IMPLEMENTACIÓN INTEGRAL DE SEGURIDAD PERIMETRAL CON ENDIAN FIREWALL

Anderson Montes De Arco
amontesde@unadvirtual.edu.co
José Lisandro Salazar Nieto
jlsalazarn@unadvirtual.edu.co
Johanna Andrea Castrillón Yepes
jacastrillony@unadvirtual.edu.co
Santiago Bermúdez Cáceres
sbermudezc@unadvirtual.edu.co
Naida Lemus Zúñiga
nlemusz@unadvirtual.edu.co

RESUMEN: *Este artículo describe la implementación de reglas de Traducción de Direcciones de Red (NAT) en la distribución GNU/Linux Endian Firewall Community, desplegada en un entorno virtualizado mediante VirtualBox. El objetivo principal fue permitir la comunicación controlada entre la red LAN (zona verde), la zona DMZ (zona naranja) y el acceso hacia la red WAN simulada (zona roja). A través de la configuración de reglas NAT tipo masquerade, logré habilitar la salida hacia Internet tanto desde la LAN como desde los servicios ubicados en la DMZ, asegurando un manejo adecuado del tráfico y manteniendo un esquema de seguridad perimetral funcional. Los resultados obtenidos evidencian el correcto funcionamiento del firewall, la efectividad del enmascaramiento de direcciones y el fortalecimiento de las competencias técnicas relacionadas con la administración de redes y la protección perimetral basada en software libre.*
PALABRAS CLAVE: Endian Firewall, NAT, Máscara de origen, Seguridad Perimetral, Redes Linux.

1. INTRODUCCIÓN

En el panorama actual de la seguridad perimetral, la Network Address Translation (NAT) se elige un pilar fundamental para proteger y optimizar las redes internas. El propósito de esta etapa no es solo implementar la distribución GNU/Linux Endian (EFW) como Firewall, sino dominar la configuración de las reglas NAT que permiten el flujo controlado de datos. El direcciona|miento IP definido para las zonas VERDE (LAN), NARANJA (DMZ) y ROJA (WAN) nos obliga a utilizar técnicas de traducción de direcciones para que los dispositivos internos puedan iniciar sesiones con la Red simulada de Internet (WAN), manteniendo oculta su topología de red real.

Esta fase se centrará en dos objetivos principales: primero, establecer la comunicación saliente tanto de la Red Interna (LAN) como de la Zona Desmilitarizada (DMZ) hacia la WAN, permitiendo la navegación y el acceso a recursos externos. Segundo, y no menos importante, abordaremos la configuración de reenvío de puertos (DNAT) para validar la capacidad de exponer servicios específicos de la DMZ (como el servidor web) a Internet de forma segura. El éxito de esta implementación es crucial, ya que sienta las bases para las siguientes temáticas de seguridad y control de tráfico.

1.1 JUSTIFICACION TECNICA

La implementación de un firewall perimetral basado en software libre permite comprender de forma práctica cómo se gestionan los flujos de comunicación entre segmentos de red con diferentes niveles de seguridad. Endian Firewall se convierte en un laboratorio ideal porque integra servicios como NAT, control de tráfico, proxy y publicación de servicios en una sola plataforma.
A través del despliegue de este entorno fue posible analizar cómo se comporta el tráfico cuando atraviesa una DMZ, qué riesgos existen al exponer servicios hacia el exterior y qué mecanismos se emplean para esconder la topología interna utilizando enmascaramiento de direcciones.
Este enfoque no solo permitió la configuración del sistema, sino también comprender por qué detrás de cada decisión técnica, elemento fundamental para un diseño perimetral efectivo.

1.2 CARACTERISTICAS GENERALES

El entorno desarrollado se basó en la distribución Endian Firewall Community, una solución de seguridad perimetral orientada a la administración de redes segmentadas y al control del tráfico entre zonas. Esta plataforma, ejecutada sobre VirtualBox, permitió configurar un esquema de red con tres áreas claramente definidas: zona verde (LAN interna), zona naranja (DMZ) y zona roja (WAN). Cada zona fue asociada a una interfaz de red distinta, lo que facilitó el control del flujo de información según los niveles de seguridad requeridos.
Dentro de las funcionalidades empleadas se destacan la implementación de reglas NAT fuente (masquerade), la administración de políticas de tráfico interzonal, monitoreo de paquetes y control de servicios expuestos. Estas características permitieron simular un firewall corporativo, asegurando el aislamiento de servicios críticos y habilitando la comunicación segura hacia el exterior cuando fue necesario.

2. TÍTULO PRINCIPAL

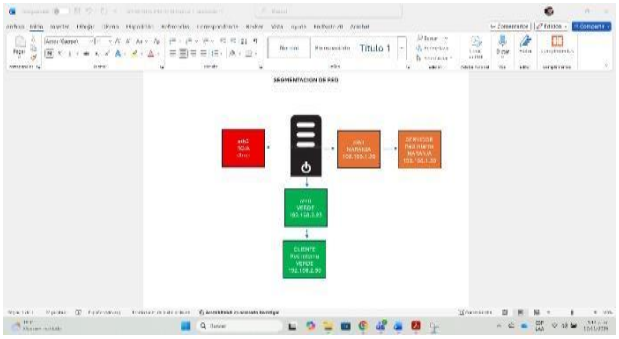
Implementación Integral de Seguridad Perimetral con Endian Firewall: Segmentación, NAT, Políticas Interzonas, Servicios DMZ y Proxy Autenticado.

3. INSTALACIÓN Y CONFIGURACIÓN

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

Dada la siguiente segmentación procedemos a la configuración.

