IMPLEMENTACIÓN Y EVALUACIÓN DE UNA ARQUITECTURA DE SEGURIDAD BASADA EN DMZ UTILIZANDO ENDIAN FIREWALL EN GNU/LINUX: UN ESTUDIO DE CASO SOBRE SEGMENTACIÓN DE RED Y CONTROL DE ACCESO

Daniela Alexandra Ordoñez Betancour
daordonezb@unadvirtual.ecu.co
Jeyson Fernando Nieto Roldán
jfnietor@unadvirtual.edu.co
Leder Ramos Sanchez
lramossan@unadvirtual.edu.co
Marleny Marcela Toro Zambrano
mmtoroz@unadvirtual.edu.co
Natalia Yamileth Rodriguez Solarte
nyrodriguezso@unadvirtual.edu.co

ABSTRACT: *This article documents the implementation of perimeter security in GNU/Linux using Endian Firewall (EFW), developed as a collaborative project. We addressed five key aspects: 1) Configuration of LAN/WAN/DMZ zones in VirtualBox; 2) NAT rules for bidirectional communication; 3) Service management (HTTP/FTP) with ICMP blocking; 4) Inter-zone filtering; and 5) HTTP proxy with authentication and blacklists. The Command Line Interface (CLI) methodology demonstrated EFW's effectiveness in isolating critical services in the DMZ, controlling access via NAT/proxy, and validating communications through technical tests. Our results offer a replicable model for educational environments and SMEs, integrating open-source tools (GNU/Linux, Endian) with best security practices. This study evidences that network segmentation and granular filtering are essential for mitigating external threats.*

KEYWORDS: DMZ**,** Endian Firewall, NAT, Perimeter security, GNU/Linux.

RESUMEN: *Este artículo documenta la implementación de seguridad perimetral en GNU/Linux usando Endian Firewall (EFW), desarrollado como proyecto colaborativo. Se abordaron cinco aspectos: 1) Configuración de zonas LAN/WAN/DMZ en VirtualBox; 2) Reglas NAT para comunicación bidireccional; 3) Gestión de servicios (HTTP/FTP) con bloqueo ICMP; 4) Filtrado inter-zonas; y 5) Proxy HTTP con autenticación y listas negras. La metodología CLI demostró la eficacia de EFW para aislar servicios críticos en DMZ, controlar accesos mediante NAT/proxy, y validar comunicaciones mediante pruebas técnicas. Los resultados ofrecen un modelo replicable para entornos educativos y PYMES, integrando herramientas open-source (GNU/Linux, Endian) con mejores prácticas de seguridad. El estudio evidencia que la segmentación de red y filtrado granular son esenciales para mitigar amenazas externas.*

PALABRAS CLAVE: DMZ, Endian Firewall, NAT, Seguridad perimetral, GNU/Linux.

1 INTRODUCCIÓN

En el actual panorama tecnológico, la seguridad informática constituye un pilar fundamental para la protección de la integridad, disponibilidad y confidencialidad de los sistemas de información. En este contexto, se presenta la implementación y evaluación de una arquitectura de seguridad basada en DMZ utilizando Endian Firewall Community sobre entornos GNU/Linux, bajo un enfoque práctico y replicable. A través de un estudio de caso desarrollado en un entorno virtualizado, se aborda la configuración de zonas de red (LAN, WAN y DMZ), la aplicación de reglas NAT y políticas de cortafuegos, así como la gestión de servicios web y FTP desde la DMZ. Además, se incluye la implementación de un proxy HTTP con autenticación y listas negras como mecanismo de control de navegación. La metodología empleada combina el uso de la interfaz web de Endian y comandos desde la línea de comandos (CLI), con el objetivo de validar la efectividad de los controles de seguridad aplicados.

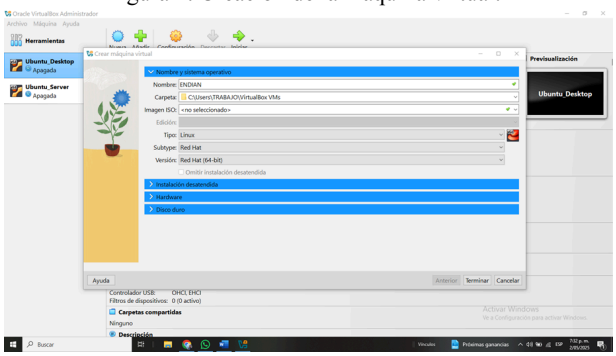
2 INSTALACIÓN DE ENDIAN

En primer lugar se descarga el sistema Endian Firewall Community en su versión 3.3.2, desde su página oficial y posteriormente se instala el sistema en un entorno virtualizado utilizando el programa 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.

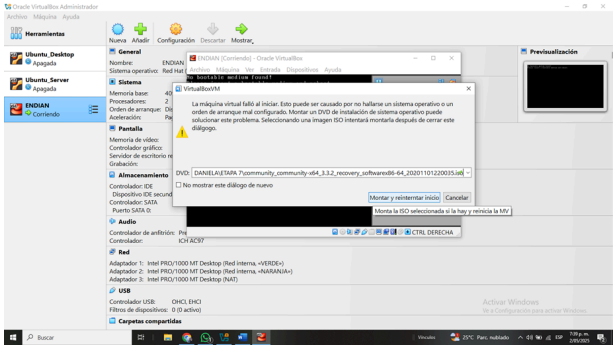


Fuente: Autoría Propia.

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

2.2 PROCESO DE INSTALACIÓN

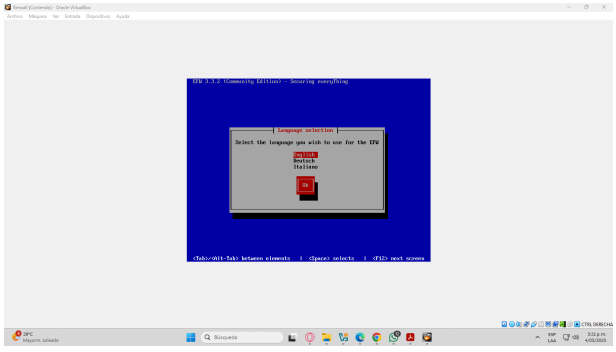
Figura 2. Selección de imagen ISO Endian.



Fuente: Autoría Propia.

Se inicia la máquina virtual creada y se selecciona la imagen ISO de Endian descargada (ver Figura 2).

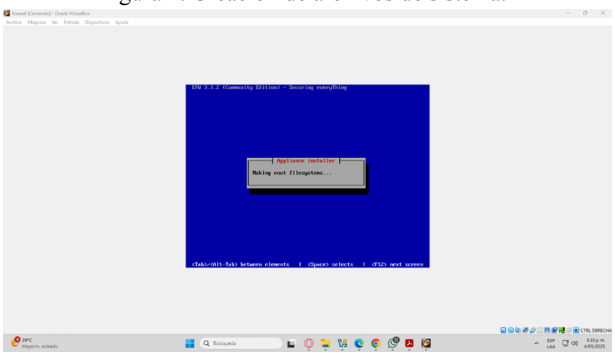
Figura 3. Selección de un idioma.



Fuente: Autoría Propia.

Al iniciar el medio de instalación, se presenta una interfaz para la selección del idioma del entorno (ver Figura 3).

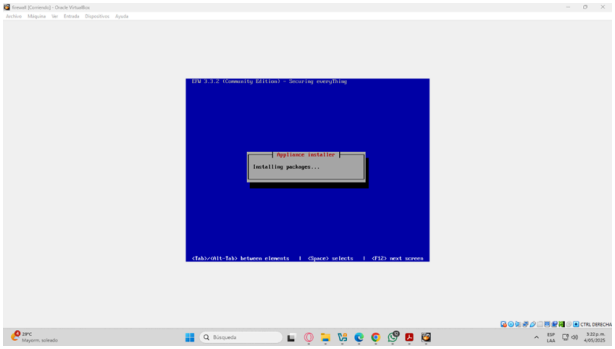
Figura 4. Creación de archivos de sistema.



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 4).

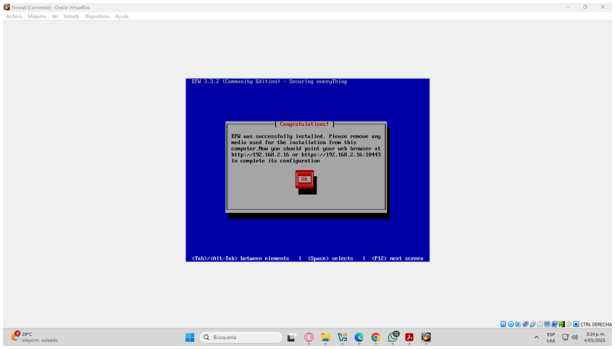
Figura 5. Instalación de paquetes.



