CONFIGURACIÓN INTEGRAL DE ENTORNOS VIRTUALIZADOS CON GNU/LINUX ENDIAN EN VIRTUALBOX: IMPLEMENTACIÓN DE NAT, DMZ, REGLAS DE ACCESO Y PROXY HTTP AUTENTICADO PARA REDES SEGURAS

Aguilar Ramírez, Blanca Yanine
e-mail: byaguilarr@unadvirtual.edu.co
Amell Gonzáles, Fernando José
e-mail: fjamellg@unadvirtual.edu.co
Palau Garcia, Marilyn Daniely
e-mail: mdpalaug@unadvirtual.edu.co
Ramírez, Edwin Alexander
e-mail: earamirez1@unadvirtual.edu.co
Sigua Guache, Edinson Alexander
e-mail: easiguag@unadvirtual.edu.co

ABSTRACT: *This project documents the installation and configuration of a virtualized network environment with Endian Firewall in VirtualBox, structured in three zones: LAN (green), DMZ (orange) and Internet (red). NAT rules are established to allow controlled outbound traffic from internal networks to the Internet. In addition, firewall policies are created to allow specific services such as HTTP and FTP, and the ICMP protocol is blocked to enhance security. Finally, a non-transparent HTTP proxy with user authentication and a blacklist of restricted sites is configured. The results obtained validate the correct network segmentation, effective traffic control and the implementation of perimeter security measures that guarantee a secure and functional network environment.*

KEYWORDS: Endian, Firewall, NAT, Network, Proxy, Segmentation.

RESUMEN: *Este proyecto documenta la instalación y configuración de un entorno de red virtualizado con Endian Firewall en VirtualBox, estructurado en tres zonas: LAN (verde), DMZ (naranja) e Internet (roja). Se establecen reglas NAT que permiten la salida controlada de tráfico desde las redes internas hacia Internet. Además, se crean políticas de firewall para permitir servicios específicos como HTTP y FTP, y se bloquea el protocolo ICMP para mejorar la seguridad. Finalmente, se configura un proxy HTTP no transparente con autenticación de usuarios y una lista negra de sitios restringidos. Los resultados obtenidos validan la correcta segmentación de la red, el control efectivo del tráfico y la aplicación de medidas de seguridad perimetral que garantizan un entorno de red seguro y funcional.*

PALABRAS CLAVE: Endian, Firewall, NAT, Proxy, Red, Segmentación.

1 INTRODUCCIÓN

La seguridad perimetral es una necesidad crítica en la administración de redes modernas, especialmente ante el crecimiento constante de amenazas cibernéticas. En este contexto, las soluciones basadas en software libre, como Endian Firewall, permiten implementar mecanismos eficaces de protección en entornos controlados y adaptables. Este proyecto tiene como objetivo la creación de un entorno virtualizado utilizando VirtualBox, donde se configura Endian Firewall en una arquitectura de red segmentada compuesta por tres zonas: LAN (verde), DMZ (naranja) y WAN (roja).

La implementación abarca la configuración de reglas de NAT para habilitar la comunicación segura entre zonas internas y externas, así como la definición de políticas de firewall para permitir o denegar servicios específicos como HTTP, FTP e ICMP. Adicionalmente, se integra un proxy HTTP no transparente con autenticación de usuarios y filtrado mediante listas negras, con el propósito de controlar el acceso a Internet desde la red interna.

Esta propuesta permite simular un entorno empresarial real, reforzando conceptos como segmentación de red, control de tráfico y autenticación de usuarios. La virtualización facilita la validación práctica de configuraciones seguras, convirtiéndose en una herramienta didáctica esencial para la formación en ciberseguridad y administración de redes.

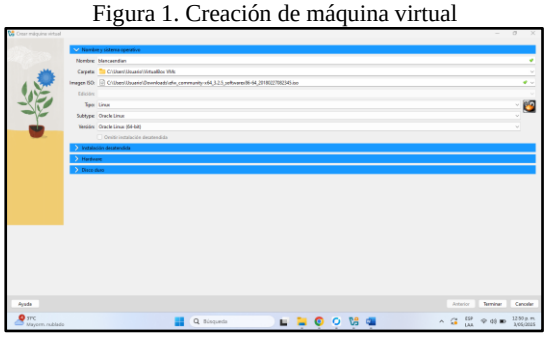
2 INSTALACIÓN ENDIAN

2.1 CARACTERÍSTICAS GENERALES

Se descarga Endian desde su sitio oficial y se instala en VirtualBox o hardware físico, compatible con arquitecturas x86. Para crear la máquina virtual, se configura Oracle VM VirtualBox con tipo Linux, versión Oracle Linux (64 bit) y unidad óptica virtual ISO.

Se crea una máquina virtual para Endian en VirtualBox y se ajustan los parámetros de instalación, como se evidencia en la figura 1.

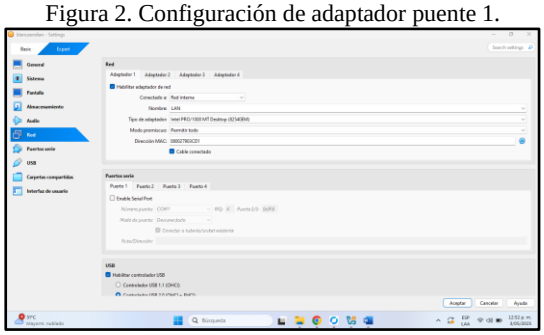
Figura 1. Creación de máquina virtual



Fuente: Autoría propia

El adaptador 1 de Endian, se ajusta como un adaptador puente para la red (WAN), como se muestra en la figura 2.

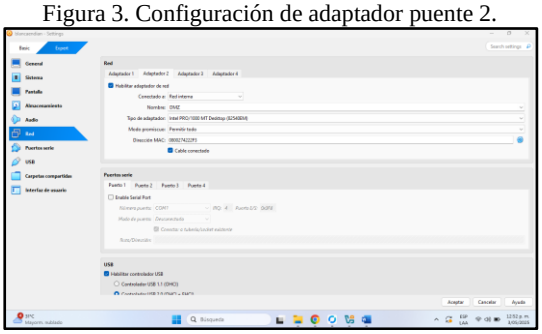
Figura 2. Configuración de adaptador puente 1.



Fuente: Autoría propia.

El adaptador 2 de Endian se ajusta para operar como una red interna para la red LAN, como se evidencia en la figura 3.

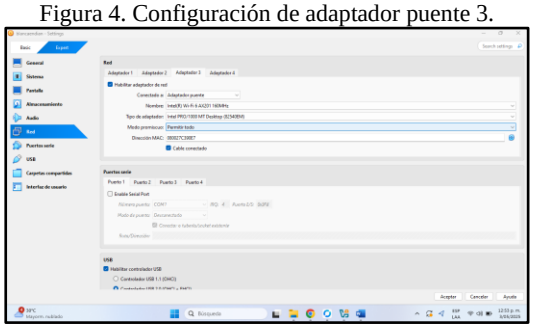
Figura 3. Configuración de adaptador puente 2.



Fuente: Autoría propia.

Finalmente, se ajusta el adaptador 3 de Endian como una red interna (DMZ), como se observa en la figura 4.

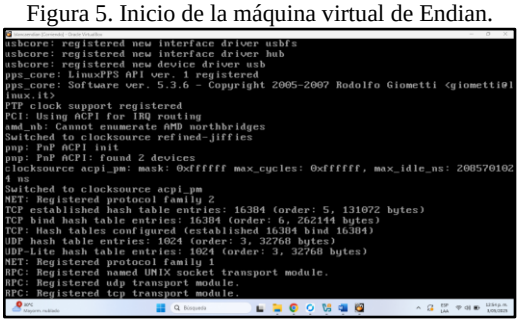
Figura 4. Configuración de adaptador puente 3.



Fuente: Autoría propia.

Una vez realizado los todos los ajustes a Endian, se verifica el inicio de la máquina virtual, como evidencia la figura 5.

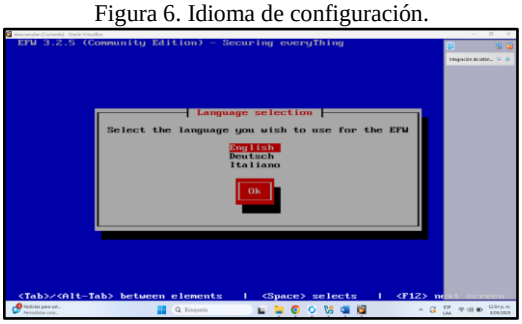
Figura 5. Inicio de la máquina virtual de Endian.



Fuente: Autoría propia.

Se elige el idioma inglés, como se observa en la figura 6.

