IMPLEMENTACIÓN DE SEGURIDAD PERIMETRAL CON GNU/LINUX ENDIAN EN VIRTUALBOX

Claudia Patricia Gómez Garnica
cpgomezg@unadvirtual.edu.co
Martin Andrés Quevedo Quimbayo
maquevedoq@unadvirtual.edu.co
Luis Eduardo Sánchez Arenas
lesanchezar@unadvirtual.edu.co
Carlos Alexander Beltran Bejarano
cabeltranbej@unadvirtual.edu.co
Stiven Alejandro Poveda Lemus
sapovedal@unadvirtual.edu.co

RESUMEN: *Este proyecto aborda la implementación colaborativa de un sistema de seguridad perimetral empleando la distribución GNU/Linux Endian Firewall (EFW) para proteger los servicios críticos alojados en una infraestructura basada en LAN, WAN y una zona DMZ. Cada integrante del grupo instaló y configuró EFW en VirtualBox, definiendo las zonas verde, roja y naranja, así como el direccionamiento IP correspondiente. Las actividades incluyeron la creación de reglas NAT, la habilitación de servicios HTTP y FTP desde un servidor Ubuntu en la DMZ, el bloqueo de ICMP, y la configuración de reglas de acceso entre LAN, DMZ y WAN. Además, se implementó un proxy HTTP no transparente con políticas de autenticación y listas negras de navegación. Cada procedimiento fue validado mediante pruebas funcionales y verificación de servicios por consola, fortaleciendo competencias prácticas en segmentación de red, control de tráfico y seguridad perimetral.*

PALABRAS CLAVE: DMZ (Zona Desmilitarizada), Endian Firewall (EFW), NAT (Network Address Translation) Seguridad perimetral,

1 INTRODUCCIÓN

En los entornos organizacionales actuales, la protección de la infraestructura tecnológica se ha convertido en una necesidad fundamental para garantizar la continuidad operativa y la integridad de la información. A medida que las redes corporativas integran servicios internos (LAN), servicios expuestos a usuarios externos (WAN) y servidores críticos que requieren una capa adicional de aislamiento, se vuelve indispensable implementar mecanismos de seguridad perimetral robustos y eficientes.

En este contexto, el grupo desarrolló una solución basada en la distribución GNU/Linux Endian Firewall (EFW), una plataforma especializada en filtrado, control de tráfico y gestión de zonas de seguridad. El propósito de la actividad fue comprender y aplicar los principios de segmentación de red mediante la creación de una DMZ, la configuración de reglas de acceso entre zonas, la implementación de NAT y el despliegue de un proxy con políticas de autenticación.

El trabajo se desarrolló de forma colaborativa, permitiendo que cada integrante asumiera una temática específica, aplicara configuraciones reales dentro de un entorno virtualizado y validara el funcionamiento de cada servicio mediante comandos, pruebas de conectividad y verificación de reglas. Este proceso no solo fortaleció las competencias técnicas en seguridad perimetral, sino que también fomentó el análisis crítico y la toma de decisiones frente a escenarios reales de protección de redes.

2 ACTIVIDAD GRUPAL

2.1 ¿QUÉ ES ENDIAN?

Endian es una distribución GNU/Linux libre, que está especializada en seguridad de redes, diseñada para funcionar como un firewall que significa cortafuegos que permite una gestión unificada de amenazas (UTM). Esta distribución convierte un equipo estándar en un dispositivo de seguridad integral que controla el tráfico de entrada y salida mediante un firewall bidireccional, junto con funciones adicionales como VPN, proxy, filtro de contenido, detección de intrusiones y gestión de múltiples zonas de red. Endian se caracteriza por ser una solución open source que facilita la administración y protección de redes mediante una interfaz web amigable y múltiples servicios de seguridad incorporados, lo que lo hace útil tanto para entornos domésticos como empresariales.

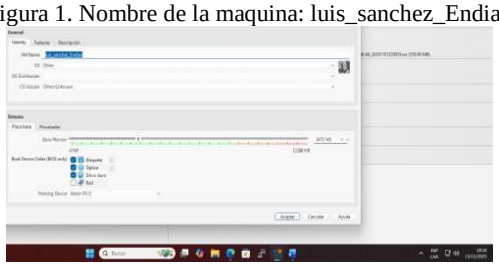
2.2 TEMÁTICA 1: CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX (TARJETAS DE RED) E INSTALACIÓN EFECTIVA DEL MISMO.

La configuración de la instancia para GNU/Linux Endian en VirtualBox requiere asignar y configurar adecuadamente las tarjetas de red para simular la arquitectura de red deseada, usualmente estableciendo zonas como Verde (LAN), Roja (WAN) y Naranja (DMZ). Esto implica asignar a cada tarjeta de red virtual una zona específica que permita el correcto manejo del tráfico de red y la segmentación, garantizando la seguridad y la funcionalidad del firewall.