Fuente: Autoría Propia.

Se realiza la copia y descompresión de los paquetes esenciales del sistema, incluyendo los módulos de red, el sistema de administración web y servicios esenciales como proxy, firewall, antivirus, filtrado de contenido, entre otros (ver Figura 5).

Figura 6. Instalación completada exitosamente.

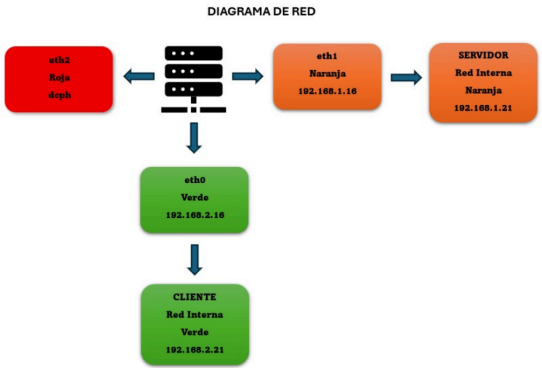


Fuente: Autoría Propia.

Una vez completada la instalación de los paquetes, se muestra la dirección IP a través de la cual se puede acceder mediante HTTP o HTTPS para finalizar la configuración de Endian desde un equipo conectado a la misma red (ver Figura 6).

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

Figura 7. Diagrama de la red.

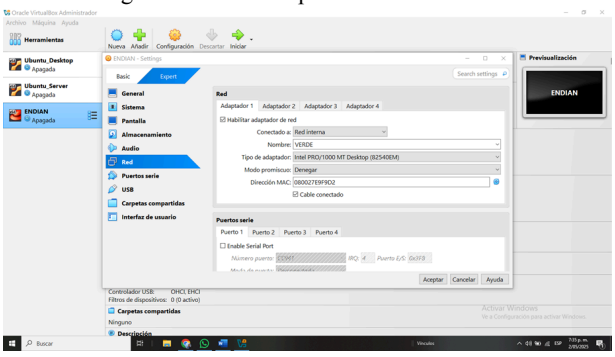


Fuente: Autoría Propia.

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

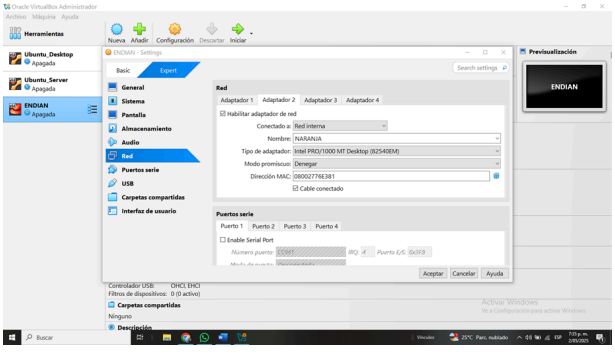
Figura 8. Primer adaptador de red Endian.



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).

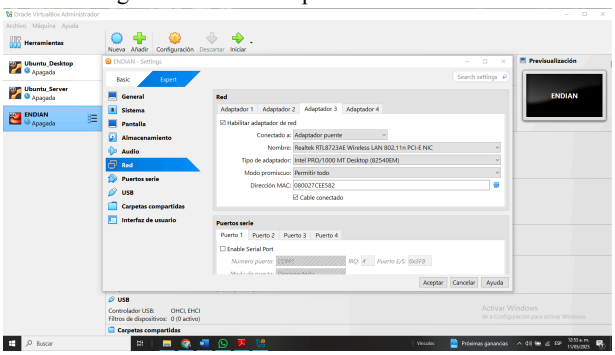
Figura 9. Segundo adaptador de red Endian.



Fuente: Autoría Propia.

Ahora se configura el segundo adaptador de red en Endian también como red interna, y en este caso se utiliza para establecer la zona NARANJA (DMZ) (ver Figura 9).

Figura 10. Tercer adaptador de red Endian.

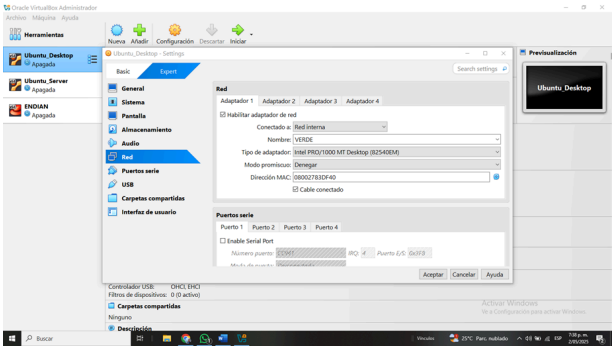


Fuente: Autoría Propia.

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

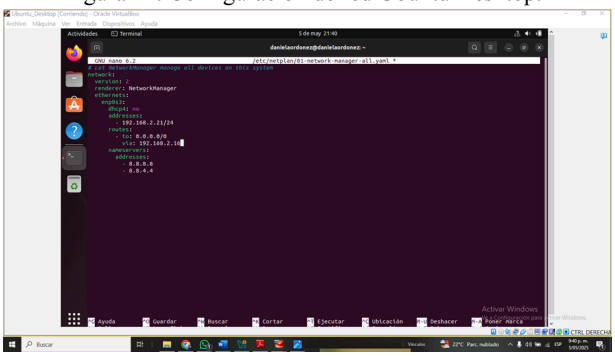
Figura 11. Adaptador de red Ubuntu Desktop.



Fuente: Autoría Propia.

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

Figura 12. Configuración de red Ubuntu Desktop.



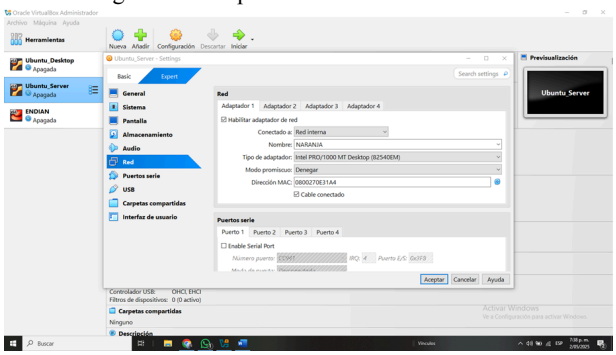
Fuente: Autoría Propia.

Luego, se accede a Ubuntu Desktop y, desde la terminal, se modifica el archivo de configuración de la red para asignar

la dirección IP 192.168.2.21/24 correspondiente a la zona VERDE (LAN), con una puerta de enlace (192.168.2.16) que apunta al firewall Endian (ver Figura 12).

3.3 CONFIGURACIÓN DE ADAPTADOR DE RED EN UBUNTU SERVER

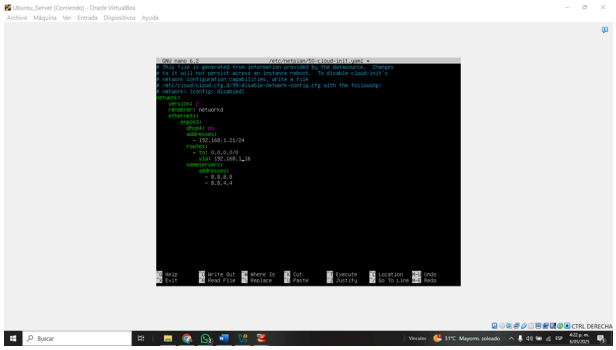
Figura 13. Adaptador de red Ubuntu Server.



Fuente: Autoría Propia.

Se configura en ubuntu server un adaptador de red como red interna, el cual se conecta a la zona NARANJA (DMZ) (ver Figura 13).

Figura 14. Configuración de red Ubuntu Server.

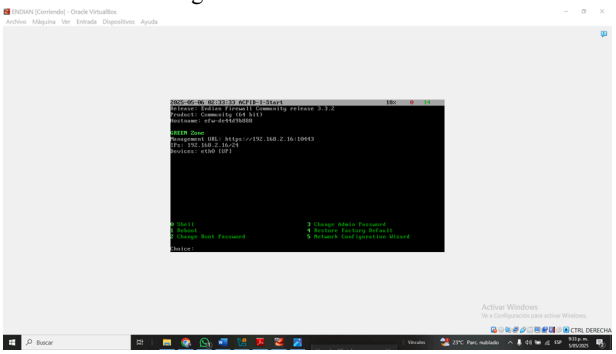


Fuente: Autoría Propia.