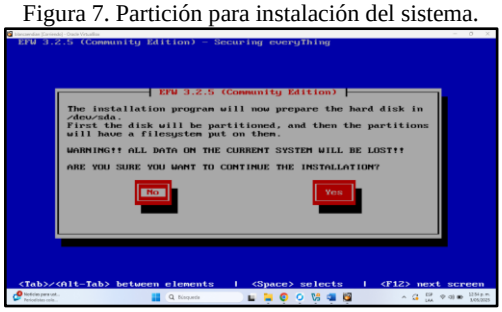
Figura 6. Idioma de configuración.



Fuente: Autoría propia.

Se elige “yes” para que cree una partición e instale el sistema, como se demuestra en la figura 7.

Figura 7. Partición para instalación del sistema.



Fuente: Autoría propia.

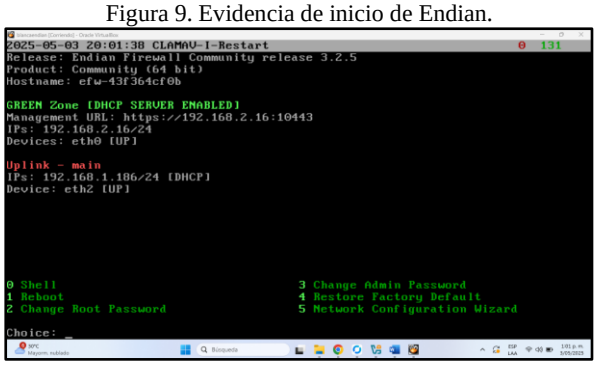
Se crea la IP 192.168.2.16 y la máscara de subred 255.255.255.0 para la red verde, como muestra la figura 8.

Figura 8. Establecimiento de ip verde.

Fuente: Autoría propia.

Una vez terminado el proceso, se observa la interfaz de Endian, la cual muestra la dirección IP asignada a la zona verde, como se evidencia en la figura 9.

Figura 9. Evidencia de inicio de Endian.



Fuente: Autoría propia.

Una vez realizada la instalación, se inicia el proceso guiado a través de las temáticas planteadas a continuación:

3 TEMÁTICA 1: CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX (TARJETAS DE RED) E INSTALACIÓN EFECTIVA DEL MISMO

Se describe el proceso de implementación de una red segmentada utilizando Endian Firewall para garantizar seguridad y eficiencia en la comunicación entre zonas críticas.

Se detallan los pasos de configuración de adaptadores de red, asignación de direcciones IP y establecimiento de políticas de firewall. Los resultados demuestran la efectividad de la segmentación en redes LAN, DMZ y WAN, proporcionando un modelo replicable para entornos similares.

En el ámbito de la seguridad de redes, la segmentación es una estrategia clave para aislar recursos críticos y minimizar riesgos. Este trabajo presenta la implementación de una red dividida en tres zonas:

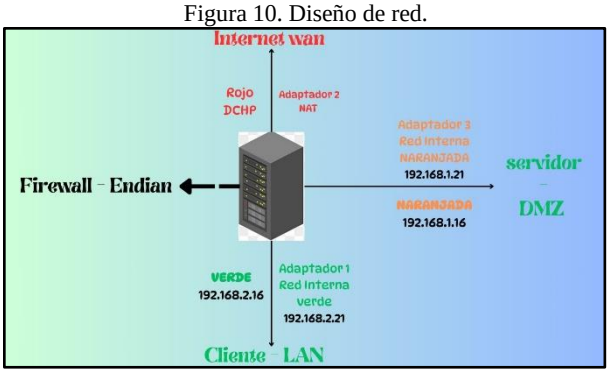
- Zona verde (LAN): Red interna para dispositivos locales (192.168.2.0/24).
- Zona naranja (DMZ): Servidores accesibles de forma controlada (192.168.1.0/24).
- Zona roja (WAN): Conexión a internet mediante NAT.

La solución se basó en Endian Firewall, una distribución Linux diseñada para gestión de firewall y seguridad perimetral, configurada en una máquina Ubuntu.

3.1 DISEÑO DE LA TOPOLOGÍA

El diseño de red se planteó considerando los principios de seguridad por capas y mínimo privilegio, como se observa en la figura 10.

Figura 10. Diseño de red.



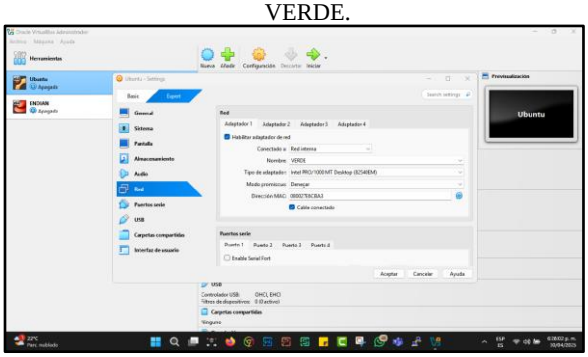
Fuente: Autoría propia.

La topología implementada consta de:

3.1.1 ADAPTADOR 1 (LAN)

El esquema de red implementado utiliza el segmento 192.168.2.0/24 con máscara de subred 255.255.255.0, donde el firewall Endian opera con la IP 192.168.2.16 como puerta de enlace predeterminada. La asignación de direcciones IP se gestiona dinámicamente mediante DHCP, incluyendo reservas específicas para dispositivos críticos que requieren accesibilidad permanente. Adicionalmente, se aplica una política de firewall restrictiva que bloquea conexiones entrantes no autorizadas, reforzando la seguridad de la red mientras se mantiene la flexibilidad en la distribución de direcciones internas.

Figura 11. Instalación de Ubuntu escritorio en la red interna VERDE.

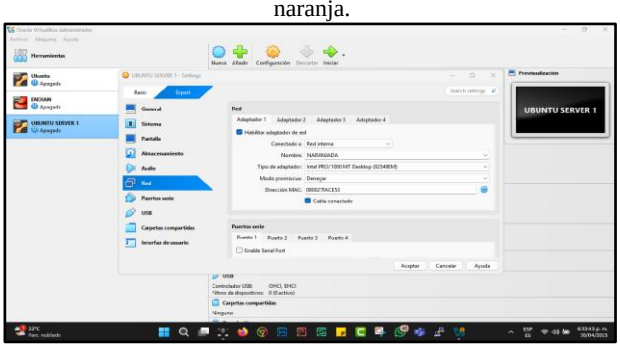


Fuente: Autoría propia.

3.1.2 ADAPTADOR 2 (WAN)

El sistema se configura para obtener automáticamente una dirección IP pública mediante DHCP, optimizando la conectividad a Internet. Se implementa NAT overload (PAT) para permitir que múltiples dispositivos internos compartan la única dirección pública disponible, maximizando el uso de recursos. La seguridad se refuerza con una política de estado que únicamente permite tráfico iniciado desde dentro de la red, bloqueando cualquier intento de conexión externa no solicitada. Adicionalmente, se aplica un filtrado estricto de puertos no esenciales, cerrando posibles vectores de ataque y reduciendo la superficie de exposición. Esta configuración ofrece un equilibrio óptimo entre conectividad, eficiencia en el uso de IPs públicas y protección perimetral avanzada.

Figura 12. Instalación de Ubuntu servidor en la red interna naranja.

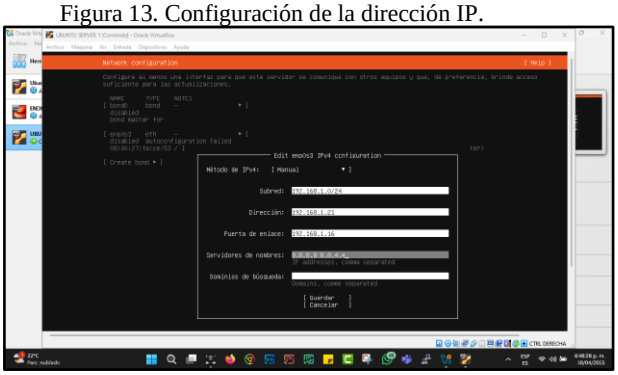


Fuente: Autoría propia.

3.1.3 ADAPTADOR 3 (DMZ)

La red configurada utiliza el segmento 192.168.1.0/24 con máscara de subred 255.255.255.0, donde el servidor Ubuntu opera con la dirección IP estática 192.168.1.21, utilizando 192.168.1.16 como puerta de enlace predeterminada. Para garantizar la seguridad, se implementan reglas de firewall personalizadas para cada servicio expuesto: HTTP (puerto 80), HTTPS (puerto 443) y SMTP (puerto 25), permitiendo sólo el tráfico autorizado hacia estos puertos. Adicionalmente, el sistema incluye monitoreo en tiempo real de conexiones activas y aplicación de límites de tasa (rate limiting) para prevenir saturación o ataques DDoS. Esta configuración asegura tanto la accesibilidad de los servicios críticos como la protección contra amenazas externas.

Figura 13. Configuración de la dirección IP.



Fuente: Autoría propia.

