Seguridad perimetral en GNU/Linux: configuración de firewall, NAT y servicios en zona DMZ

Diego Alejandro Mendez Lopez
damendezl@unadvirtual.edu.co
Jose Guillermo Mojica Espitia
jgmojicae@unadvirtual.edu.co

RESUMEN: *La actividad grupal se enfoca en implementar una solución de seguridad perimetral para proteger los servidores de una intranet (LAN) y extranet (WAN) mediante la creación de una zona DMZ. El objetivo principal es garantizar la seguridad e integridad de las bases de datos y aplicaciones web que funcionan sobre plataformas GNU/Linux. Para ello, todos los integrantes del grupo deben descargar, instalar y configurar la distribución GNU/Linux Endian Firewall (EFW), que actuará como firewall entre la LAN y la WAN. Además, cada estudiante deberá seleccionar y desarrollar de manera individual una de las cinco temáticas propuestas, evidenciando desde la consola el estado, inicio, detención y reinicio de los servicios, mostrando fecha y hora de ejecución.*
La infraestructura propuesta contempla estaciones de trabajo GNU/Linux para la red LAN, Endian como firewall principal y un servidor GNU/Linux ubicado en la DMZ, encargado de alojar bases de datos y aplicaciones web. También se destaca la importancia de definir y mantener correctamente los direccionamientos IP en toda la red, ya que estas configuraciones deberán ser utilizadas de manera uniforme por todos los integrantes del grupo durante el desarrollo de las actividades y la consolidación del trabajo final colaborativo.
.

PALABRAS CLAVE: seguridad perimetral, DMZ, GNU/Linux, firewall, NAT, red, iptables, reglas

1 INTRODUCCIÓN

La seguridad perimetral es un elemento fundamental en la protección de redes y sistemas informáticos, especialmente en entornos donde se administran bases de datos y aplicaciones web. En esta actividad se plantea la implementación de una infraestructura segura mediante el uso de GNU/Linux y la distribución Endian Firewall (EFW), con el propósito de controlar y proteger el tráfico entre la red interna (LAN), la red externa (WAN) y una zona desmilitarizada (DMZ). Esta arquitectura permite fortalecer la integridad, disponibilidad y confidencialidad de los servicios alojados en los servidores.

A través del trabajo colaborativo, cada integrante desarrollará la instalación, configuración y administración de los servicios requeridos, aplicando comandos desde consola para supervisar y gestionar el funcionamiento de la plataforma. Además, se pondrán en práctica conceptos relacionados con direccionamiento IP, administración de redes y seguridad informática, fortaleciendo las competencias técnicas necesarias para la implementación de soluciones de protección perimetral en entornos reales.

2 OBJETIVOS DEL PROYECTO

Objetivo General

Implementar una configuración de seguridad perimetral en GNU/Linux mediante Endian Firewall Community, aplicando reglas NAT para permitir la comunicación controlada desde las zonas GREEN y ORANGE hacia la red externa, con el fin de proteger la infraestructura interna, validar el funcionamiento de la LAN y la DMZ, y fortalecer la administración segura del tráfico de red en un entorno académico simulado.

Objetivos Específicos

- Instalar y configurar Endian Firewall Community en un entorno virtualizado, asignando correctamente las interfaces de red para las zonas GREEN, ORANGE y RED.
- Configurar reglas NAT en Endian Firewall para permitir la salida controlada hacia Internet desde la red interna LAN y desde la zona DMZ.
- Verificar la conectividad entre el equipo desktop, el firewall Endian y las redes configuradas, mediante pruebas básicas de comunicación desde consola.
- Validar el funcionamiento de las reglas NAT utilizando herramientas de administración y comandos de red que permitan evidenciar el tráfico saliente.
- Analizar la importancia de la seguridad perimetral en GNU/Linux, reconociendo el papel del firewall en la protección de servicios, bases de datos y aplicaciones ubicadas en la LAN y la DMZ.