La instalación efectiva de Endian en VirtualBox comienza con la creación de la máquina virtual, seguido de la asignación de recursos como CPU, memoria y tarjetas de red, para luego proceder con la instalación del sistema operativo GNU/Linux Endian a través de su ISO, configurando parámetros iniciales como el idioma, almacenamiento, y las credenciales de acceso para administrar el firewall una vez este instalado.
Es por lo que en el proceso de configuración del entorno controlado en Hipervisor de vitualbox se deben tener estos pasos en cuenta:

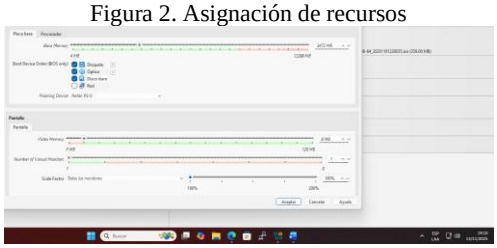
1. Creación de la máquina virtual Endian

Figura 1. Nombre de la maquina: luis_sanchez_Endian



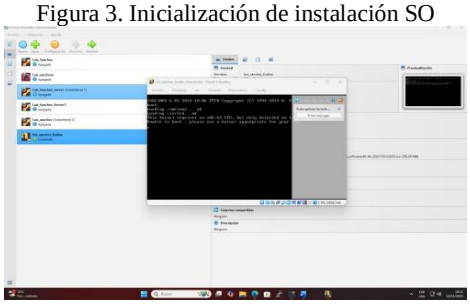
Fuente: Autoría Propia

Figura 2. Asignación de recursos



Fuente: Autoría Propia

Figura 3. Inicialización de instalación SO



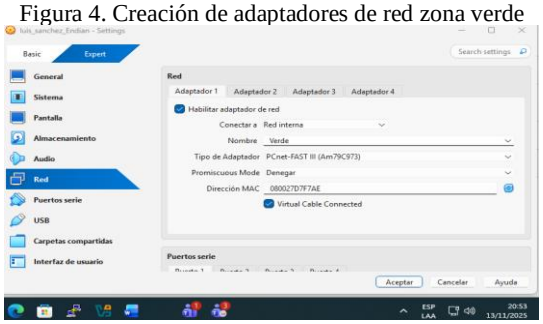
Fuente: Autoría Propia

Las figuras anteriores muestran el proceso de crear la máquina virtual, en la cual en la Fig.1 se le asigna un nombre en este caso luis_sanchez_Endian. En la fig.2 se le asignan los respectivos recursos con los cuales va a contar esta máquina virtual como la capacidad de la CPU y la memoria. Finalmente al guardar las respectivas configuraciones se observa el proceso de inicio de la distribución Fig.3

2. Creación en VirtualBox el adaptador para las diferentes zonas

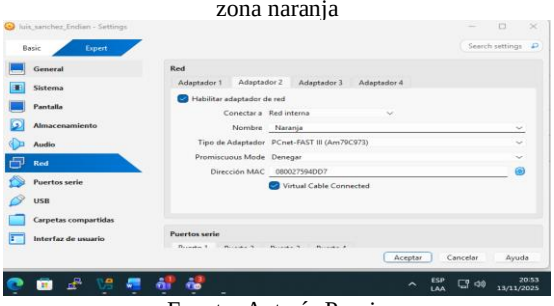
En la Fig.4, Fig.5, Fig.6 se observa la configuración de los tres adaptadores con los cuales va a funcionar la maquina los cuales son el adaptador 1 con la red interna verde, el adaptador 2 red interna naranja y el adaptador 3 la red NAT con el acceso a internet. Posteriormente se crean otras dos máquinas virtuales las cuales van a servir como cliente Fig. 7 y como servidor Fig.8.

Figura 4. Creación de adaptadores de red zona verde



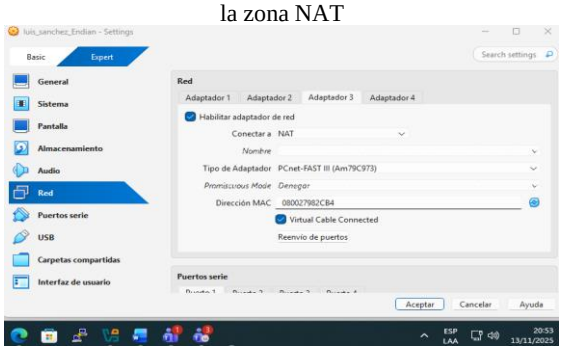
Fuente: Autoría Propia

Figura 5. Creación en VirtualBox el adaptador para la zona naranja



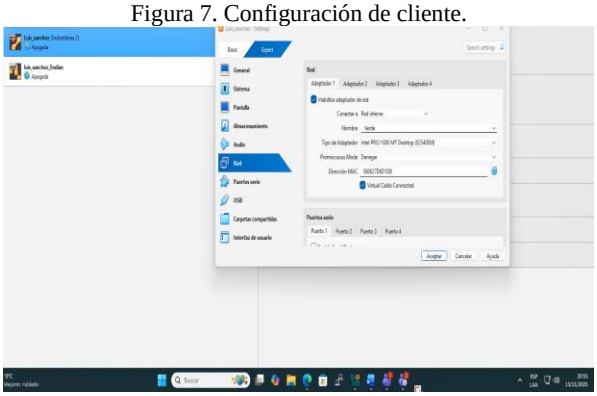
Fuente: Autoría Propia

Figura 6. Creación en VirtualBox el adaptador para la zona NAT



Fuente: Autoría Propia

Figura 7. Configuración de cliente.