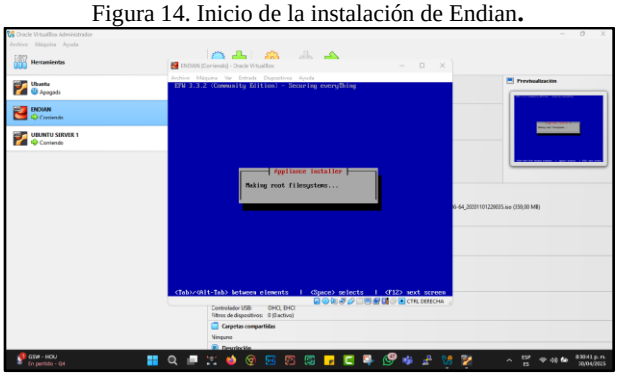
3.2 INSTALACIÓN Y CONFIGURACIÓN DETALLADA

El proceso de implementación se realizó en las siguientes etapas:

1. Preparación del Entorno:

- Instalación de máquinas virtuales para cada componente.
- Asignación de recursos hardware (CPU, RAM, almacenamiento).
- Configuración básica de red para cada adaptador.

Figura 14. Inicio de la instalación de Endian.

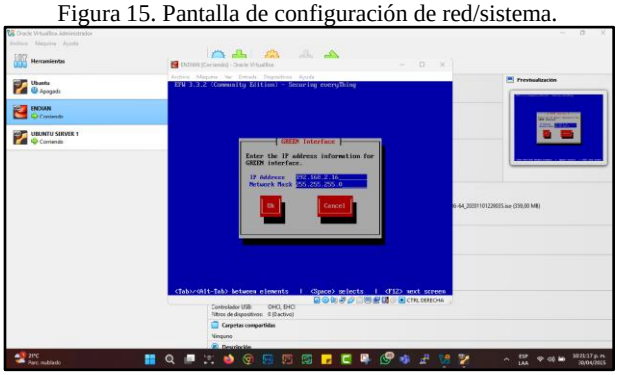


Fuente: Autoría propia.

2. Despliegue de Endian Firewall:

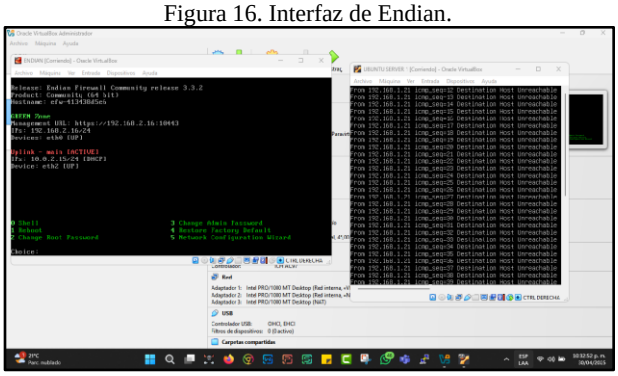
El proceso comenzó con la descarga e instalación de la versión Community 3.5.7 desde los repositorios oficiales [1], asegurando la autenticidad y procedencia del software. La configuración inicial se realizó a través de la interfaz web administrativa (accesible mediante HTTPS en https://192.168.2.16:10443), donde se implementaron credenciales seguras que cumplen con los requisitos de complejidad definidos (mayúsculas, minúsculas, números y caracteres especiales). Finalmente, se ejecutó la actualización de paquetes y firmas de seguridad para corregir vulnerabilidades conocidas y garantizar la estabilidad del sistema desde el primer momento.

Figura 15. Pantalla de configuración de red/sistema.



Fuente: Autoría propia.

Figura 16. Interfaz de Endian.



Fuente: Autoría propia.

3. Configuración Avanzada de Red:

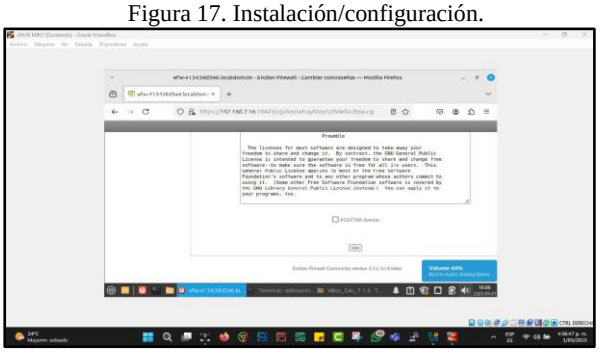
- Asignación estática de IPs para dispositivos críticos.
- Creación de reglas NAT para redirección de puertos.
- Configuración de políticas QoS para priorizar tráfico crítico.
- Habilitación de logging detallado para auditoría.

4. Políticas de Seguridad:

- Reglas de filtrado por dirección IP y puerto.
- Protección contra ataques comunes (DoS, port scanning).
- Configuración de VPN para acceso remoto seguro.
- Implementación de bloqueo automático por intentos fallidos.

Una vez aceptada la licencia, se procedió con la instalación/configuración.

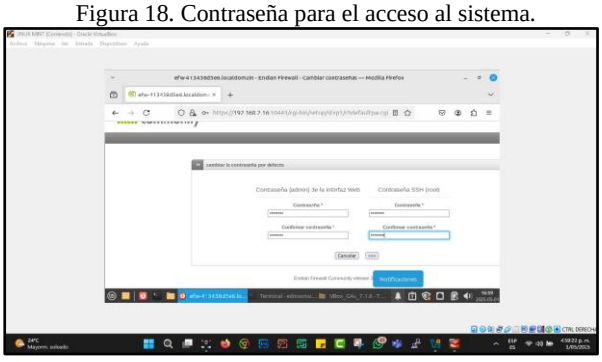
Figura 17. Instalación/configuración.



Fuente: Autoría propia.

Se procedió a asignar una contraseña para el acceso al sistema.

Figura 18. Contraseña para el acceso al sistema.



Fuente: Autoría propia.

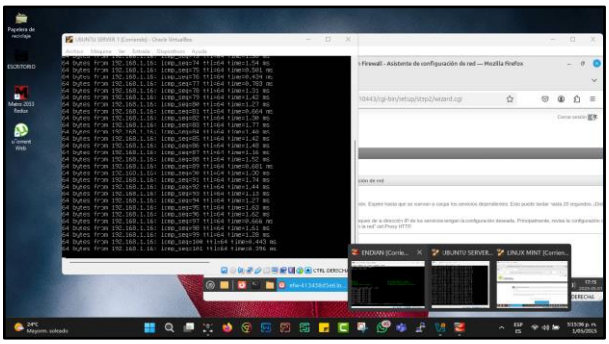
3.3 RESULTADOS Y DISCUSIÓN

La implementación completa del sistema permitió obtener los siguientes resultados:

1. Conectividad Exitosa:

- Las máquinas en LAN (192.168.2.0/24) y DMZ (192.168.1.0/24) comunicaron sin interferencias.
- Endian Firewall filtró correctamente el tráfico no autorizado entre zonas.

Figura 19. Se evidencia que el servidor Ubuntu está recibiendo datos/conexiones.



Fuente: Autoría propia.

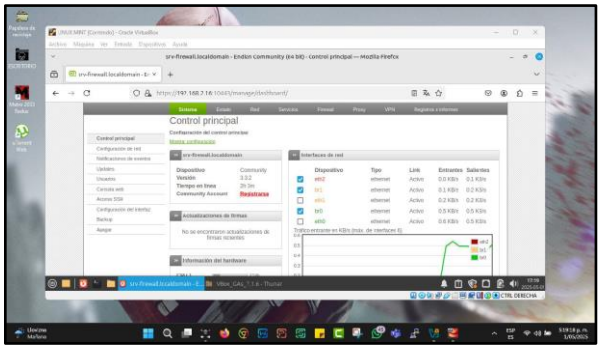
2. Seguridad:

- La DMZ aisló los servidores de la red interna, reduciendo riesgos de ataques externos.
- Las políticas de NAT ocultaron las IPs internas desde la WAN.

3. Limitaciones:

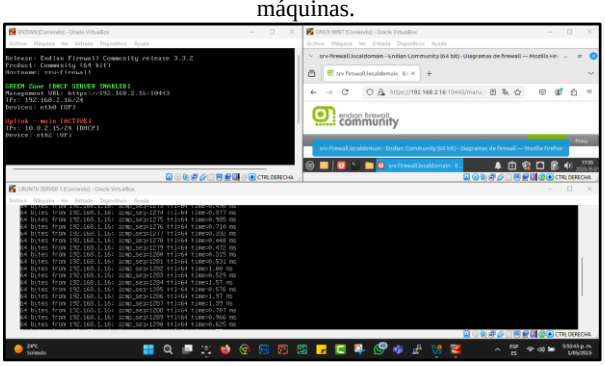
- La configuración inicial requirió ajustes manuales en las tablas de rutas.
- La falta de redundancia en los adaptadores podría ser un punto crítico.

Figura 20. La interfaz de Endian Firewall Community exhibe un dashboard con métricas de tráfico.



Fuente: Autoría propia.

Figura 21. Se comprueba el correcto funcionamiento de las tres máquinas.