3 METODOLOGÍA

La metodología aplicada fue práctica y experimental, debido a que se desarrolló una implementación técnica en un entorno virtualizado con Endian Firewall Community. El proceso inició con la instalación y configuración de la máquina virtual, la asignación de interfaces para las zonas GREEN, ORANGE y RED, y la definición de la arquitectura de red. Luego se configuraron las reglas NAT para permitir la comunicación desde la LAN y la DMZ hacia Internet. Finalmente, se realizaron pruebas de conectividad y validación desde consola, con el fin de comprobar que el tráfico saliente fuera gestionado correctamente por el firewall y que la infraestructura cumpliera con los criterios de seguridad perimetral establecidos para la actividad.

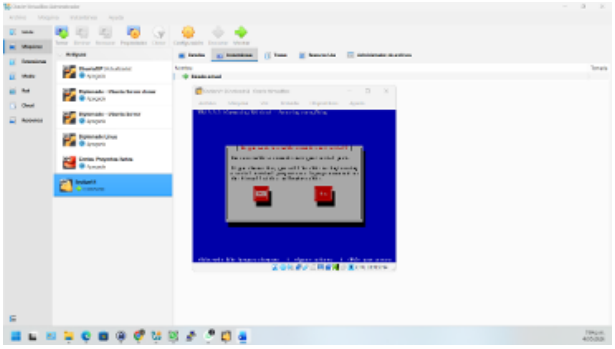
4 DESARROLLO DEL CONTENIDO

4.1 TEMÁTICA 2

En esta temática se realizó la configuración de NAT en Endian Firewall Community, con el propósito de permitir la salida controlada a Internet desde las zonas internas de la infraestructura implementada. NAT, o traducción de direcciones de red, permite que los equipos ubicados en redes privadas puedan comunicarse con redes externas utilizando la interfaz de salida del firewall, evitando exponer directamente las direcciones IP internas de la LAN y de la DMZ.

Para el desarrollo de la práctica se tomó como base la arquitectura definida para la Etapa 7, donde Endian actúa como firewall principal entre las zonas GREEN, ORANGE y RED. La zona GREEN corresponde a la red interna o LAN, la zona ORANGE corresponde a la DMZ donde se ubican los servicios GNU/Linux Server, y la zona RED representa la conexión hacia la red externa o Internet. Esta distribución permite controlar el tráfico entre segmentos de red y aplicar políticas de seguridad perimetral de forma centralizada.

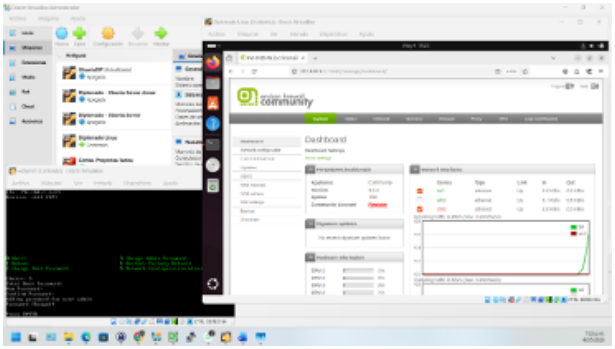
Figura 1. Instalación de Endian Firewall.



Fuente. Autoría propia

Se evidencia el proceso inicial de instalación de Endian Firewall Community sobre una máquina virtual en VirtualBox. Esta instalación permite disponer de una plataforma especializada en seguridad perimetral, la cual será utilizada como firewall principal para controlar el tráfico entre la red interna, la zona DMZ y la red externa.

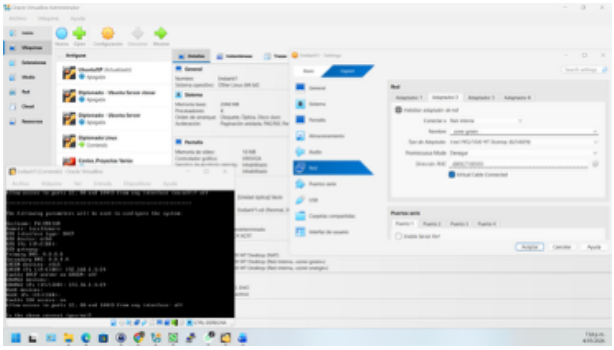
Figura 2. Funcionamiento de Endian Firewall.