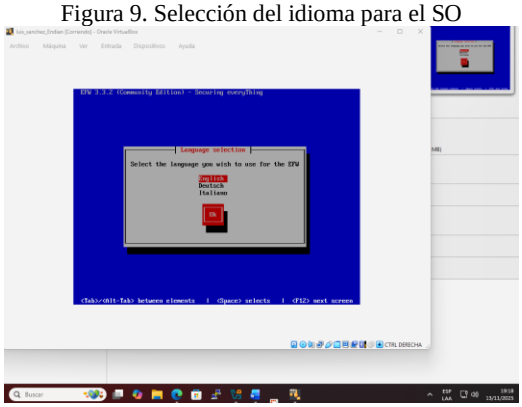


Fuente: Autoría Propia

Figura 8. Configuración Servidor

Fuente: Autoría Propia

Figura 9. Selección del idioma para el SO

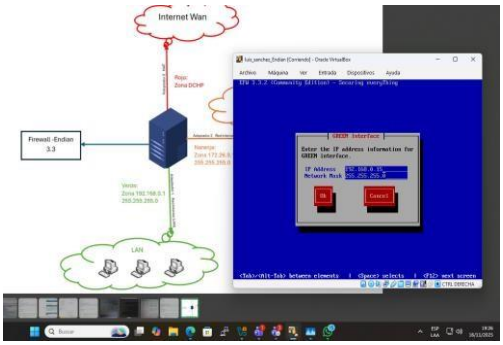


Fuente: Autoría Propia

Figura 10. Preparación del disco

Fuente: Autoría Propia

Figura 11. Configuración de Ip en Endian



Fuente: Autoría Propia

En las Fig.9, Fig.10, se observa las configuraciones de Endian como la selección de idioma, preparación del disco e instalación de paquetes para ejecutar la distribución Endian. Por su parte en la Fig.11 se realiza la configuración de la Ip respectiva en base a las configuraciones establecidas en el mapa de la izquierda.

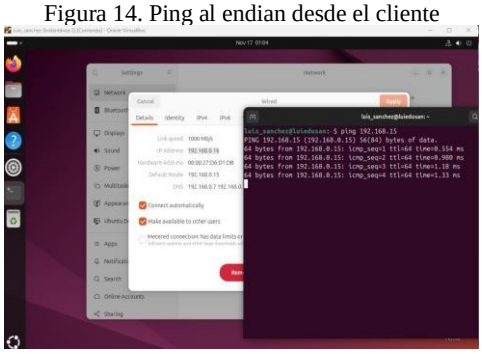
Figura 12. Inicio de Interfaz de Endian.