Luego, se accede a Ubuntu Server y, desde la terminal, se modifica también el archivo de configuración de la red para asignar la dirección IP 192.168.1.21/24 correspondiente a la zona NARANJA (DMZ), con una puerta de enlace (192.168.1.16) que apunta al firewall Endian (ver Figura 14).

3.4 CONFIGURACIÓN DE ENDIAN

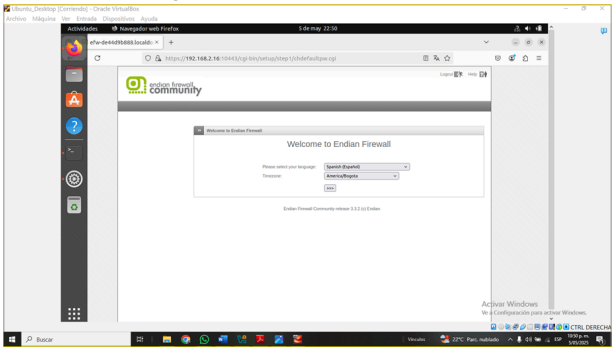
Figura 15. Consola Endian.



Fuente: Autoría Propia.

El sistema Endian se ejecuta de forma predeterminada en modo consola (ver Figura 15), pero 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.

Figura 16. Selección de idioma.



Fuente: Autoría Propia.

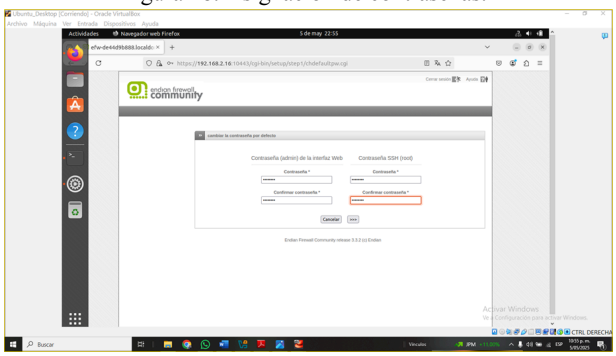
Con el sistema Endian en ejecución, se procede con la configuración inicial accediendo a la dirección web https://192.168.2.16:10443. En esta etapa, se selecciona el idioma de la interfaz gráfica (ver Figura 16).

Figura 17. Términos y condiciones.

Fuente: Autoría Propia.

Se aceptan los términos y condiciones de la licencia ofrecidos por Endian (ver Figura 17).

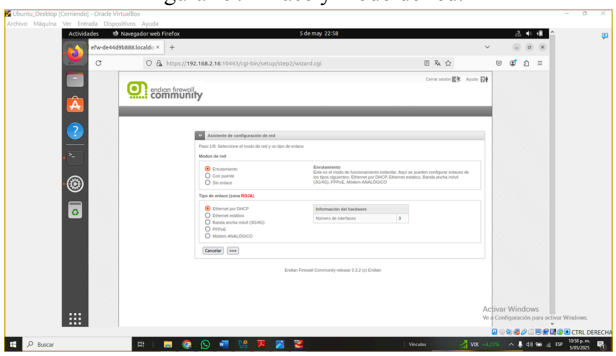
Figura 18. Asignación de contraseñas.



Fuente: Autoría Propia.

Se asignan las contraseñas para la administración del firewall (ver Figura 18).

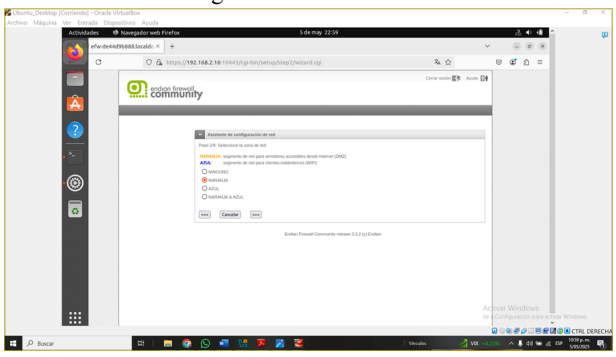
Figura 19. Enlace y modo de red.



Fuente: Autoría Propia.

El modo de red que se selecciona es Enrutamiento, el cual es un modo de funcionamiento estándar en el firewall. En cuanto a la zona ROJA, se configura el enlace mediante asignación DHCP (ver Figura 19).

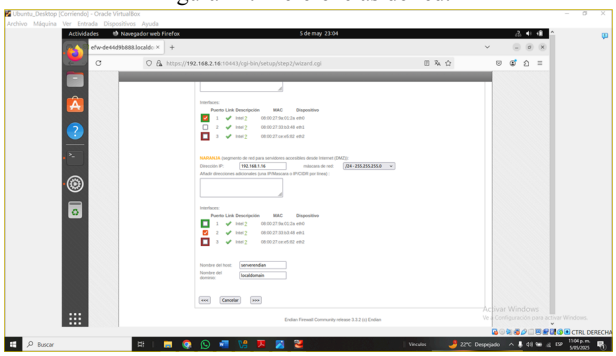
Figura 20. Zona de red.



Fuente: Autoría Propia.

Una vez seleccionado el enlace y modo de red, se procede a seleccionar la zona de red. En este caso se selecciona la zona NARANJA, la cual representa el segmento de red para servidores accesibles desde internet (DMZ) (ver Figura 20).

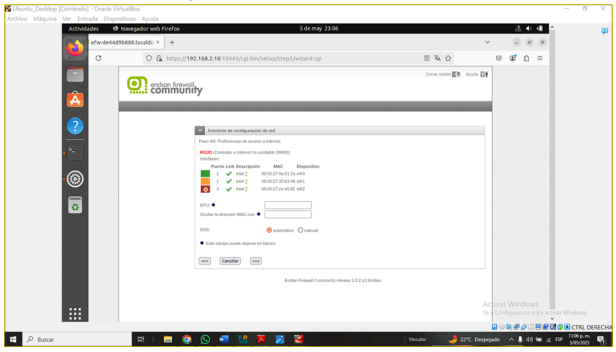
Figura 21. Preferencias de red.



Fuente: Autoría Propia.

En el siguiente paso, dentro del apartado de las preferencias de red, se configuran las zonas VERDE (LAN) y NARANJA (DMZ), donde a cada una se le asigna una dirección IP, una máscara de red y su interfaz correspondiente. Para la zona VERDE se asigna la dirección IP 192.168.2.16 y para la zona NARANJA la dirección IP 192.168.1.16 (ver Figura 21).

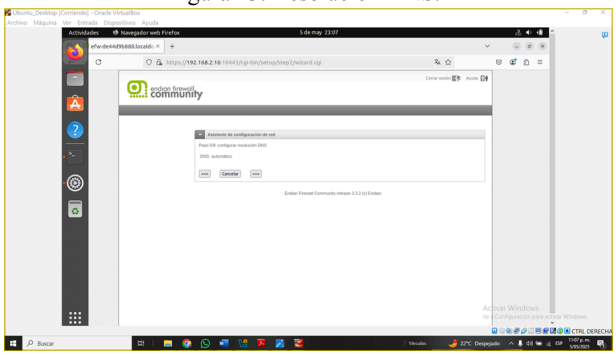
Figura 22. Acceso a internet.



Fuente: Autoría Propia.

Siguiendo con la configuración, se llega al apartado de la preferencia de acceso a internet, el cual corresponde a la zona ROJA (WAN) asignada a la interfaz eth2 (ver Figura 22).

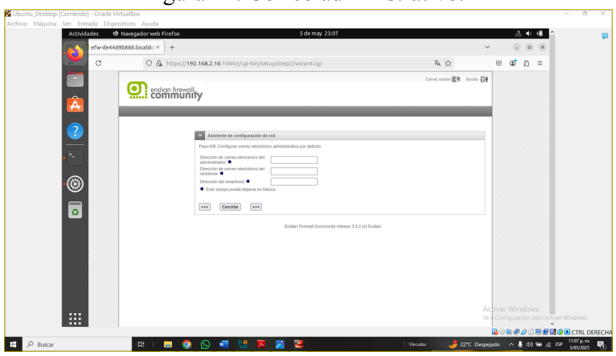
Figura 23. Resolución DNS.



