Implementación de un Esquema de Seguridad Perimetral en GNU/Linux mediante Endian Firewall

Jhon Deivy Garcia Caicedo
e-mail: jdgarciacai@unadvirtual.edu.co
Jhonnathan Alexander Marines
e-mail: jamarinesb@unadvirtual.edu.co
Ingrid Tatiana Lenis Gutiérrez
e-mail: itlenisg@unadvirtual.edu.co
Juan Camilo Rincón Ruiz
e-mail: jcrinconru@unadvirtual.edu.co
Leonardo Galvis Ramirez
e-mail: lgalvisra@unadvirtual.edu.co

RESUMEN: *Este artículo presenta el desarrollo de una serie de actividades prácticas orientadas a la administración de sistemas operativos basados en GNU/Linux y la implementación de un esquema de seguridad perimetral mediante el firewall Endian. A lo largo del trabajo se abordan conceptos fundamentales de arquitectura de sistema, procesos de arranque, gestión de hardware, servicios del sistema, administración de redes y configuración avanzada de zonas de seguridad (GREEN, ORANGE y RED). Se incluye la instalación de Endian en un entorno virtualizado, la creación de reglas de NAT para permitir la comunicación entre LAN, DMZ y WAN, y la verificación funcional mediante pruebas de conectividad. Los resultados evidencian la correcta aplicación de enmascaramiento de direcciones, segmentación de red y control de tráfico, demostrando el uso efectivo de herramientas Open Source para la seguridad perimetral.*

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

I. INTRODUCCIÓN

El diplomado de profundización en sistemas operativos Open Source integra actividades prácticas orientadas al fortalecimiento de habilidades técnicas en áreas como arquitectura del sistema, administración del arranque, gestión de servicios, monitoreo del sistema y configuración de redes.

La Etapa aborda la implementación de un esquema de seguridad perimetral utilizando el firewall Endian, integrando conceptos avanzados como segmentación de redes mediante zonas (LAN, DMZ y WAN), traducción de direcciones de red (NAT), políticas de firewall y reenvío de puertos. A través del análisis y aplicación de estas herramientas, se busca que el estudiante adquiera competencias sólidas en la configuración de servicios esenciales, la protección del perímetro de red y la administración eficiente de entornos virtualizados.

El presente artículo documenta el desarrollo completo de la actividad, desde el análisis teórico inicial hasta la implementación técnica y verificación de resultados, proporcionando un aporte significativo a la comprensión de la seguridad de redes en entornos basados en Linux.

II. METODOLOGIA

La metodología aplicada en este proyecto se estructuró en cinco etapas: configuración inicial del firewall Endian y sus zonas GREEN, RED y ORANGE; implementación de reglas NAT para permitir la comunicación de la LAN y la DMZ hacia la WAN; habilitación de servicios HTTP y FTP dentro de la DMZ junto con el bloqueo de ICMP; creación de reglas de acceso entre zonas para controlar el tráfico según los protocolos requeridos; y finalmente, la configuración de un proxy HTTP no transparente con autenticación y lista negra para restringir dominios específicos. Cada una de estas etapas se desarrolla detalladamente en las subsecciones siguientes.

A. Configuración de la instancia para GNU/Linux Endian en Virtualbox (tarjetas de red) e instalación efectiva del mismo (Temática 1)

Este artículo presenta el proceso de configuración y validación del firewall GNU/Linux Endian dentro de un entorno virtualizado. El objetivo principal se basa en establecer una arquitectura de red segmentada mediante las zonas verde (LAN), roja (WAN) y naranja (DMZ). Se describe la metodología aplicada para la asignación de interfaces, la definición de direcciones IP por zona y la comprobación del enrutamiento interno. Los resultados obtenidos demuestran una comunicación

funcional entre zonas, así como una operación correcta del firewall al gestionar el tráfico entre redes internas y externas.

La segmentación de redes se convirtió en una práctica esencial en la administración moderna de infraestructuras tecnológicas. La separación en zonas permite controlar el flujo de datos, reducir vulnerabilidades y mejorar la eficiencia operativa. En este escenario, Endian representa una herramienta sólida para implementar un esquema basado en redes segregadas.

A través de VirtualBox es posible reproducir un entorno que simula condiciones reales, creando interfaces independientes para representar la red interna, la conexión externa y la zona de servicios. Esta aproximación permite entender el comportamiento del firewall y sus mecanismos de control del tráfico.

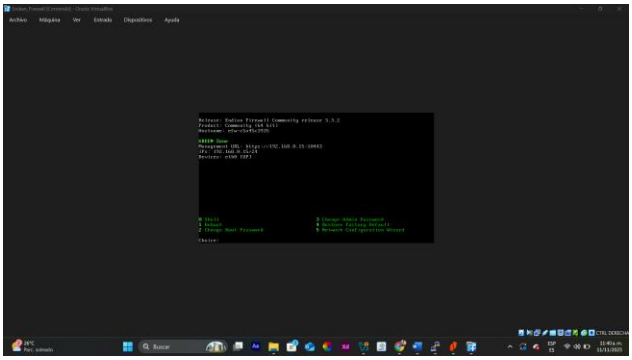
La implementación se realizó utilizando Endian Community 3.3.2 en una máquina virtual con tres adaptadores de red configurados desde VirtualBox. Cada adaptador representó una zona específica: verde para la red interna, naranja para la DMZ y roja para la conexión hacia Internet. Durante el asistente inicial se asignaron las interfaces a cada zona, configurando las direcciones IP correspondientes. Finalmente se verificó la conectividad mediante herramientas de diagnóstico como ping y la revisión de tablas ARP y rutas activas.

Las tres zonas quedaron configuradas correctamente. La zona verde operó como segmento interno principal, la zona naranja respondió como DMZ y la zona roja simuló una conexión externa. Las pruebas de conectividad confirmaron comunicación estable entre zonas internas y salida hacia destinos externos. La tabla de enrutamiento mostró rutas activas consistentes con el diseño establecido.

Los resultados obtenidos muestran que la estructura implementada se comporta de forma estable en un entorno virtualizado. La correcta asignación de interfaces dentro de VirtualBox permitió tener un funcionamiento coherente del firewall. Este tipo de ejercicios facilita la comprensión de la segmentación de redes y la importancia de los firewalls en la seguridad.

Podemos observar la interfaz de consola del firewall Endian con la zona GREEN configurada en la dirección IP 192.168.0.15/24 sobre la interfaz eth0, permitiendo la administración del sistema y evidenciando la correcta implementación de la red LAN requerida en la práctica.

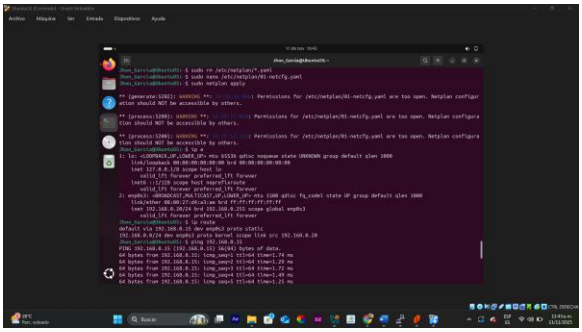
Figura 1. Estado inicial de la zona GREEN (LAN)



Fuente: Autoría Propia

Asimismo, se evidencia la conectividad mediante la respuesta exitosa a un ping dirigido al firewall, confirmando el funcionamiento de la zona LAN (GREEN).