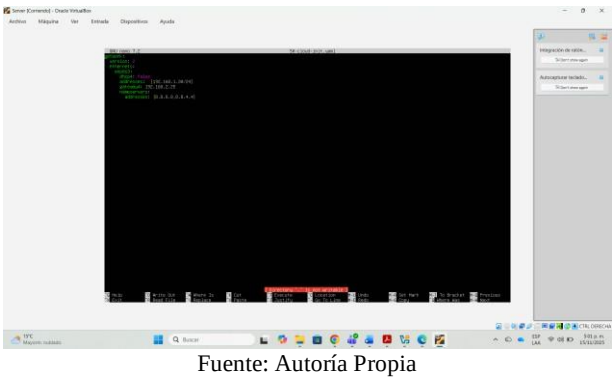
Figura 1. Segmentación de red.



Fuente: Autoría Propia

Asignación ip estática al servidor Ubuntu editando la configuración de red en el archivo 50-club-init. Yaml

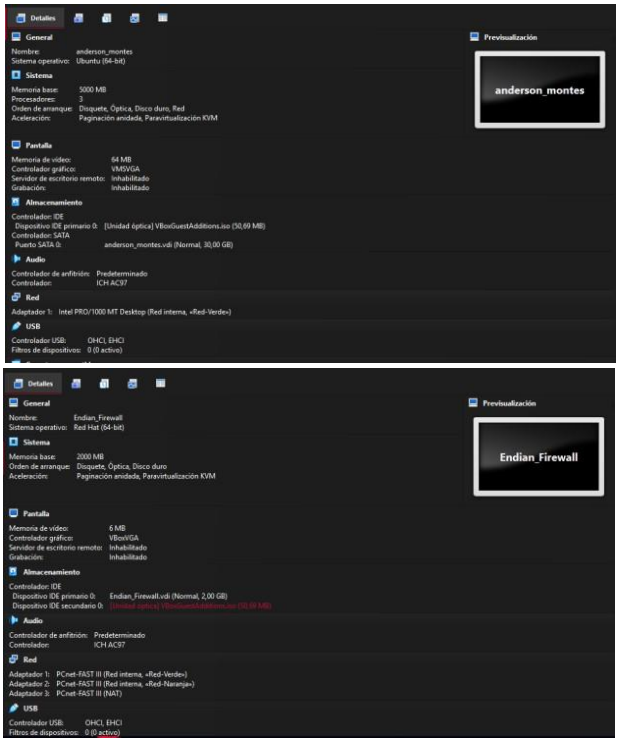
Figura 2. Asignando ip estática al servidor.



Fuente: Autoría Propia

Configuramos en la máquina de Endian los 3 adaptadores de red que usaremos para configurar las diferentes zonas de red, Red interna (Red-Verde), Red interna (Red-Naranja) y NAT (Zona Roja).

Figura 3-4. Configurando en Endian los 3 adaptadores de red.

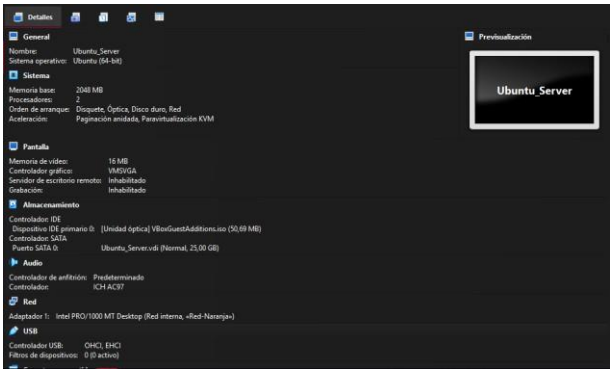


Fuente: Autoría Propia

Configuramos el adaptador de la MV del Cliente Desltop en la Red-Verde, el cual se conectará a internet a través de la maquina Endian del Firewall.

De igual manera configuramos el adaptador del servidor en la Red-Naranja.

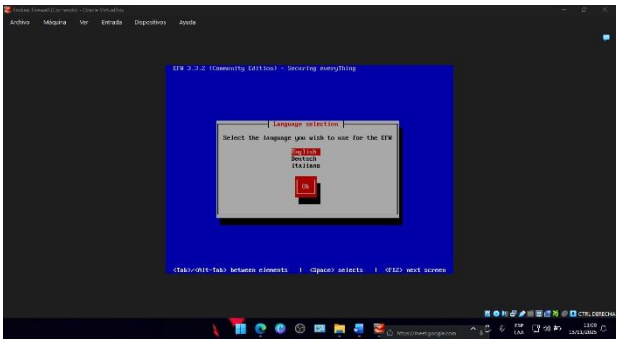
Figura 5. Configurando adaptador del servidor en la red Naranja.

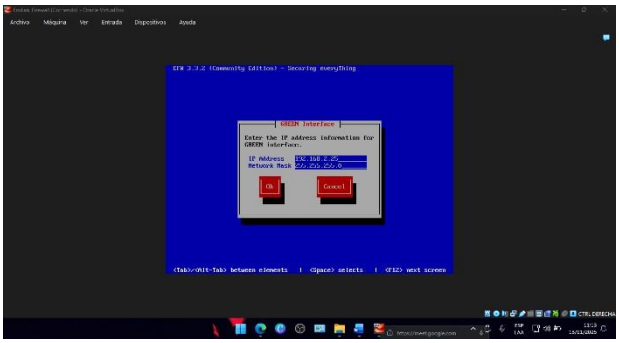


Fuente: Autoría Propia

Durante el arranque e instalación de Endian a partir de la imagen ISO, el asistente solicita configurar la dirección IP correspondiente a la zona verde. En este punto asigné la dirección definida previamente en la segmentación de red, establecida por el compañero encargado de la temática 1 para funcionar como puerta de enlace de la LAN.

