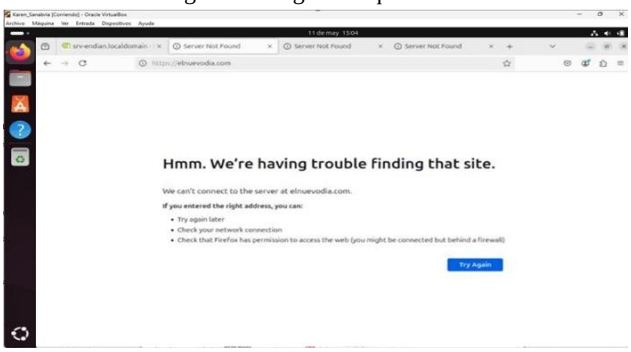
Figura 35. Creando Usuarios



Fuente: Autoría Propia.

Se configura una regla de filtrado por URL en Endian Firewall para bloquear o permitir el acceso a sitios web específicos desde el proxy HTTP (ver Figura 35).

Figura 36. Página bloqueada.



Fuente: Autoría Propia.

Se muestra un mensaje de error al intentar acceder a un sitio web, indicando que el servidor no se encuentra disponible. Esto puede deberse a que el acceso fue bloqueado por el proxy configurado en Endian Firewall. (ver Figura 36).

9. CONCLUSIONES

La implementación de una arquitectura de red segmentada con Endian Firewall Community demostró ser una solución eficaz y accesible para fortalecer la seguridad perimetral en entornos GNU/Linux. Al definir correctamente las zonas LAN, WAN y DMZ, y asignar IPs estáticas, se logró una infraestructura ordenada que facilita el monitoreo y control del tráfico.

Se configuraron reglas NAT para optimizar la comunicación entre redes sin comprometer la seguridad, además de políticas de filtrado que combinaron accesos permitidos y restricciones específicas. Desde la interfaz web se habilitaron servicios hacia la DMZ, como HTTP (puerto 80) y FTP (puerto 21), y se denegó el tráfico ICMP.

Las reglas de firewall permitieron controlar el flujo de red, habilitando o bloqueando el acceso según origen, destino o servicio. Por ejemplo, se creó una regla para permitir el acceso a un enlace activo desde la zona WAN con servicio FTP.

Finalmente, la configuración de un proxy HTTP no transparente permitió controlar el acceso a Internet dentro de la red interna, aplicando listas negras para bloquear sitios web específicos, reforzando así el control y la seguridad de navegación.

10. REFERENCIAS

[1] Endian. (n.d.). *Endian UTM 3.2 Reference Manual*. docs.endian.com. https://docs.endian.com/3.2/utm/index.html

[2] Lopez, J. S. M., Galvis, R. S., & Diaz, A. F. A. (n.d.). IMPLEMENTACIÓN DE SERVICIOS IT EN ZENTYAL SERVER. Edu.Co. Retrieved May 12, 2025, from https://repository.unad.edu.co/bitstream/handle/10596/49417/jsmejial.pdf?sequence=1&isAllowed=y

[3] R. Kurose and K. Ross, COmputer Networking: A Top-Down Approach, 7th ed. Bostos: Pearson, 2017.

[4] What is a Proxy Server, Definition How it Work & More. Digital Guardia. 2022 from https://www.digitalguardian.com/blog/what-proxy-server-definition-how-it-works-more

[5] Canonical. (2023). Guía del Ubuntu desktop 20.04 LTS. Help Ubuntu. https://help.ubuntu.com/20.04/ubuntu-help/index.html

[6] Configuring networks. (n.d.). Ubuntu Server. https://documentation.ubuntu.com/server/explanation/networking/configuring-networks/index.html

[7] Koromicha. (2024, July 25). Install and configure Endian Firewall on VirtualBox - Kifarunix.com. kifarunix.com. https://kifarunix.com/install-and-configure-endian-firewall-on-virtualbox/

[8] Fredysyw. (n.d.). Configuración de Firewall en Endian. Scribd. https://es.scribd.com/document/96063735/Configuracion-de-Firewall-en-Endian

[9] InfoRed. (2019, 9 de febrero). Cómo Configurar Endian Firewall Paso a Paso Parte 3 [Video]. YouTube. www.youtube.com/watch?v=oeDawngVv6g

[10] ¿Qué es ICMP? Explicación del protocolo ICMP - AWS. (n.d.). Amazon Web Services, Inc. https://aws.amazon.com/es/what-is/icmp/