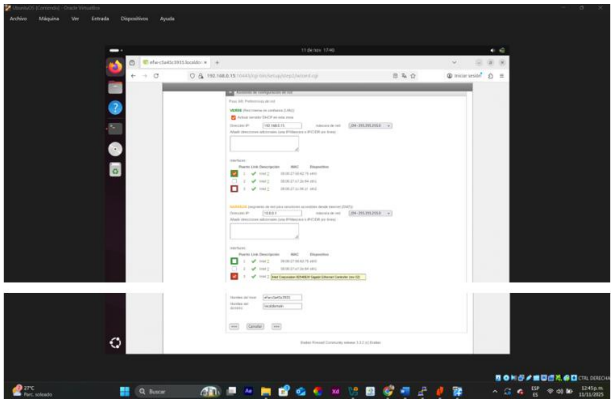
Figura 2. Asignación de dirección IP fija y verificación de conectividad del cliente



Fuente: Autoría Propia

Se desarrollo una asignación de direccionamiento y selección de interfaces de red dentro del asistente de configuración de Endian Firewall. La zona VERDE, correspondiente a la red interna de confianza (LAN), se configuró con la dirección 192.168.0.15/24 y se asignó a la interfaz eth0, habilitando el servicio DHCP para los equipos de la red local. La zona NARANJA, destinada a la DMZ para servidores expuestos, se configuró con la dirección 10.0.0.1/24 y se asoció a la interfaz eth2, manteniendo separación lógica respecto de la LAN para garantizar mayor seguridad.

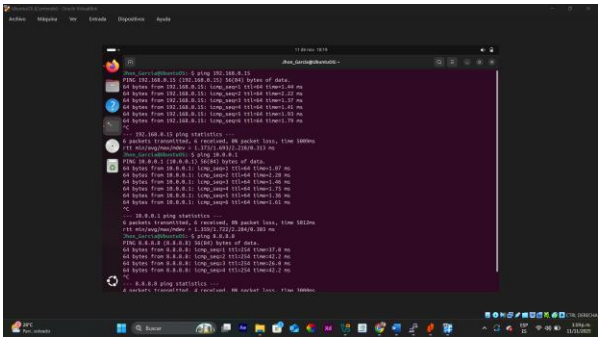
Figura 3. Configuración de zonas



Fuente: Autoría Propia

Por medio de los presentes comandos se logró evidenciar la correcta conexión de las 3 zonas para el correcto desarrollo de la temática.

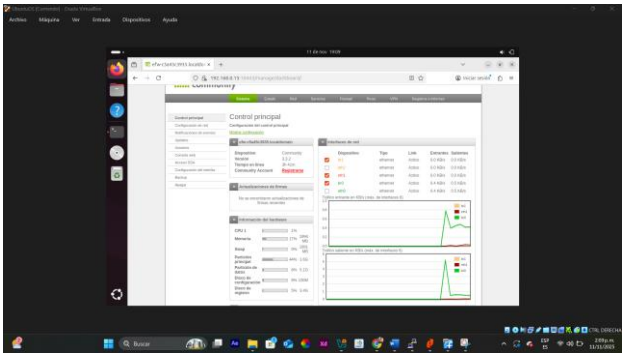
Figura 4. Conexión entre zonas



Fuente: Autoría Propia

Las interfaces de red activas del sistema Endian, evidenciando la asignación de las zonas Verde (eth0), Roja (eth1) y Naranja (eth2).

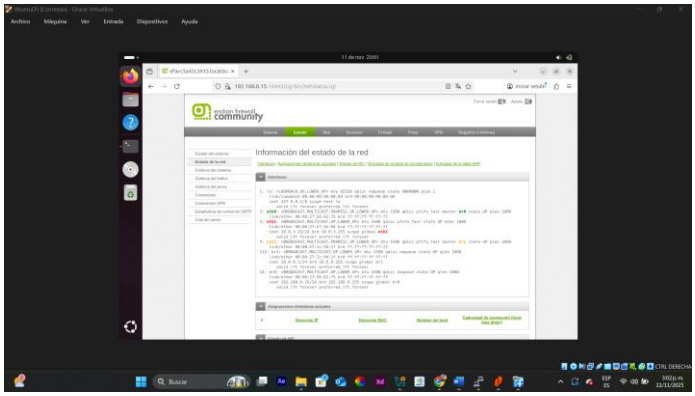
Figura 5. Interfaces de red



Fuente: Autoría Propia

Información detallada del estado actual de las interfaces de red en el sistema Endian Firewall, incluyendo direcciones IP, estado de enlace y configuración de cada adaptador de red.

Figura 6. Estado de red



Fuente: Autoría Propia

Conclusión de la temática

La implementación del firewall permitió simular un entorno segmentado funcional, facilitando la comprensión de los conceptos de seguridad y control del tráfico.

Las pruebas realizadas confirmaron que el sistema gestiona de manera correcta la comunicación entre redes internas y hacia redes externas simuladas.

Este ejercicio reforzó conocimientos sobre configuración, diagnóstico y diseño de arquitecturas de red utilizando software libre.

B. Configuración NAT (Temática 2)

Se procedió a la instalación del firewall Endian dentro de un entorno virtualizado en VirtualBox. Se configuraron las interfaces de red, asignando la zona GREEN en la dirección 192.168.0.15/24 y habilitando la interfaz de administración Web mediante HTTPS.

Se validó la conectividad desde un equipo host, confirmando comunicación con la IP del firewall y acceso exitoso a la interfaz web en el puerto 10443.

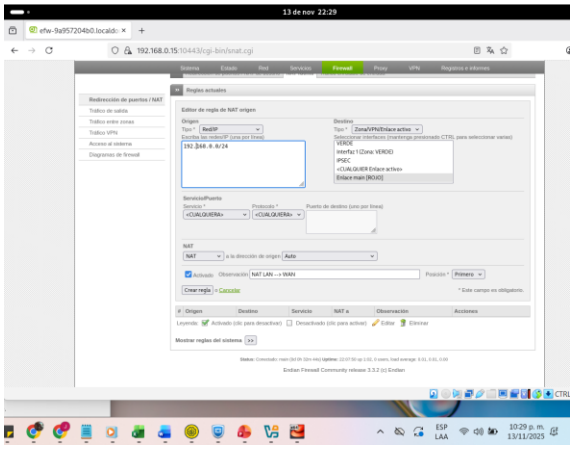
1) Configuración de NAT para la comunicación LAN → WAN

Se implementó una regla de NAT de salida que permite a los equipos de la LAN navegar en Internet utilizando la dirección de la zona RED. Los parámetros configurados fueron:

- Origen: 192.168.0.0/24 (zona GREEN)
- Destino: Enlace RED
- Servicio/protocolo: cualquiera
- Modo NAT: Auto

La validación se realizó mediante pruebas de ping a la puerta de enlace y a dominios públicos, evidenciando correcta resolución DNS y acceso a Internet.

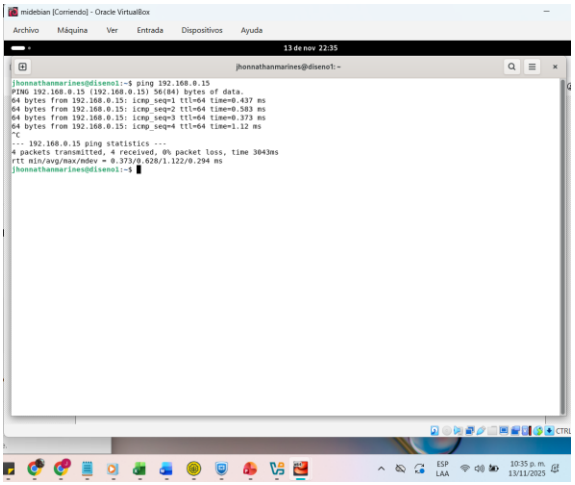
Figura 7. LAN → WAN



Fuente: Autoría Propia

Se realiza la comprobación de que la regla quedo bien creada mediante la ejecución de un ping hacia el getway 192.168.0.15, en la cual se observa una correcta respuesta del ping.