Figura 6-7. Asistente de instalación seleccionando lenguaje y direccionamiento ip.

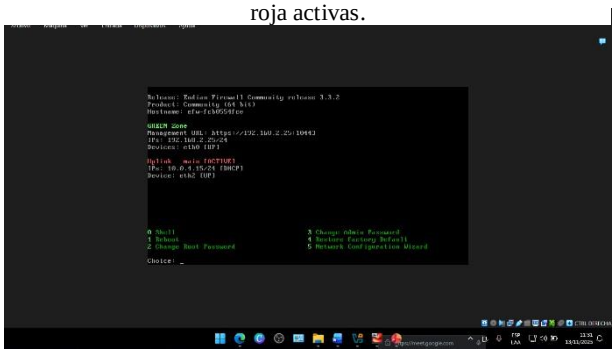




Fuente: Autoría Propia

Podemos observar que el Firewall Edian quedo correctamente instalado y con la zona verde y zona roja activas.

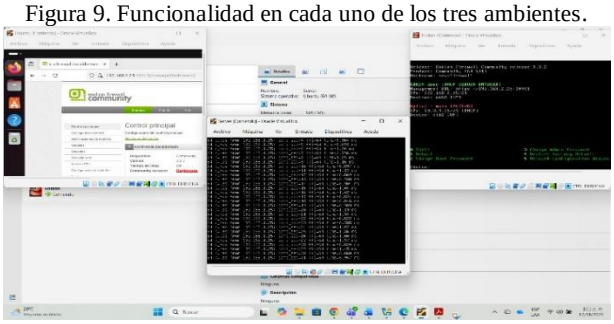
Figura 8. Mostrando instalación de Endian con zona verde y roja activas.



Fuente: Autoría Propia

Mostrando funcionalidad en cada uno de los tres ambientes.

Figura 9. Funcionalidad en cada uno de los tres ambientes.



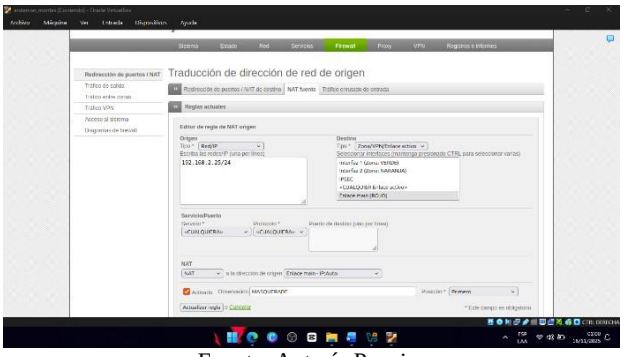
Fuente: Autoría Propia

4. TEMÁTICA 2 CONFIGURACIÓN NAT.

4.1 Creación de las reglas NAT

Nos dirigimos al apartado Firewall y en la pestaña NAT fuente le damos a añadir nueva regla, posterior colocamos la dirección IP de Origen: 192.168.2.25/24 y Destino: el enlace main [Rojo] que viene siendo el internet, en Observación Modo: MASQUERADE Estado → Activado.

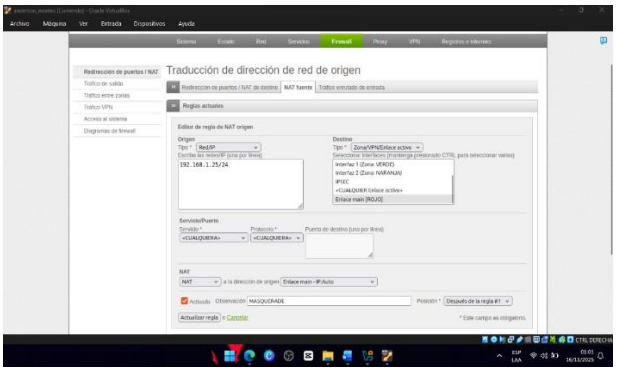
Figura 10. Añadiendo nueva regla NAT.



Fuente: Autoría Propia

De igual forma configuramos la regla para la ORANGE ZONE, pero esta vez con la IP Origen: 192.168.1.25/24.

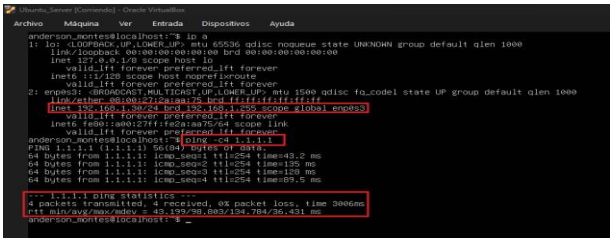
Figura 11. Configurando la regla para la zona Orange.



Fuente: Autoría Propia

Verificación de la conectividad del server, Desde La LAN Hacia La WAN.

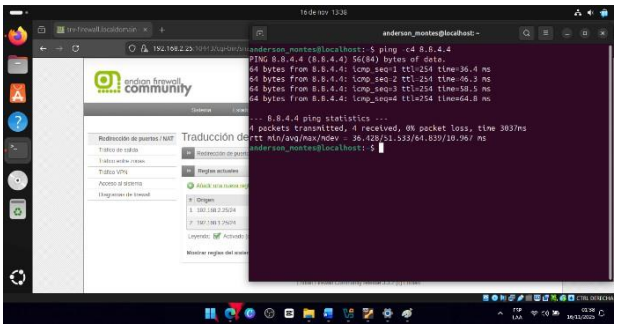
Figura 12. Verificando conectividad desde la LAN hacia la WAN.