Fuente: Autoría Propia

Figura 13. Cliente Se deja el equipo con DHCP

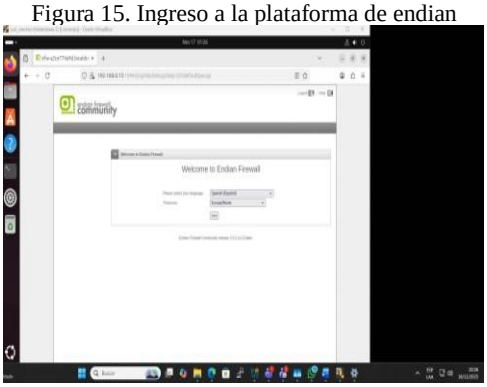
Fuente: Autoría Propia

Figura 14. Ping al endian desde el cliente



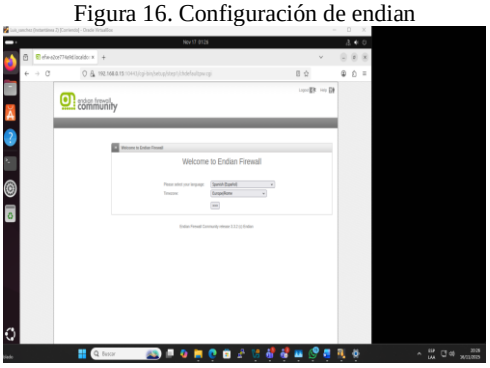
Fuente: Autoría Propia

Figura 15. Ingreso a la plataforma de endian



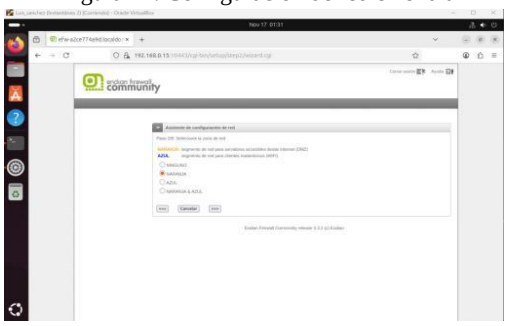
Fuente: Autoría Propia

Figura 16. Configuración de endian



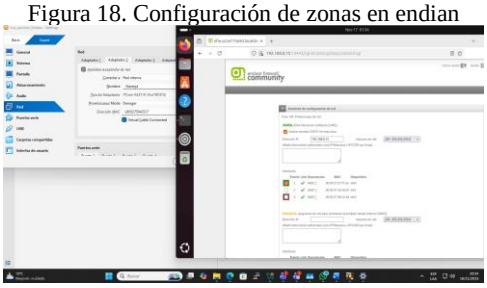
Fuente: Autoría Propia

Figura 17. Configuración de red en endian



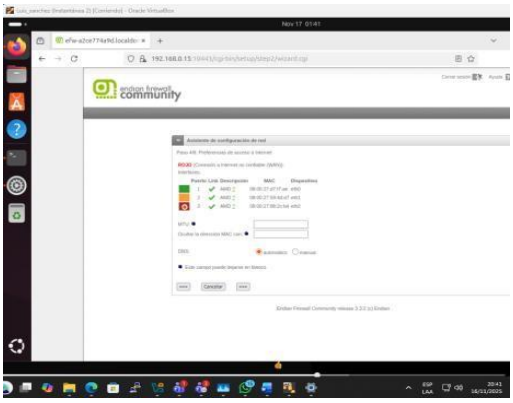
Fuente: Autoría Propia

Figura 18. Configuración de zonas en endian



Fuente: Autoría Propia

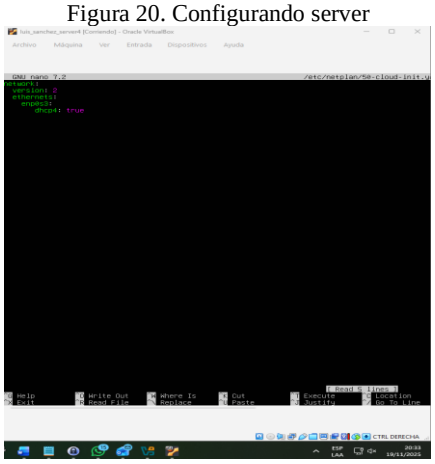
Figura 19. Configuración de red en endian



Fuente: Autoría Propia

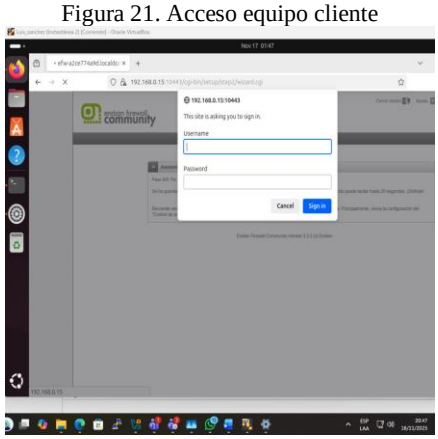
En las Fig.15 a la Fig. 19 se observa las configuraciones realizadas a la plataforma de Endian desde la dirección https, para configurar idiomas, aceptar los términos y condiciones, configurar las contraseñas de acceso y permitir el acceso de internet, la configuraciones realizadas para las zonas naranja, azul y rojo, la aceptación y guardado de las configuraciones realizadas para que se pueda acceder al entorno de trabajo

Figura 20. Configurando server



Fuente: Autoría Propia

Figura 21. Acceso equipo cliente



Fuente: Autoría Propia

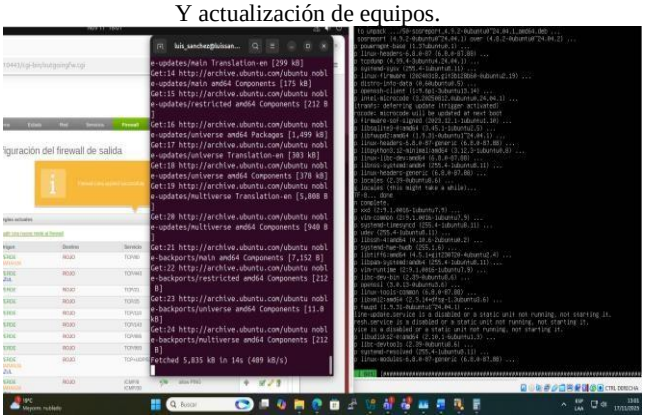
Figura 22. Prueba de conectividad desde el server

Fuente: Autoría Propia

Figura 23. Validación de trafico

Fuente: Autoría Propia

Figura 24. Reglas de Firewall en Endian para el tráfico.
Y actualización de equipos.



Fuente: Autoría Propia

2.3 TEMÁTICA 2: CONFIGURACIÓN NAT.

Posterior a la implementación de Endian y sus respectivas zonas como lo son DMZ, LAN y WAN en virtual box, se procedió a configurar NAT (Network Address Translation) buscando establecer la comunicación desde la LAN y DMZ hacia Internet.Para esto se procedió a ingresar a Endian web y realizar la configuración de reglas de firewall para tráfico saliente. De igual forma se procedió a realizar la configuración en Port Forwarding de dos reglas (HTTP/HTTPS) hacia DMZ, dicha configuración se realizó primeramente para el puerto 80 (HTTP) y de igual forma para el puerto 443 (HTTPS) lo anterior para acceso externo a servicios en la web en DMZ. Dicho proceso dio como resultado una configuración NAT exitosa, estableciendo comunicación entre la LAN e internet y de igual forma de la DMZ a internet, todo ello validado por medio de sus respectivos comandos asegurando su funcionalidad.

Todo ello permitió la implementación y practica de los conocimientos adquiridos durante las diferentes fases y principalmente en la actual, despertando aún más el deseo de continuar el aprendizaje de este sistema operativo tan importante e interesante llamado Linux.

Figura 25. Reglas de tráfico saliente

Fuente: Autoría Propia

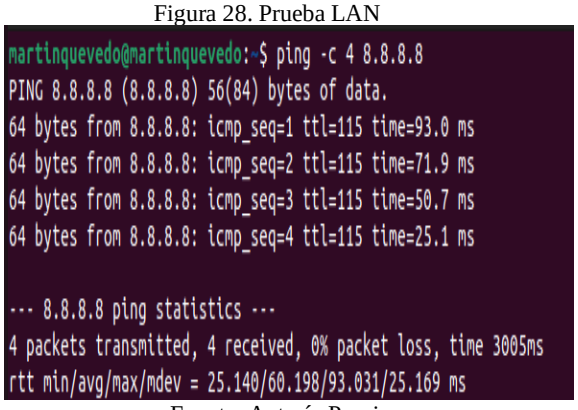
Figura 26. Configuración Internet a DMZ Port80