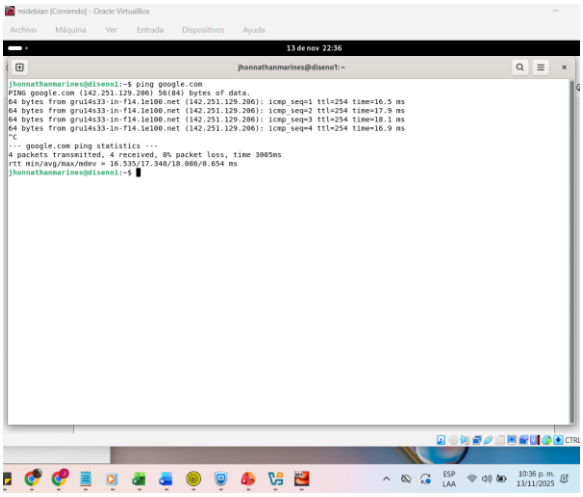
Figura 8. Comprobación de la regla



Fuente: Autoría Propia

De igual forma se realiza una segunda comprobación confirmado que haya resolución del DNS por medio de la ejecución de ping a Google.com, en el cual también responde correctamente.

Figura 9. Resolución de DNS



Fuente: Autoría Propia

2) Configuración de la zona DMZ y NAT DMZ → WAN

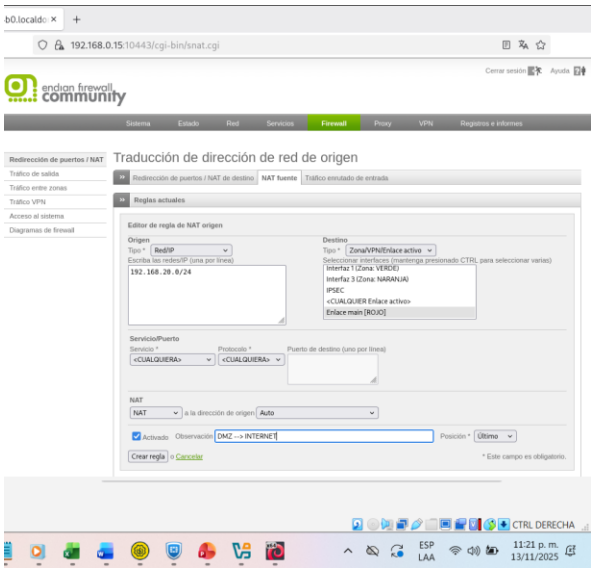
Se creó la zona ORANGE con la dirección 192.168.20.1/24 y se configuró un equipo dentro de dicha red. Posteriormente, se añadió una regla de NAT que permite la salida de la DMZ hacia Internet, utilizando direcciones enmascaradas por la interfaz RED.

Se verificó el funcionamiento mediante pruebas de conectividad desde el equipo en la DMZ hacia Internet.

La configuración de la regla se realizó con los siguientes ítems y valores configurados en la herramienta del firewall

- ORIGEN → Tipo: Red/IP y la red verde 192.168.20.0/24
- DESTINO → Tipo: Zona/VPN/Enlace activo Enlace main [ROJO]
- Servicio/Puerto → los dejo por defecto, Servicio: <CUALQUIERA>
- Protocolo: <CUALQUIERA>, Puerto: vacío
- NAT → NAT: NAT, Dirección origen: Auto
- Activado: Si
- Observación: DMZ → INTERNET

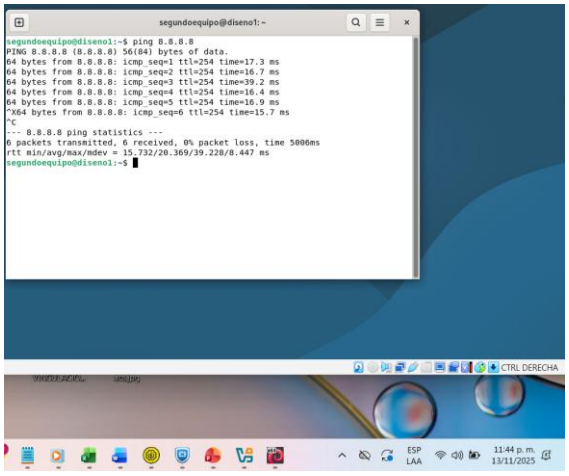
Figura 10. DMZ → Internet



Fuente: Autoría Propia

Se ejecuta la prueba para confirmar la conectividad desde el DMZ hacia internet por medio de un ping el cual responde sin problemas.

Figura 11. Comprobación DMZ – Internet



Fuente: Autoría Propia

3) Verificación del reenvío de puertos

Se realiza la creación de la regla en la sección Reenvío de puertos / NAT de destino, confirmando que Endian realiza correctamente la asociación entre puertos expuestos y equipos ubicados en la zona DMZ, permitiendo la publicación de servicios internos hacia Internet de forma controlada.

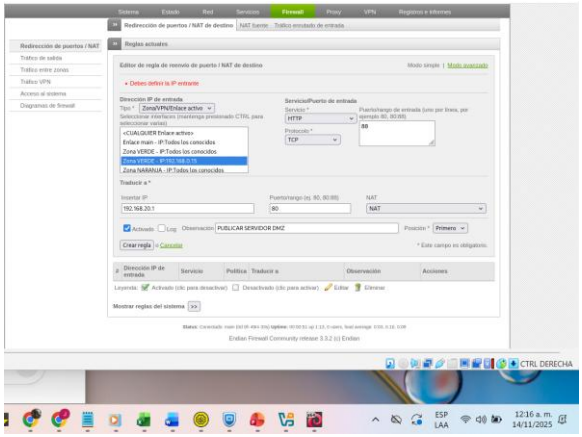
A continuación, se presenta la evidencia formal del proceso de verificación realizado en la sección **Firewall → Redirección de puertos / NAT de destino**, donde se comprueba que el Firewall Endian registró correctamente la regla de publicación del servicio HTTP ubicado en la zona DMZ.

En la sección de creación de reglas se definieron los siguientes parámetros:

- **Dirección IP de entrada (RED/WAN):** 192.168.0.15
- **Zona:** Red verde (IP origen 192.168.0.15)
- **Servicio:** HTTP
- **Protocolo:** TCP
- **Puerto de entrada:** 80
- **IP destino (DMZ):** 192.168.20.1
- **Puerto destino:** 80
- **Tipo de NAT:** NAT
- **Observación:** PUBLICAR SERVIDOR DMZ
- **Estado:** Activado

Esta configuración permite exponer el servicio HTTP del servidor en la DMZ hacia la red WAN interna del laboratorio.

Figura 12. Reenvió de puerto



Fuente: Autoría Propia

Conclusión de la temática

La instalación de Endian en un entorno virtual demostró la importancia de la segmentación de red mediante zonas de seguridad para una administración eficaz del tráfico.

La implementación de NAT en la zona GREEN permitió validar el enmascaramiento de direcciones internas y la correcta salida de la LAN hacia Internet.

La configuración de la DMZ mostró cómo aislar servicios expuestos al exterior sin comprometer la seguridad de la red interna.

La verificación de reglas en el reenvío de puertos confirmó que Endian gestiona adecuadamente la publicación controlada de servicios hacia la red WAN.

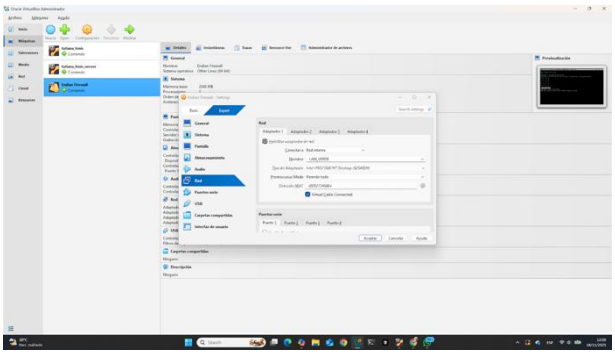
C. Permitir servicios de la zona DMZ para la red (Temática 3)

Su propósito es explicar la configuración realizada para habilitar servicios desde un servidor alojado en la zona DMZ y permitir que fueran accedidos desde la red interna, garantizando al mismo tiempo un nivel adecuado de seguridad. Durante la práctica se habilitaron los puertos en el servidor que se encontraba dentro de la DMZ, se configuraron servicios como Apache y FTP, y se bloquearon paquetes ICMP para evitar actividades como ping y traceroute.