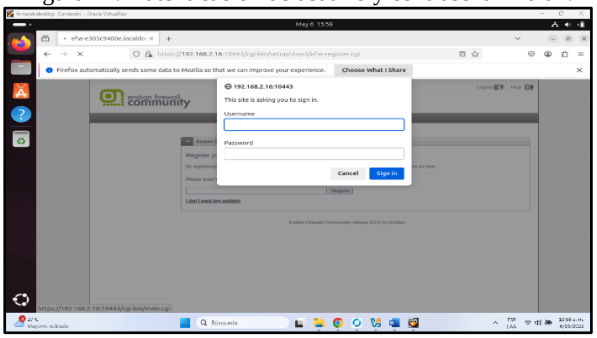
Fuente: Autoría propia.

4 TEMÁTICA 2: CONFIGURACIÓN NAT

Producto esperado**:** Se configura la regla de NAT para permitir la comunicación desde la LAN hacia la WAN y desde la Zona DMZ hacia Internet, verificando el reenvío de puertos y la correcta creación de las reglas de NAT.

Se abre el navegador Firefox y se introduce la dirección https://192.168.2.16:10443 para acceder a Endian, como evidencia la figura 22.

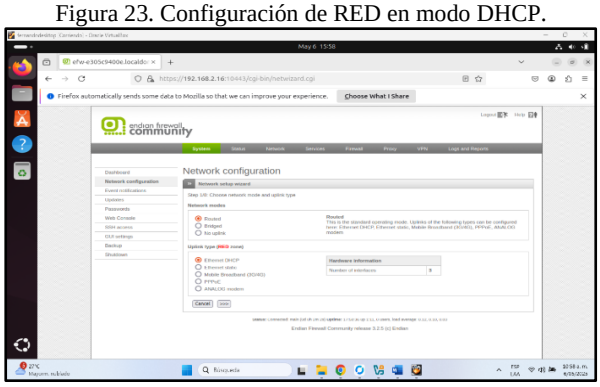
Figura 22. Autenticación de usuario y contraseña Endian.



Fuente: Autoría propia.

Se confirma el ajuste DHCP para la red roja (WAN), como se muestra en la figura 23.

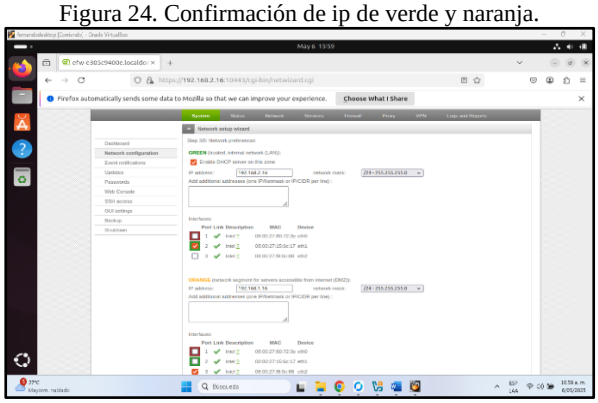
Figura 23. Configuración de RED en modo DHCP.



Fuente: Autoría propia.

Se configura correctamente las dos direcciones IP LAN y DMZ, como se observa en la figura 24.

Figura 24. Confirmación de ip de verde y naranja.



Fuente: Autoría propia.

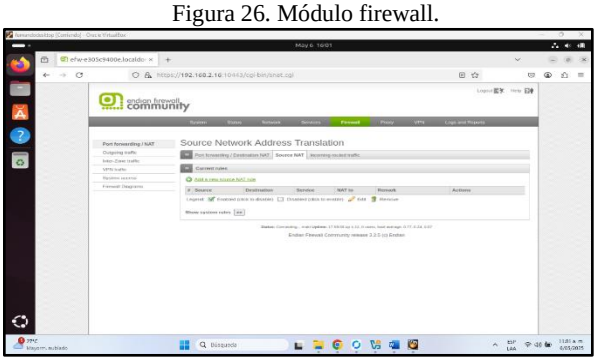
Se puede evidenciar que la red WAN está en el puerto eth0, como demuestra la figura 25.

Figura 25. Confirmación de configuración de RED en DHCP.

Fuente: Autoría propia.

Se accede al módulo de Firewall, en la sección de Source NAT y se crea una nueva regla NAT utilizando la opción de añadir, como se evidencia la figura 26.

Figura 26. Módulo firewall.



Fuente: Autoría propia.

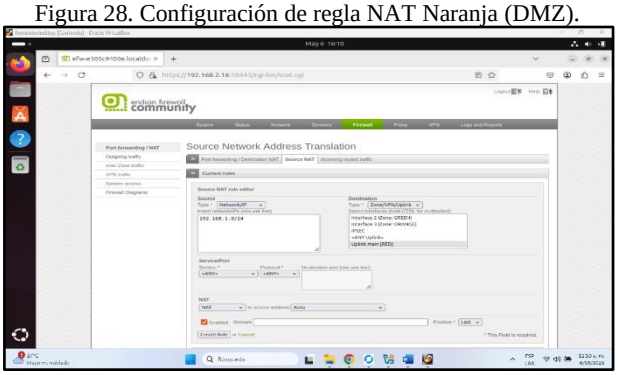
Se crea una primera regla NAT en el módulo source NAT, para habilitar el acceso del tráfico originado de la red verde (LAN) hacia Internet a través de la red roja (WAN), como se evidencia la figura 27.

Figura 27. Configuración de regla NAT Verde (LAN).

Fuente: Autoría propia.

Se crea una segunda regla Source NAT para la red naranja (DMZ), permitiendo que el tráfico de la red 192.168.1.0/24 se enmascare y salga hacia la interfaz roja (WAN). Esto habilita que la red DMZ tenga acceso a Internet a través de la red externa, como se observa en la figura 28.

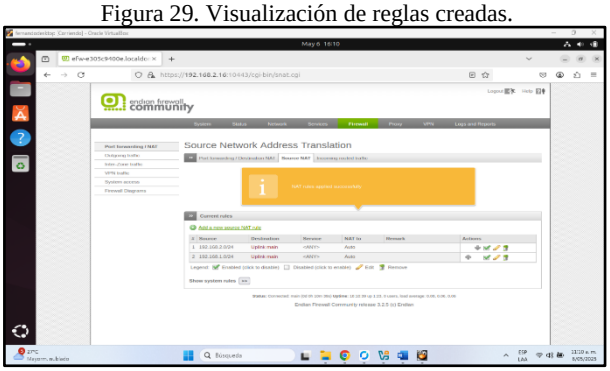
Figura 28. Configuración de regla NAT Naranja (DMZ).



Fuente: Autoría propia.

Una vez terminado el proceso, se observa el almacenamiento de las reglas NAT, como muestra la figura 29.

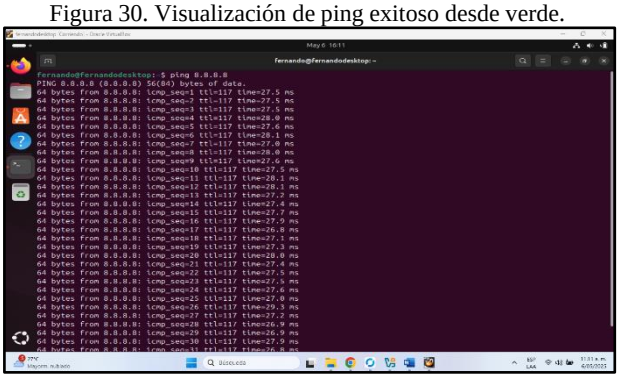
Figura 29. Visualización de reglas creadas.



Fuente: Autoría propia.

El Desktop realiza con éxito un ping a 8.8.8.8, lo que significa que la máquina tiene acceso a Internet y que la configuración de NAT en Endian para permitir la salida a la WAN desde la red verde funciona correctamente, como se muestra en la figura 30.

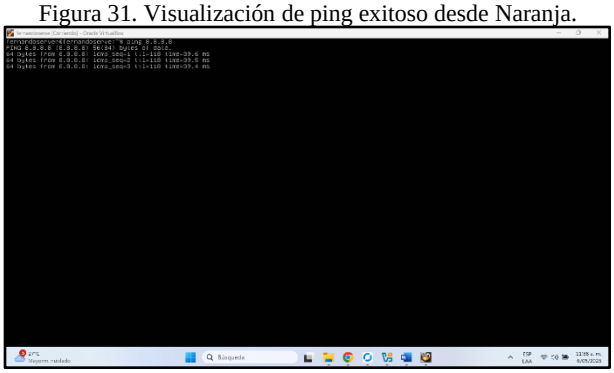
Figura 30. Visualización de ping exitoso desde verde.



Fuente: Autoría propia.

El servidor realiza exitosamente un ping a la dirección IP 8.8.8.8, lo que confirma la conectividad del dispositivo a internet. Este resultado valida la correcta implementación de la configuración de red y de la traducción de direcciones de red (NAT) en el firewall Endian, así como en el servidor, asegurando la comunicación bidireccional de ambos sistemas con redes externas, como se evidencia en la figura 31.