Fuente: Autoría Propia

Figura 27. Configuración Internet a DMZ Port443

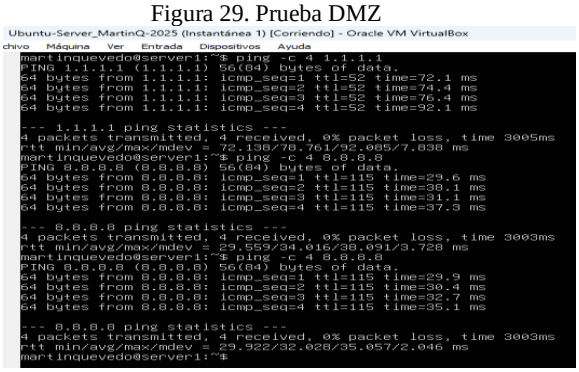
Fuente: Autoría Propia

Figura 28. Prueba LAN



Fuente: Autoría Propia

Figura 29. Prueba DMZ



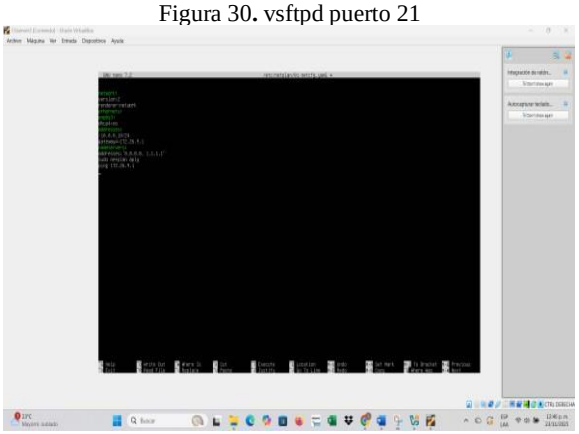
Fuente: Autoría Propia

2.4 TEMÁTICA 3: PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED. PRODUCTO ESPERADO

Inicialmente la configuración de la instancia de Endian, haciendo énfasis en la correcta asignación y funcionamiento de sus tres zonas principales: verde (LAN), roja (WAN) y naranja (DMZ). Posteriormente, se implementarán reglas de NAT (Network Address Translation) con el fin de validar la comunicación entre las distintas zonas, tanto hacia la red interna como hacia una red simulada de Internet.

De manera progresiva, se configurarán políticas de acceso que permitan o restrinjan servicios como HTTP, FTP e ICMP, verificando el comportamiento del tráfico en cada una de las zonas definidas y asegurando la correcta aplicación de reglas de firewall y reenvío de puertos. Finalmente, se llevará a cabo la implementación de un Proxy HTTP no transparente, incorporando mecanismos de autenticación por usuario y la creación de listas negras para el control de la navegación. Esta actividad no solo permite afianzar conceptos teóricos sobre seguridad perimetral, segmentación de redes y servicios de infraestructura, sino que también fomenta el trabajo colaborativo entre los integrantes del grupo, quienes deberán aportar comentarios, sugerencias y análisis técnicos sobre cada temática desarrollada. De esta manera, se garantiza un aprendizaje integral orientado al diseño y gestión de soluciones de red acordes a las necesidades reales de las organizaciones.