Fuente: Autoría Propia

Verificación de conectividad del Cliente Desktop, de LAN hacia la WAN.

Figura 13. Verificando conexión del cliente desde LAN hacia la WAN.



Fuente: Autoría Propia

4.2 Explicación técnica del NAT implementado

La función principal del NAT en este escenario fue permitir que tanto la LAN como la DMZ accedieran hacia la red WAN sin exponer sus direcciones internas. Gracias al modo MASQUERADE, Endian Firewall sustituye la IP de origen del host interno por la IP de la zona roja, logrando un enmascaramiento completo del tráfico.

Esto garantiza que:

- Los equipos internos no se expongan directamente a Internet.
- El firewall gestione las conexiones salientes, manteniendo una tabla de seguimiento.
- Los paquetes de retorno puedan ser redirigidos al host correcto.

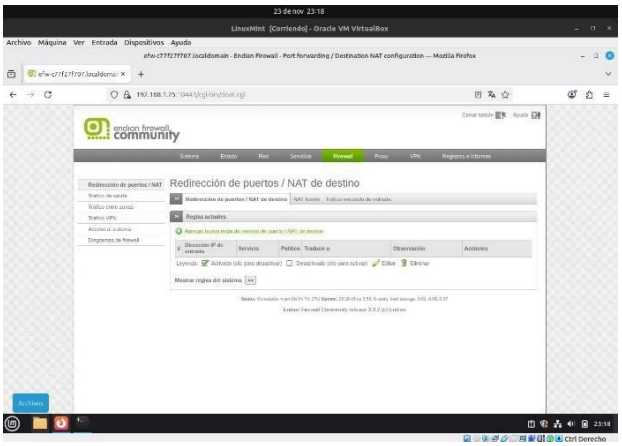
La verificación mediante pruebas de conectividad (ping, navegación y resolución DNS) evidenció que el proceso de traducción se estaba realizando de manera correcta.
Este comportamiento es equivalente al de un firewall corporativo, lo que permitió simular escenarios reales de salida controlada al exterior.

5. TEMATICA 3

5.1 Permitir servicios de la zona DMZ para la red

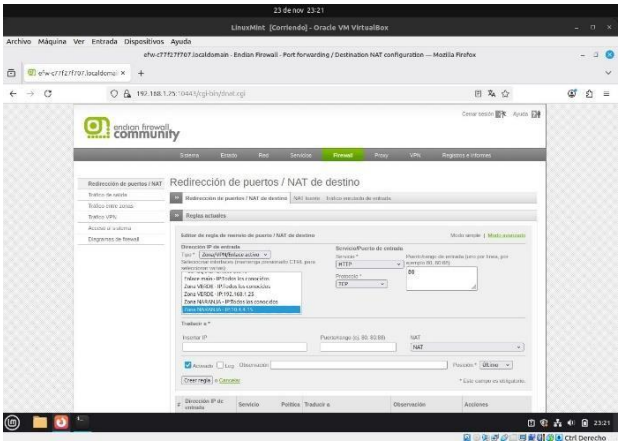
Permitir los servicios HTTP (Puerto 80) y FTP (Puerto 21) desde el servidor Web bajo Ubuntu Server.

Figura 14. Interfaz firewall.



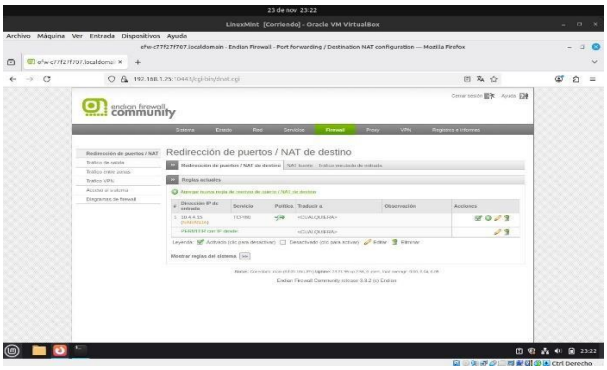
Fuente: Autoría Propia

Figura 15. Creando regla permitir desde el http el puerto 80.



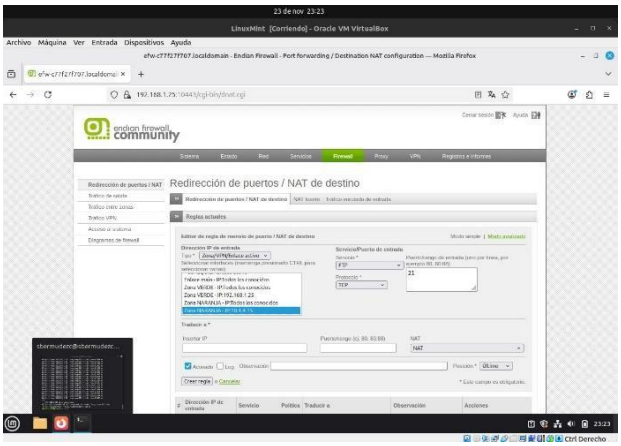
Fuente: Autoría Propia

Figura 16. Guardando regla http.