Figura 31. Visualización de ping exitoso desde Naranja.



Fuente: Autoría propia.

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

Producto esperado: permitir los servicios HTTP (Puerto 80) y FTP (Puerto 21) desde el servidor Web bajo Ubuntu Server, denegar el protocolo ICMP (Puerto 8 y puerto 30) para no permitir hacer ping en la red, probar a través de una consola o terminal la no respuesta del comando ping hacia una IP de la red y verificar en el tráfico de salida, la creación de las reglas.

En Endian Firewall, la configuración para permitir los servicios HTTP (puerto 80) y FTP (puerto 21) desde un servidor Ubuntu Server se puede realizar mediante varias formas de establecer las reglas de firewall en la interfaz de administración. Primero, en la sección de Firewall, se crea una nueva regla de tráfico saliente, definiendo los puertos 80 y 21 como permitidos, garantizando el acceso a servicios web y transferencia de archivos. Posteriormente, se guarda y aplica la configuración, verificando la conectividad mediante pruebas para HTTP y con clientes FTP para la transferencia de archivos. Esta gestión de tráfico permite un control efectivo sobre la comunicación de la red, asegurando accesibilidad sin comprometer la seguridad.

También se puede realizar creando una regla en la subsección tráfico entre zonas, en origen se selecciona la zona verde (LAN) y en destino la zona naranja (DMZ), y se debe escoger el servicio definido por el usuario, protocolo TCP y puerto 80, 21; en esta regla se utiliza la política PERMITIR y se posiciona en las primeras reglas. En la interfaz de reglas actuales se observa que la política está activa. 1.

El bloqueo del protocolo ICMP (puertos 8 y 30) en redes informáticas se implementa como una medida de seguridad para evitar la exploración no autorizada y el monitoreo de dispositivos en una infraestructura de red. El denegar el tráfico ICMP utilizando Endian Firewall es con el objetivo de prevenir ataques de reconocimiento y mitigar riesgos de accesibilidad no deseada.

Para llevar a cabo esta restricción es necesario configurar las reglas en Endian firewall ingresando a la interfaz de administración y navegar a la sección de firewall para la gestión de reglas y definir la regla de filtrado de tráfico en el puerto 8 y puerto 30.

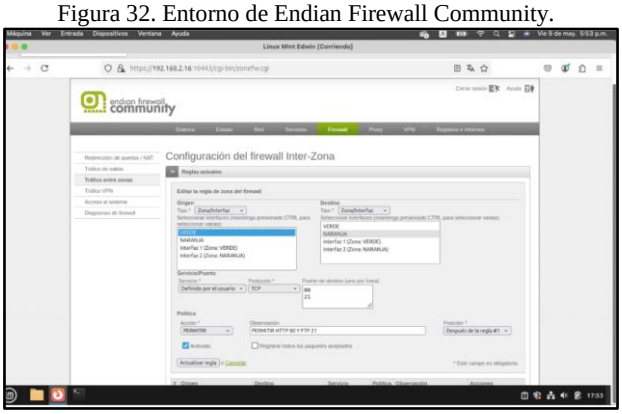
En la subsección tráfico entre zonas, se añade la regla con origen y destino cualesquiera, se filtra el protocolo ICMP y los puertos 8 y 30, en seleccionando protocolo ICMP y puertos 8 y 30, en el apartado política se define la acción identificada con el nombre DENEGAR, en observación es recomendable colocar información para identificar la regla establecida.

Después de configurar el bloqueo de ICMP (ping) en Endian Firewall, es importante realizar pruebas y verificaciones para asegurar que la regla está funcionando correctamente.

La verificación de ping se realiza abriendo una terminal y escribiendo ping y después la dirección ip del equipo destino. Si la configuración es correcta, no debería haber respuesta del servidor, indicando que el tráfico ICMP está bloqueado. Otra forma de garantizar que la regla se cumpla es accediendo a los logs de Endian.

Para comprobar que los servicios http y ftp están permitidos, se puede corroborar ingresando desde un navegador en el desktop y colocando la ip del servidor, y debe cargar la información de apache o de webservice utilizado. Para corroborar el funcionamiento de ftp es posible hacerlo desde la terminal de desktop y escribiendo ftp y la ip del servidor o utilizando programas como filezilla.

Figura 32. Entorno de Endian Firewall Community.

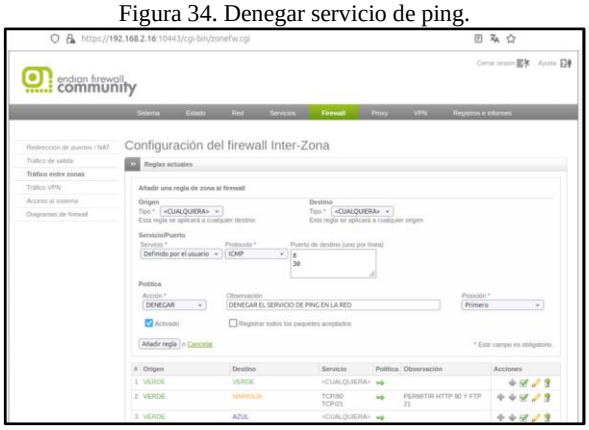


Fuente: Autoría propia.

Figura 33. Reglas activas.

Fuente: Autoría propia.

Figura 34. Denegar servicio de ping.



Fuente: Autoría propia.

Figura 35. Validar que no se permita el ping desde DMZ.

Fuente: Autoría propia.

Figura 36. Validar restricción de ping desde y hacia la LAN.

Fuente: Autoría propia.

La configuración de reglas de acceso en el firewall Endian tiene como objetivo controlar la comunicación entre las distintas zonas de red (LAN, WAN y DMZ), estableciendo políticas que permitan o restrinjan el tráfico de forma segura. Esto se realiza para proteger la red interna frente a accesos no autorizados desde Internet.

6 TEMÁTICA 4: REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO

Producto esperado: establecer y verificar las reglas de acceso entre las distintas zonas de la red implementadas (LAN, WAN y DMZ) a través del firewall Endian. Se configurarán políticas específicas que permitan o restrinjan el tráfico mediante los protocolos HTTP (puerto 80) y FTP (puerto 21), con el fin de garantizar una comunicación controlada y segura entre las estaciones de trabajo, los servidores y el acceso a Internet.

Para permitir la comunicación entre la zona Verde y la zona Naranja utilizando los protocolos HTTP y FTP, se deben crear reglas de firewall que permitan o restrinjan el tráfico desde la zona Verde hacia la zona Naranja específicamente con los protocolos HTTP (puerto 80), HTTPS (puerto 443), ICMP (puertos 8/30) y FTP (puerto 21), esto implica autorizar las conexiones entrantes y salientes entre ambas zonas.

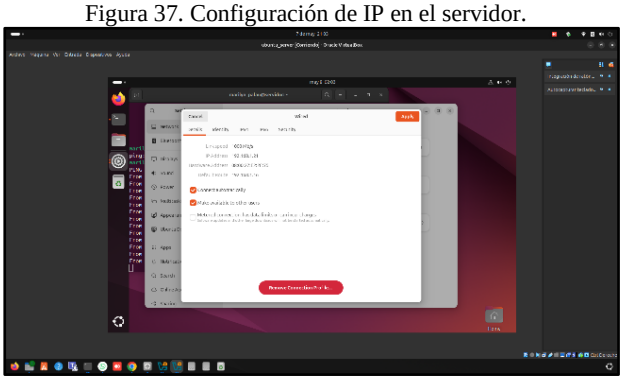
Asimismo, para controlar la comunicación entre la zona Internet con la LAN (utilizada como red interna y segura de una organización, donde se ubican computadoras de los usuarios y recursos confiables) se deben establecer reglas que permitan o denieguen el tráfico desde Internet hacia la LAN, considerando servicios específicos como HTTP/HTTPS, FTP, ICMP.

En el caso de la zona Internet con la zona DMZ (zona desmilitarizada, que se utiliza típicamente para servidores accesibles desde Internet, como servidores web o FTP), también es necesario definir reglas que permitan o denieguen el tráfico desde Internet hacia la DMZ con ciertos servicios específicos como HTTP/HTTPS, FTP, ICMP.

Una vez realizada la configuración, se debe revisar y asegurar que todas las reglas entre zonas estén correctamente configuradas. Por ejemplo: si una zona no debe comunicarse con otra, se debe verificar que el tráfico esté bloqueado por defecto, y que solo el tráfico explícitamente autorizado esté permitido.