Figura 30. vsftpd puerto 21

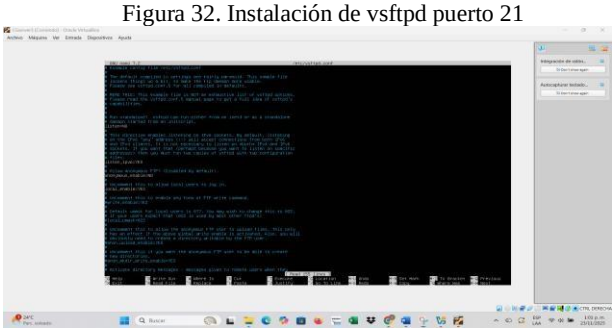


Fuente: Autoría Propia

Figura 31. HTTP puerto 80

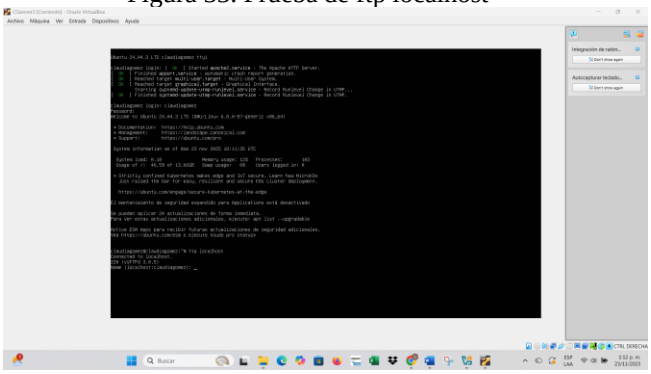
Fuente: Autoría Propia

Figura 32. Instalación de vsftpd puerto 21



Fuente: Autoría Propia

Figura 33. Prueba de ftp localhost



Fuente: Autoría Propia

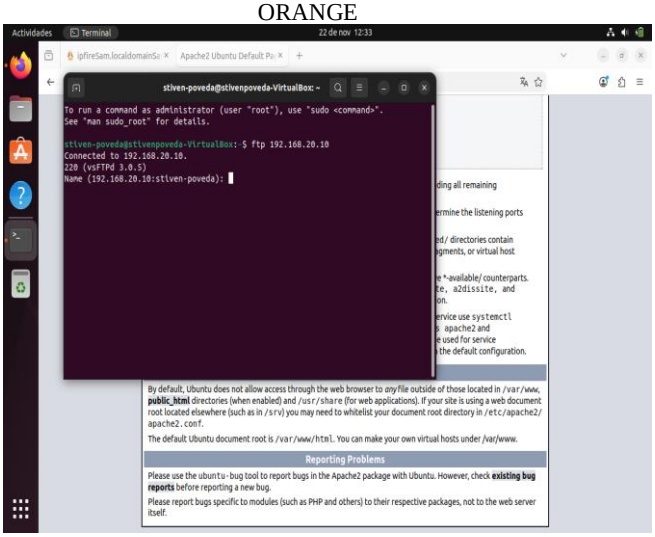
2.5 TEMÁTICA 3: PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED. PRODUCTO ESPERADO

La temática 4 consistió en la creación y validación de reglas de firewall dentro de IPFire con el fin de controlar la comunicación entre las zonas GREEN (LAN), ORANGE (DMZ) y RED (Internet). Estas reglas permiten definir qué servicios pueden circular entre segmentos de red diferenciados, fortaleciendo la seguridad perimetral y reduciendo el riesgo de accesos no autorizados. Para esta actividad se configuraron reglas específicas para habilitar servicios HTTP y FTP entre zonas internas, permitir acceso controlado desde Internet hacia la DMZ y verificar el comportamiento del tráfico en tiempo real mediante los registros Inter-Zona de IPFire.

Figura 34. Cortafuegos

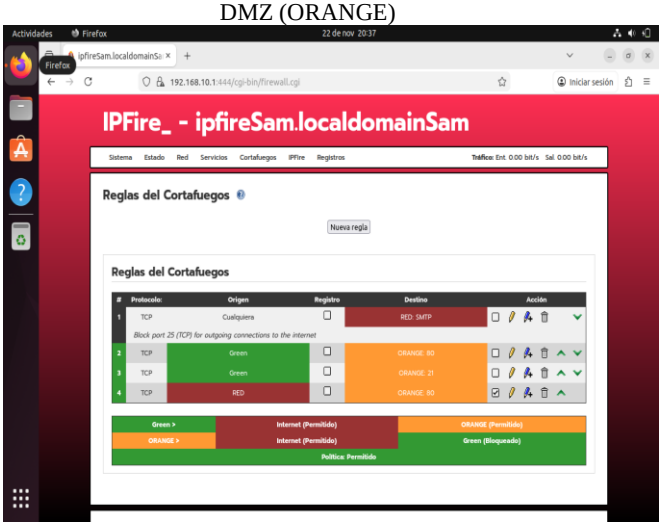
Fuente: Autoría Propia

Figura 35. Comunicación entre la zona GREEN y la zona ORANGE



Fuente: Autoría Propia

Figura 36. Comunicación entre Internet (RED) y la zona DMZ (ORANGE)

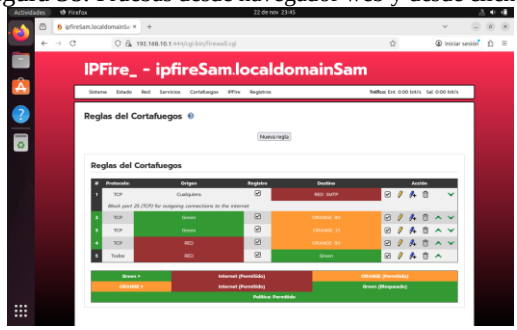


Fuente: Autoría Propia

Figura 37. Verificación del tráfico Inter-Zona

Fuente: Autoría Propia

Figura 38. Pruebas desde navegador web y desde clientes

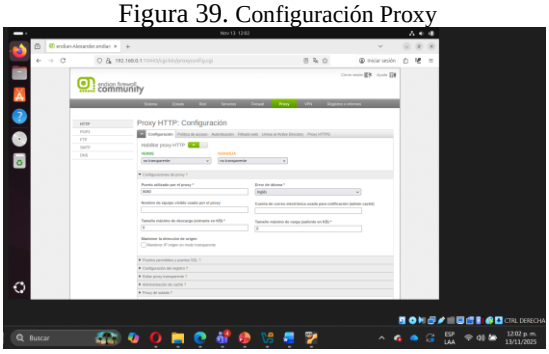


Fuente: Autoría Propia

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

La implementación de un proxy HTTP no transparente con políticas de autenticación para navegación en internet consiste en configurar un servidor proxy que no intercepta automáticamente el tráfico del usuario, sino que requiere que los dispositivos clientes estén configurados explícitamente para enviar su tráfico HTTP a través del proxy. Este tipo de proxy permite mayor control y seguridad, ya que se pueden aplicar políticas de autenticación que obligan a los usuarios a validar su identidad antes de acceder a internet. Además, facilita la administración de permisos y restricciones de navegación, filtrado de contenidos y registro de actividades para cada usuario, asegurando un control riguroso del acceso web en la red.