Fuente: Autoría Propia.

Hasta este punto, ya se ha configurado lo más importante del sistema Endian. Ahora se procede a definir la configuración del DNS en modo automático (ver Figura 23).

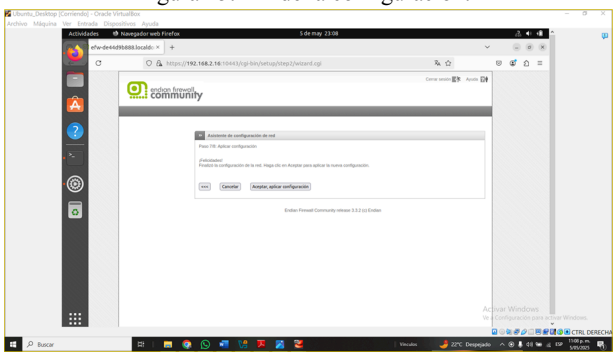
Figura 24. Correo administrativo.



Fuente: Autoría Propia.

Opcionalmente, se puede configurar un correo electrónico administrativo (ver Figura 24).

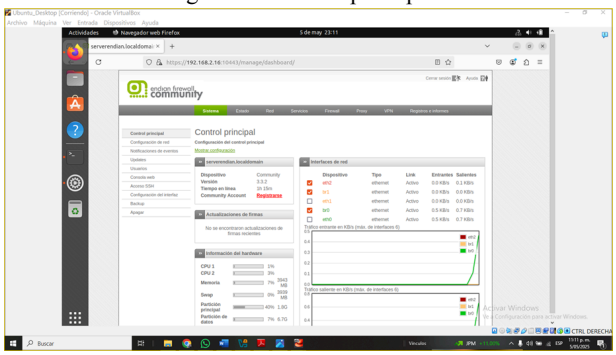
Figura 25. Fin de la configuración.



Fuente: Autoría Propia.

Para finalizar, se aceptan y aplican las configuraciones realizadas (ver Figura 25).

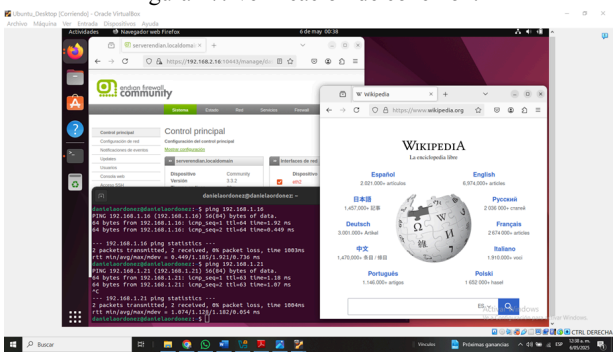
Figura 26. Control principal.



Fuente: Autoría propia.

Una vez finalizada la configuración del sistema de Endian, se inicia sesión con las credenciales del usuario administrador para ingresar a la interfaz principal de control, donde se muestra información relevante como las interfaces de red, información de hardware, versión del sistema, tiempo en línea, entre otros (ver Figura 26).

Figura 27. Verificación de conexión.

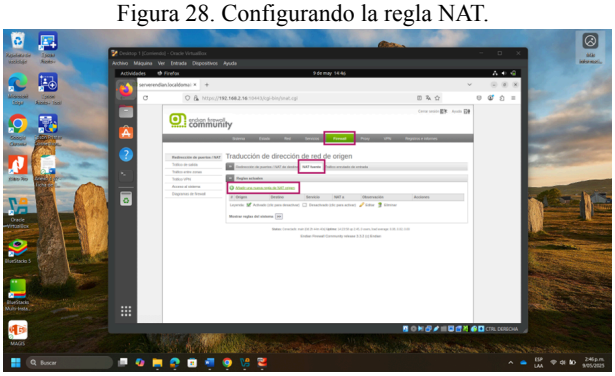


Fuente: Autoría propia.

Se verifica que toda la red esté correctamente configurada y funcionando (ver Figura 27).

4 TEMÁTICA 2 CONFIGURACIÓN NAT

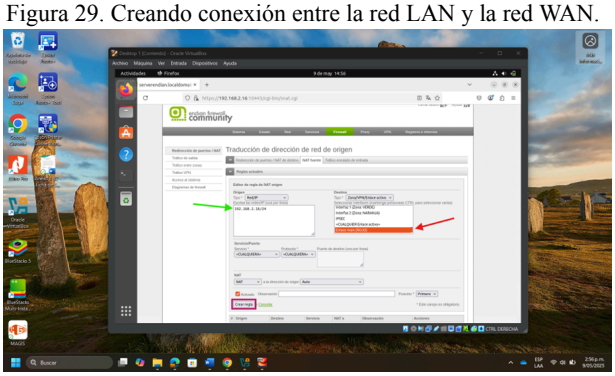
Figura 28. Configurando la regla NAT.



Fuente: Autoría Propia.

Se configura la red NAT fuente ingresando a la interfaz de Endian, desde la pestaña “Cortafuegos” se elige la opción “NAT fuente”, luego se selecciona la opción “Añadir una nueva regla” (ver Figura 28).

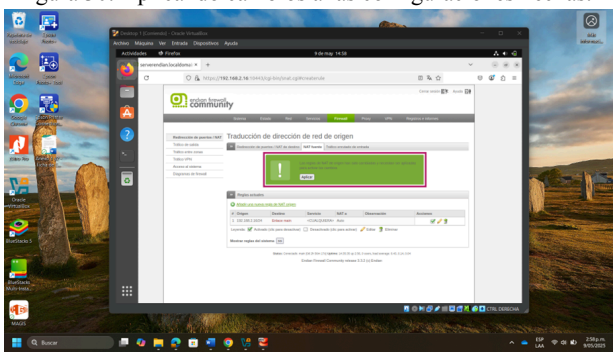
Figura 29. Creando conexión entre la red LAN y la red WAN.



Fuente: Autoría Propia.

Ahora se configura la conexión entre la zona verde (LAN) y la zona roja (WAN). Al finalizar se selecciona la opción “Crear Regla” (ver Figura 29).

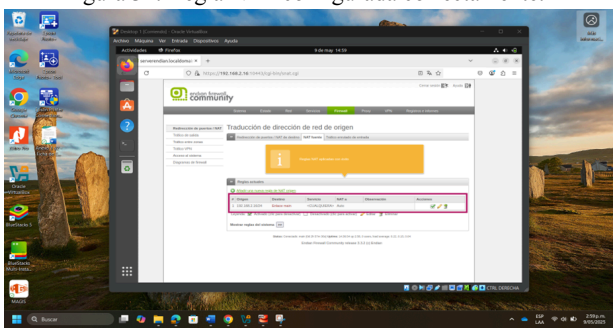
Figura 30. Aplicando cambios a las configuraciones hechas.



Fuente: Autoría Propia.

Como se han hecho configuraciones, se deben aplicar cambios para activarlos (ver Figura 30).

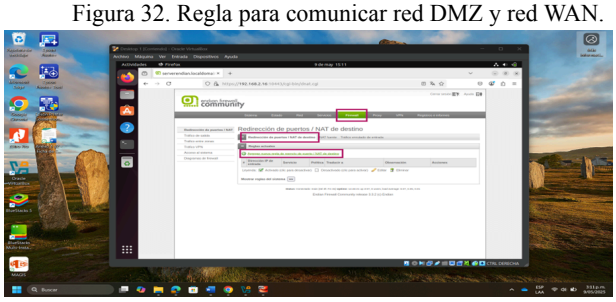
Figura 31. Regla NAT configurada correctamente.



Fuente: Autoría Propia.

Se observa que la regla NAT se ha configurado y aplicado con éxito (ver Figura 31).

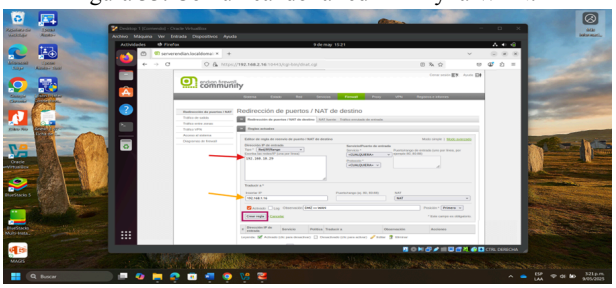
Figura 32. Regla para comunicar red DMZ y red WAN.