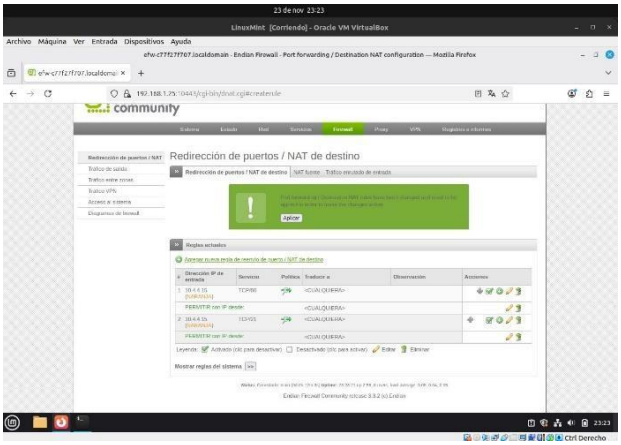
Fuente: Autoría Propia

Figura 17. Añadiendo regla ftp para puerto 21.



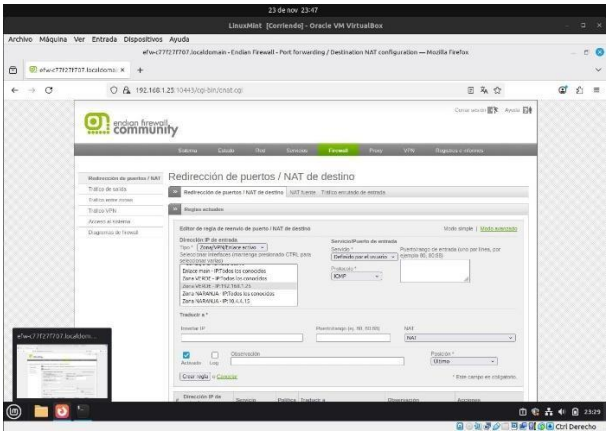
Fuente: Autoría Propia

Figura 18. Aplicando cambios para http y ftp.



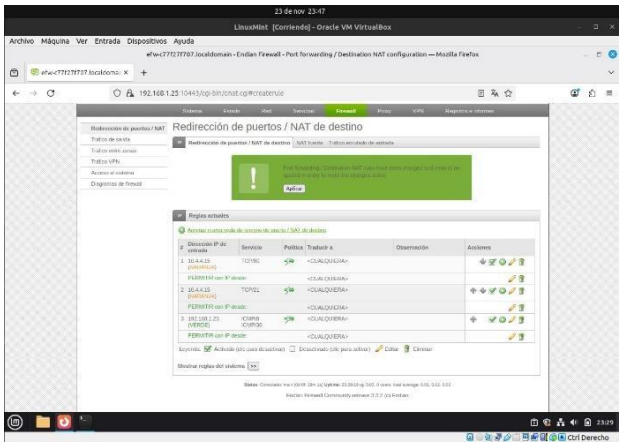
Fuente: Autoría Propia

Figura 19. Denegar el protocolo ICMP (Puerto 8 y puerto 30) para no permitir hacer ping en la red.



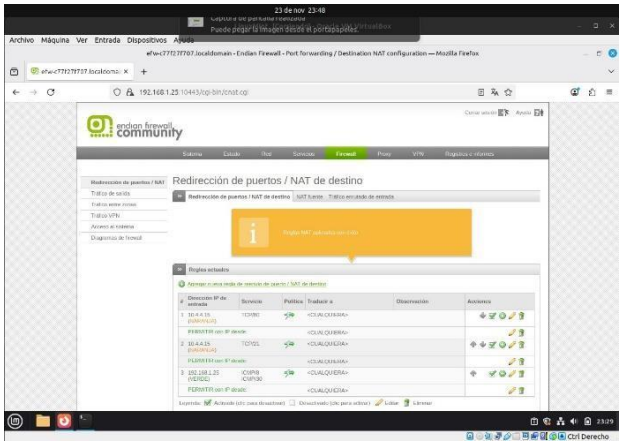
Fuente: Autoría Propia

Figura 20. Creando regla para bloquear IP por el puerto 8 y 30.



Fuente: Autoría Propia

Figura 21. Aplicando cambio de regla para bloqueo de IP, configuración exitosa.



Fuente: Autoría Propia

5.2 Análisis de seguridad y funcionamiento del acceso desde la DMZ

La DMZ sirve como contenedor aislado para servicios que deben ser accesibles desde redes externas o desde segmentos internos bajo reglas controladas. Al permitir únicamente puertos HTTP y FTP para la DMZ, se garantizó que el servidor Ubuntu expusiera únicamente los servicios estrictamente necesarios.

Bloquear ICMP también fue una medida relevante, ya que evita que un atacante realice barridos de red o reconozca la estructura de la DMZ. Esto reduce la superficie de ataque al impedir la recolección de información sobre la disponibilidad de equipos o rutas.

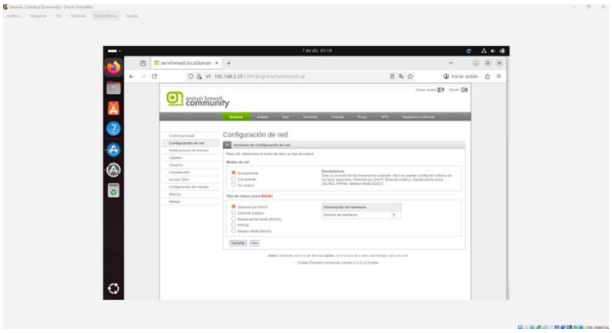
En conjunto, estas reglas permitieron mantener un equilibrio entre disponibilidad y seguridad, controlando el flujo hacia un servidor que opera en un entorno aislado

6. TEMATICA 4: Reglas de acceso para permitir o denegar el tráfico

6.1 Pasos en Endian Firewall:

Se ingresa a la URL asignada utilizando un equipo de escritorio, que ha sido configurado mediante el adaptador verde en la máquina de Endian, en este caso la dirección Ip es 192.168.2.25, después de acceder al navegador con esta dirección se realizan las configuraciones necesarias.