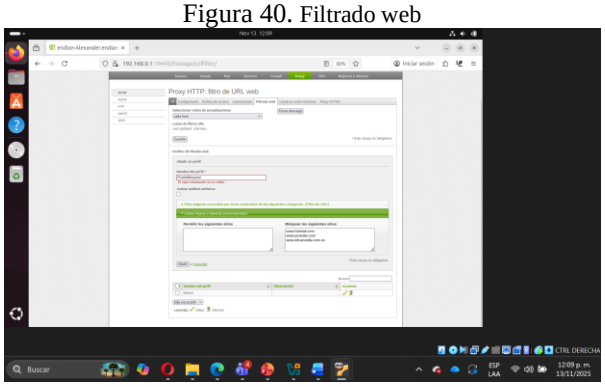
Figura 39. Configuración Proxy



Fuente: Autoría Propia

En la Fig.39 se observa el entorno para configurar el proxy y por ello se debe habilitar el recuadro que se observa en color verde, las demás configuraciones se dejan por defecto.

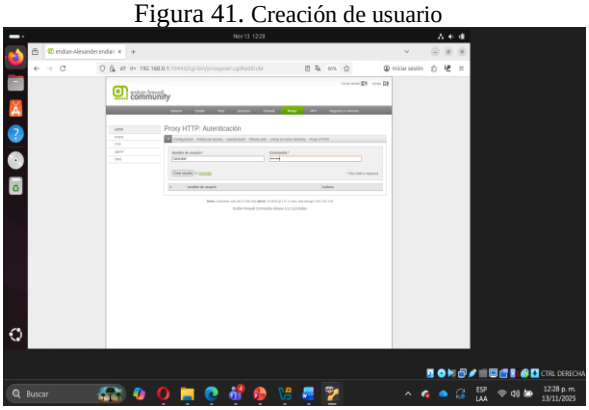
Figura 40. Filtrado web



Fuente: Autoría Propia

En la Fig.40 se observa que se le asigna un nombre al filtrado y se añade en la parte de listas negras las url a bloquear, luego de ello se da clic en guardar.

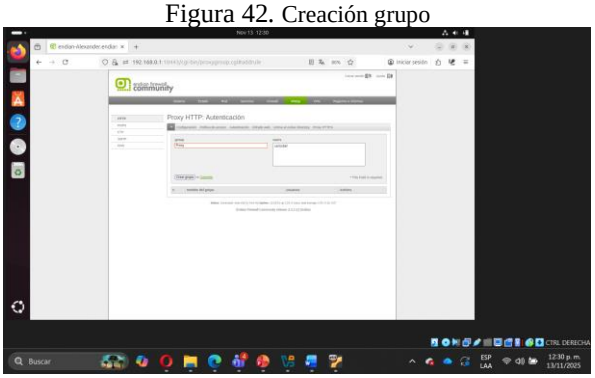
Figura 41. Creación de usuario



Fuente: Autoría Propia

En la Fig.41 se observa el proceso de asignarle una contraseña al usuario.

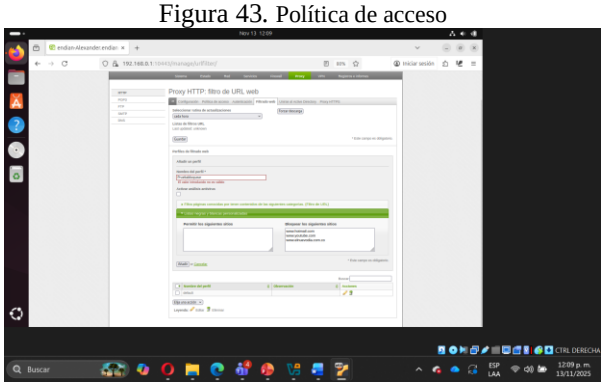
Figura 42. Creación grupo



Fuente: Autoría Propia

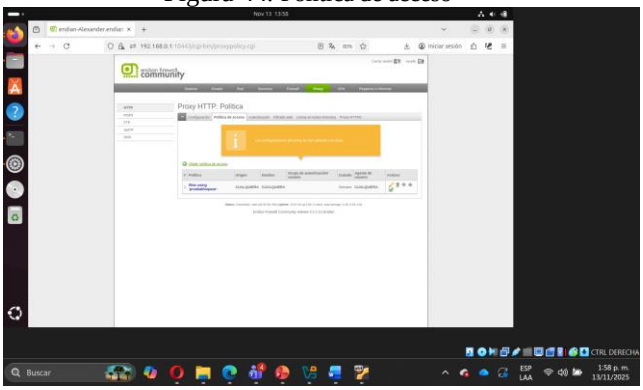
En la Fig.42 se le asigna el usuario creado anteriormente en la Fig.41 a un grupo para que quede registrado.

Figura 43. Política de acceso



Fuente: Autoría Propia

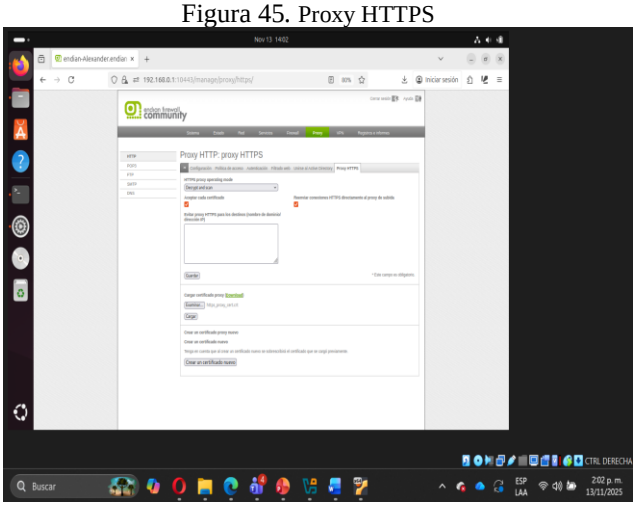
Figura 44. Política de acceso



Fuente: Autoría Propia

En las Fig.43 y Fig.44 se observa el proceso de crear la política de acceso de tal forma que se autentica a través del grupo, se selecciona el navegador y se permite el acceso a través de el filtro creado.