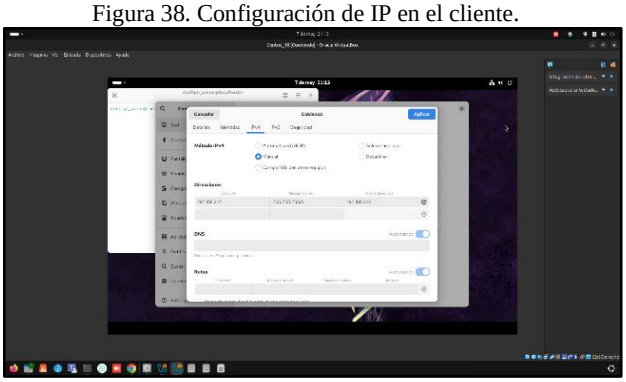
Finalmente se llevan a cabo pruebas desde un navegador Web las directivas de acceso, con el fin de confirmar que las reglas funcionan conforme a lo esperado.

Figura 37. Configuración de IP en el servidor.



Fuente: Autoría propia.

Figura 38. Configuración de IP en el cliente.



Fuente: Autoría propia.

Figura 39. Regla para denegar tráfico por defecto desde la zona Verde hacia la zona Naranja.

Fuente: Autoría propia.

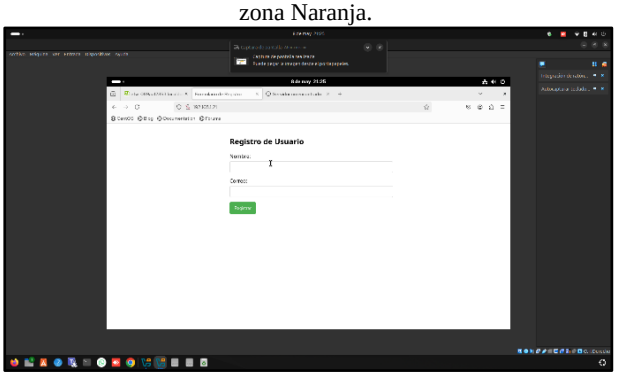
Figura 40. Validación del bloqueo de acceso desde la zona Verde hacia la zona Naranja.

Fuente: Autoría propia.

Figura 41. Regla para permitir tráfico desde la zona Verde hacia la zona Naranja.

Fuente: Autoría propia.

Figura 42. Validación de acceso desde la zona Verde hacia la zona Naranja.



Fuente: Autoría propia.

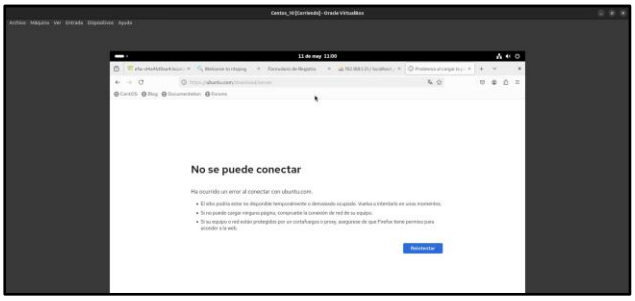
Figura 43. Configuración del servidor DHCP.

Fuente: Autoría propia.

Figura 44. Regla para denegar tráfico de salida en las zonas Verde y Naranja (acceso a conexiones externas).

Fuente: Autoría propia.

Figura 45. Validación del bloqueo de acceso desde la zona Verde hacia la zona Internet.



Fuente: Autoría propia.

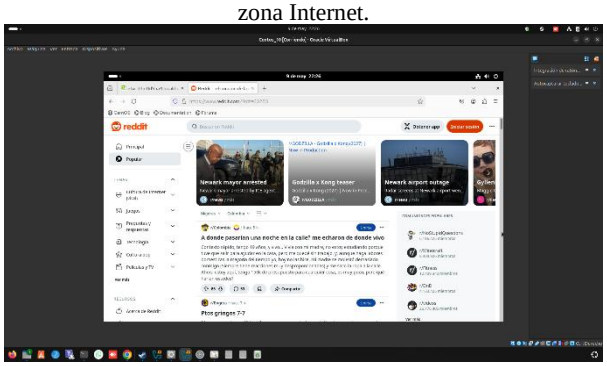
Figura 46. Validación del bloqueo de acceso desde la zona Naranja hacia la zona Internet.

Fuente: Autoría propia.

Figura 47. Regla para permitir tráfico de salida en las zonas Verde y Naranja (acceso a conexiones externas).

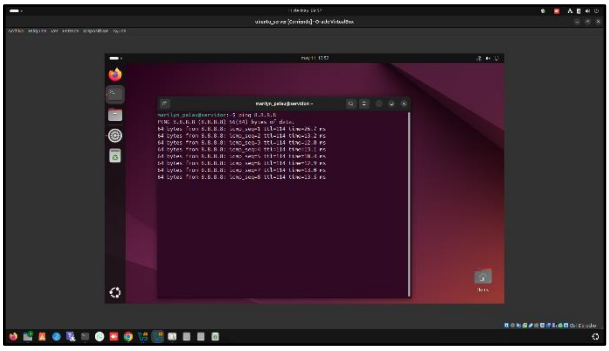
Fuente: Autoría propia.

Figura 48. Validación de acceso desde la zona Verde hacia la zona Internet.



Fuente: Autoría propia.

Figura 49. Validación de acceso desde la zona Naranja hacia la zona Internet.



Fuente: Autoría propia.

Figura 50. Verificación de las conexiones entre zonas.

Fuente: Autoría propia.

La configuración de reglas de acceso en el firewall Endian tiene como objetivo controlar la comunicación entre las distintas zonas de red (LAN, WAN y DMZ), estableciendo políticas que permitan o restrinjan el tráfico de forma segura. Esta configuración protege la red interna frente a accesos no autorizados desde Internet, autorizando únicamente los servicios necesarios como HTTP, HTTPS, FTP e ICMP, y garantiza una segmentación adecuada entre zonas. Además, simula escenarios reales de redes empresariales, donde se requiere exponer ciertos servicios al exterior (por ejemplo, los ubicados en la DMZ) sin comprometer la seguridad de la red interna.

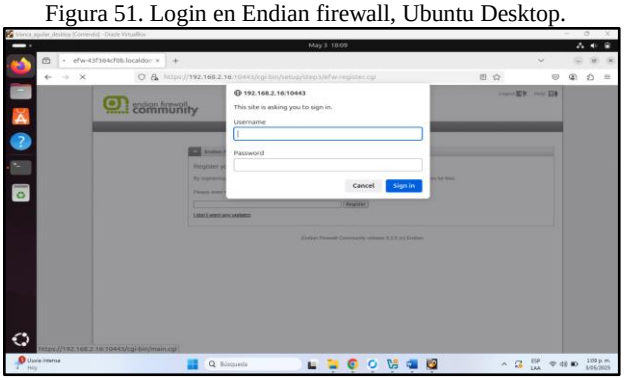
Como resultado, se obtiene una red protegida y funcional, con reglas de firewall correctamente aplicadas que permiten únicamente el tráfico autorizado entre zonas. Asegurando que los servicios críticos sean accesibles cuando corresponde, y bloqueando el tráfico no deseado por defecto. A través de pruebas prácticas como el acceso a servicios vía navegador o el uso de comandos de red, se verifica que las políticas cumplan con los objetivos definidos. Esto proporciona un entorno controlado, seguro y validado para la operación de los distintos componentes de la red.

7 TEMÁTICA 5: IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE) CON POLÍTICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET

Producto esperado: Se debe configurar un perfil de navegación que incluya una lista negra para bloquear el acceso a páginas como www.hotmail.com, www.youtube.com y www.elnuevodia.com.co. También se debe activar la autenticación por usuario, creando un usuario específico y asignándolo a un grupo. A este grupo se le aplicará una política de acceso, la cual se asociará al perfil previamente creado. Como prueba final, se verificará desde la red LAN que el navegador no permita ingresar a los sitios bloqueados.

Una vez configuradas las zonas, se procede a acceder al Endian Firewall desde el navegador de Ubuntu Desktop: a través de 192.168.2.16, e ingresamos las credenciales previamente asignadas.

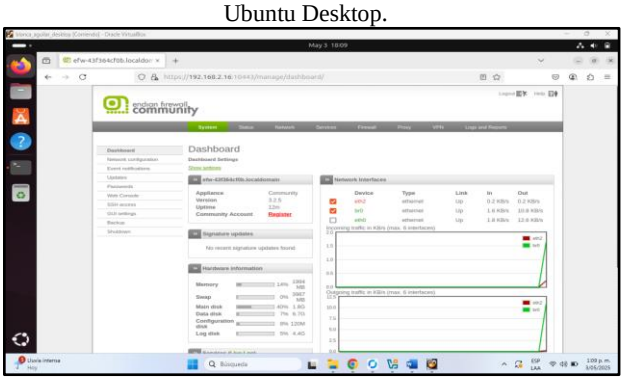
Figura 51. Login en Endian firewall, Ubuntu Desktop.



Fuente: Autoría propia.

Una vez logueado correctamente, se accede a Endian Firewall, como se evidencia en la figura 52.