Fuente: Autoría Propia.

Para crear la regla, se sigue la siguiente ruta: Firewall / "Redirección de puertos / NAT" / Agregar nueva regla de reenvío de puerto/NAT (ver Figura 32).

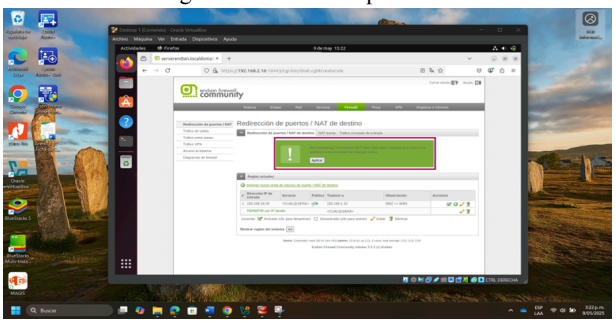
Figura 33. Comunicando la red DMZ y la WAN.



Fuente: Autoría Propia.

Se configura la conexión entre la zona naranja cuya IP es 192.168.1.16, y la zona roja (WAN) cuya IP es la 192.168.18.29. Al finalizar se selecciona la opción "Crear Regla" (ver Figura 33).

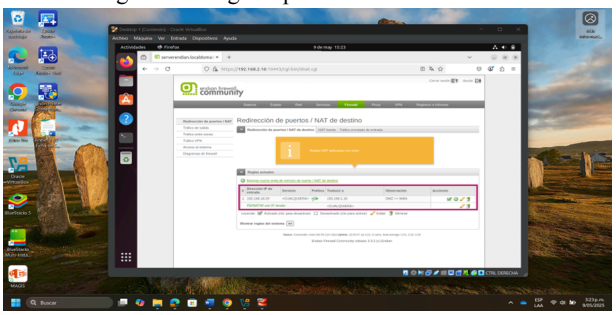
Figura 34. Cambios aplicados.



Fuente: Autoría Propia.

Como se han realizado configuraciones, se deben aplicar cambios. Clic en "Aplicar" (ver Figura 34).

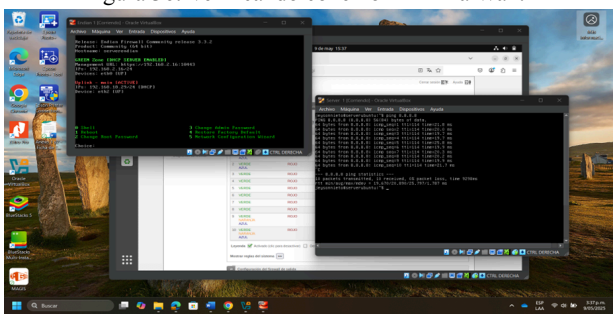
Figura 35. Reglas aplicadas correctamente.



Fuente: Autoría Propia.

Se observa que la regla se ha aplicado correctamente y ahora aparecen las dos reglas creadas anteriormente (ver Figura 35).

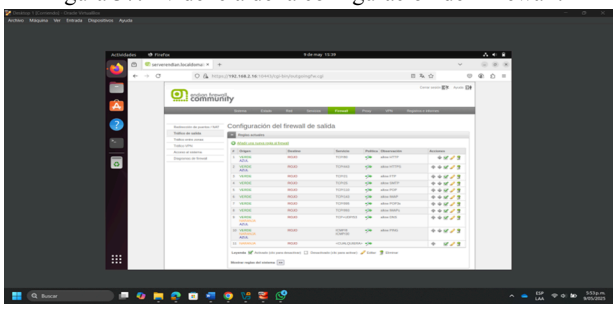
Figura 36. Verificando conexión DMZ a Wan.



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 8.8.8.8 (DNS de Google) (ver Figura 36).

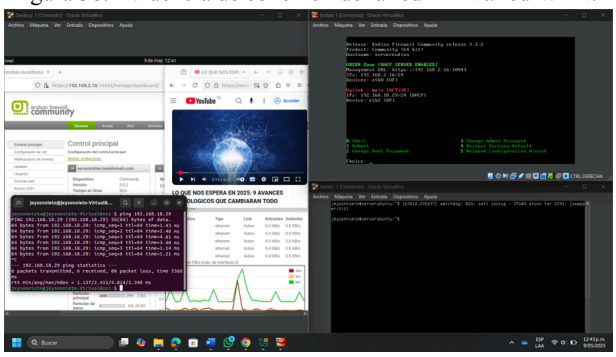
Figura 37. Evidencia de la configuración del Firewall.



Fuente: Autoría Propia.

Se comparte la configuración del Firewall de salida (ver Figura 37).

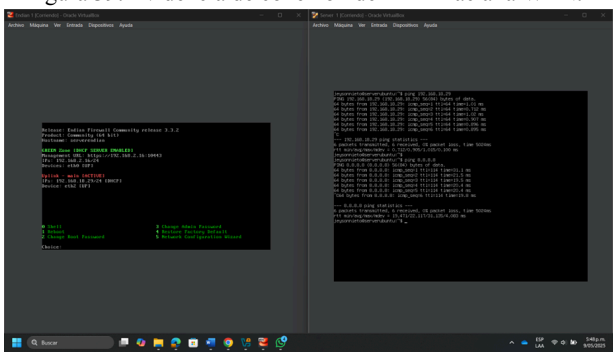
Figura 38. Evidencia de conexión de la red LAN a red WAN.



Fuente: Autoría Propia.

Prueba de conexión desde el Desktop en la red LAN a una IP pública, en este caso haciendo ping a la dirección IP 192.168.18.29, que es el host simulado de internet y abriendo una página web para acceder a internet (ver Figura 38).

Figura 39. Evidencia de conexión de DMZ hacia la WAN.

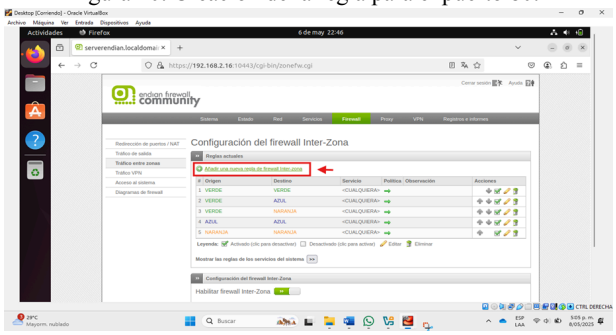


Fuente: Autoría Propia.

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

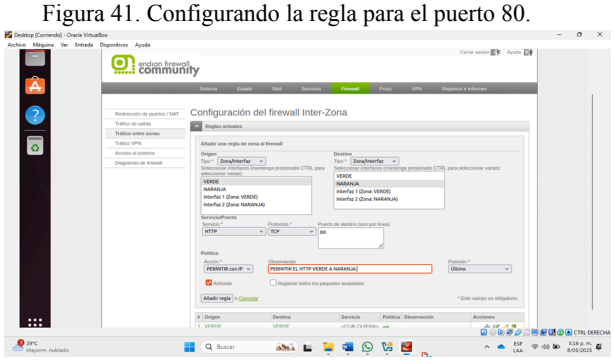
Figura 40. Creación de la regla para el puerto 80.



Fuente: Autoría Propia.

Se configura la primera regla para el puerto 80, ingresando a la interfaz de Endian, desde la pestaña “Cortafuegos” se elige la opción “ Tráfico entre zonas”, luego se selecciona la opción “Añadir una nueva regla” (ver Figura 40).

Figura 41. Configurando la regla para el puerto 80.

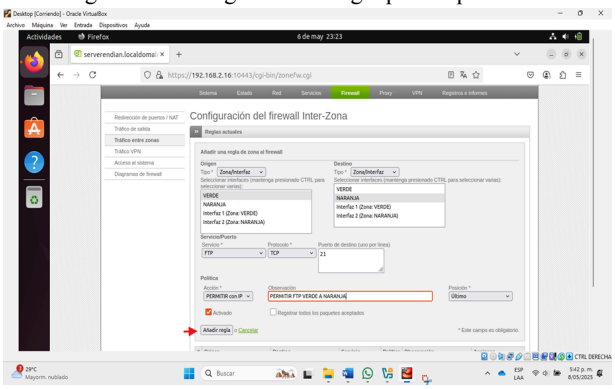


Fuente: Autoría Propia.

Configuración de reglas de Port Forwarding para permitir tráfico HTTP (puerto 80) desde la LAN hacia la DMZ

en un firewall Endian. Al finalizar se selecciona la opción “Crear Regla” (ver Figura 41).

