DISEÑO DE UN LABORATORIO VIRTUAL PARA SEGURIDAD Y GESTIÓN DE RED

Cesar Luis Benítez Benítez
e-mail: clbenitezb@unadvirtual.edu.co
Cristian David Ruiz Diaz
e-mail: cdruizd@unadvirtual.edu.co
Jean Marcos Perafan García
e-mail: jmperafang@unadvirtual.edu.co
Juandiego Suárez Yepes
e-mail: jsuarezy@unadvirtual.edu.co
Pablo Alonso Ruiz Merlo
e-mail: paruizme@unadvirtual.edu.co

RESUMEN: *El proyecto presenta la implementación de una solución integral de seguridad perimetral basada en GNU/Linux mediante Endian Firewall Community. La infraestructura se desplegó en VirtualBox con tres zonas de seguridad: GREEN (LAN), ORANGE (DMZ) y RED (WAN), integrando un cliente Ubuntu Desktop y un servidor Ubuntu Server con IP estática. Se configuraron reglas de NAT para permitir el acceso seguro a Internet y se verificó la conectividad con herramientas como ping y DNS. Posteriormente, se aplicaron reglas de Port Forwarding (DNAT) para publicar servicios web (Apache) y FTP (vsFTPd) desde la DMZ, junto con políticas de filtrado que bloquearon ICMP. Finalmente, se implementó un servidor Proxy HTTP con autenticación y listas negras para restringir el acceso a sitios específicos. Los resultados evidencian que la segmentación de red, NAT, filtrado y proxy fortalecen la seguridad perimetral y optimizan el control del tráfico en entornos virtualizados modernos.*

PALABRAS CLAVE: Index Terms—Firewall, Endian Firewall, GNU/Linux, NAT, DMZ, seguridad perimetral, segmentación de red, ciberseguridad, virtualización, administración de redes.

1. INTRODUCCIÓN

La seguridad de las infraestructuras de red constituye un elemento esencial en la administración de sistemas informáticos modernos, debido a la necesidad de proteger los recursos corporativos, controlar el acceso a los servicios y garantizar la integridad, confidencialidad y disponibilidad de la información. En este contexto, los firewalls desempeñan un papel fundamental al actuar como mecanismos de defensa perimetral capaces de supervisar, filtrar y regular el tráfico entre diferentes segmentos de red, aplicando políticas de seguridad acordes con los requerimientos de la organización.

El presente trabajo aborda el diseño e implementación de una arquitectura de seguridad perimetral basada en Endian Firewall Community, desplegada en un entorno virtualizado mediante VirtualBox. La infraestructura se organizó en tres zonas de seguridad claramente diferenciadas: GREEN (LAN), correspondiente a la red interna; ORANGE (DMZ), destinada al alojamiento de servicios públicos; y RED (WAN), que simula el acceso a Internet. Esta segmentación permite separar funciones, restringir accesos y reducir el impacto potencial de amenazas externas.

Durante el desarrollo de la práctica se realizó la instalación y configuración inicial del firewall, la asignación de interfaces de red y la integración de un cliente con Ubuntu Desktop y un servidor con Ubuntu Server. Posteriormente, se implementaron reglas de Traducción de Direcciones de Red (NAT) para permitir la comunicación segura desde la LAN y la DMZ hacia Internet, así como reglas de Port Forwarding (DNAT) para publicar servicios internos de forma controlada. Estas Configuraciónes permitieron comprender la importancia del enmascaramiento de direcciones y del reenvío de puertos como mecanismos esenciales para la conectividad y la seguridad. Adicionalmente, se instalaron y configuraron servicios de red como Apache HTTP Server y vsFTPd, los cuales fueron expuestos a través de la DMZ mediante reglas específicas del firewall. También se aplicaron políticas de filtrado para bloquear el protocolo ICMP, limitando las respuestas al comando ping y reduciendo la capacidad de reconocimiento de la infraestructura por parte de terceros. Estas actividades permitieron profundizar en la administración de servicios y en la aplicación de controles de acceso inter-zona.

Finalmente, se implementó un Proxy HTTP en Endian Firewall en modo no transparente, con autenticación local de usuarios y listas negras para restringir el acceso a determinados sitios web. La configuración del navegador Firefox y las pruebas de navegación permitieron verificar el funcionamiento de las políticas de filtrado y evidenciar la capacidad del proxy para controlar el acceso a Internet de acuerdo con criterios definidos por el administrador.

En conjunto, este trabajo integra conceptos fundamentales de redes, virtualización y ciberseguridad, demostrando cómo la segmentación de redes, el uso de NAT, el reenvío de puertos, el filtrado de protocolos y la implementación de proxies constituyen herramientas clave para fortalecer la seguridad perimetral en entornos basados en GNU/Linux. Los resultados obtenidos evidencian la eficacia de Endian Firewall como solución robusta para la protección, administración y control del tráfico de red en infraestructuras modernas.

2. FORMATO

3. CARACTERÍSTICAS GENERALES

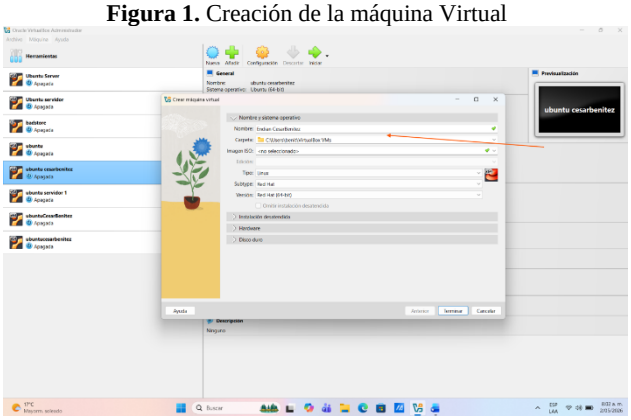
La solución desarrollada se fundamenta en Endian Firewall Community (EFW), una plataforma UTM (Unified Threat Management) orientada a la protección, monitoreo y administración de redes informáticas. Esta distribución está basada en tecnologías GNU/Linux y reúne en una sola solución servicios de firewall, traducción de direcciones de red (NAT), redes privadas virtuales (VPN), proxy web, filtrado de contenido, control de acceso, prevención de intrusiones y administración centralizada. Gracias a estas características, Endian se convierte en una herramienta robusta para implementar esquemas de seguridad perimetral tanto en ambientes empresariales reales como en laboratorios académicos.

La infraestructura fue desplegada en un entorno virtualizado mediante Oracle VM VirtualBox, lo que permitió simular una red empresarial sin necesidad de hardware adicional.
Sobre esta plataforma se integraron tres máquinas virtuales principales: el firewall Endian, un cliente con Ubuntu Desktop y un servidor con Ubuntu Server. Cada sistema fue configurado con interfaces y direcciones IP específicas para representar distintos segmentos de red y validar la interacción entre ellos.

Instalación y configuración de Endian

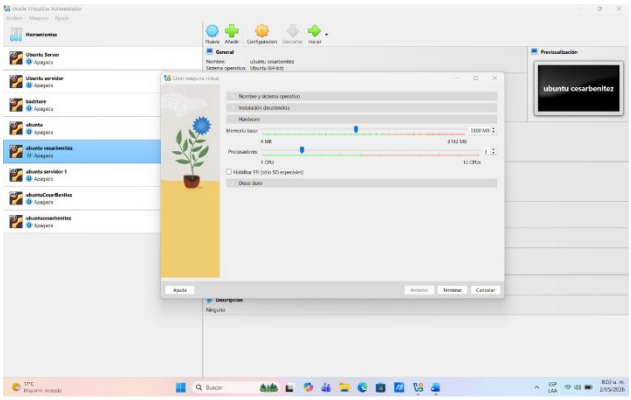
Se inició con la creación de una máquina virtual en VirtualBox, asignando 3800 MB de memoria RAM, tres procesadores y un disco duro de 20 GB. Posteriormente, se cargó la imagen ISO de GNU/Linux Endian para iniciar el proceso de instalación.

Figura 1. Creación de la máquina Virtual



Fuente: Autoría propia

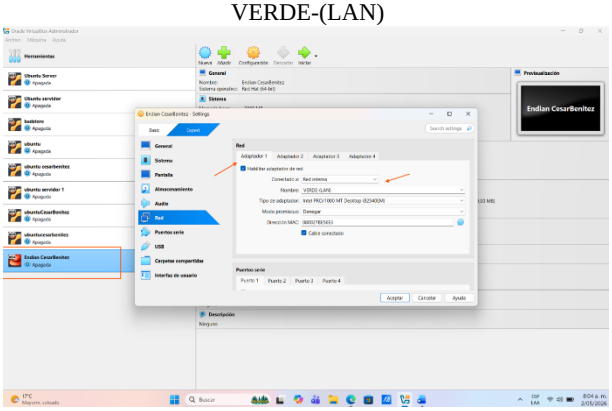
Figura 2. Requerimientos de Hardware



Fuente: Autoría propia

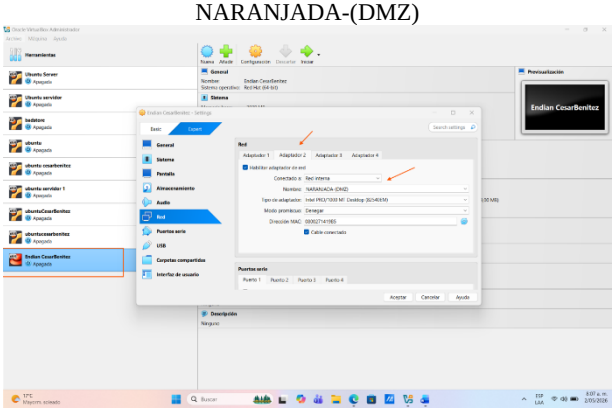
Durante la configuración de red, se definieron tres adaptadores: uno para la red interna (LAN), otro para la DMZ y un tercero mediante NAT para la conexión a internet (WAN). Adicionalmente, se configuró un cliente Ubuntu Desktop en la LAN y un servidor Ubuntu en la DMZ con IP estática 192.168.1.22. Finalmente, se accedió a la interfaz web del firewall para completar la configuración.