Fuente. Autoría propia

Se muestra la verificación del correcto funcionamiento de Endian Firewall después de su instalación. En esta etapa se valida que el sistema inicie adecuadamente, que los servicios básicos estén activos y que la máquina virtual se encuentre preparada para realizar las configuraciones de red.

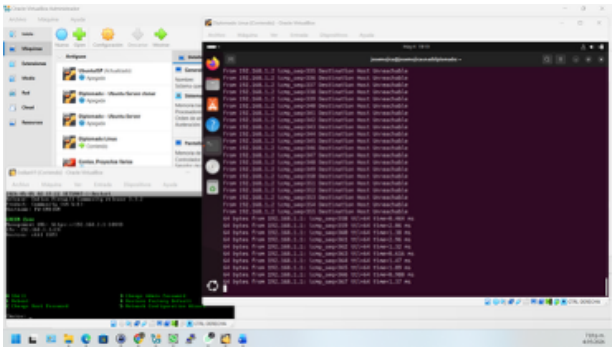
Figura 3. Conexión con sus redes.



Fuente. Autoría propia

Se presenta la configuración de las interfaces de red asignadas a Endian Firewall dentro de VirtualBox. Esta configuración es fundamental porque permite separar las zonas GREEN, ORANGE y RED, garantizando que cada segmento de red tenga una función específica dentro de la arquitectura de seguridad perimetral.

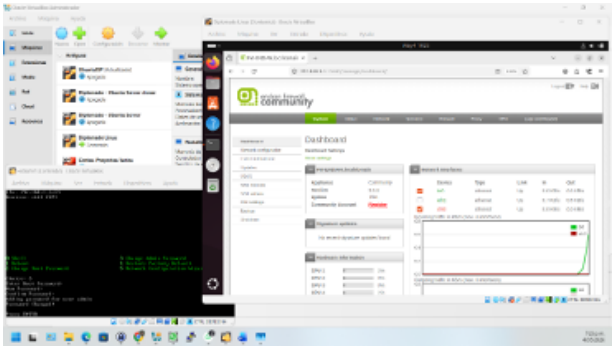
Figura 4. Conexión desde el equipo desktop hacia Endian.



Fuente. Autoría propia

Se realiza una prueba de conectividad desde el equipo Ubuntu Desktop hacia Endian Firewall, con el fin de comprobar que existe comunicación entre la estación de trabajo y el firewall. Esta validación permite confirmar que la zona interna o LAN puede alcanzar correctamente la puerta de enlace definida.

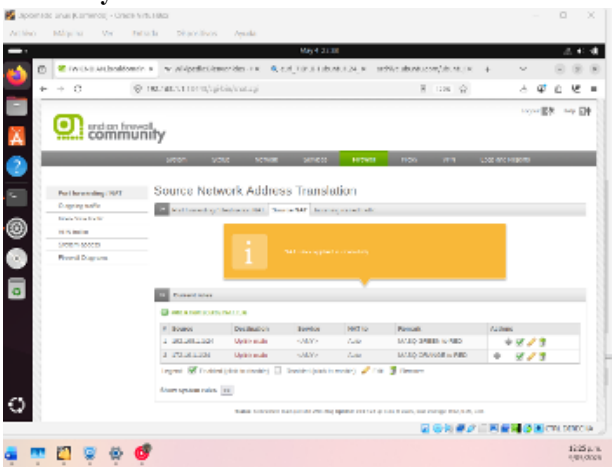
Figura 5. Ingreso al panel de administración de Endian.



Fuente. Autoría propia

Se evidencia el acceso al panel web de administración de Endian Firewall desde el navegador. Desde esta interfaz gráfica se gestionan las principales configuraciones del firewall, incluyendo reglas de red, políticas de tráfico, servicios y opciones de seguridad necesarias para el desarrollo de la temática.