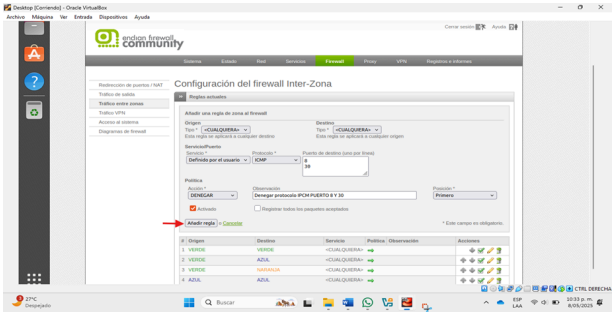
Figura 42. Configurando la regla para el puerto 21.



Fuente: Autoría Propia.

Configuración de reglas de Port Forwarding para permitir tráfico HTTP (puerto 21) desde la LAN hacia DMZ en un firewall Endian. Al finalizar se selecciona la opción “Crear Regla” (ver Figura 42).

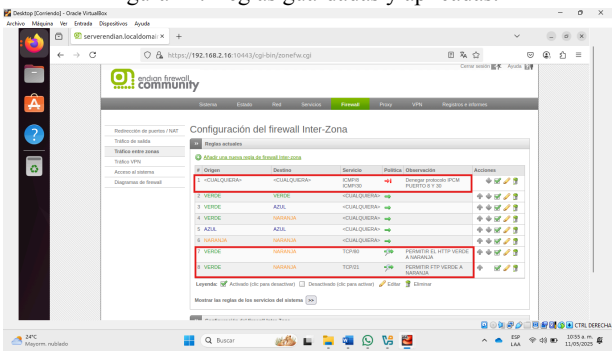
Figura 43. Reglas para denegar.



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 43).

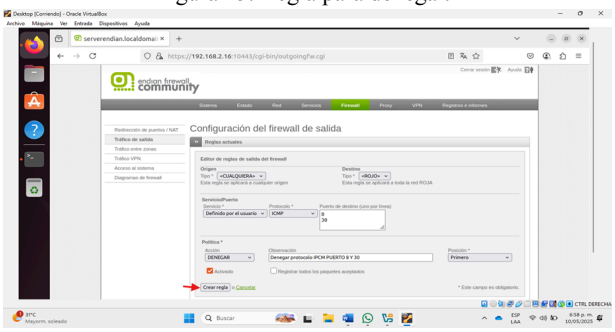
Figura 44. Reglas guardadas y aplicadas.



Fuente: Autoría Propia.

Reglas NAT aplicadas para permitir el tráfico HTTP (puerto 80) y FTP (puerto 21) hacia la IP interna en la zona DMZ. Regla para bloquear la conexión a los puertos 8 y 30 (ver Figura 44).

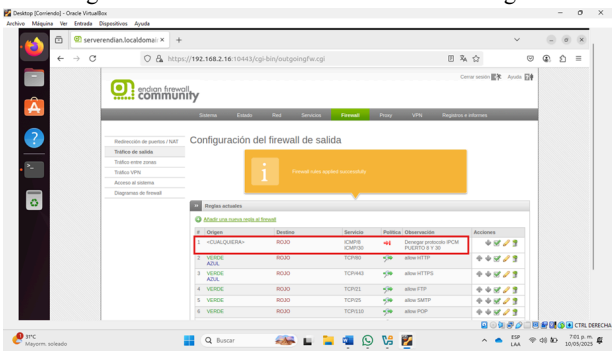
Figura 45. Regla para denegar.



Fuente: Autoría Propia.

Se configura una nueva regla para bloquear la conexión a los puertos 8 y 30 en tráfico de salida (ver Figura 45).

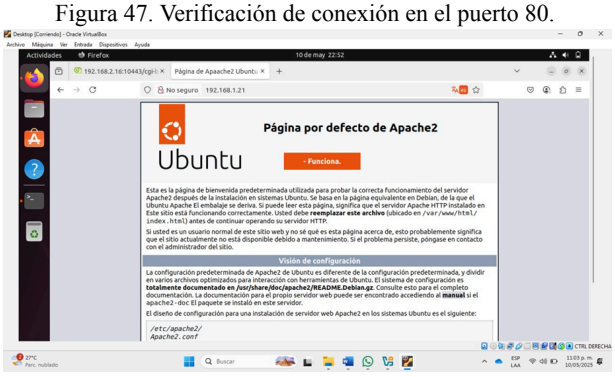
Figura 46. Verificación de la creación de la regla.



Fuente: Autoría Propia.

Se verifica que la regla de para bloquear la conexión a los puertos 8 y 30 ha sido configurada y creada (ver Figura 46).

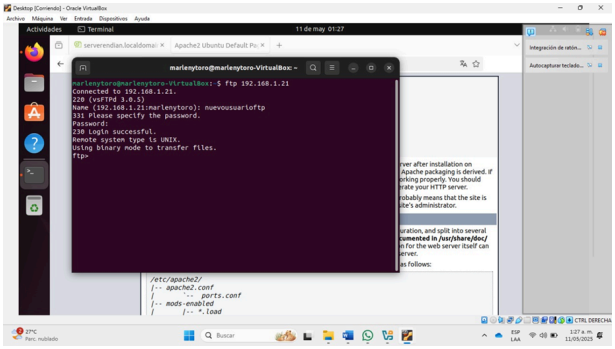
Figura 47. Verificación de conexión en el puerto 80.



Fuente: Autoría Propia.

Se verifica el funcionamiento del puerto HTTP desde del Desktop ingresando la IP del servidor http://192.168.1.21 comprobando que hay conexión (ver Figura 47).

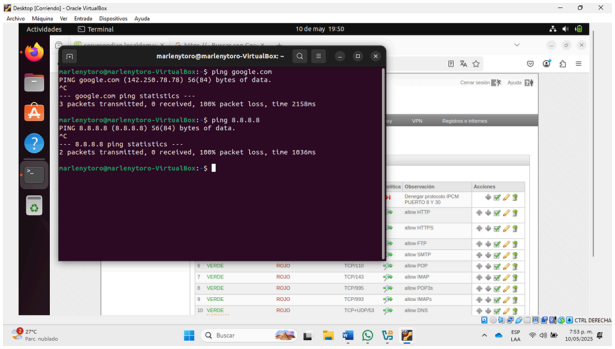
Figura 48. Funcionamiento del puerto 21.



Fuente: Autoría Propia.

Se prueba el funcionamiento del puerto 21, mediante FTP desde el Desktop haciendo conexión al servidor a la red DMZ: ftp 192.168.1.21 (ver Figura 48).

Figura 49. Verificación de la regla de negación.

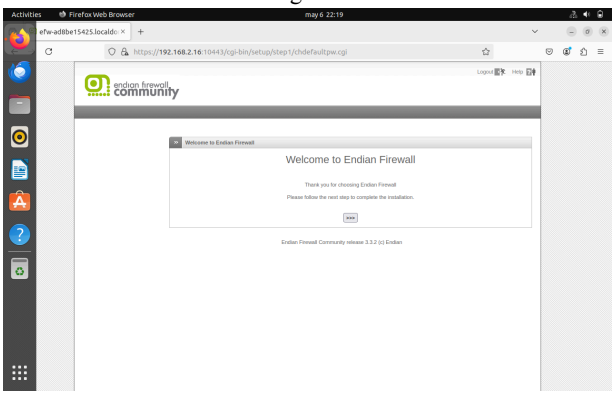


Fuente: Autoría Propia.

Se prueba el funcionamiento desde la terminal de Desktop ejecutando el comando ping 8.8.8.8 que es la DNS de Google. se puede verificar que NO existe conectividad a internet (ver Figura 49).

6 TEMÁTICA 4 REGLAS DE ACCESO

Figura 50. Verificar en el tráfico inter-zona, la creación de las reglas.

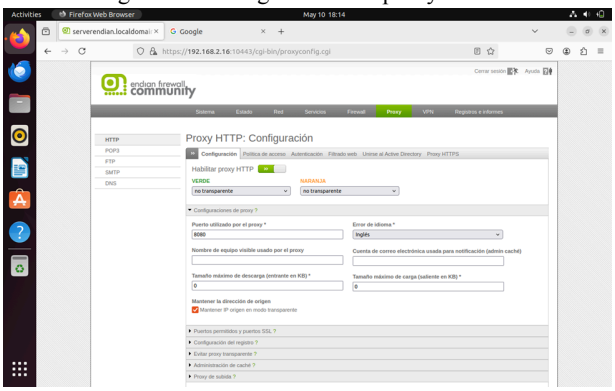


Fuente: Autoría Propia.