1) Diseño de la arquitectura de red

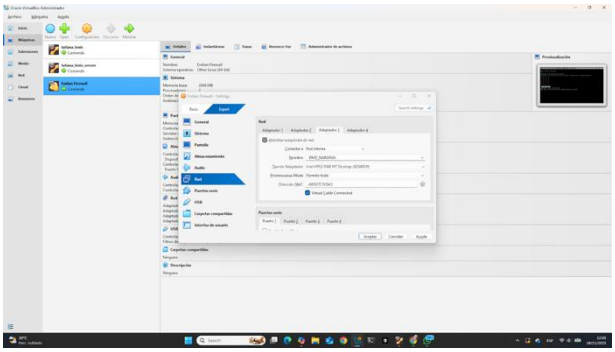
El escenario se construyó utilizando tres máquinas virtuales. En la zona verde se ubicó un Desktop Ubuntu, desde donde se realizaron todas las pruebas de conectividad. En la zona naranja (DMZ) se instaló un servidor, encargado de ofrecer los servicios configurados para la práctica. Finalmente, se implementó un firewall Endian, cuya función principal fue separar ambas zonas y permitir su comunicación sin mezclar los segmentos de red. La zona verde manejó direcciones dentro del rango 192.168.x.x, mientras que la DMZ utilizó la red 10.0.0.x. Esta separación permitió que los servicios del servidor fueran accesibles desde la red interna, pero sin quedar expuestos directamente al resto de la infraestructura.

Figura 13. Configuración del adaptador 1 como red interna para la interfaz LAN (VERDE) del firewall Endian



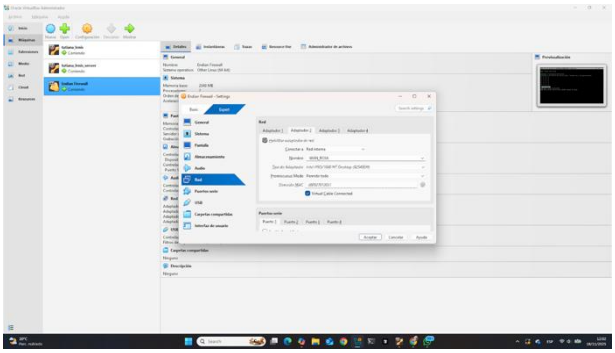
Fuente: Autoría Propia

Figura 14. Configuración del adaptador 2 como red interna para la interfaz WAN (ROJA) del firewall Endian



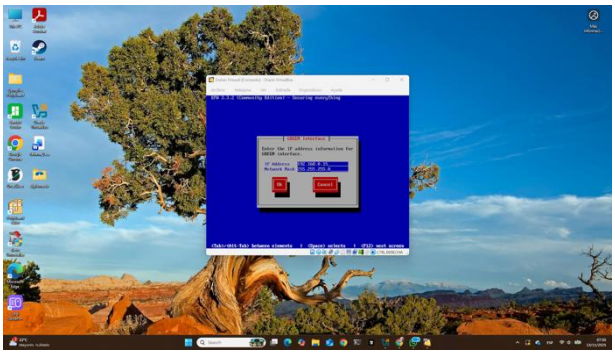
Fuente: Autoría Propia

Figura 15. Configuración del adaptador 3 como red interna para la interfaz DMZ (NARANJA) del firewall Endian



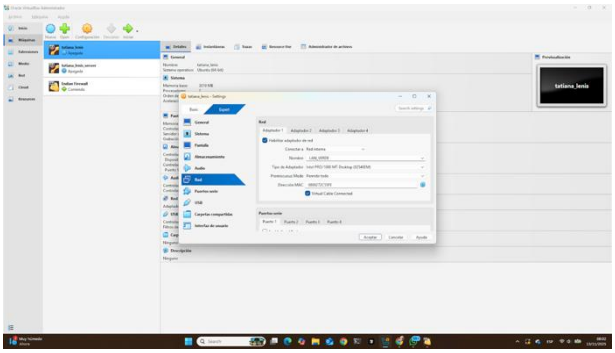
Fuente: Autoría Propia

Figura 16. Asignación de la IP 192.168.0.15/24 para la interfaz VERDE, correspondiente a la red interna de confianza (LAN) utilizada en la segmentación del firewall



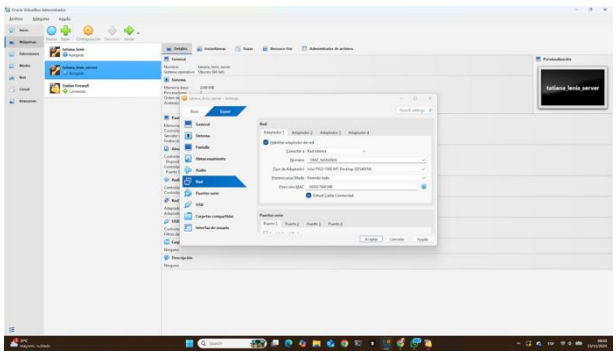
Fuente: Autoría Propia

Figura 17. Configuración del cliente Ubuntu en la red interna LAN_VERDE



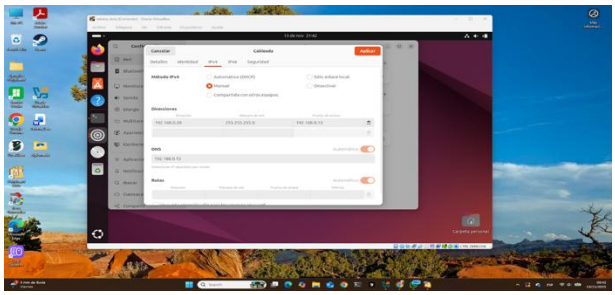
Fuente: Autoría Propia

Figura 18. Configuración del servidor Ubuntu en la red interna DMZ_NARANJA



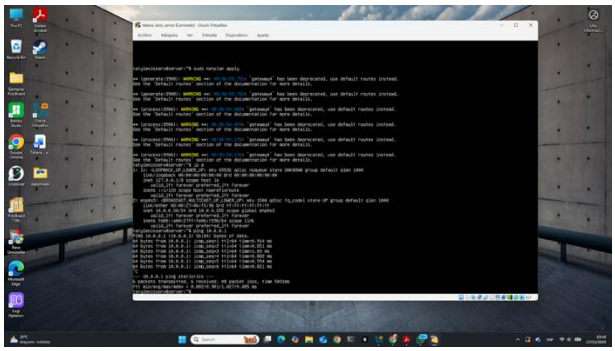
Fuente: Autoría Propia

Figura 19. Configuración manual de la dirección IPv4 en el Desktop dentro de la zona LAN (VERDE)



Fuente: Autoría Propia

Figura 20. Comprobación de la IP asignada (10.0.0.50/24) en el servidor Ubuntu y prueba de conectividad hacia el firewall Endian en la zona ORANGE



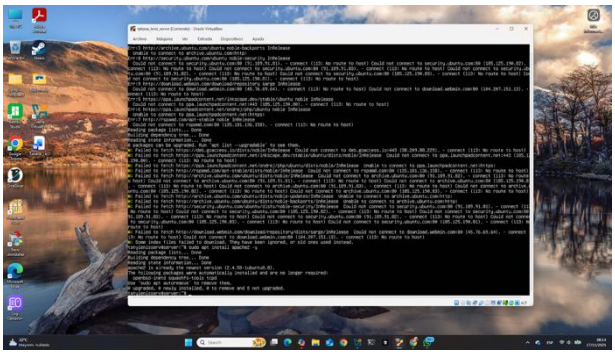
Fuente: Autoría Propia

2) Configuración de servicios en el servidor DMZ

Una vez definidas las zonas, se procedió a configurar los servicios dentro del servidor ubicado en la DMZ. El primer servicio habilitado fue Apache, el cual funciona sobre el puerto 80, y posteriormente se habilitó el servicio FTP, disponible en el puerto 21. Ambas configuraciones se realizaron directamente sobre el servidor, ya que los puertos necesitaban estar activos y escuchando desde dentro de la DMZ.