Figura 3. Adaptador 1 conectado a Red interna nombre VERDE-(LAN)



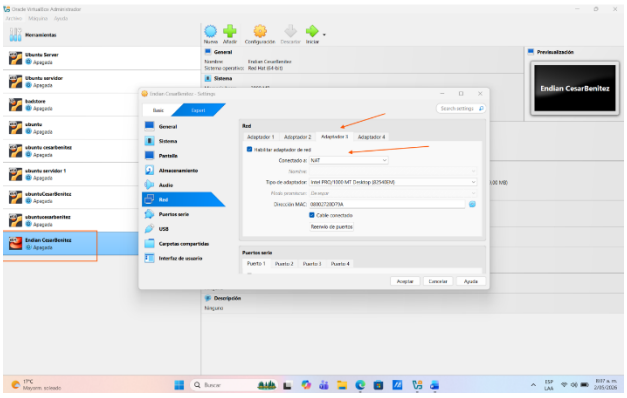
Fuente: Autoría propia

Figura 4. Adaptador 2, conectado a Red interna nombre NARANJADA-(DMZ)



Fuente: Autoría propia

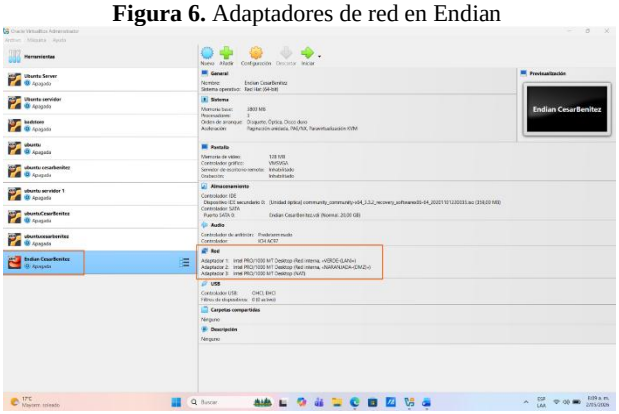
Figura 5. Adaptador 3, conectado a NAT.



Fuente: Autoría propia

Configurando cada adaptador de red en Endian podemos ver los 3 adaptadores guardados y listos para utilizarlos en Ubuntu desktop y el servidor de Ubuntu.

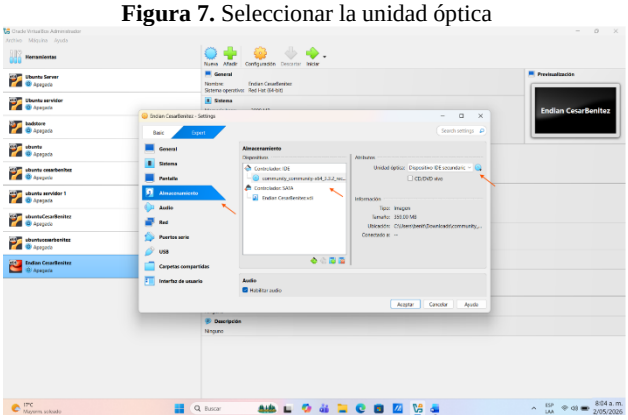
Figura 6. Adaptadores de red en Endian



Fuente: Autoría propia

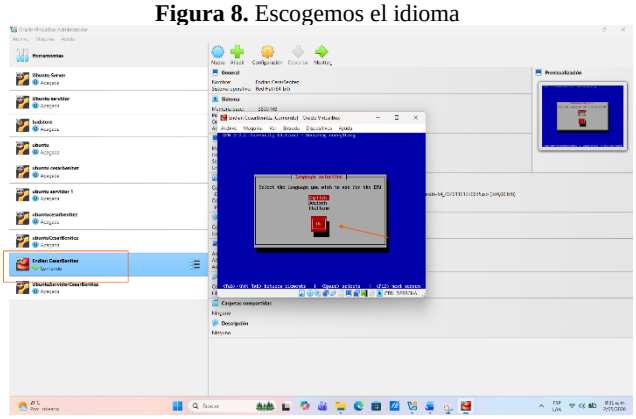
En VirtualBox vamos a almacenamiento, Controlador IDE y seleccionamos la Unidad óptica el archivo que descargamos de internet para que arranque Endian.

Figura 7. Seleccionar la unidad óptica



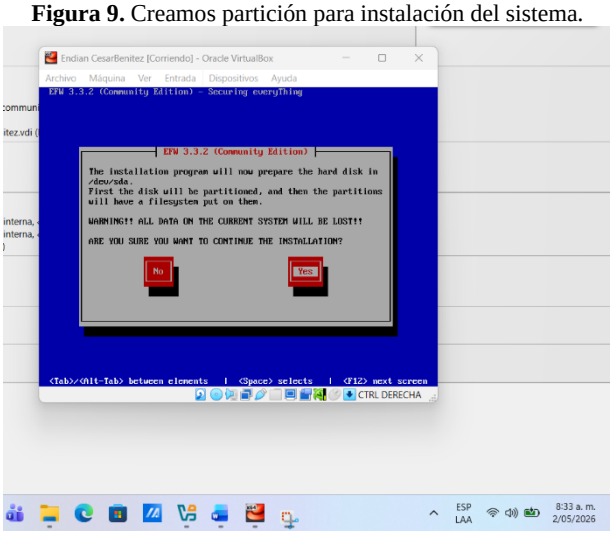
Fuente: Autoría propia

Figura 8. Escogemos el idioma



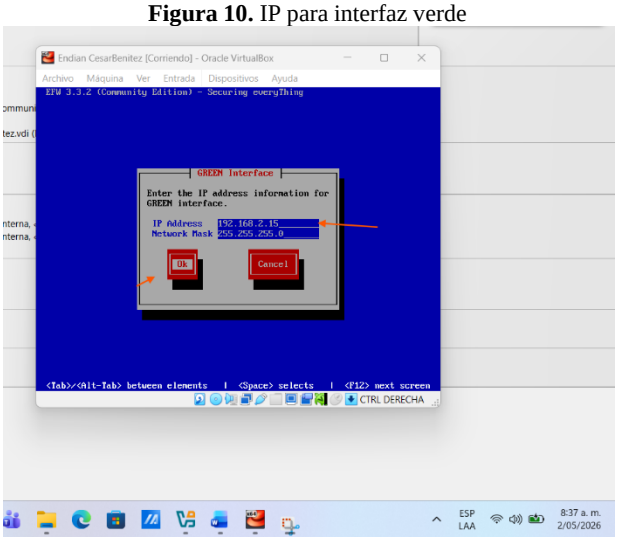
Fuente: Autoría propia

Figura 9. Creamos partición para instalación del sistema.



Fuente: Autoría propia

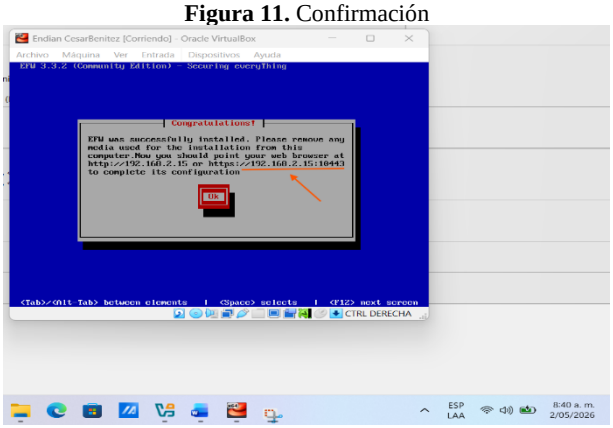
Figura 10. IP para interfaz verde



Fuente: Autoría propia

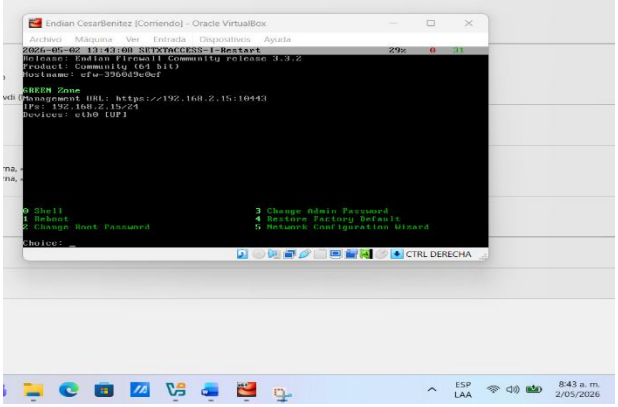
Confirma acceso vía navegador web a las direcciones: HTTP://192.168.2.15 o HTTPs://192.168.2.15:10443 que es la IP o la dirección con la que podemos ingresar desde cliente Ubuntu Desktop para configurar.

Figura 11. Confirmación



Fuente: Autoría propia

Figura 12. Evidencia de inicio de Endian.



Fuente: Autoría propia

Una vez finalizada la instalación, se accedió a la interfaz gráfica de Endian (dashboard) a través HTTPs://:10443.

3. IMPLEMENTANDO SEGURIDAD EN GNU/LINUX

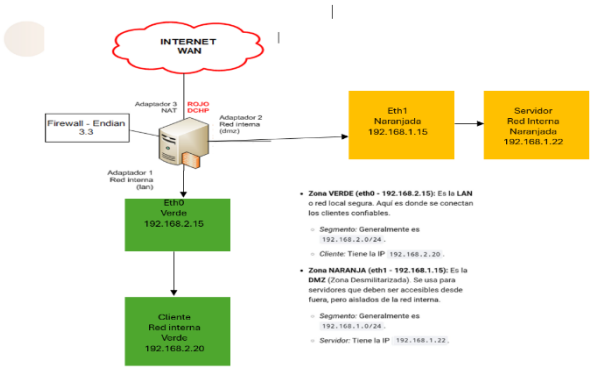
3.1 CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX (TARJETAS DE RED) E INSTALACIÓN EFECTIVA DEL MISMO.

Objetivo General

Realizar la configuración de una máquina virtual de Endian UTM en VirtualBox, ajustando las tarjetas de red y llevando a cabo la instalación del sistema. La implementación contempla el uso de las zonas de seguridad verde, roja y naranja, donde la zona verde corresponde a la red interna (LAN), la zona roja al acceso a Internet (WAN) y la zona naranja al segmento destinado a servidores o DMZ.