En este paso hacemos la verificación de reglas de tráfico para asegurar que la red esté funcionando como se espera (ver Figura 50).

6.1 CONFIGURACIÓN HTTP

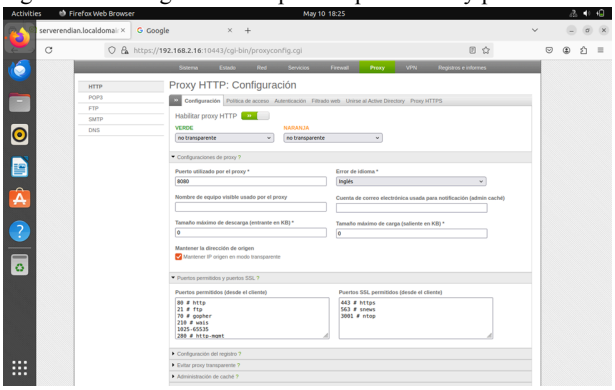
Figura 51. Configuración del proxy HTTP.



Fuente: Autoría Propia.

En esta parte se hace la configuración del proxy, ya que funciona como un intermediario entre el cliente y el servidor web (ver Figura 51).

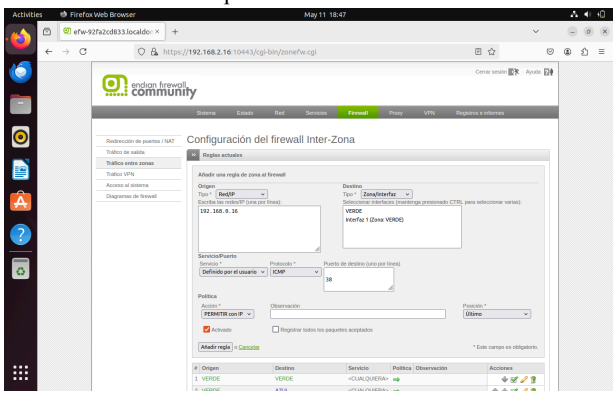
Figura 52. Configuración de puertos permitidos y puertos SSL.



Fuente: Autoría Propia.

Como podemos observar en la imagen anterior (ver Figura 52), se hace este procedimiento para controlar el tráfico de red.

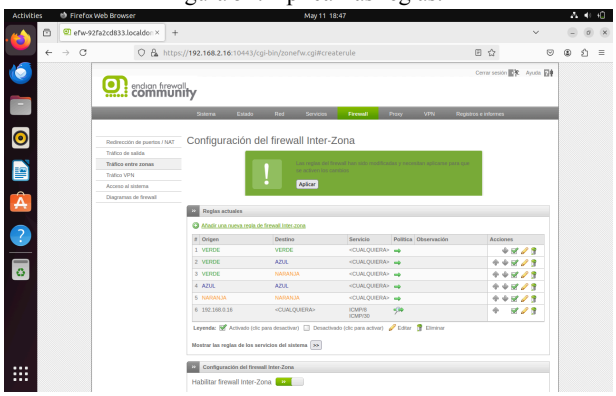
Figura 53. Creación de una nueva regla para el firewall de protocolo ICMP.



Fuente: Autoría Propia.

Se configura una regla de firewall para permitir o bloquear el tráfico ICMP (ver Figura 53).

Figura 54. Aplicar las reglas.

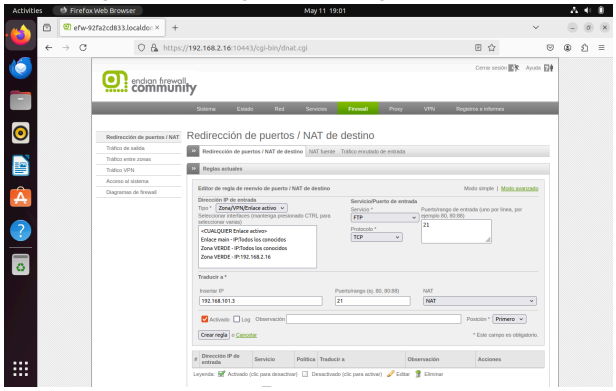


Fuente: Autoría Propia.

Se aplica la creación de la regla para activar las reglas de acceso recientemente creadas (ver Figura 54).

6.3 REGLAS DE REENVÍOS PORT FORWARDING / DESTINATION NAT RULE EDITOR.

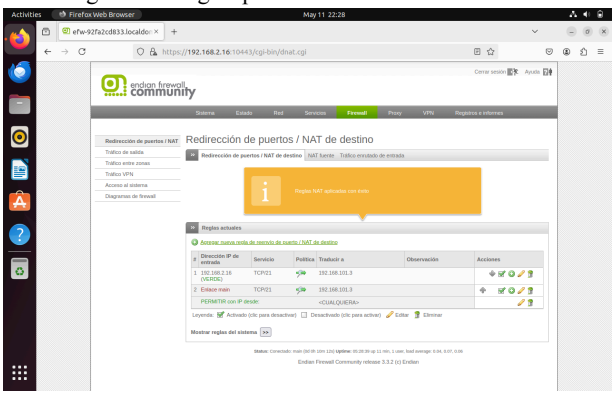
Figura 55. Configuración de reglas de reenvío.



Fuente: Autoría Propia.

Se crean reglas de port Forwarding, que permite redirigir el tráfico entrante a servicios internos según las políticas de acceso establecidas (ver Figura 55).

Figura 56. Reglas para servicios FTP en la DMZ.



Fuente: Autoría Propia.

Se establece la configuración de una regla que permite el acceso al servicio FTP en la zona DMZ, mapeando el tráfico desde la WAN a la IP interna correspondiente bajo el control del firewall (ver Figura 56).

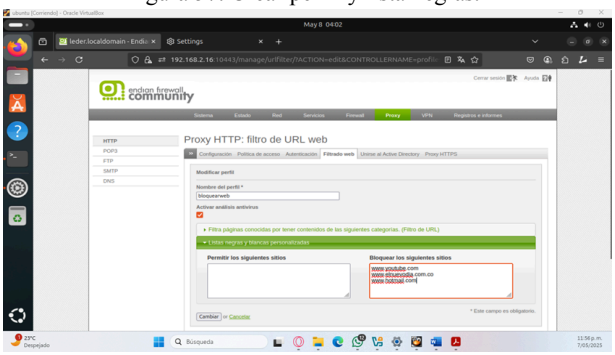
7 TEMÁTICA 5 IMPLEMENTACIÓN DE PROXY HTTP

Como bien se sabe un proxy HTTP no transparente actúa como un intermediario entre los clientes de una red y los servidores web, pero requiere que el navegador del usuario esté configurado explícitamente para su uso, A diferencia del proxy transparente este tipo permite aplicar autenticadores y políticas más robustas.

En esta sección se describe cómo se implementa dicho proxy en el sistemas de Endian Firewall Community, estableciendo control de navegación por usuario y dominios.

7.1 FILTRADO WEB

Figura 57. Crear perfil y lista negras.



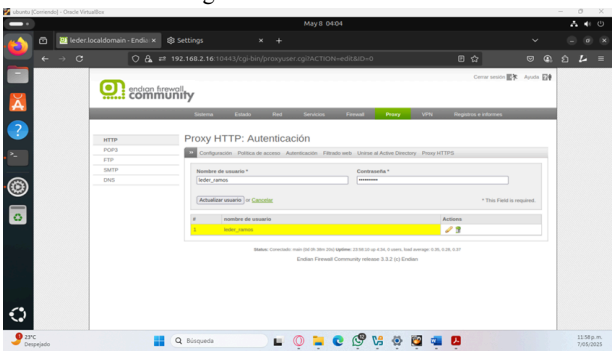
Fuente: Autoría Propia.

En el apartado de filtrado web se realiza la creación de un perfil (bloquearweb) el cual tendrá tres dominios bloqueados a los cuales no se les va permitir el acceso (Ver Figura 57).