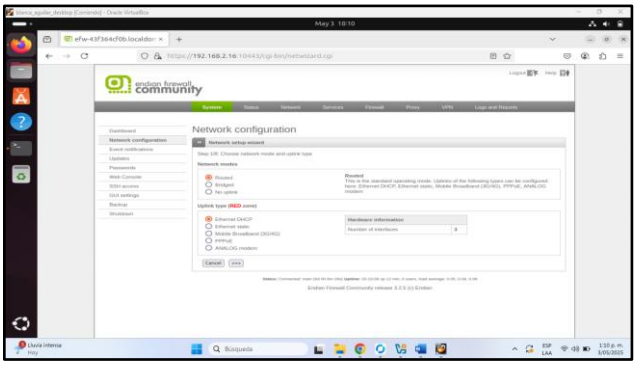
Figura 52. Entorno de trabajo Endian Firewall Comunnity, Ubuntu Desktop.



Fuente: Autoría propia.

Para iniciar con el cumplimiento de la temática 5, se trabaja sobre el módulo de Network configuration y se procede a configurar la zona roja de manera DHCP.

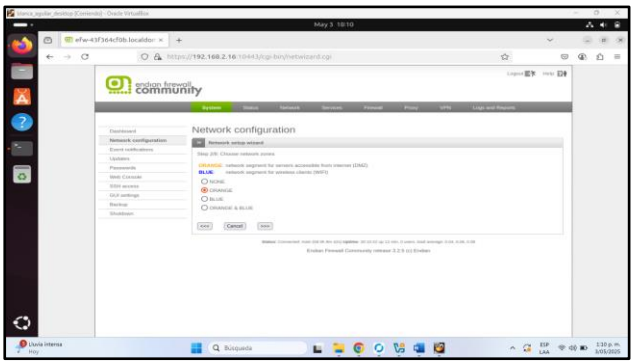
Figura 53. Configuración de red Endian, zona roja de manera DHCP.



Fuente: Autoría propia.

En este paso, se está configurando el tipo de red para las zonas del firewall. Se ha seleccionado naranja para definir el segmento de red que será accesible desde Internet (DMZ).

Figura 54. Configuración del tipo de red para las zonas del firewall.



Fuente: Autoría propia.

Se verifican las ip de verde 192.168.2.16 y naranja 192.168.1.16.

Figura 55. ip de la zona verde y zona naranja.

Fuente: Autoría propia.

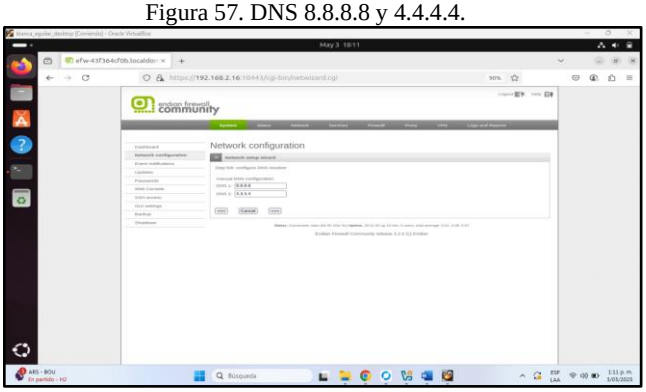
De igual forma se confirma la zona roja DHCP.

Figura 56. Zona roja DHCP.

Fuente: Autoría propia.

Se procede a verificar o ajustar los DNS 8.8.8.8 y 4.4.4.4.

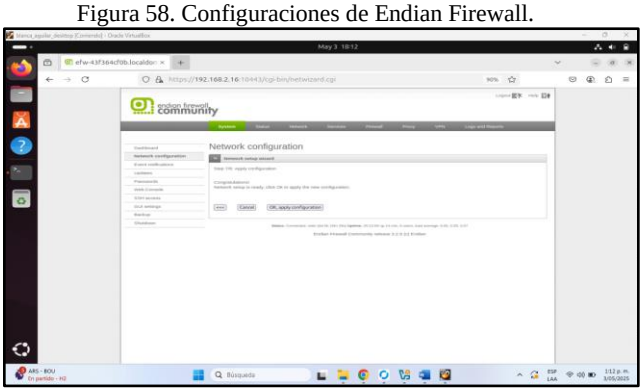
Figura 57. DNS 8.8.8.8 y 4.4.4.4.



Fuente: Autoría propia.

Se pregunta si se desean aplicar los cambios, a lo cual se responde positivamente.

Figura 58. Configuraciones de Endian Firewall.



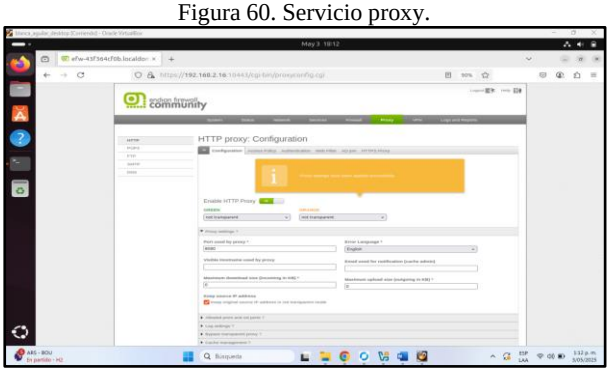
Fuente: Autoría propia.

Figura 59. Mensaje de configuración exitosa de Endian Firewall.

Fuente: Autoría propia.

La figura 60, evidenció el mensaje de aplicación exitosa. Al continuar con el proceso, se habilita el servicio de proxy.

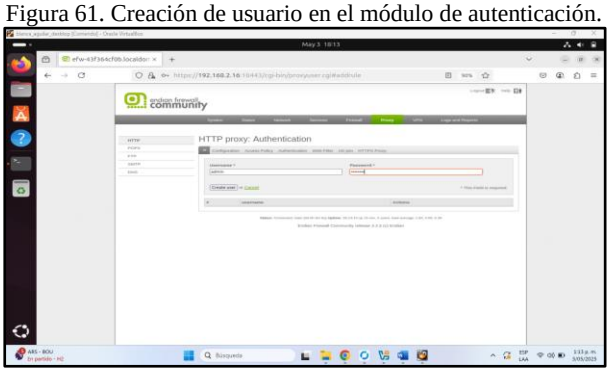
Figura 60. Servicio proxy.



Fuente: Autoría propia.

Se crea el usuario en el módulo de autenticación.

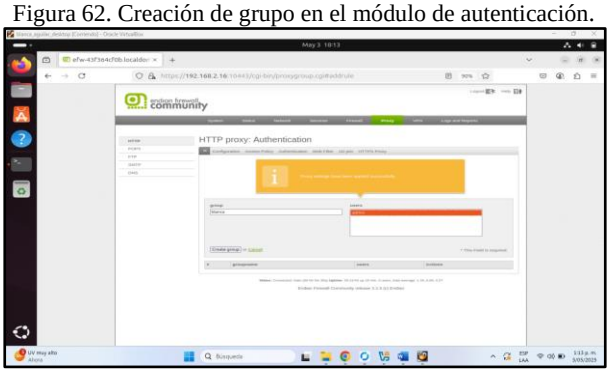
Figura 61. Creación de usuario en el módulo de autenticación.



Fuente: Autoría propia.

Una vez creado el usuario admin, se crea el grupo llamado blanca y se asocia a dicho grupo.

Figura 62. Creación de grupo en el módulo de autenticación.



Fuente: Autoría propia.

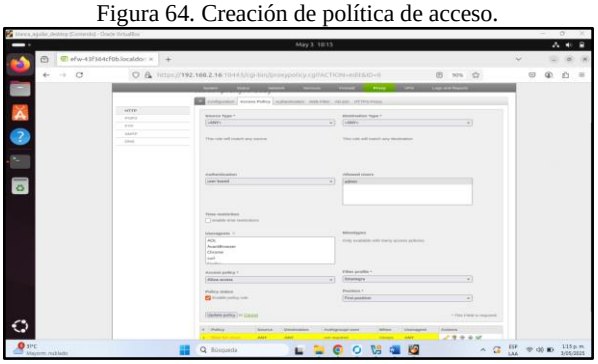
Una vez asociado el usuario admin, al grupo blanca; se crea un nuevo filtro con el nombre lista negra, donde se bloquean las 3 páginas sugeridas en la temática: www.hotmail.com, www.youtube.com, www.elnuevodia.com.co, se aplican y se guardan los cambios.

Figura 63. Creación de filtro.

Fuente: Autoría propia.

Se procede a crear una política de acceso donde se asocia el usuario admin, y se admite que apruebe la regla que se creó llamada lista negra.

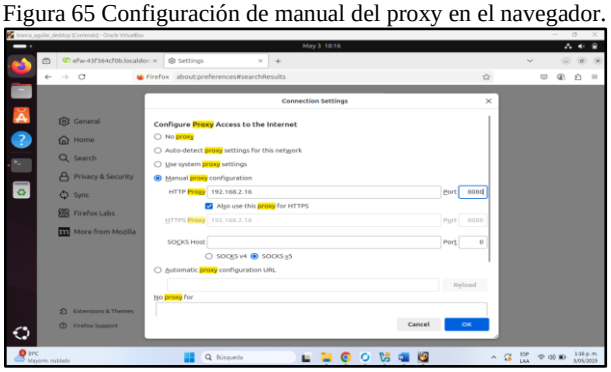
Figura 64. Creación de política de acceso.