A través de un diagrama podemos ver la segmentación de red que será usada para el desarrollo de cada una de las temáticas, El diagrama nos muestra a través de señalización y color para una interpretación más eficiente.

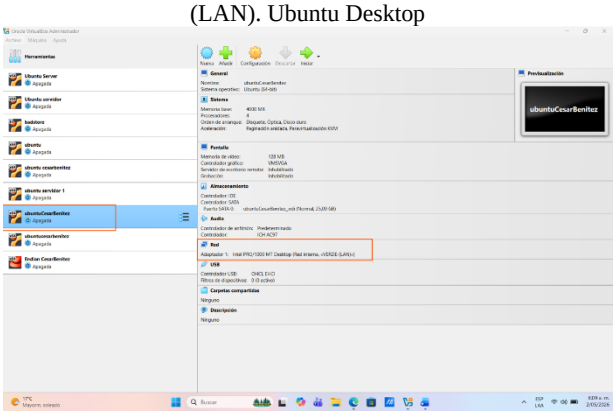
Figura 13. Diagrama de segmentación de red



Fuente: Autoría propia

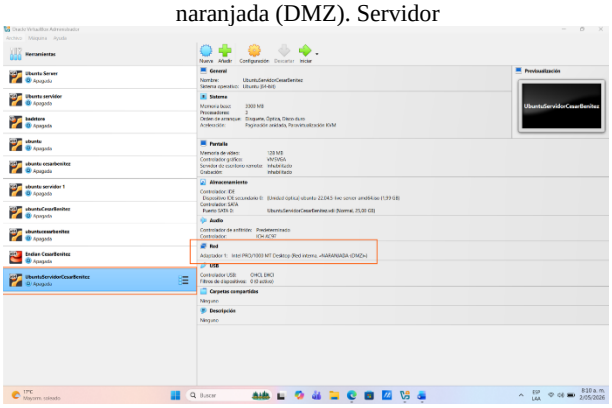
Configuración de red en el desktop y en el server.

Figura 14. Red adaptador1, conectado a Red interna, VERDE (LAN). Ubuntu Desktop



Fuente: Autoría propia

Figura 15. Red adaptador1, conectado a Red interna, naranjada (DMZ). Servidor

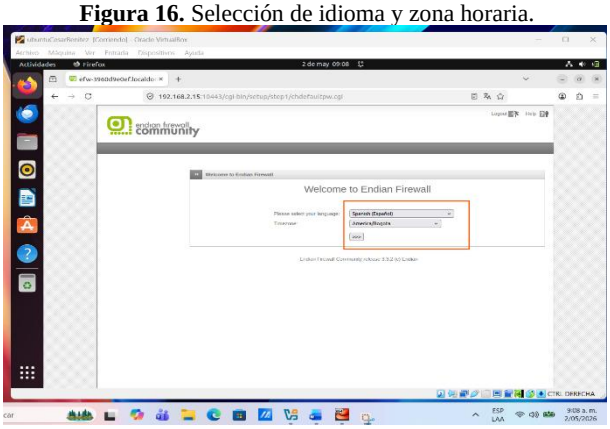


Fuente: Autoría propia

Proceso de instalación y configuración Endian a nivel web.

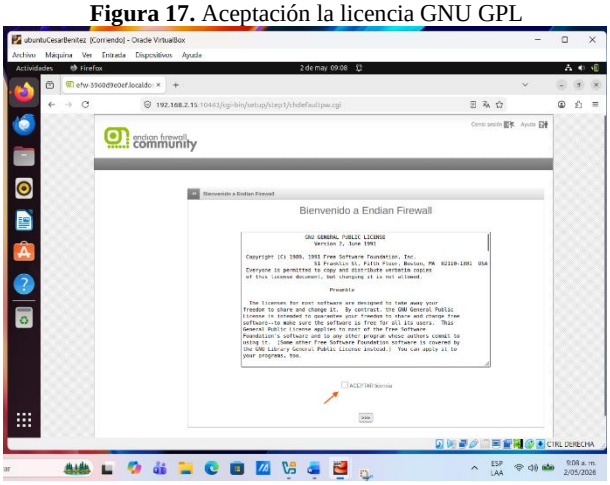
Accedemos a la interfaz gráfica de Endian a través de HTTPs://192.168.2.15:10443

Figura 16. Selección de idioma y zona horaria.



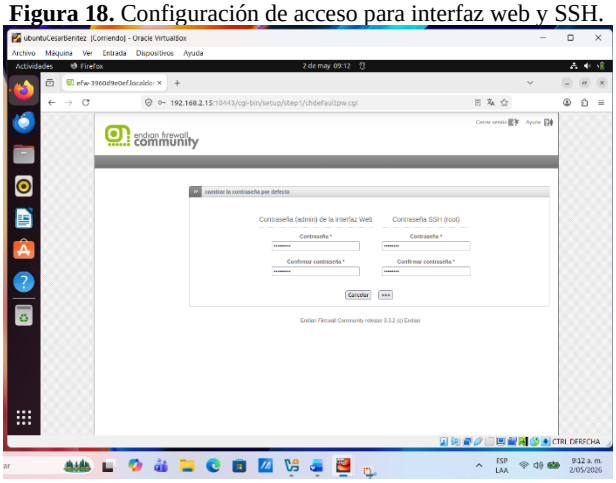
Fuente: Autoría propia

Figura 17. Aceptación la licencia GNU GPL



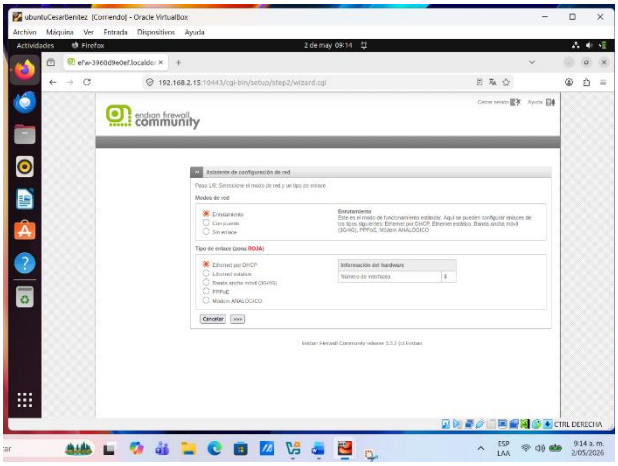
Fuente: Autoría propia

Figura 18. Configuración de acceso para interfaz web y SSH.



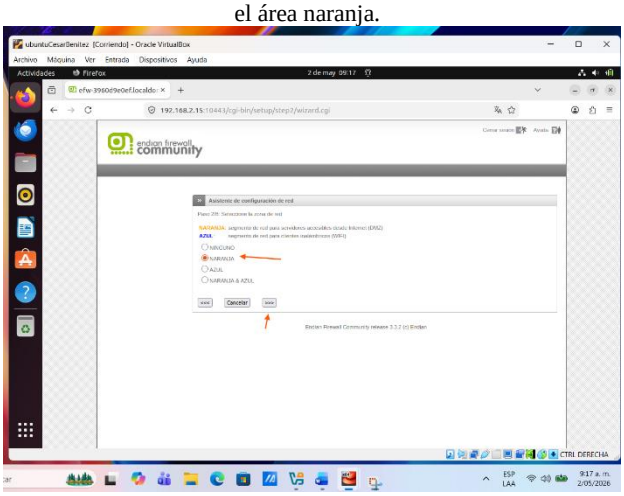
Fuente: Autoría propia

Figura 19. indica los modos de red por enrutamiento, Ethernet por DHCP, el cual tiene 3 tarjetas de red configuradas el servidor de Endian.



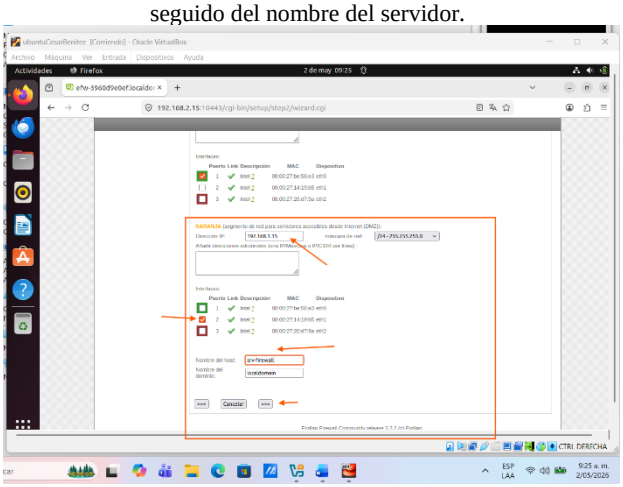
Fuente: Autoría propia

Figura 20. Podemos ver el proceso para configurar el área naranja, como ya tenemos una tarjeta verde en la cual estamos trabajando, roja que es la del internet, entonces seleccionamos el área naranja.



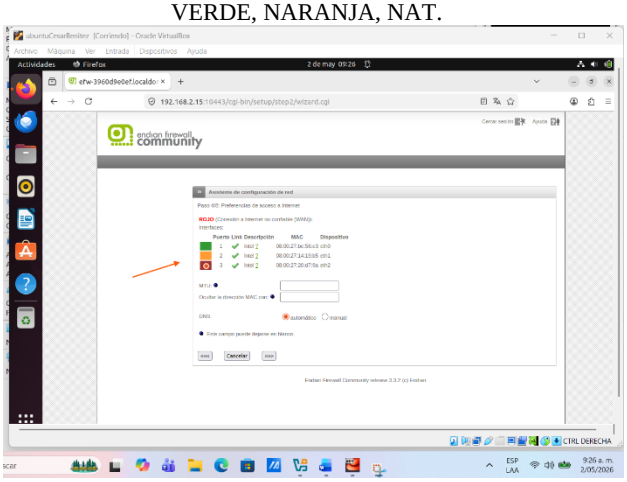
Fuente: Autoría propia

Figura 21. Demostración del ingreso de la ip de la red anaranjada asignada en la segmentación y selección de interfaz seguido del nombre del servidor.