Para permitir el uso de estos servicios, fue necesario abrir ambos puertos en el servidor y asegurarse de que los procesos estuvieran funcionando correctamente. Esto incluyó comandos de verificación, revisión del estado de los servicios y validación de que las conexiones entrantes fueran aceptadas. De esta manera, los servicios quedaron listos para ser consultados desde la red verde.

Figura 21. Comando sudo apt update y sudo apt install apache2 -y para instalar el servidor HTTP Apache2 en Ubuntu Server



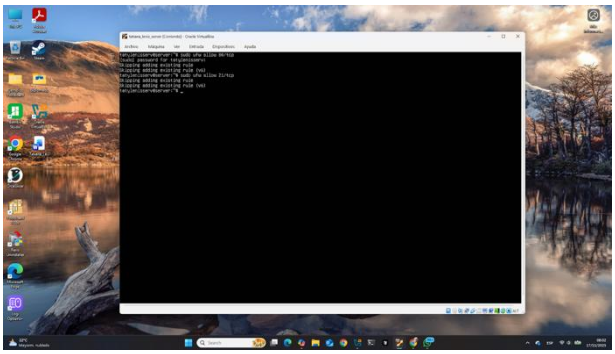
Fuente: Autoría Propia

3) Habilitación de puertos y bloqueo de ICMP en el servidor

En esta etapa se configuraron los puertos y los bloqueos, pero todo se hizo directamente en el servidor, no en el firewall. Se habilitaron únicamente los puertos 80 (HTTP) y 21 (FTP), ya que eran los servicios que debían ser accesibles desde el Desktop. Esta apertura se realizó mediante las herramientas de firewall propias del servidor, permitiendo exclusivamente lo necesario para la práctica.

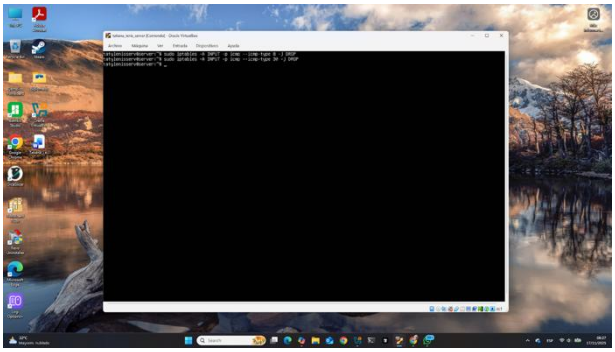
Adicionalmente, se configuraron reglas para bloquear los paquetes ICMP tipo 8 (ping) y tipo 30 (traceroute). Este bloqueo tuvo el propósito de evitar que el servidor respondiera a pruebas de reconocimiento o rastreo, lo cual es útil en entornos donde se desea limitar la visibilidad del equipo. Con estas reglas, cualquier intento de hacer ping o trazar la ruta hacia el servidor desde la red verde debía fallar.

Figura 22. Ejecución de los comandos sudo ufw allow 80/tcp y sudo ufw allow 21/tcp para habilitar el acceso a los servicios HTTP y FTP en el servidor Ubuntu Server mediante el firewall UFW



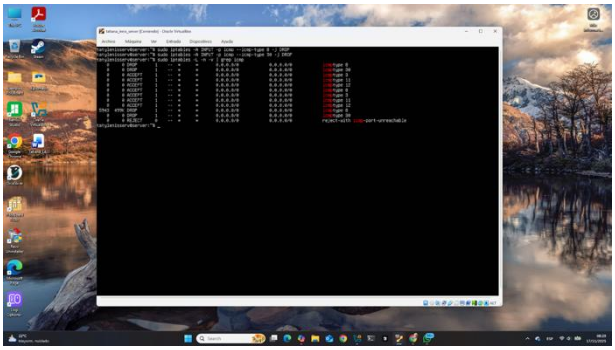
Fuente: Autoría Propia

Figura 23. Comando sudo iptables -A INPUT -p icmp --icmp-type 8 -j DROP sudo iptables -A INPUT -p icmp --icmp-type 30 -j DROP para bloquear las solicitudes ICMP de tipo 8 y 30 en el servidor Ubuntu Server



Fuente: Autoría Propia

Figura 24. Ejecución del comando sudo iptables -L -n -v | grep icmp para verificar el estado de las reglas de bloqueo ICMP tipo 8 y 30 en el servidor Ubuntu Server



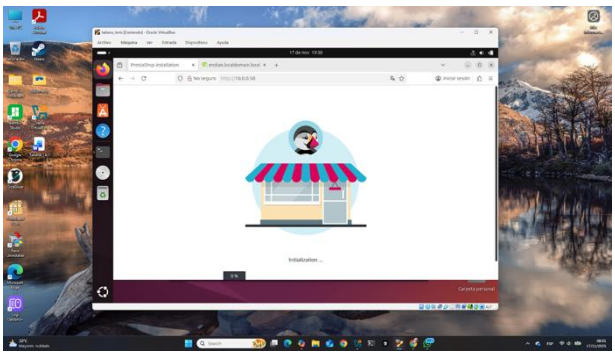
Fuente: Autoría Propia

4) Pruebas de conectividad entre zonas

Una vez configurados los puertos y bloqueos, se realizaron pruebas desde el Desktop en la red verde. Como se esperaba, los intentos de ping hacia el servidor fallaron, así como las pruebas con traceroute, confirmando que los ICMP estaban correctamente bloqueados.

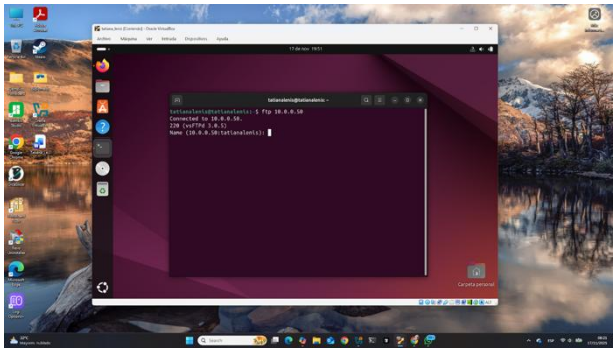
Posteriormente se probaron los servicios habilitados. Desde el Desktop se realizó una conexión al servicio web alojado en Apache, comprobando que el servidor respondía por el puerto 80. De igual manera, se probó el acceso por FTP en el puerto 21, verificando que el servicio estaba disponible y funcional. Estas pruebas confirmaron que, aunque no se permitieran paquetes ICMP, los servicios configurados sí estaban accesibles para los usuarios de la red verde.