7.2 POLÍTICAS DE ACCESO

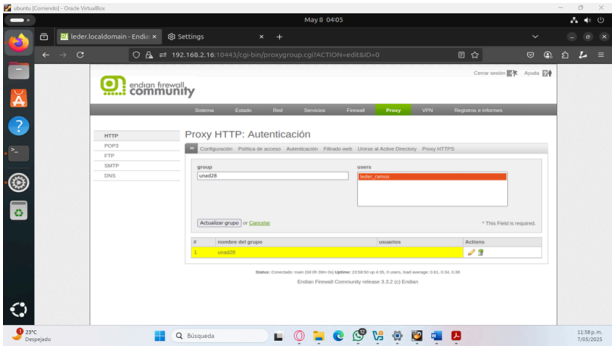
El servidor proxy actúa como un filtro que aplica políticas de acceso, sólo permite navegar a usuarios que cumplen ciertos requisitos como el autenticarse con usuario y contraseña o tener permisos para el acceso a determinados sitios web.

Figura 58. Crear usuario.



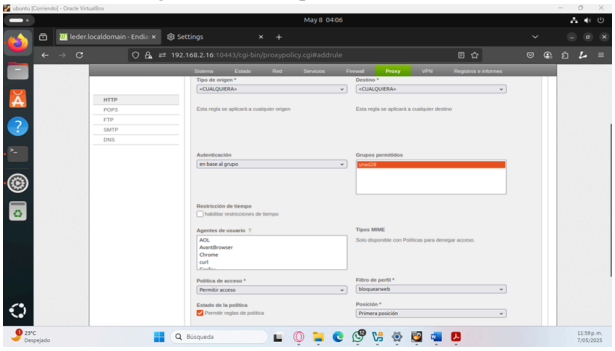
Fuente: Autoría Propia.

Figura 59. Crear grupo.



Fuente: Autoría Propia.

Figura 60. Crear política de acceso



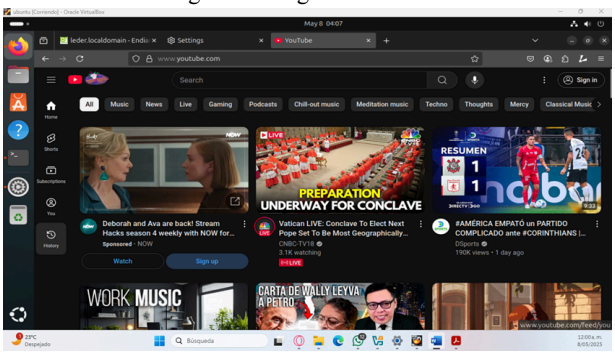
Fuente: Autoría Propia.

Para la implementación de la política de acceso se requirió la creación de un usuario y su contraseña (ver Figura 58) al cual se lo va asociar a un grupo (ver Figura 59) y en la política de acceso estará relacionado con el perfil bloquearweb (ver Figura 60).

7.3 PÁGINAS WEB

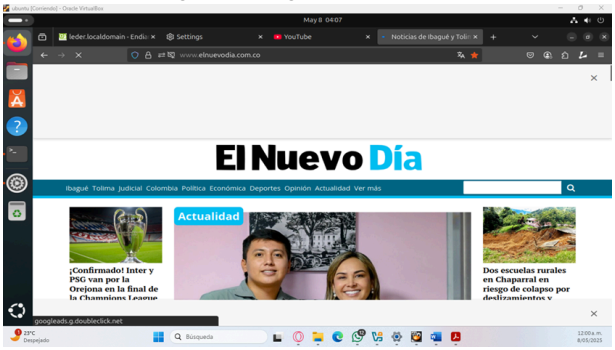
Las páginas web son los destinos que se intentan visitar desde el navegador, más sin embargo el acceso estará restringido por el proxy.

Figura 61. Página YouTube.



Fuente: Autoría Propia.

Figura 62. Página Elnuevodia.



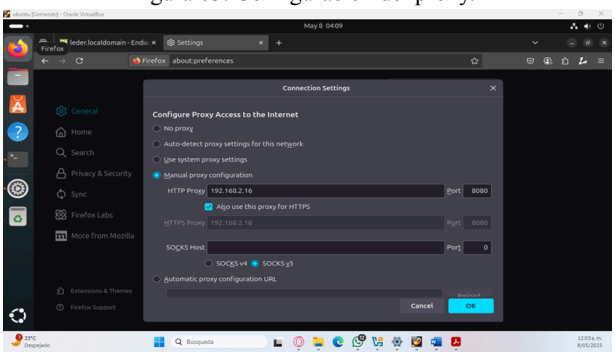
Fuente: Autoría Propia.

Se indicaron dos de las páginas que fueron registradas en la lista negra del perfil, como aún no se activa el proxy entonces estás aún tendrán permitido navegar (ver Figura 61 y 62).

7.4 PROXY EN EL NAVEGADOR

El proxy en el navegador actúa como un filtro entre el equipo y la internet, para controlar o proteger la navegación.

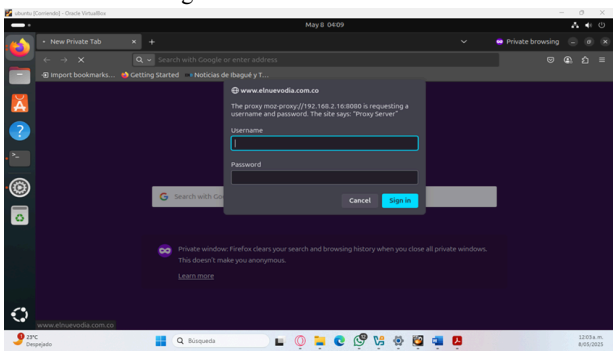
Figura 63. Configuración del proxy.



Fuente: Autoría Propia.

Para hacer efectivo los pasos anteriores y se aplique el bloqueo de las páginas en la lista negra debemos configurar en el navegador el proxy del servidor. (ver Figura 63) Con esto ya se estaría aplicando la política de acceso creada anteriormente.

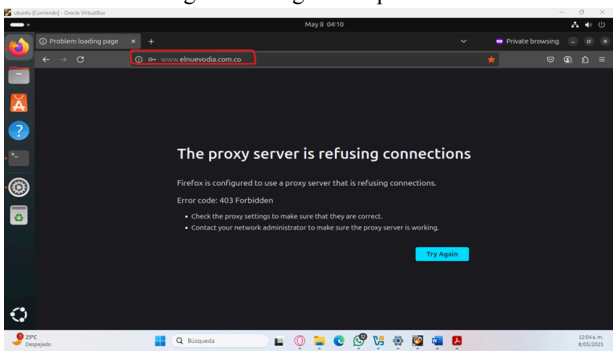
Figura 64. Usuario de acceso.



Fuente: Autoría Propia.

Cuando el proxy ya está activado al momento de visitar una página entonces el proxy intercepta la solicitud y pedirá la autenticación (ver Figura 64).

Figura 65. Página bloqueada.



Fuente: Autoría Propia.

El código de error 403 indicará que el acceso a dicha página estará prohibido, por que el proxy ha bloqueado el acceso a el sitio visitado (ver Figura 65).

9. CONCLUSIONES

La configuración de una arquitectura de red segmentada mediante Endian Firewall Community demostró ser una solución efectiva y accesible para el fortalecimiento de la seguridad perimetral en entornos basados en GNU/Linux. A través de la correcta definición de las zonas de red (LAN, WAN y DMZ), y la asignación adecuada de direcciones IP estáticas, fue posible establecer una infraestructura organizada que facilita el control y monitoreo del tráfico de red.

Se logró configurar reglas de NAT que permitieron optimizar el flujo de tráfico entre redes manteniendo altos estándares de seguridad e implementar políticas de filtrado que combinaron accesos permitidos con restricciones estratégicas.

A través de la configuración de reglas en la interfaz web de Endian, se permiten los servicios a la zona DMZ. De igual forma se permiten los servicios HTTP por el puerto 80 y los servicios FTP por el puerto 21 y se denegaron los servicios de red a través del protocolo ICMP.

A través de la configuración de las reglas de acceso o reglas de firewall, se tiene en cuenta el control sobre el flujo de tráfico de red, en el cual permitimos o rechazamos el acceso a recursos, por ejemplo para tener acceso a cualquier enlace activo creamos una regla con la opción Zona/VPN/Enlace activo, la cual nos permite buscar el enlace activo de nuestra WAN, con servicio FTP.

La implementación de un proxy HTTP no transparente mediante Endian Firewall Community demostró ser una solución para el control del acceso a Internet dentro de una red, gracias a la integración de listas negras fue posible restringir el acceso a sitios específicos

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/