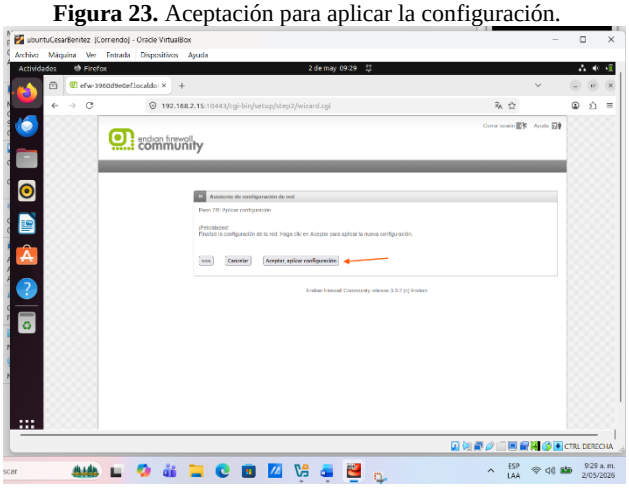
Fuente: Autoría propia

Figura 22. Demostración de la configuración de las 3 zonas VERDE, NARANJA, NAT.



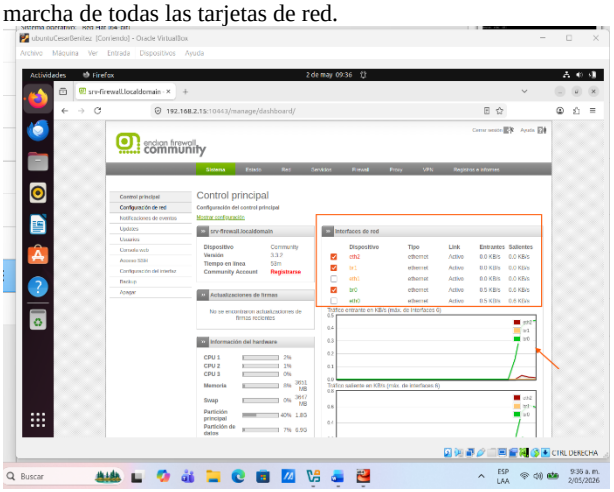
Fuente: Autoría propia

Figura 23. Aceptación para aplicar la configuración.



Fuente: Autoría propia

Figura 24. Demostración de la configuración y puesta en marcha de todas las tarjetas de red.

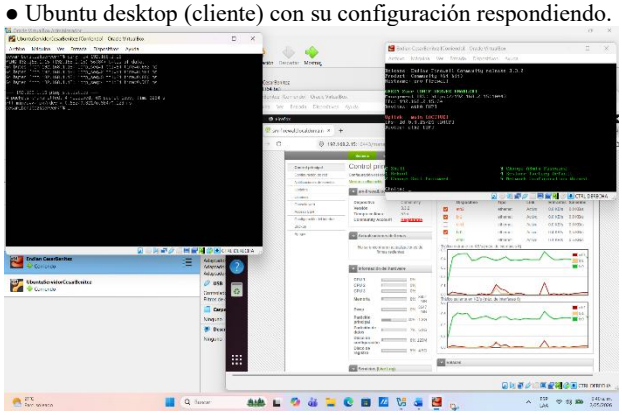


Fuente: Autoría propia

Demostración e implementación de GNU/Linux Endian con las zonas verde, roja y naranja, así: Zona verde: Red interna (LAN), Zona roja: Acceso a internet (WAN) y Zona naranja: Servidores (DMZ).

Figura 25. Muestra que funcionó la instalación y los 3 ambientes.

- Endian con sus Configuraciónes.
- Ubuntu Server con su configuración y conexión con el servidor.
- Ubuntu desktop (cliente) con su configuración respondiendo.



Fuente: Autoría propia

3.2 CONFIGURACIÓN NAT MEDIANTE GNU/LINUX ENDIAN PARA LA COMUNICACIÓN ENTRE LAN, DMZ Y WAN

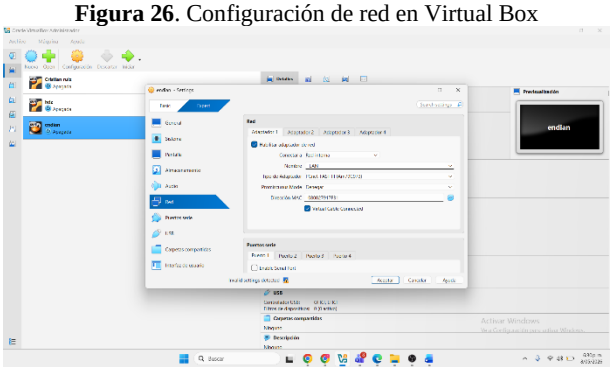
Objetivo general

La Traducción de Direcciones de Red (NAT) constituye uno de los mecanismos más utilizados en la administración de redes modernas debido a su capacidad para permitir la comunicación entre redes privadas y redes externas como Internet. En entornos empresariales, NAT desempeña un papel fundamental tanto en la optimización de direcciones IP como en la seguridad de las infraestructuras tecnológicas.

En el desarrollo de la presente temática se implementó un escenario de seguridad perimetral utilizando GNU/Linux Endian Firewall Community como plataforma principal de administración y control de tráfico. La arquitectura de red implementada estuvo compuesta por tres segmentos fundamentales: una red local o LAN destinada a los clientes internos, una zona desmilitarizada (DMZ) utilizada para alojar servidores y una red WAN encargada de simular el acceso hacia Internet.

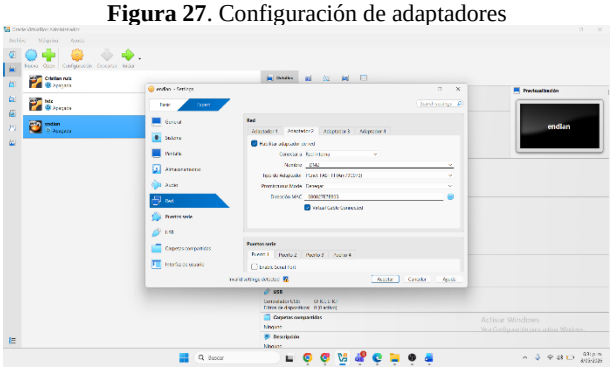
La finalidad principal de la configuración consistió en establecer reglas NAT que permitieran la salida controlada de tráfico desde la red LAN hacia la WAN y desde la DMZ hacia Internet, verificando además la correcta creación y funcionamiento de dichas reglas dentro del firewall.
Inicialmente se procedió a la instalación y configuración de GNU/Linux Endian en un entorno virtualizado mediante VirtualBox. Posteriormente se configuraron las interfaces de red correspondientes a cada zona. La zona GREEN fue utilizada para representar la LAN, la zona ORANGE para la DMZ y la zona RED para la conexión hacia Internet.

Figura 26. Configuración de red en Virtual Box



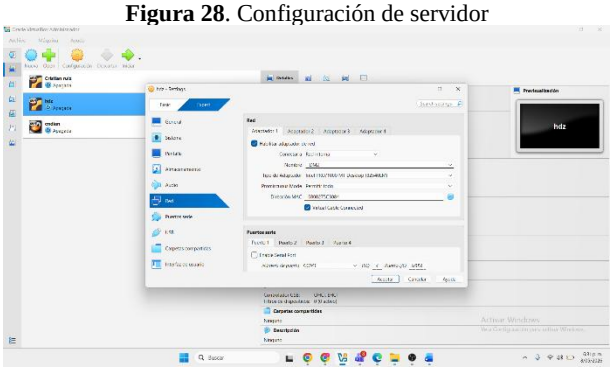
Fuente: Autoría propia

Figura 27. Configuración de adaptadores



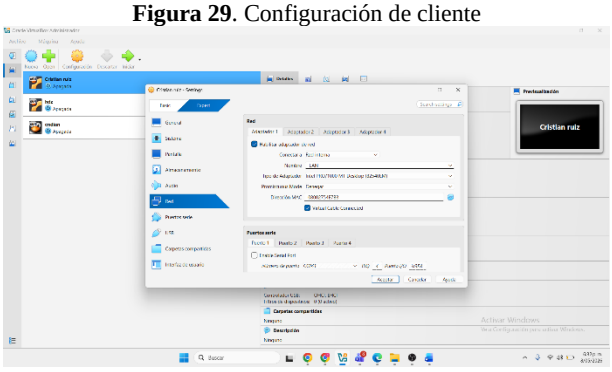
Fuente: Autoría propia

Figura 28. Configuración de servidor



Fuente: Autoría propia

Figura 29. Configuración de cliente



Fuente: Autoría propia

Una vez establecida la arquitectura de red, se configuraron direcciones IP estáticas para cada segmento. El cliente perteneciente a la LAN fue configurado con direccionamiento interno, mientras que el servidor ubicado en la DMZ recibió una dirección independiente con el fin de segmentar adecuadamente el tráfico de red.

Posteriormente se accedió a la interfaz administrativa de Endian Firewall para la creación de reglas NAT tipo Source NAT. La primera regla permitió el establecimiento de comunicación desde la red LAN hacia la WAN, posibilitando que los equipos internos accedieran a servicios externos mediante traducción de direcciones IP privadas.

La segunda regla NAT permitió el acceso desde la zona DMZ hacia Internet. Esta configuración resultó fundamental para garantizar que el servidor pudiera establecer conexiones externas controladas sin comprometer la seguridad de la red interna.

Las reglas fueron configuradas desde el apartado “Firewall > NAT > Source NAT”, especificando las redes de origen, zonas de destino y políticas de traducción automática de direcciones.