Figura 25. Acceso desde la zona GREEN al servidor HTTP ubicado en la DMZ a través de la dirección http://10.0.0.50



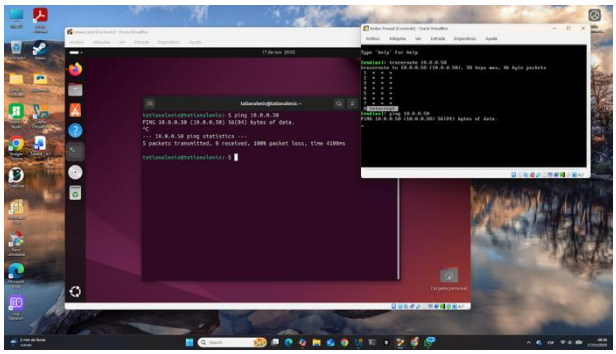
Fuente: Autoría Propia

Figura 26. Ejecución del comando ftp 10.0.0.50 desde Ubuntu Desktop para verificar la conexión exitosa con el servidor FTP alojado en la DMZ



Fuente: Autoría Propia

Figura 27. Prueba bloqueo de ping y traceroute



Fuente: Autoría Propia

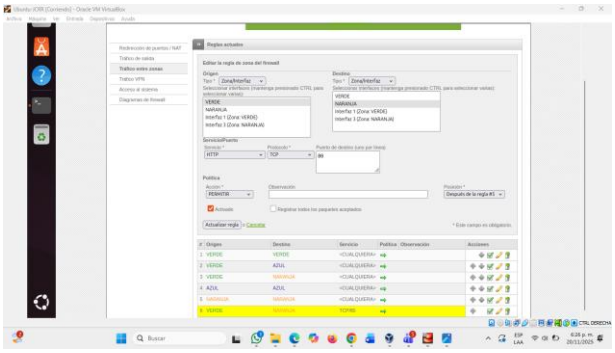
Conclusión de la temática

En resumen, la práctica mostró de manera clara cómo un servidor ubicado en la zona DMZ puede ofrecer servicios a la red interna sin comprometer su seguridad. La habilitación de puertos específicos, junto con el bloqueo de protocolos ICMP directamente en el servidor, permitió un control adecuado sobre el tráfico recibido. Esto demuestra la importancia de gestionar correctamente las reglas en cada equipo, especialmente en entornos segmentados por zonas.

D. Reglas de acceso para permitir o denegar el tráfico (Temática 4)

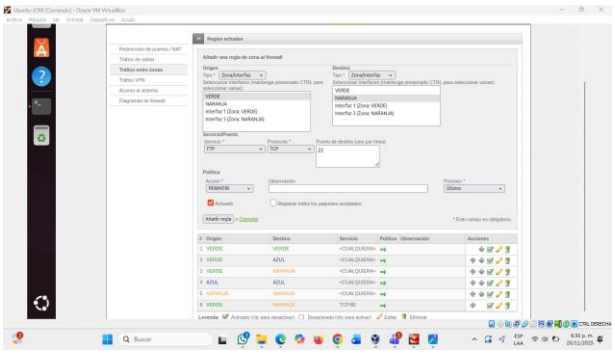
Establecimos las reglas necesarias para habilitar la comunicación entre los dispositivos de la red local (Zona Verde) y los servidores situados en la DMZ (Zona Naranja), empleando los protocolos HTTP (puerto TCP 80) y FTP (puerto TCP 21).

Figura 28. Regla para el servicio HHTP puerto 80



Fuente: Autoría Propia

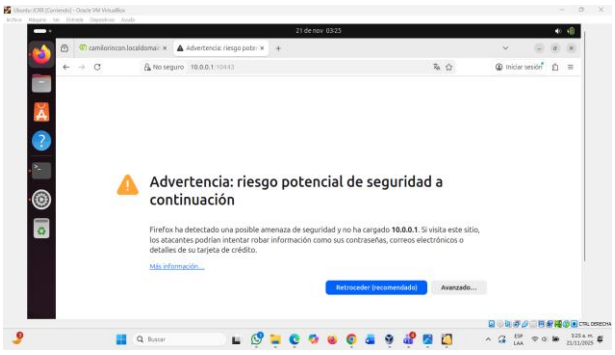
Figura 29. Regla para el servicio FTP 21



Fuente: Autoría propia

Hacemos prueba de conexión de los servicios desde una página web con DMZ.

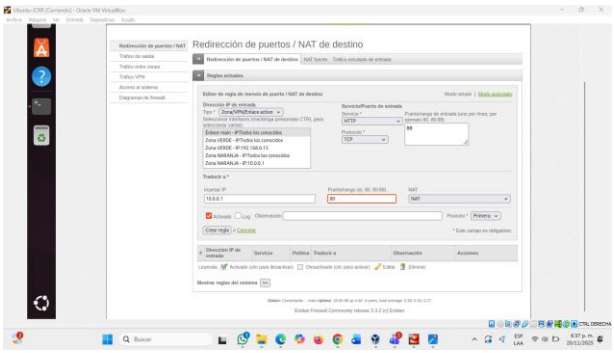
Figura 30. Comunicación a la zona internet con la zona DMZ



Fuente: Autoría propia

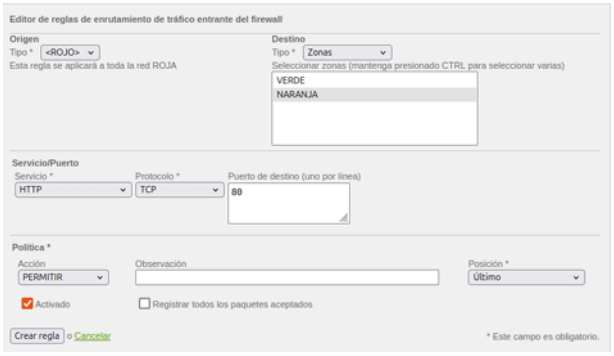
En la sección de Redirección de puertos/NAT, se configura la regla correspondiente para el protocolo HTTP (puerto 80) que permite el acceso desde internet. Después de ello, se crea la regla de firewall que autoriza la entrada del tráfico hacia la DMZ.

Figura 31. Configuración de la regla NAT con el puerto 80



Fuente: Autoría propia

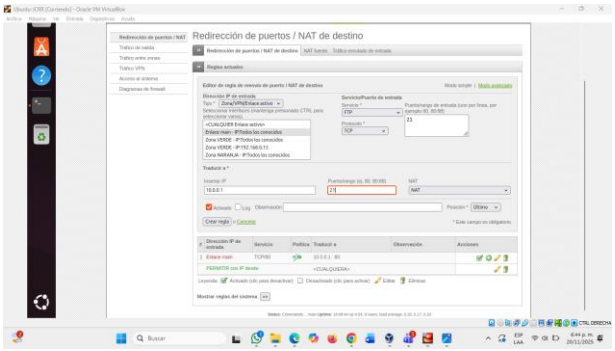
Figura 32. Regla de enrutamiento de firewall con el puerto 80



Fuente: Autoría propia

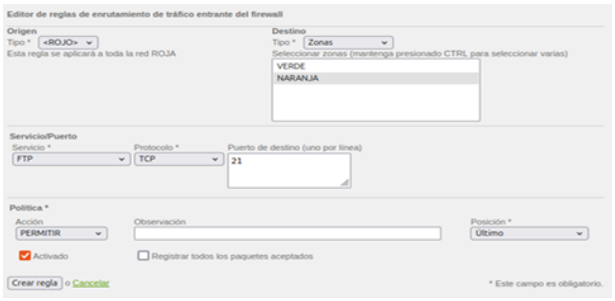
Una vez configurado el puerto 80, se procede a habilitar el enrutamiento para el puerto 21. El proceso es similar, pero en este caso se utiliza el protocolo TCP para permitir el servicio FTP.

Figura 33. Regla NAT para el puerto 21



Fuente: Autoría propia

Figura 34. Regla de enrutamiento para el puerto 21



Fuente: Autoría propia

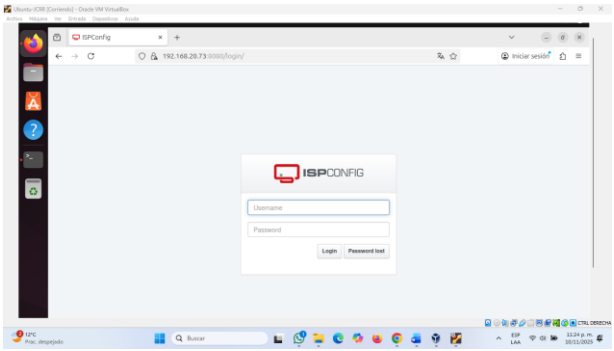
Se comprueba en el trafico entre zonas que las reglas hayan sido creadas correctamente. Para ello, se ingresa a la seccion de Registro e informes dentro del Firewall, donde es posible verificar el trafico generado.