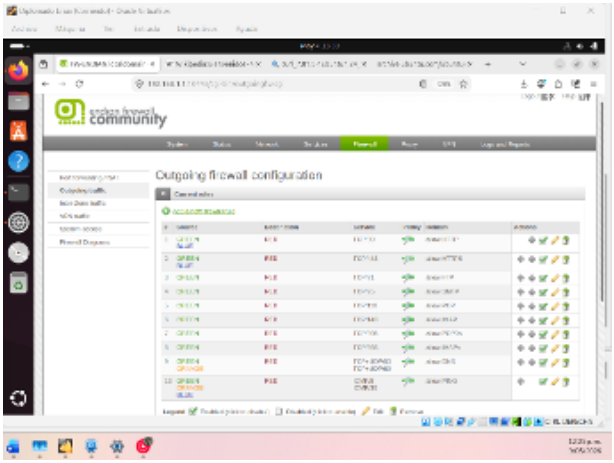
Figura 6. Configuración SNAT para las redes GREEN y ORANGE.



Fuente. Autoría propia

Se muestra la creación de las reglas SNAT para permitir que las redes GREEN y ORANGE puedan salir hacia la red externa utilizando la dirección IP de la interfaz RED del firewall. Esta configuración evita que las direcciones privadas internas sean expuestas directamente, fortaleciendo la seguridad de la LAN y de la DMZ.

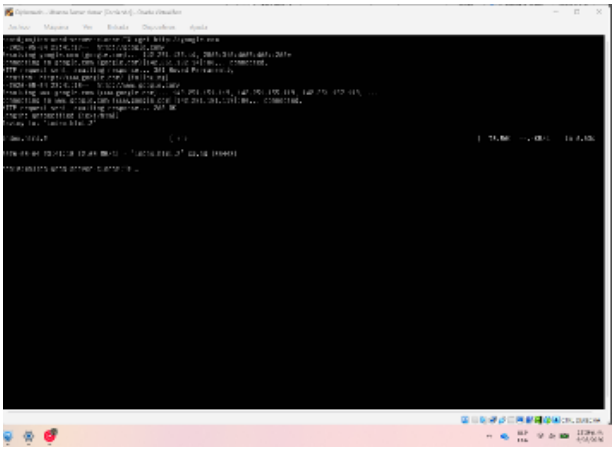
Figura 7. Tráfico saliente permitido desde GREEN y ORANGE.



Fuente. Autoría propia

Se evidencia la configuración de las reglas que autorizan el tráfico saliente desde las zonas GREEN y ORANGE hacia la red externa. Con esta validación se confirma que Endian Firewall permite la navegación o comunicación hacia Internet de manera controlada, aplicando políticas de seguridad sobre los segmentos internos.

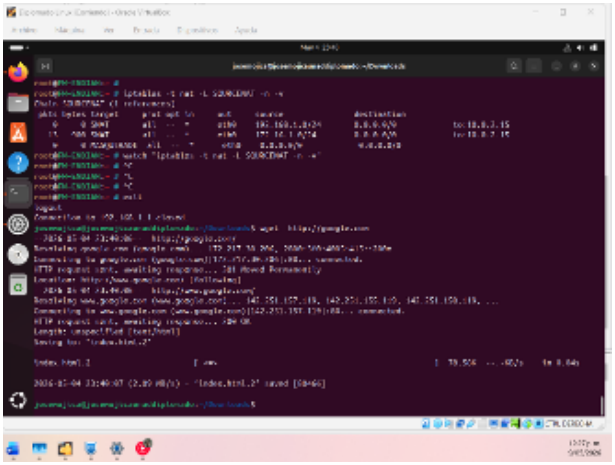
Figura 8. Prueba de conectividad hacia Internet desde la zona ORANGE.



Fuente. Autoría propia

Se realiza una prueba de conectividad desde la zona ORANGE, correspondiente a la DMZ, hacia Internet. Esta comprobación permite verificar que los servidores ubicados en la DMZ pueden comunicarse con la red externa mediante NAT, sin necesidad de exponer directamente sus direcciones IP privadas.