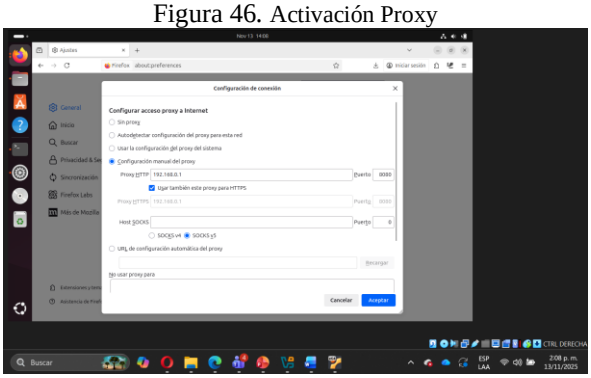
Figura 45. Proxy HTTPS



Fuente: Autoría Propia

La Fig.45 se observa la configuración del proxy a través de https con el descargue y cargue de un certificado.

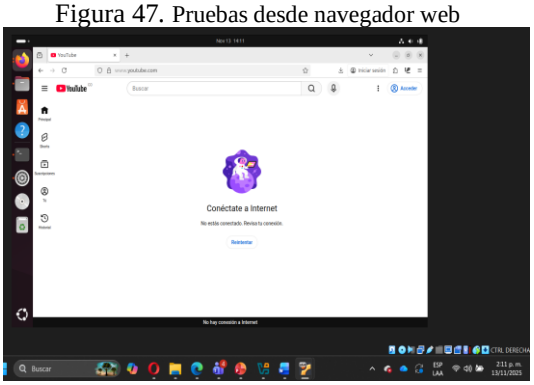
Figura 46. Activación Proxy



Fuente: Autoría Propia

En la Fig.46 se observa la activación del proxy desde los ajustes del navegador.

Figura 47. Pruebas desde navegador web



Fuente: Autoría Propia

Finalmente la Fig.47 muestran el resultado de la activación y configuración del proxy.

3 CONCLUSIONES

Las pruebas de conectividad y verificación de reglas fueron esenciales para validar que las configuraciones realmente cumplían los objetivos de seguridad. La correcta aplicación de reglas HTTP, FTP, ICMP y NAT permitió demostrar el impacto directo que tiene una política de firewall bien implementada en la protección y el funcionamiento de la red.

El uso de herramientas libres como Endian y Ubuntu Server reafirmó el valor de las tecnologías abiertas en los entornos educativos y profesionales. Estas plataformas no solo facilitan el aprendizaje práctico, sino que también ofrecen soluciones reales y escalables que fortalecen las competencias en redes, administración de sistemas y ciberseguridad.

Se reconoce la importancia de los firewall como Endian ya que por medio de distintas reglas logramos controlar el tráfico de red de entrada y salida para la DMZ y la LAN. Todo ello bajo estrictos procedimientos y coadyuvan a una mejor usabilidad y seguridad de bases de datos y redes.

El uso de un proxy HTTP con políticas estrictas de control y autenticación mejora significativamente la seguridad de la red al permitir filtrar y bloquear el acceso a contenidos maliciosos o no autorizados, protegiendo así los recursos internos y reduciendo riesgos de ciberataques. Además, las reglas de acceso permiten definir con precisión qué tráfico es permitido o denegado, lo que contribuye a un control granular y personalizado del entorno de navegación.

La configuración adecuada de reglas de acceso en el proxy no solo optimiza la gestión del ancho de banda y la experiencia del usuario al limitar el acceso a sitios no permitidos, sino que también facilita la auditoría y monitoreo del uso de internet, ayudando a identificar actividades sospechosas o no conformes con las políticas de la organización. Esto convierte al proxy en una herramienta clave para garantizar tanto la seguridad como la eficiencia operativa en redes corporativas o educativas.

4 REFERENCIAS

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

[2] Debian (2023). *El manual del administrador de Debian12.5.0.*Debian.https://www.debian.org/releases/stable/amd64/index. es.html.

[3] Endian (2016), *Endian UTM 3.2 Manual referencia*. Endian. http://docs.endian.com/3.2/utm/index.html

[4] Hernandez, P. F., & Sánchez, J. (2022). *Monitoreo y administración de sistemas Linux* . [Objeto_virtual_de_información_OVI]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/53211

[5] Hernández, P. F., & Sánchez, J. (2022). *Servidores para administración remota y compartir recursos* . [Objeto_virtual_de_información_OVI]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/53212

[6] Jiménez, J. H. (2016). *Shell Script para-Bash.* [Objeto_virtual_de_información_OVI]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/9758

[7] LPI LPIC-1 Exam 101. (2022). *Tema 102:Comandos GNU y Unix.* https://learning.lpi.org/es/learning-materials/101- 500/102/

[8] Oracle (2020), *Manual de usuario VirtualBox*. VirtualBox. https://www.virtualbox.org/manual/

[9] *¿Qué es un servidor proxy? Definición, usos y más* (s.f.). Fortinet. https://www.fortinet.com/lat/resources/cyberglossary/proxy-server

[10]Vargas, Carlos H. (2020). *OVI Implementando el entorno de trabajo GNU Linux*. [Archivo de video]. Repositorio UNAD. https://repository.unad.edu.co/handle/10596/38598