Figura 35. Visualización de reglas en el tráfico del enrutado

Fuente: Autoria propia

se realiza una prueba desde un navegador web siguiendo las directrices correspondientes. En este caso, se verifica el acceso al servicio HTTP desde la LAN hacia la zona DMZ para ingresar al servidor web Apache2.

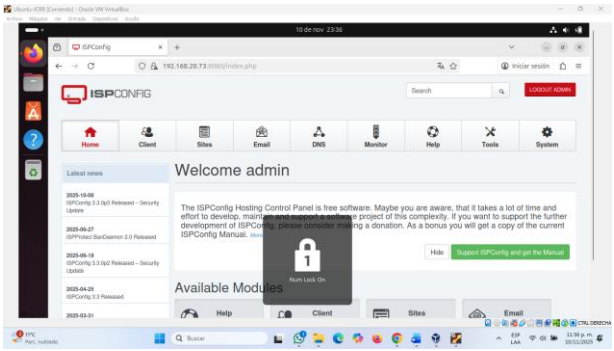
Figura 36. Ingreso a la página ISPConfig



Fuente: Autoría propia

Se verifica que los protocolos funcionen correctamente.

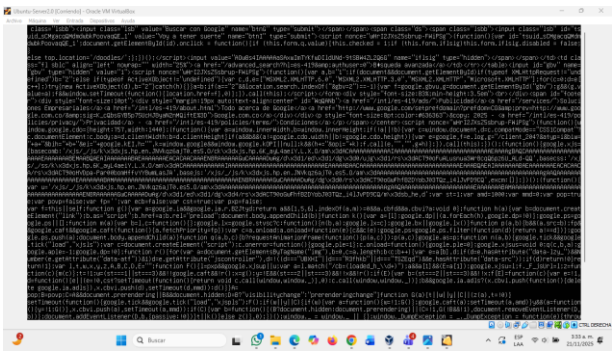
Figura 37. Verificación de acceso a los protocolos



Fuente: Autoría propia

Asi mismo comprobamos desde la WAN

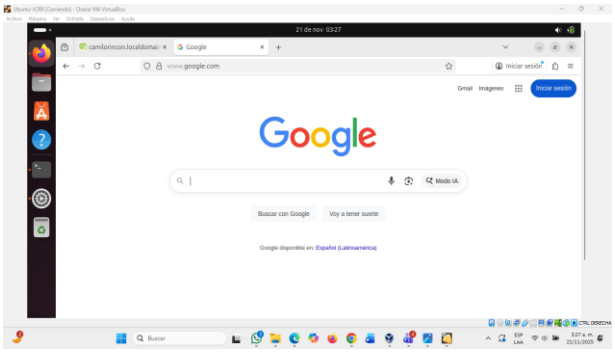
Figura 38. Descarga de archivos de Google



Fuente: Autoría propia

Ingreso a internet.

Figura 39. Acceso a internet



Fuente: Autoría propia

Conclusión de la temática

Durante la implementación se comprendió que una Zona Desmilitarizada (DMZ) no es solo un segmento aislado de la red, sino un enlace controlado cuidadosamente entre la red interna y el exterior. En esta arquitectura se puso en evidencia la relevancia de publicar únicamente los servicios esenciales, como HTTP y FTP, lo que contribuye a disminuir la forma notable de los riesgos de seguridad. Asi mismo, bloquear el protocolo ICMP se reconoció como una estrategia discreta pero efectiva para reducir la visibilidad de la red ante posibles escaneos, fortaleciendo el enfoque de seguridad por capas y evitando la exposición de información innecesaria.

E. Implementación de un proxy HTTP (no transparente) con políticas de autenticación (Temática 5)

Se implementó un proxy HTTP no transparente con autenticación por usuario usando Squid. Esta implementación definió dos perfiles lógicos (estudiantes vs. docentes) y un perfil de lista negra para bloquear dominios específicos (hotmail.com, youtube.com, elnuevodia.com.co). El objetivo general fue establecer un proxy HTTP no transparente con autenticación, y los específicos se centraron en: (i) instalar y habilitar Squid; (ii) configurar autenticación básica NCSA y crear usuarios; (iii) definir ACLs por perfiles; y (iv) validar el bloqueo/permiso con curl y navegador.

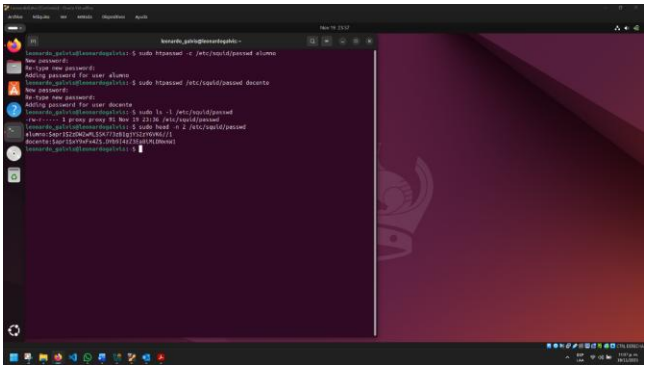
1) Metodología y configuración

La implementación se realizó en un entorno Ubuntu 24.04 (o similar, según el entorno de la práctica).

A. Instalación y Creación de Usuarios (Autenticación NCSA)

Se instalaron los paquetes esenciales y se procedió a crear la base de datos de contraseñas NCSA para los perfiles alumno y docente.

Figura 40. Creación y verificación de alumno y docente

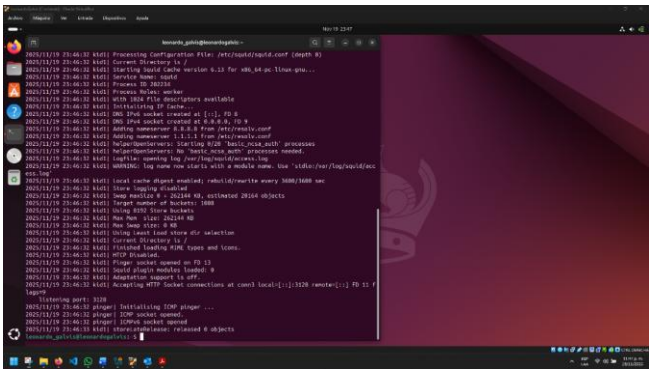


Fuente: Autoría propia

B. Definición de Lista Negra

Se estableció la lista de dominios restringidos en un archivo plano, que posteriormente sería referenciado por una ACL en Squid.

Figura 41. Contenido correcto del domains.txt

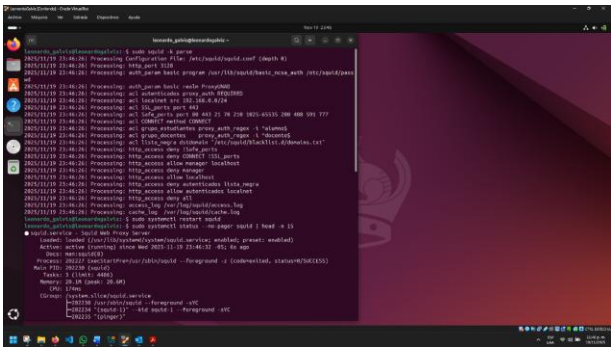


Fuente: Autoría propia

C. Configuración de ACLs y Reglas en squid.conf

La configuración de Squid se basó en la definición de ACLs para la autenticación, los grupos de usuario (grupo_estudiantes, grupo_docentes) y la lista negra (lista_negra). La regla de acceso clave fue la línea http_access deny grupo_estudiantes listas_negra, que aplica la restricción solo al perfil alumno.