Figura 30. Creacion de reglas en NAT

Fuente: Autoría propia

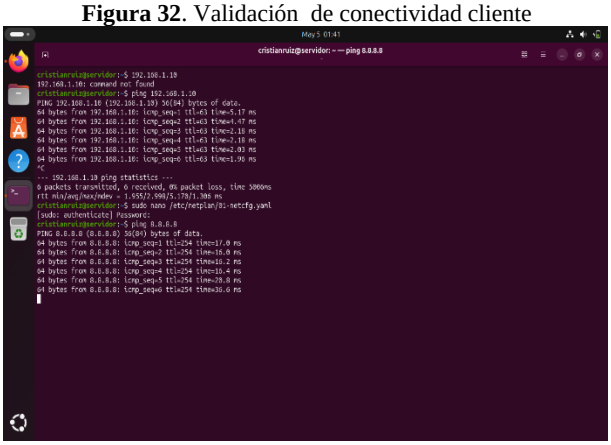
Figura 31. Creación de regla en Destination NAT

Fuente: Autoría propia

Posteriormente se realizaron pruebas de conectividad desde la LAN utilizando herramientas de diagnóstico de red como el comando ping y pruebas de navegación web. Los resultados obtenidos permitieron comprobar el acceso exitoso desde la red interna hacia direcciones externas, validando el correcto funcionamiento de la primera regla NAT implementada.

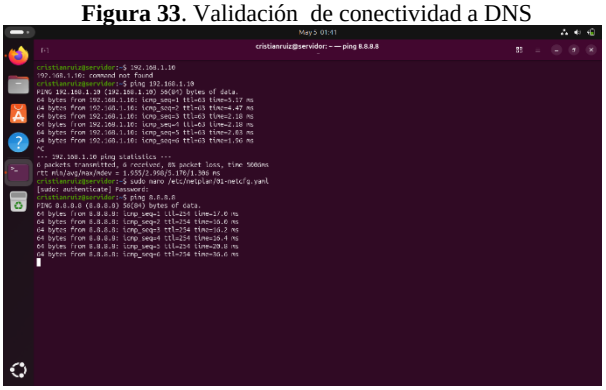
De igual manera se efectuaron pruebas desde el servidor ubicado en la DMZ hacia Internet, verificando la conectividad mediante el envío de paquetes ICMP hacia direcciones públicas como 8.8.8.8. Las pruebas demostraron una comunicación satisfactoria desde la DMZ hacia la WAN, evidenciando el correcto comportamiento de las políticas NAT configuradas en el firewall

Figura 32. Validación de conectividad cliente



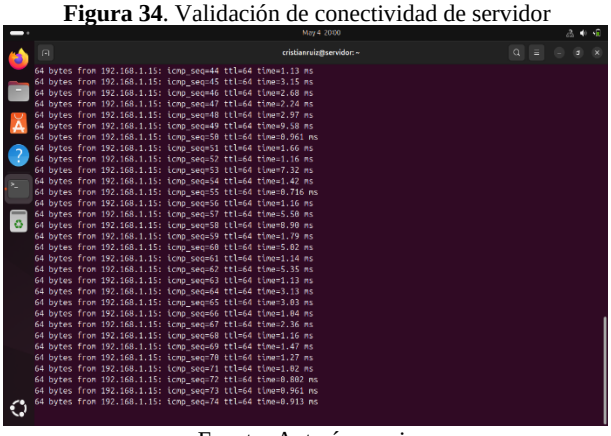
Fuente: Autoría propia

Figura 33. Validación de conectividad a DNS



Fuente: Autoría propia

Figura 34. Validación de conectividad de servidor

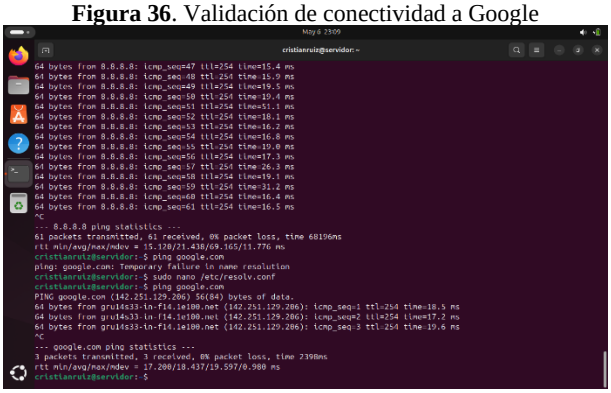


Fuente: Autoría propia

Figura 35. Validación de conectividad a DNS

Fuente: Autoría propia

Figura 36. Validación de conectividad a Google



Fuente Autoría propia

La implementación desarrollada permitió comprender la importancia de la traducción de direcciones de red dentro de infraestructuras empresariales basadas en GNU/Linux. Asimismo, se evidenció que el uso de zonas segmentadas como LAN y DMZ incrementa significativamente la seguridad de los servicios expuestos a redes externas.

Finalmente, los resultados obtenidos demostraron que GNU/Linux Endian constituye una herramienta eficiente para la administración de seguridad perimetral, permitiendo centralizar el control de tráfico, aplicar reglas NAT y segmentar redes de manera organizada y segura

3.3 PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED.

La administración de la seguridad perimetral se basó en la segmentación de tráfico y la exposición controlada de servicios críticos hacia redes externas. Para ello, se configuró una arquitectura de Zona Desmilitarizada (DMZ) utilizando un firewall como nodo de inspección, permitiendo el flujo de datos hacia el servidor interno con dirección IP 192.168.1.22 mediante políticas de Traducción de Direcciones de Red (NAT) y reglas de filtrado de paquetes.

IMPLEMENTACIÓN Y VALIDACIÓN DEL SERVICIO HTTP (PUERTO 80)

Se procedió a la creación de una regla de redireccionamiento de puerto (DNAT) en el firewall. Esta

política vincula de forma estricta las peticiones entrantes por el puerto 80 hacia el servidor web ubicado en el segmento DMZ. Esta configuración permite que el servidor web sea accesible desde internet de forma controlada, canalizando el tráfico de hipertexto sin comprometer la integridad de la red interna.

Figura 37. Creación de la regla para el servicio HTTP.

Fuente: Autoría propia

La validación se ejecutó en dos fases. Primero, en el servidor destino, se auditó el estado del servicio apache2 mediante la herramienta systemctl, confirmando su operatividad.

Figura 38. Verificación del servicio HTTP instalado.

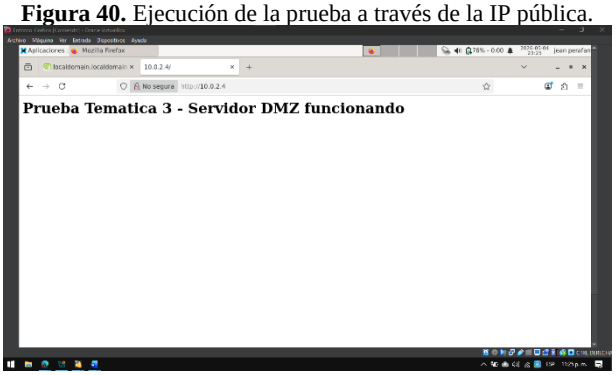
Fuente: Autoría propia

Segundo, se desplegó una página de prueba personalizada (index.html) en la ruta /var/www/html/. Finalmente, se realizó una petición externa a través de la dirección IP pública 10.0.2.4, obteniendo una respuesta visual exitosa que ratifica la correcta conmutación de paquetes a través del firewall.

Figura 39. Creación de la página web.

Fuente: Autoría propia

Figura 40. Ejecución de la prueba a través de la IP pública.

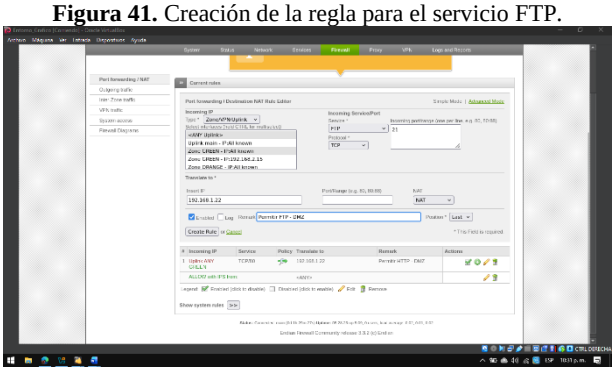


Fuente: Autoría propia

Implementación y validación del servicio FTP (Puerto 21)

Se estableció una política de direccionamiento para el protocolo FTP sobre el puerto 21. La regla se diseñó para permitir el intercambio de activos en la "Zona Naranja", asegurando que el flujo de datos para la transferencia de archivos se realice bajo los parámetros de filtrado y las tablas de NAT definidas. Esto garantiza una gestión de archivos centralizada y protegida por la infraestructura de seguridad.

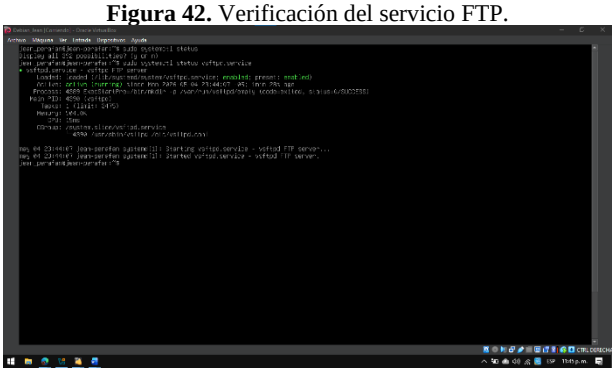
Figura 41. Creación de la regla para el servicio FTP.



Fuente: Autoría propia

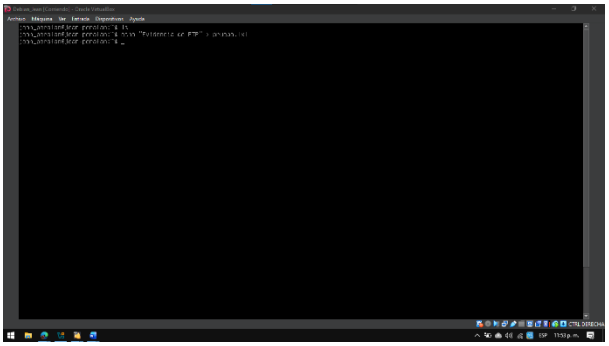
Para corroborar el acceso, se verificó inicialmente que el demonio vsFTPd estuviera activo en el servidor Debian. Posteriormente, se generó un archivo de control denominado prueba.txt con metadatos de evidencia.

Figura 42. Verificación del servicio FTP.