Figura 22. Mostrando interfaz de bienvenida a Endian.



Fuente: Autoría Propia

6.2 Creación de reglas

6.2.1 Crear reglas de Allow para HTTP y FTP entre Zona Verde → Zona Naranja.

Para habilitar el acceso interno hacia los servicios web ubicados en la DMZ, se creó una regla específica en Endian Firewall que permite el tráfico HTTP (puerto 80) proveniente de la red LAN. En dicha regla se definieron la dirección IP de origen 192.168.2.25 y el segmento de destino correspondiente a la DMZ, asegurando una comunicación adecuada y controlada entre ambas zonas de la red.

Las reglas del firewall se diseñaron y aplicaron dentro del apartado Inter-Zonas de Endian Firewall, siguiendo una metodología organizada que permitió mantener uniformidad en las políticas de seguridad. Desde los paneles de configuración se implementaron tres reglas principales:

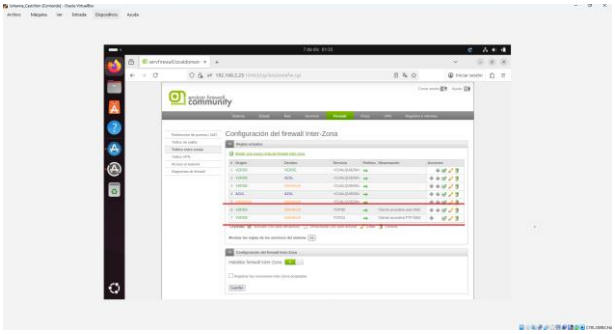
- **HTTP LAN → DMZ:** Se autorizó el tráfico web (TCP/80) desde los equipos de la red interna hacia los servidores ubicados en la DMZ, permitiendo así el acceso a las aplicaciones corporativas alojadas en esta zona.
- **FTP LAN → DMZ:** Se activó el flujo para transferencia de archivos (TCP/21) desde la LAN hacia los servidores FTP en la DMZ, garantizando un manejo seguro de los datos mediante autenticación básica.

Tabla 1. Configuración de las 2 primeras reglas.

De zona	A zona	Servicio	Acción	Observación
GREEN	ORANGE	HTTP (80/TCP)	Aceptar	Cliente accederá web DMZ
GREEN	ORANGE	FTP (21/TCP)	Aceptar	Cliente accederá FTP DMZ

Fuente: Elaboración propia

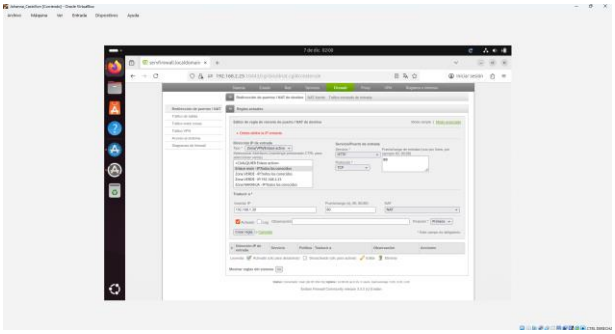
Figura 23. Configuración reglas en Endian.



Fuente: Autoría Propia

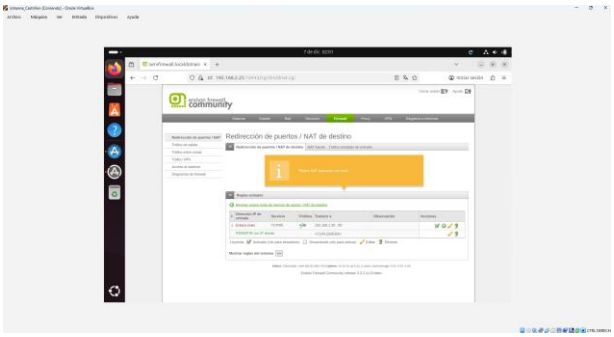
- **Regla NAT de destino (RED → ORANGE):** En la siguiente imagen se observa la ventana del firewall Endian donde se configura una regla de redirección de puertos para permitir que un servicio interno pueda ser accedido desde la red externa. En este caso, se está creando una regla NAT de destino para que cualquier solicitud que llegue al firewall por el puerto 80 (HTTP) desde la zona roja, es decir, desde Internet sea enviada al servidor ubicado en la zona naranja (DMZ), cuya dirección IP es 192.168.1.30.

Figura 24. Regla NAT de destino.



Fuente: Autoría Propia

Figura 25. Regla NAT aplicada con éxito.

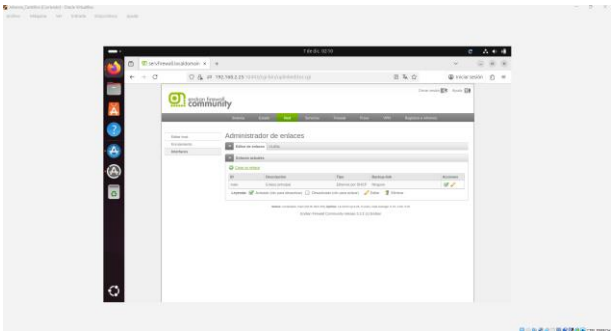


Fuente: Autoría Propia

En la figura 25 se observa la interfaz del firewall Endian después de crear y activar una regla de redirección de puertos (NAT de destino). El sistema muestra un mensaje de confirmación indicando que la regla fue aplicada correctamente, lo que significa que el firewall ya está preparado para recibir solicitudes externas y enviarlas al servidor ubicado en la zona DMZ.