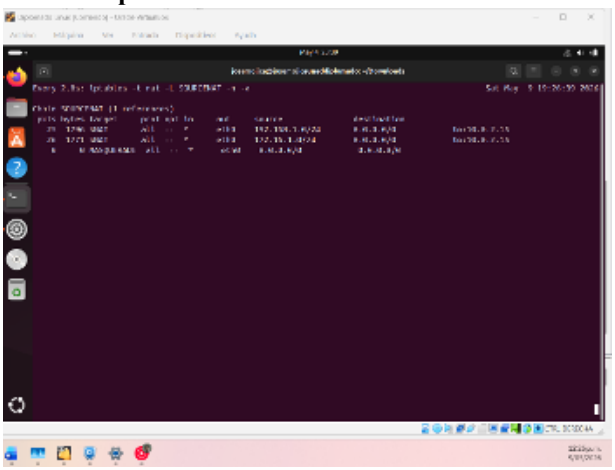
Figura 9. Prueba de conectividad hacia Internet desde la zona GREEN.



Fuente. Autoría propia

Se presenta la validación de conectividad desde la zona GREEN o red LAN hacia Internet. Esta prueba permite confirmar que los equipos internos pueden acceder a servicios externos a través del firewall, manteniendo el control del tráfico y la traducción de direcciones mediante las reglas NAT configuradas.

Figura 10. Validación de reglas NAT desde terminal mediante iptables.



Fuente. Autoría propia

Se evidencia la revisión de las reglas NAT desde la terminal utilizando comandos asociados a iptables. Esta validación permite comprobar a nivel técnico que las reglas de traducción de direcciones se encuentran activas y que el firewall está aplicando correctamente el enmascaramiento del tráfico saliente.

4.2 TEMÁTICA 4

Desarrolla: Diego Alejandro Mendez Lopez

En este trabajo se realizó la implementación de un entorno de red segmentado utilizando un firewall de tipo UTM, específicamente Endian Firewall Community. El objetivo principal fue simular una arquitectura de red empresarial basada en la separación de tráfico mediante zonas de seguridad, con el fin de controlar la comunicación entre diferentes segmentos de red.

La red se estructuró en tres zonas principales: GREEN como red interna de usuarios, ORANGE como zona desmilitarizada o DMZ donde se ubican los servicios, y RED como la conexión hacia Internet. En la zona DMZ se configuró un servidor sobre Ubuntu Server, en el cual se instaló y configuró el servicio web mediante Apache HTTP Server, permitiendo la publicación de contenido accesible bajo ciertas condiciones de seguridad.

Las direcciones a tener en cuenta respecto a las zonas serán

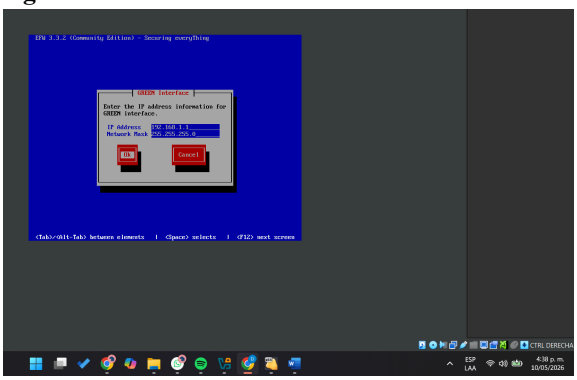
Tabla 1 zonas a implementar

Zona	IP del firewall	Red
GREEN	192.168.1.1	192.168.1.0/24
ORANGE	192.168.2.1	192.168.2.0/24
RED	DHCP	La asigna VirtualBox

Fuente. Autoría propia

en la siguiente imagen se puede observar evidencia de la instalación de Endian

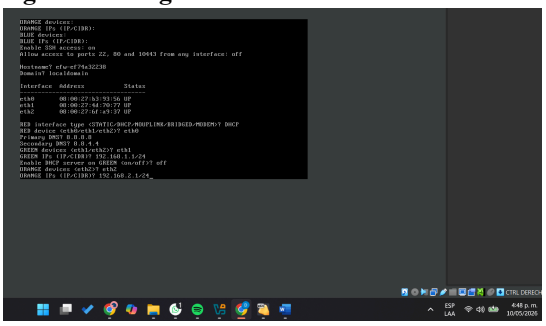
Figura 1 instalación de Endian



Fuente. Autoría propia

Luego, se debe configurar las dos zonas asignando las ips de acuerdo a lo establecido por las zonas creadas