Fuente: Autoría propia

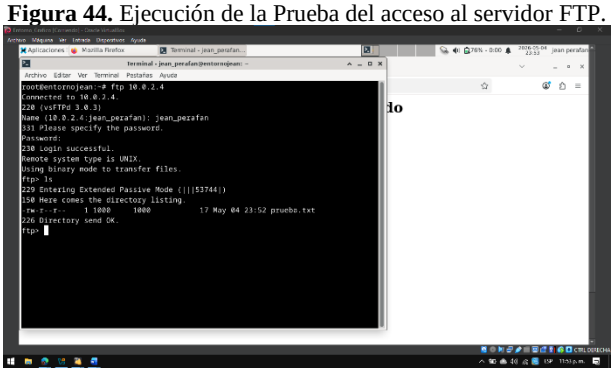
Figura 43. Creación del archivo de prueba.



Fuente: Autoría propia

La prueba final consistió en la autenticación desde un cliente externo mediante la IP pública 10.0.2.4; tras la validación de credenciales, se realizó un listado de directorios y la descarga del archivo de prueba, certificando la transparencia y efectividad del canal de comunicación.

Figura 44. Ejecución de la Prueba del acceso al servidor FTP.

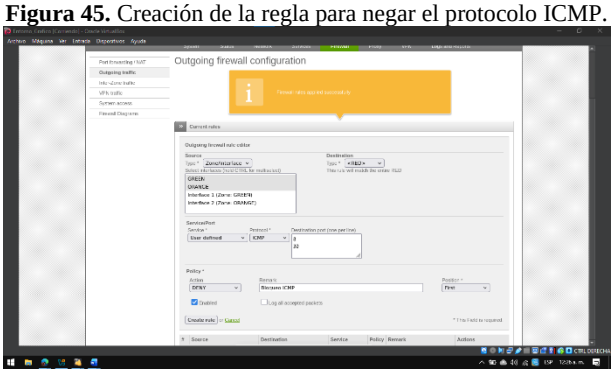


Fuente: Autoría propia

Restricción y bloqueo del protocolo ICMP (PING)

Con el objetivo de mitigar vectores de reconocimiento de red y escaneo de hosts, se implementó una regla de denegación absoluta (DENY) para el protocolo ICMP, específicamente para los tipos 8 (Echo Request) y 30. La directiva se posicionó en la parte superior de la cadena de reglas del firewall para garantizar su prioridad jerárquica sobre cualquier otra política de tráfico permitida.

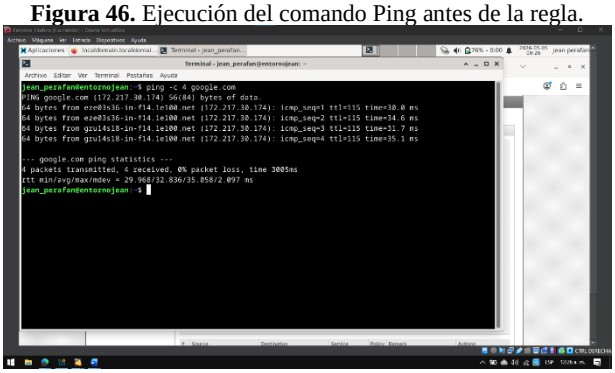
Figura 45. Creación de la regla para negar el protocolo ICMP.



Fuente: Autoría propia

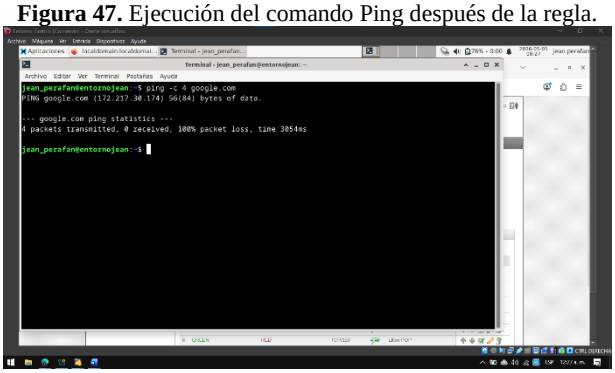
Se realizó una auditoría de conectividad mediante el comando ping hacia dominios externos (ej. google.com) antes y después de la aplicación de la regla. Mientras que inicialmente se registraba una respuesta estable, tras la activación de la política de bloqueo se obtuvo una pérdida de paquetes del 100%. Este resultado confirma que el firewall intercepta y descarta correctamente las solicitudes de eco, invisibilizando los dispositivos de la red ante diagnósticos externos.

Figura 46. Ejecución del comando Ping antes de la regla.



Fuente: Autoría propia

Figura 47. Ejecución del comando Ping después de la regla.



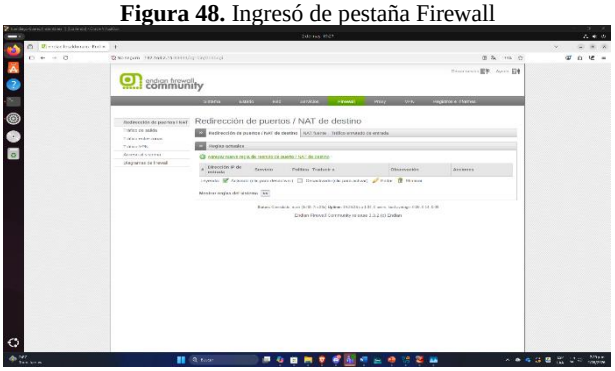
Fuente: Autoría propia

3.4 REGLAS DE ACCESO PARA PERMITIR O DENEGAR TRÁFICO

Objetivo General

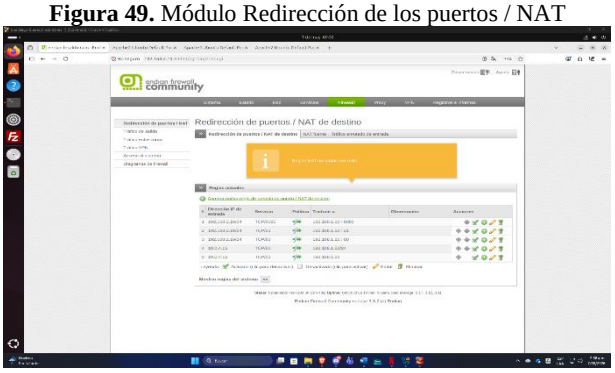
Establecer, configurar y verificar reglas de acceso en una arquitectura de red segmentada, con el fin de permitir y controlar el tráfico entre las zonas LAN, DMZ e Internet mediante los protocolos HTTP y FTP, garantizando la conectividad requerida y la seguridad de los servicios expuestos, mediante pruebas de acceso en un navegador web y otras herramientas de red.

Figura 48. Ingresó de pestaña Firewall



Fuente: Autoría propia

Figura 49. Módulo Redirección de los puertos / NAT



Fuente: Autoría propia

Redireccionamiento de los puertos (NAT)

En el módulo se demuestra la creación de la tabla con las reglas para la redirección de puertos HTTP y FTP, zona internet con DMZ.

Regla 1, Conexión zona internet con DMZ

- IP origen: 192.168.2.16/24
- Servicio: TCP/8080
- IP destino traducido: 192.168.1.22:8080

Regla 2, Conexión FTP mediante puerto 21

- IP origen: 192.168.2.16/24
- Servicio: TCP/21
- IP destino traducido: 192.168.1.22:21

Regla 3, Conexión HTTP mediante puerto 80

- IP origen: 192.168.2.16/24
- Servicio: TCP/80
- IP destino traducido: 192.168.1.22:80

Regla 4, Conexión WAN - HTTP mediante puerto 80

- IP origen: 10.0.4.15
- Servicio: TCP/80
- IP destino traducido: 192.168.1.22/24

Regla 5, Conexión WAN - FTP mediante puerto 21

- IP origen: 10.0.4.15
- Servicio: TCP/21
- IP destino traducido: 192.168.1.22

Figura 50. Tráfico entre Zonas "Firewall Inter-Zona"

Fuente: Autoría propia

Configuración tráfico Entre Zonas

Regla 3, Tráfico Internet con DMZ

- Origen: VERDE
- Destino: NARANJA
- Servicio: TCP/8080
- Política: Permitir

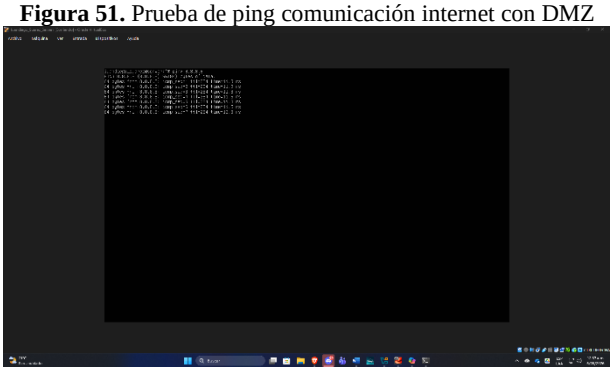
Regla 4, Tráfico de servicio mediante FTP

- Origen: VER
- Destino: NARANJA
- Servicio: TCP/21
- Política: Permitir

Regla 5, Tráfico de servicio mediante HTTP

- Origen: VERDE
- Destino: NARANJA
- Servicio: TCP/80
- Política: Permitir

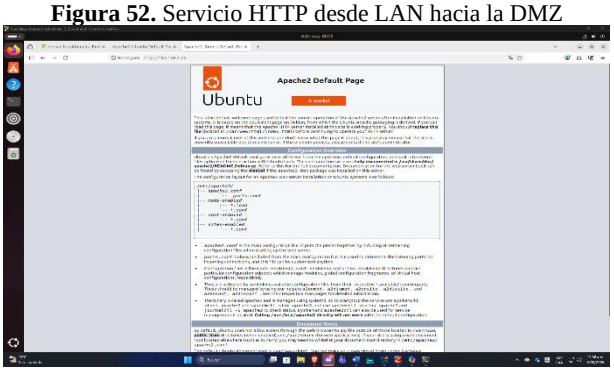
Figura 51. Prueba de ping comunicación internet con DMZ



Fuente: Autoría propia

- Se corrobora el ping 8.8.8.8, desde el servidor DMZ y se evidencia que hay respuesta de forma acertada.