Ahora, se muestra la sección del firewall Endian destinada a la administración de enlaces de red. Desde este panel es posible identificar y configurar las interfaces físicas que utiliza el sistema para conectarse a las diferentes zonas de la red.

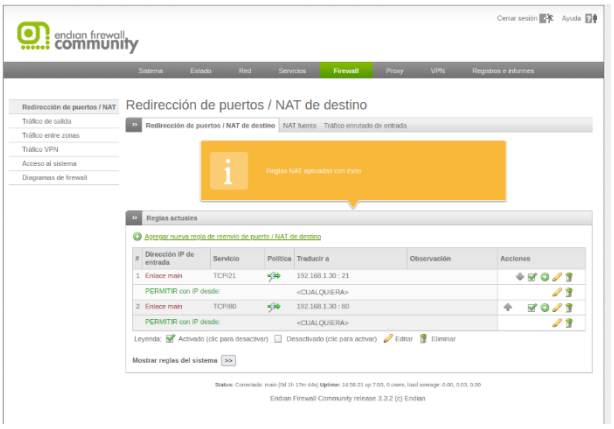
Figura 26. Administrador de enlaces en Endian Firewall.



Fuente: Autoría Propia

La vista presenta un único enlace activo denominado “main”, el cual está configurado para obtener su dirección IP mediante DHCP. Este enlace corresponde a la interfaz que Endian utiliza como conexión principal hacia la red externa o zona roja (WAN). Su estado aparece como “activado”, lo que indica que el firewall está utilizando correctamente esta interfaz para gestionar el tráfico entrante y saliente hacia Internet. La presencia de este enlace es esencial para que las reglas de redirección de puertos y filtrado de tráfico funcionen correctamente, ya que define el punto de entrada para cualquier solicitud proveniente del exterior.

Figura 27. Reglas NAT para servicios HTTP y FTP aplicadas correctamente.



Fuente: Autoría Propia

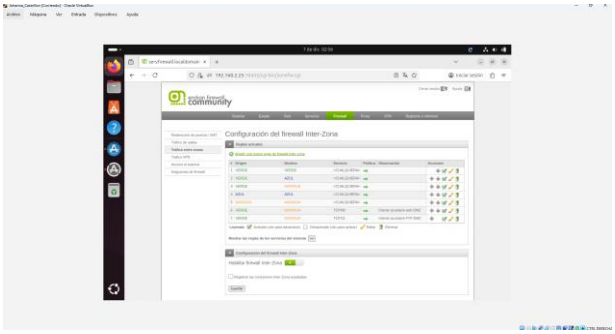
En esta figura se observa la sección del firewall Endian donde se administran las reglas de redirección de puertos o NAT de destino. El sistema muestra un mensaje indicando que las reglas fueron aplicadas con éxito, lo que confirma que la configuración realizada ha sido aceptada y se encuentra activa. En la tabla inferior se visualizan dos reglas fundamentales para la práctica:

- La primera permite que las solicitudes externas que llegan por el puerto 21/TCP sean enviadas al servidor interno con dirección 192.168.1.30, donde se encuentra alojado el servicio FTP.
- La segunda regla cumple la misma función para el servicio HTTP, redirigiendo el tráfico entrante por el puerto 80/TCP hacia el mismo servidor en la zona DMZ.

Ambas reglas están marcadas como activas, lo cual garantiza que el firewall está gestionando correctamente las conexiones provenientes de la red WAN y permitiendo el acceso controlado a los servicios internos publicados en la DMZ.

Por último, necesitamos validar las reglas en la parte de firewall Inter Zona.

Figura 28. Configuración del firewall Inter-Zona.



Fuente: Autoría Propia

En la tabla se muestran varias reglas activas, entre ellas las que permiten que los equipos de la red VERDE puedan acceder a los servicios HTTP y FTP del servidor ubicado en la DMZ. Estas reglas autorizan el uso de los puertos 80/TCP y 21/TCP,

lo que permite que la red interna acceda de manera controlada al servidor de pruebas. Además, se observan otras reglas predeterminadas que gestionan la comunicación entre zonas según la política de seguridad configurada. La parte inferior confirma que el firewall Inter-Zona se encuentra habilitado, lo cual garantiza que todas estas reglas están activas y gestionando el tráfico entre segmentos de red de manera correcta.

6.2.2 Funcionamiento del Tráfico Interzonas

En esta etapa se estudió cómo Endian Firewall filtra el tráfico según la relación entre zonas y puertos. Aunque las reglas NAT permiten la salida general, las políticas interzonas definen qué servicios pueden comunicarse entre segmentos internos. Al habilitar HTTP y FTP desde la zona verde hacia la zona naranja, se logró que usuarios internos accedieran al servidor web ubicado en la DMZ sin riesgo de que la DMZ iniciara conexiones hacia la LAN.
Este comportamiento confirma uno de los principios de diseño perimetral: las comunicaciones desde zonas de mayor seguridad hacia zonas menos seguras deben estar estrictamente controladas.

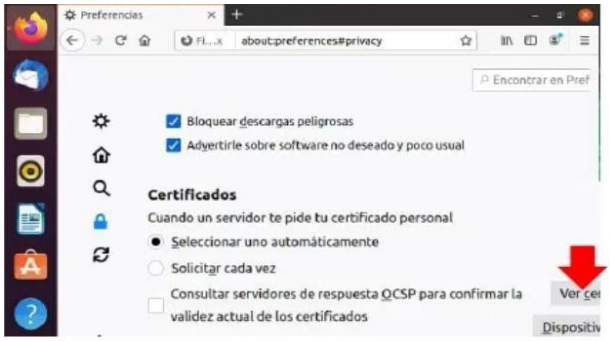
La validación permitió observar cómo el firewall ejecutaba las reglas con prioridad, descartando cualquier tráfico no autorizado.