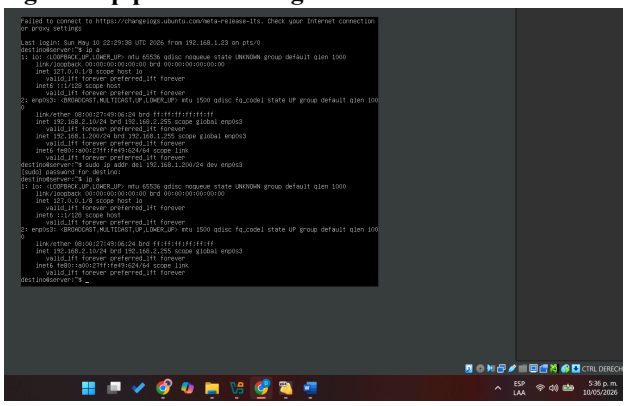
Figura 2 configuración de las zonas



Fuente. Autoría propia

Se configura la IP de Ubuntu server y se confirma que pertenece la red Orange desde la zona green se intentará conectar a esta ip para ver la página disponible

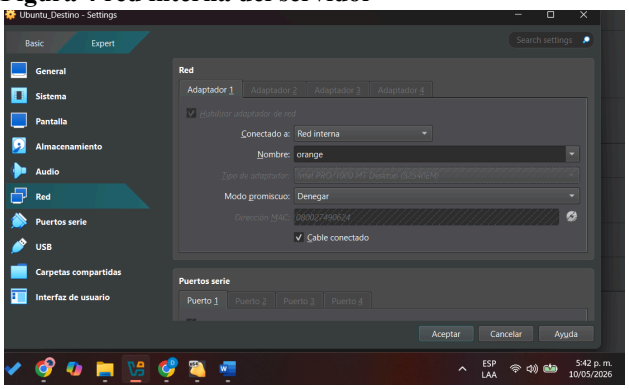
Figura 3 ip para red orange



Fuente. Autoría propia

La red interna usada para el servidor es Orange, por lo tanto se requiere asegurar que en virtual box se añada dicha red interna

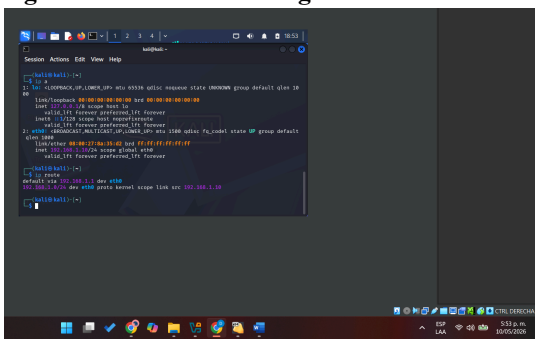
Figura 4 red interna del servidor



Fuente. Autoría propia

Ahora de manera similar se usa la red interna Green en este caso para una máquina virtual kali y se comprueba que la ruta es correcta

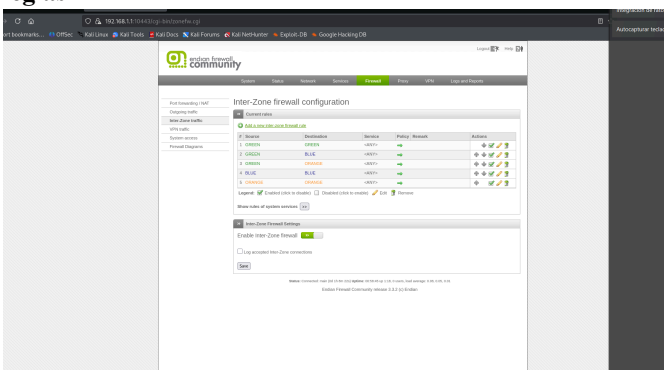
Figura 5 red interna zona green -kali linux