Figura 52. Servicio HTTP desde LAN hacia la DMZ



Fuente: Autoría propia

- Se ingreso al navegador con la ip de la zona DMZ, este caso nuestro server, mediante la dirección ip HTTP://192.168.1.22:80

Figura 53. Servicio HTTP desde LAN hacia la zona WAN

Fuente: Autoría propia

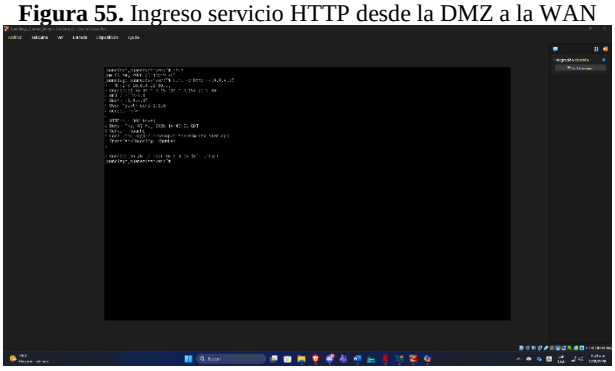
- Se ingreso al navegador con la ip de la zona DMZ, este caso nuestro server, mediante la dirección ip HTTP://10.0.4.15:80

Figura 54. Servicio HTTP desde LAN hacia la hacia la WAN

Fuente: Autoría propia

- Se ingresa al navegador con la dirección ip zona DMZ en el caso de nuestro server con la dirección HTTP://10.0.4.15:80

Figura 55. Ingreso servicio HTTP desde la DMZ a la WAN



Fuente: Autoría propia

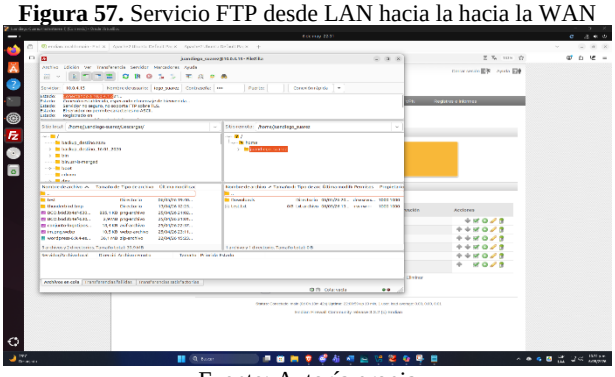
- Mediante el comando curl -v HTTP:/10.0.4.15 se ingresa a servicio HTTP DMZ hacia la WAN.

Figura 56. Ingresó servicio HTTP desde la DMZ hacia DMZ

Fuente: Autoría propia

- Por medio del servicio SSH se realiza la conexión desde Desktop en la terminal y se accede al servidor firewall Endian, para realizar la prueba de HTTP desde la WAN a DMZ, con el comando curl -v HTTP://192.168.1.22

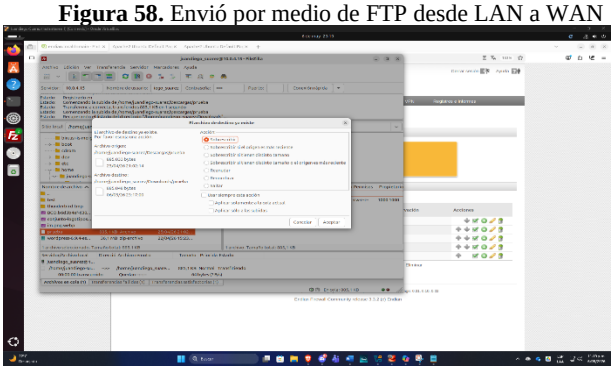
Figura 57. Servicio FTP desde LAN hacia la hacia la WAN



Fuente: Autoría propia

- Con la herramienta FileZilla, se realiza la conexión con usuario y contraseña al servicio FTP, con la dirección WAN 10.0.4.15 mediante el puerto 21, arroja conexión exitosa.

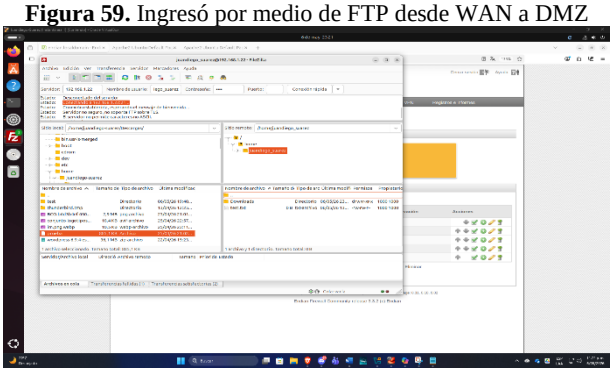
Figura 58. Envió por medio de FTP desde LAN a WAN



Fuente: Autoría propia

- Se evidencia envió desde el Desktop del servicio FTP con conexión a la WAN 10.0.4.15, arroja que se transfirió correctamente.

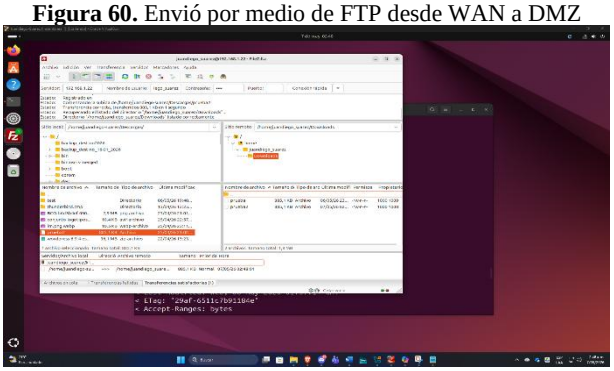
Figura 59. Ingresó por medio de FTP desde WAN a DMZ



Fuente: Autoría propia

- Mediante el servicio de FileZilla se realizó conexión de servicio FTP usando la ip del servidor 192.168.1.22 DMZ puerto 21, genera la conexión de forma correcta.

Figura 60. Envió por medio de FTP desde WAN a DMZ



Fuente: Autoría propia

- Se realiza envió de archivo prueba2 desde Ubuntu Desktop con el servicio FTP conectado al server DMZ dirección ip 192.168.1.22, transferencia exitosa.

3.5 IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE) CON POLÍTICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET.

Objetivo general

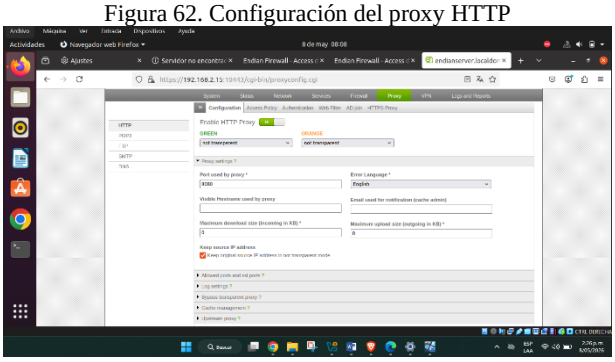
Diseñar e implementar un servidor Proxy HTTP en modo no transparente, con políticas de autenticación y filtrado de contenidos, que permita administrar y controlar de forma segura la navegación en Internet de los usuarios. Esta solución busca fortalecer la seguridad perimetral, optimizar el uso de los recursos de red y garantizar el cumplimiento de las normas de acceso en entornos basados en GNU/Linux.

Figura 61. Ingresó a Endian

Fuente: Autoría propia

Se ingresó a la interfaz web de GNU/Linux Endian Firewall mediante la dirección IP del servidor utilizando el puerto 10443.

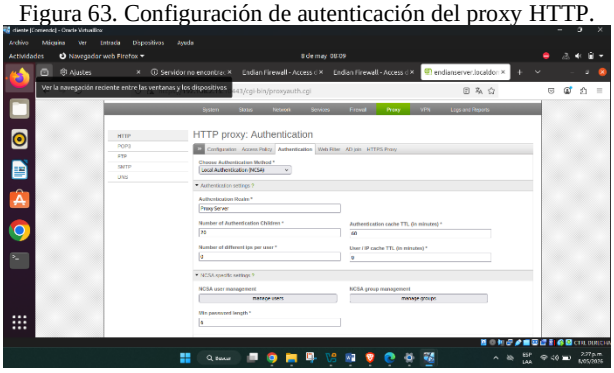
Figura 62. Configuración del proxy HTTP



Fuente: Autoría propia

En GNU/Linux Endian Firewall se habilitó el servicio HTTP Proxy configurándolo en modo no transparente para las zonas GREEN y ORANGE. Además, se estableció el puerto 8080 para controlar la navegación web de los usuarios de la red LAN

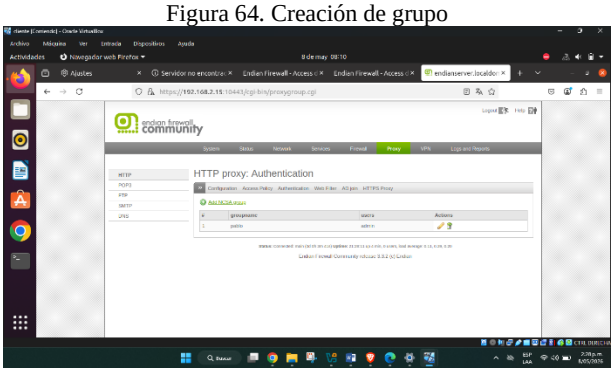
Figura 63. Configuración de autenticación del proxy HTTP.



Fuente: Autoría propia

Se configuró el método de autenticación local (NCSA) en GNU/Linux Endian Firewall para controlar el acceso al servicio proxy mediante usuarios autenticados. Además, se habilitó la administración de usuarios y grupos para aplicar políticas de acceso y filtrado web.

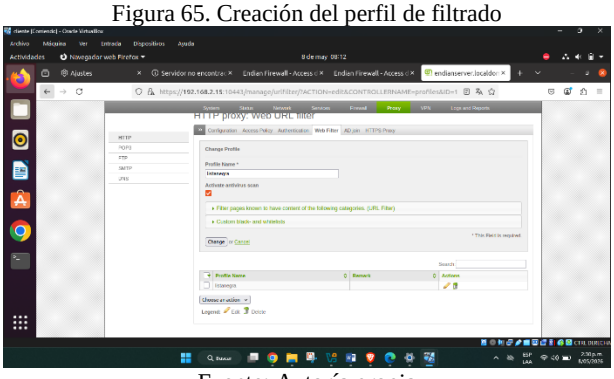
Figura 64. Creación de grupo



Fuente: Autoría propia

Se creó el grupo denominado pablo y se asoció el usuario admin para aplicar las políticas de acceso y filtrado web configuradas en el proxy HTTP.