Figura 42. OK, servicio active (running)



Fuente: Autoría propia

2) Pruebas y resultados

Las pruebas se ejecutaron mediante la herramienta de línea de comandos curl y la configuración de proxy explícita en el navegador Firefox.

Tabla 1. ACLs y políticas de acceso aplicadas

TABLA I ACLs y políticas de acceso aplicadas.
Perfil
alumno
docente

Fuente: Autoría propia

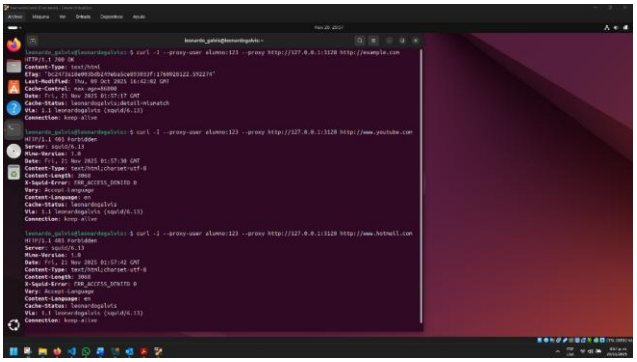
A. Validación con curl

- Bloqueo a Alumno (youtube.com): El comando curl -I --proxy-user alumno:123 --proxy http://127.0.0.1:3128 http://www.youtube.com resultó en una respuesta HTTP 403 Forbidden, confirmando la denegación.
- Permiso a Docente (youtube.com): El comando curl -I --proxy-user docente:123 --proxy http://127.0.0.1:3128 http://www.youtube.com resultó en códigos 200/301, confirmando el acceso.

B. Evidencia en Logs

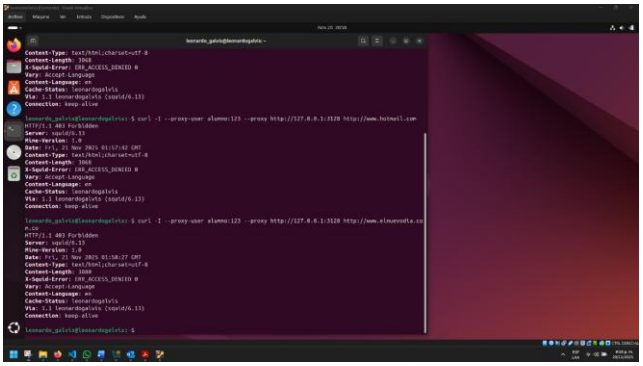
El usuario **alumno** queda bloqueado para hotmail.com, youtube.com y elnuevodia.com.co (HTTP 403). El usuario **docente** navega a dichos dominios (códigos 200/301), cumpliendo la política. La autenticación y las reglas se integran correctamente, solicitando credenciales al navegador y reflejando cada decisión en el access.log.

Figura 43. OK a example.com y 403 Forbidden a sitios de la lista negra



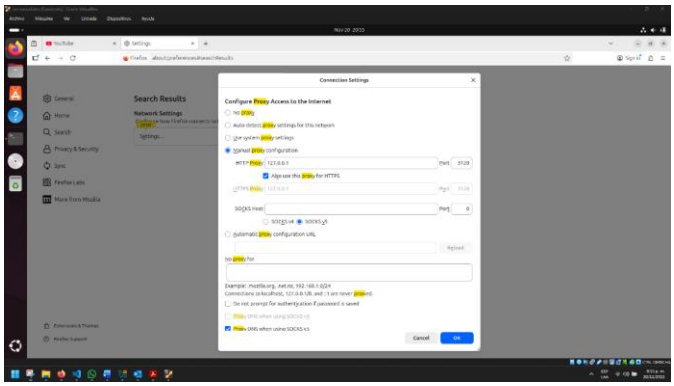
Fuente: Autoría propia

Figura 44. respuestas 301/200 (permitido) para docente.



Fuente: Autoría propia

Figura 45. pantalla de configuración de proxy manual en Firefox



Fuente: Autoría propia

Figura 46. Solicitudes credenciales de proxy

Fuente: Autoría propia

Conclusión de la temática

Se configuró en Ubuntu un **proxy HTTP no transparente** con **Squid**, autenticado por usuarios (NCSA) y con perfiles por grupo, aplicando una lista negra a alumno y permitiendo acceso a docente. Las pruebas con curl, Firefox y los registros en access.log evidenciaron bloqueos 403 a dominios restringidos y acceso correcto a los permitidos, validando las políticas de control. El resultado es un mecanismo de control de navegación efectivo, auditable y listo para ampliarse (horarios, cuotas o filtrado HTTPS)

III. CONCLUSIONES

La implementación del esquema de seguridad perimetral permitió comprender, desde la práctica, cómo la segmentación de la red fortalece el control del tráfico y reduce la exposición a riesgos. La definición de las zonas GREEN, ORANGE y RED mostró la importancia de separar adecuadamente la red interna, los servicios expuestos y la salida hacia Internet, manteniendo un flujo de datos ordenado y consistente con las buenas prácticas de seguridad.

El trabajo con reglas NAT evidenció que la traducción de direcciones y el enmascaramiento son fundamentales para proteger los recursos internos sin perder conectividad con el exterior. Las pruebas realizadas confirmaron la correcta salida a Internet desde la LAN y la DMZ, además del funcionamiento del reenvío de puertos para publicar servicios de manera controlada.

La habilitación de servicios dentro de la DMZ, junto con el bloqueo selectivo de protocolos como ICMP, permitió verificar que un servidor puede ofrecer funciones esenciales sin comprometer su seguridad. Este ejercicio reforzó la importancia de habilitar únicamente lo necesario y mantener desactivado todo aquello que no contribuya al objetivo del servicio.

Las reglas de acceso entre zonas dejaron claro que la administración del tráfico exige precisión. La verificación en el firewall demostró que los servicios HTTP y FTP respondieron correctamente tanto desde la red interna como desde la WAN, siempre respetando la separación lógica entre cada segmento.

Por último, la implementación del proxy HTTP no transparente mostró cómo es posible ejercer un control efectivo sobre la navegación mediante autenticación y listas de restricción. Las pruebas confirmaron que el sistema aplicó correctamente las políticas establecidas, diferenciando el comportamiento según el tipo de usuario y registrando cada acción en los archivos de log.

En conjunto, el proyecto permitió afianzar conceptos clave de seguridad perimetral, administración de servicios y segmentación de red. Todo ello contribuyó a una visión práctica y ordenada de cómo proteger infraestructuras basadas en GNU/Linux aprovechando herramientas Open Source.

IV. REFERENCIAS

[1] M. J. Solórzano-Cedeño, X. A. Sánchez-Granja, y F. Barboza-Gilces, Linux redes y seguridades. 2014. [En línea]. Disponible en: https://www.dspace.espol.edu.ec/handle/123456789/29731

[2] E. D. Sotelo-Salamanca, Configuración de NAT, DHCP y protocolos de enrutamiento. [En línea]. Disponible en: https://repository.unad.edu.co/handle/10596/18693

[3] I. A. C. Corpeño, Zona Desmilitarizada (DMZ), 2020. [En línea]. Disponible en: https://www.academia.edu/download/64720608/ZonaDesmilitarizada.pdf

[4] V. H. Conto-Carvajal, S. A. Segura-Salazar, M. A. Franco-Pérez y J. D. Velásquez-Ramírez, Implementación de reglas de acceso para el control de tráfico en redes segmentadas. [En línea]. Disponible en: https://repository.unad.edu.co/handle/10596/68552

[5] G. E. S. Silva-Poveda, Implementación de Proxy HTTP no Transparente con Autenticación. [En línea]. Disponible en: https://repository.unad.edu.co/handle/10596/68804