Fuente: Autoría propia.

Finalmente, en la configuración de proxy del buscador Firefox (Ubuntu Desktop), se configura manualmente el Proxy donde se agrega 192.168.2.16 y adicional se habilita que use el mismo proxy en HTTPS.

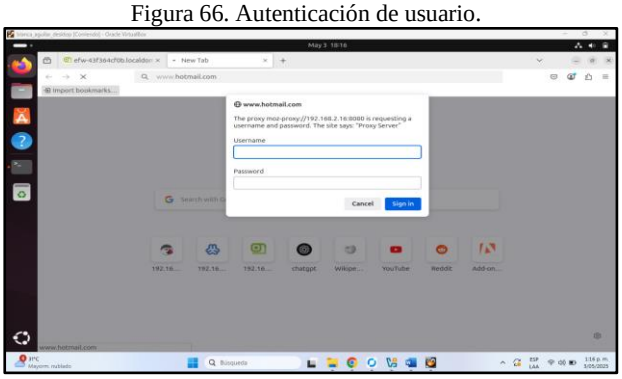
Figura 65 Configuración de manual del proxy en el navegador.



Fuente: Autoría propia.

Para cerrar con broche de oro se verifica el éxito de las configuraciones, intentando ingresar a las páginas bloqueadas a través de la lista creada, por tanto, se accede desde el buscador Firefox a las siguientes páginas: Hotmail, YouTube y Nuevo Día, respectivamente, a los cual solicita autenticación de usuario, como se observa en la figura 66.

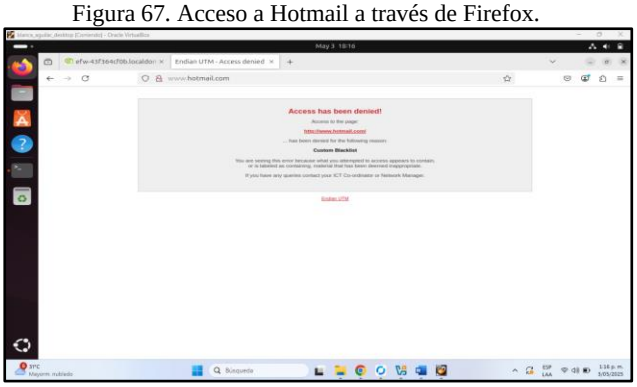
Figura 66. Autenticación de usuario.



Fuente: Autoría propia.

Luego de ingresar la autenticación, se evidencia el acceso denegado en Hotmail.

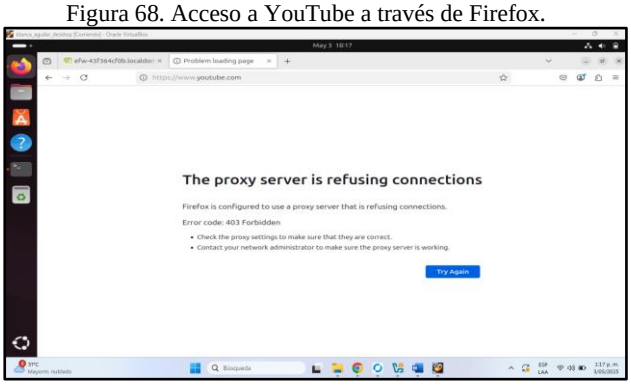
Figura 67. Acceso a Hotmail a través de Firefox.



Fuente: Autoría propia.

Respectivamente se intenta acceder a www.youtube.com y se evidencia el mismo mensaje.

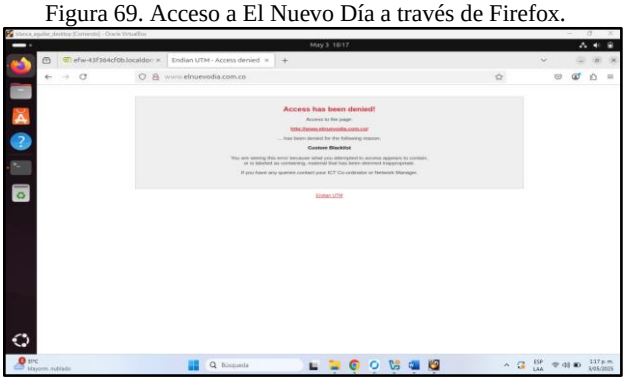
Figura 68. Acceso a YouTube a través de Firefox.



Fuente: Autoría propia.

Y por último, se intenta ingresar a www.elnuevodia.com.co y el acceso es denegado, evidenciando el cumplimiento al objetivo deseado.

Figura 69. Acceso a El Nuevo Día a través de Firefox.



Fuente: Autoría propia.

8 CONCLUSIONES

La implementación confirmó que Endian Firewall es una herramienta eficaz para redes segmentadas, ofreciendo balance entre seguridad y funcionalidad. Como trabajo futuro, se recomienda: primero, integrar VPN para acceso remoto seguro, segundo, implementar IDS/IPS (Sistemas de Detección/Prevención de Intrusos) y, por último, evaluar la escalabilidad con más dispositivos en LAN/DMZ.

La configuración de NAT en Endian Firewall y la asignación de IP estáticas en Ubuntu Server permitieron establecer comunicación efectiva entre las redes internas (LAN y DMZ) y la red externa. Las pruebas de conectividad confirmaron el acceso a Internet desde ambas zonas, mientras que las reglas de Source NAT garantizaron la correcta traducción y enrutamiento del tráfico saliente. Estos resultados validan la correcta implementación de la configuración de red y los controles de seguridad en el entorno simulado.

Se establecieron reglas para permitir o denegar acceso a servicio http y ftp, así como el bloqueo de ping entre todos los equipos de la red. El permitir los servicios HTTP y FTP es una estrategia clave para la administración de seguridad en redes. El bloqueo de ping (puertos 8 y 30) evita exploraciones no autorizadas y posibles ataques de reconocimiento, reforzando la privacidad de los servidores y dispositivos dentro de la red. Por otro lado, la habilitación de HTTP y FTP garantiza la accesibilidad a servicios web y transferencia de archivos, asegurando la operatividad sin comprometer la seguridad.

La combinación de estas reglas permite un equilibrio entre control de tráfico y funcionalidad, adaptándose a distintas necesidades y entornos corporativos. el funcionamiento de cada regla, se evidenció el correcto aislamiento y la comunicación permitida entre las distintas zonas, cumpliendo los objetivos planteados en cuanto a seguridad y accesibilidad.

9 REFERENCIAS

[1] Alemán, O. S. F., & Narváez, V. E. M. (2018). *Análisis de tecnologías de un centro de operaciones de ciberseguridad para un proveedor de servicios de Internet*. https://dspace.udla.edu.ec/bitstream/33000/10041/1/UDLA-EC-TIRT-2018-16.pdf

[2] Cabello, M. C. (2020). *Nethserver Tutorial | Instalación, actualización y primeros pasos* [Video]. YouTube. https://www.youtube.com/watch?v=FNGmM-2fa_0&t=1615s
[3] Canonical. (2023). *Guía del Ubuntu desktop 20.04 LTS*. HelpUbuntu. https://help.ubuntu.com/20.04/ubuntu-help/index.html
[4] Endian Community. (2023). *Endian Firewall Documentation*. https://www.endian.com/
[5] Endian UTM. (s. f.). *Endian UTM 3.2 Reference Manual*. https://docs.endian.com/3.2/utm/index.html
[6] LaCroix, J. (2020). *Mastering Ubuntu Server: Gain expertise in the art of deploying, configuring, managing, and troubleshooting*.
[7] Sánchez Giraldo, J. (2021). *VirtualBox con Endian 3.3.2, 3 Zonas: Verde, Naranjada y Roja* [Video]. YouTube. https://www.youtube.com/watch?v=Dvht5wCPIrI
[8] Lasl, F. [@fiislasl2954]. (s. f.). *Configuración de servidor Endian Firewall* [Video]. YouTube. https://www.youtube.com/watch?v=pVyJuCcm8z0
[9] Oracle. (2020). *Manual de usuario VirtualBox*. https://www.virtualbox.org/manual/
[10] Perfil, V. T. M. I. (2021). *Con las Redes y la Nasa*. Conlasredes.info. https://www.conlasredes.info/2021/10/endian-firewall-proteccion-de-codigo.html?m=1
[11] Wang, S. S. (2019). Integrated framework for information security investment and cyber insurance. *Pacific-Basin Finance Journal*, *57*, 101173. https://doi.org/10.1016/j.pacfin.2019.101173
[12] Yax, A. [@antonioyax9091]. (s. f.). *Instalación y configuración de Endian* [Video]. YouTube. https://www.youtube.com/watch?v=gsfdcUB1oGE