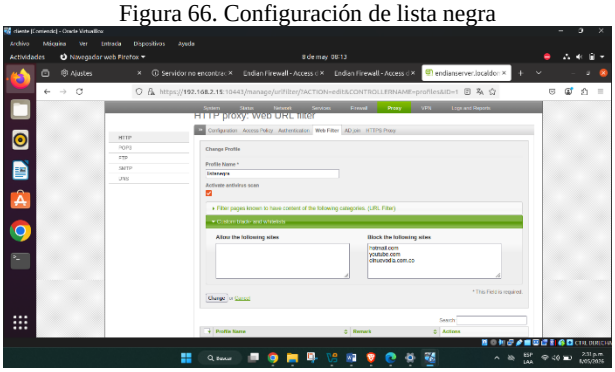
Figura 65. Creación del perfil de filtrado



Fuente: Autoría propia

Se creó el perfil de filtrado denominado lista negra para aplicar restricciones de navegación a determinados dominios web.

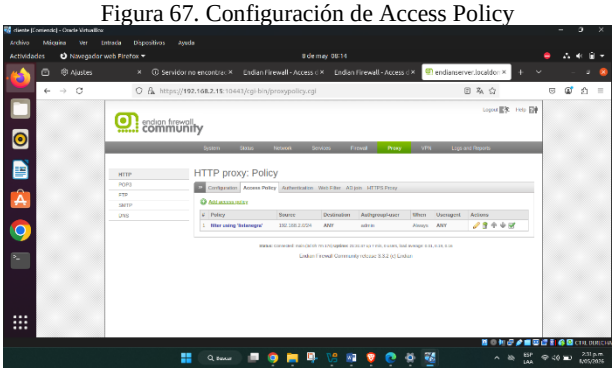
Figura 66. Configuración de lista negra



Fuente: Autoría propia

Se configuró una lista negra bloqueando los dominios hotmail.com, youtube.com y elnuevodia.com.co para restringir su acceso desde la red LAN.

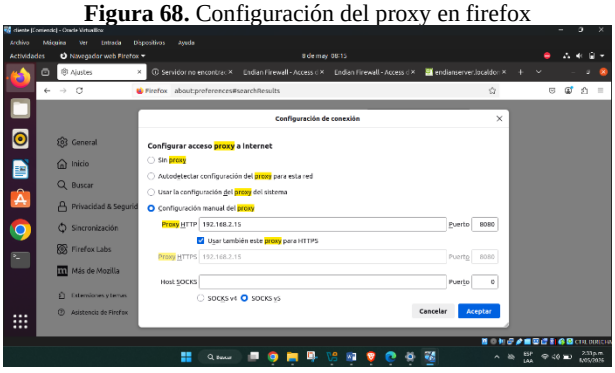
Figura 67. Configuración de Access Policy



Fuente: Autoría propia

Se configuró una política de acceso en GNU/Linux Endian Firewall asociando el usuario admin con el perfil de filtrado listanegra, permitiendo aplicar restricciones de navegación mediante el proxy HTTP a los usuarios autenticados de la red LAN.

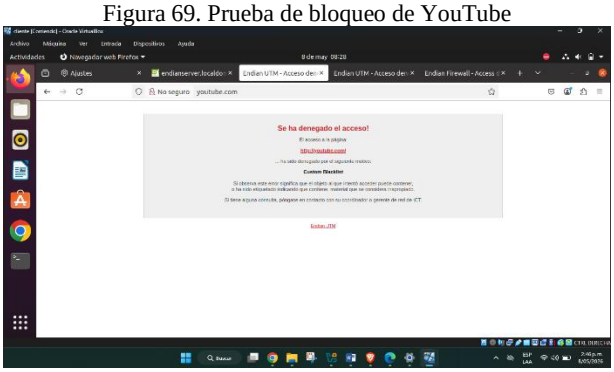
Figura 68. Configuración del proxy en firefox



Fuente: Autoría propia

En el navegador Firefox del cliente Ubuntu se configuró manualmente el proxy HTTP utilizando la dirección IP 192.168.2.15 y el puerto 8080. Además, se habilitó el uso del proxy para conexiones HTTPS con el fin de controlar la navegación web mediante GNU/Linux Endian Firewall.

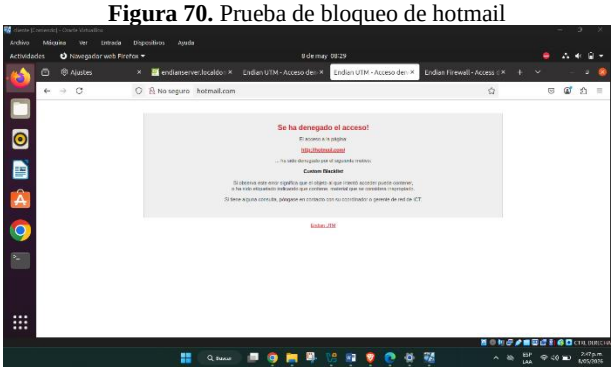
Figura 69. Prueba de bloqueo de YouTube



Fuente: Autoría propia

Al intentar acceder al sitio youtube.com, el proxy bloqueó correctamente la conexión mostrando el mensaje "Access Denied".

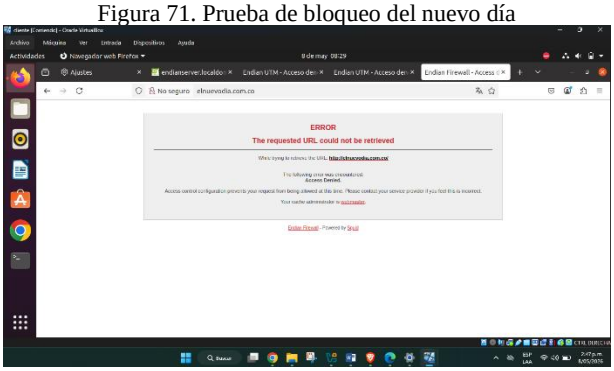
Figura 70. Prueba de bloqueo de hotmail



Fuente: Autoría propia

Se verificó el bloqueo del dominio hotmail.com mediante las políticas configuradas en el proxy HTTP.

Figura 71. Prueba de bloqueo del nuevo día



Fuente: Autoría propia

Se comprobó el correcto funcionamiento de la lista negra bloqueando el acceso al dominio elnuevodia.com.co.

4. Conclusiones.

La implementación de GNU/Linux Endian Firewall permitió establecer una infraestructura de seguridad organizada mediante la segmentación de la red en las zonas verde, roja y naranja. Esta distribución contribuye a un mejor control y administración del tráfico de red, optimizando la comunicación entre los diferentes segmentos y fortaleciendo la protección de los dispositivos frente a posibles amenazas o vulnerabilidades dentro del entorno implementado.

La configuración de NAT mediante GNU/Linux Endian Firewall permitió establecer de manera satisfactoria la comunicación entre las redes internas LAN y DMZ con la red externa WAN, evidenciando que una adecuada planificación de la arquitectura de red y el uso de un firewall como herramienta de administración centralizada son fundamentales para garantizar la conectividad, la seguridad y el control eficiente del tráfico en entornos GNU/Linux.

La configuración de reglas NAT y firewall permitió habilitar de forma segura los servicios HTTP y FTP en la zona DMZ, garantizando el acceso controlado desde redes externas, La validación de los servicios Apache2 y vsFTPd confirmó el correcto funcionamiento de los servidores y la adecuada implementación de las reglas.

La aplicación de reglas de acceso para HTTP y FTP demuestra que la seguridad en redes no se trata solo de bloquear o permitir tráfico, sino de encontrar un equilibrio entre protección y disponibilidad. Al definir políticas claras en el firewall, se asegura que los servicios funcionen de manera confiable y que los sistemas internos permanezcan resguardados frente a intentos de acceso no autorizados.

La implementación del Proxy HTTP en GNU/Linux Endian Firewall permitió controlar correctamente la navegación web de los usuarios de la red LAN. La autenticación mediante usuarios y grupos funcionó adecuadamente, permitiendo aplicar políticas de acceso específicas, además, el perfil de filtrado lista negra bloqueó exitosamente los sitios web configurados, demostrando el correcto funcionamiento del sistema de filtrado web y control de acceso. Las pruebas realizadas desde el cliente Ubuntu verificaron la efectividad de las políticas implementadas mediante mensajes de acceso denegado.

5. REFERENCIAS

[1] Apache Software Foundation. (2024). *Apache HTTP Server Documentation*. Recuperado de Apache HTTP Server Documentation

[2] Canonical Ltd. (2023). *Ubuntu Desktop Guide*. Recuperado de Canonical Ubuntu Documentation

[3]. Jay LaCroix. (2020). Mastering Ubuntu Server: Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting Packt Publishing. Disponible en: HTTPs://research-ebsco com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b881bf7 2 20a7-343c-94a8-f12e88b41952.

[4] Comer, D. E. (2018). *Internetworking with TCP/IP* (6th ed.). Pearson.

[5] Debian Documentation Project. (2023). *Debian Administrator's Handbook*. Recuperado de Debian Documentation Project

[6] Endian. (2024). *Endian Firewall Community Documentation*. Recuperado de Endian Firewall Community Documentation

[7] Internet Engineering Task Force. (1999). *RFC 2663: IP Network Address Translator (NAT) Terminology and Considerations*. Recuperado de IETF RFC 2663

[8] Linux Foundation. (2020). *Linux Networking Documentation*. Recuperado de Linux Kernel Documentation

[9] Pramatarov, M. (2026). *FTP vs HTTP: Understanding the Key Differences*. ClouDNS Blog. Recuperado de ClouDNS Blog

[10] vsFTPd Project. (2024). *Very Secure FTP Daemon Documentation*. Recuperado de vsFTPd Official Site