7. TEMÁTICA 5: Implementar un Proxy HTTP (No transparente) con políticas de autenticación para navegación en Internet.

7.1 Crear un perfil y establecer una lista negra bloqueando los siguientes sitios:

www.hotmail.com
www.youtube.com
www.elnuevodia.com.co

Figura 29. Configurando preferencias de privacidad.



Fuente: Autoría Propia

7.2 **Autenticación por usuario:** A través de la opción proxy cree un usuario y asócielo a un grupo. Establezca una política de acceso y vincule el perfil creado en el punto anterior y relaciónelo también con la política de autenticación.

Figura 30-31. Autenticación proxy HTTP por usuario.

Fuente: Autoría Propia

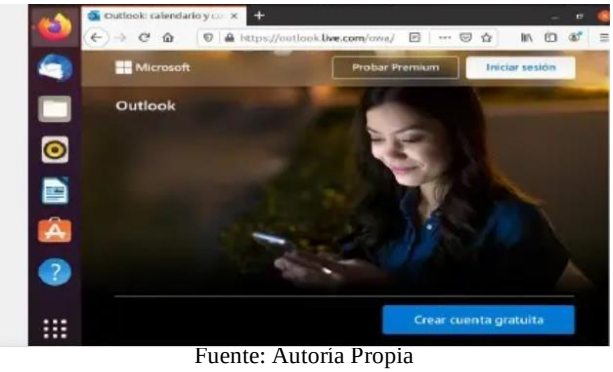
7.3 Probar desde la LAN a través de un navegador Web, el acceso a los portales referenciados en la lista negra.

Figura 32. Probando desde la LAN el acceso del navegador.

Figura 33. Probando desde la LAN el acceso a YouTube

Fuente: Autoría Propia

Figura 34. Probando desde la LAN el acceso a Outlook.



Fuente: Autoría Propia

7.4 Análisis del Proxy Autenticado

La implementación del proxy no transparente permitió centralizar la gestión de la navegación. Al requerir autenticación por usuario, Endian obliga a que cada solicitud sea verificada antes de prtmitir el acceso a Internet.
Esto aporta beneficios importantes:

- Control individual del uso de Internet.
- Aplicación de perfiles y políticas específicas.
- Registro detallado del tráfico asociado a cada usuario.
- Bloqueo de sitios mediante listas negras.

La prueba desde la LAN evidenció que el proxy actuaba como intermediario, denegando correctamente los portales incluidos en la lista negra.
De esta forma se comprobó que el sistema no solo filtra tráfico, sino que también fortalece la trazabilidad y el cumplimiento de políticas organizacionales.

8. DISCUSIÓN

El desarrollo del proyecto permitió comprender de manera práctica cómo interactúan los diferentes componentes de un firewall perimetral. Durante el proceso se identificaron desafíos relacionados con la correcta asignación de IP, el orden de las reglas de firewall y la relación entre políticas NAT e interzonas.

Un hallazgo importante fue observar que la DMZ realmente aísla los servicios expuestos, evitando que un compromiso en el servidor afecte directamente a la LAN.
Otro aspecto relevante fue comprobar que el proxy autenticado agrega un nivel adicional de control y se convierte en una herramienta esencial para monitorear el uso de Internet.

En general, la integración de Endian Firewall demostró que una solución basada en software libre puede cumplir funciones avanzadas de seguridad sin requerir infraestructura costosa.

9. CONCLUSIÓN

La implementación realizada permitió construir un entorno robusto y funcional de seguridad perimetral, en el que fue posible comprender tanto los aspectos técnicos como los conceptos estratégicos involucrados en la protección de redes.

A través de la segmentación en zonas, la configuración de NAT, la administración de políticas interzonas, la publicación de servicios en la DMZ y el uso de proxy autenticado, se evidenció cómo cada componente contribuye a un esquema integral de defensa.

Uno de los aprendizajes más significativos fue entender que la seguridad no depende únicamente de bloquear tráfico, sino de diseñar rutas y reglas que permitan la operación normal sin comprometer la integridad de la red.

Este proyecto fortaleció competencias relacionadas con la administración de redes, la gestión de servicios bajo GNU/Linux y la aplicación de buenas prácticas de seguridad, desarrollando habilidades directamente aplicables en entornos profesionales de ciberseguridad.

10. CITAS Y/O REFERENCIAS

[1] Canonical (2023). Guía del Ubuntu desktop 20.04 LTS. Help Ubuntu.
[2] Debian (2023). El manual del administrador de Debian 12.5.0. Debian
[3] Endian (2016), Endian UTM 3.2 Manual referencia. Endian.
[4] Jay LaCroix. (2020). Mastering Ubuntu Server: Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting Ubuntu Server. Packt Publishing.
[5] LPI LPIC-1 Exam 101. (2022). Tema 101: Determinar y configurar los ajustes de hardware.
[6] Oracle (2020), Manual de usuario VirtualBox. VirtualBox.
[7] Zapata Escobar, D. E., Gómez Tangarife, I. L., Acevedo Munera, J. D., Obando Ibarra, C. H., & García Arango, D. A. (2023). Implementación de un sistema de control y seguridad Informático ENDIAN FIREWALL. INGENIERÍA: Ciencia, Tecnología e Innovación, 10(1), 98–115.