Fuente. Autoría propia

Se ingresa a la dirección de la MV de endian y se puede acceder a configurar el firewall para esta práctica se hace énfasis en lo correspondiente a las reglas

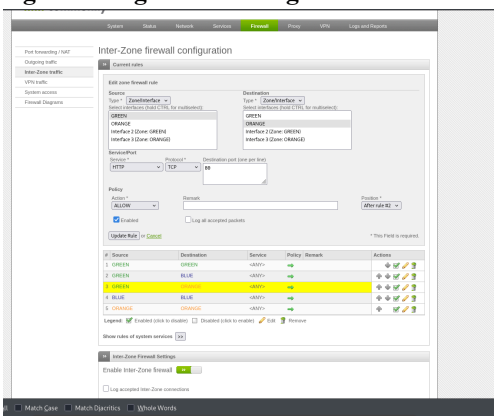
Figura 6 evidencia ingreso a la configuración de las reglas



Fuente. Autoría propia

Se crea la regla para http desde la red green hasta la Orange en el puerto 80

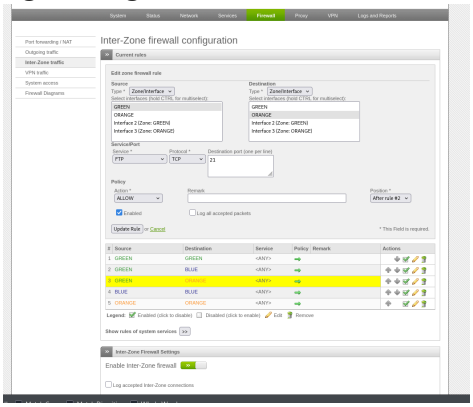
Figura 7 asignación de reglas



Fuente. Autoría propia

Se crea la regla FTP desde la zona green hasta la Orange para el protocolo TCP en el puerto 21

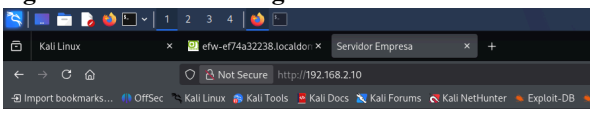
Figura 8 reglas FTP



Fuente. Autoría propia

Se demuestra el funcionamiento porque al cargar la dirección http://192.168.2.10 se puede ver el HTML configurado

Figura 9 evidencia de ingreso al HTML del server



Fuente. Autoría propia

5 CONCLUSIONES

La configuración NAT implementada en Endian permitió comprobar la salida controlada desde las zonas GREEN y ORANGE hacia la red externa. Con esta práctica se evidenció la importancia del firewall como elemento central de seguridad perimetral, ya que permite administrar el tráfico, proteger las direcciones internas y garantizar la comunicación de los servicios GNU/Linux sin exponer directamente la infraestructura de la LAN y la DMZ.

En el desarrollo de esta práctica se implementó un entorno de red segmentado mediante la utilización de Endian Firewall Community, configurando tres zonas de seguridad: GREEN (red interna), ORANGE (DMZ) y RED (Internet). Esta arquitectura permite simular un entorno empresarial real, donde se controla el tráfico entre redes mediante políticas de seguridad definidas.

Se logró la implementación de un servidor web en la zona DMZ utilizando Apache HTTP Server sobre Ubuntu Server, el cual fue accesible desde la zona GREEN mediante el protocolo HTTP, validando así la correcta comunicación inter-zona.

La creación de reglas específicas en el firewall para permitir los servicios HTTP y FTP demostró la importancia de aplicar políticas de acceso controlado entre zonas. Las pruebas realizadas desde la máquina Kali Linux confirmaron que solo el tráfico autorizado podía llegar al servidor ubicado en la DMZ, evidenciando el funcionamiento adecuado del esquema de seguridad. En conclusión, esta práctica permitió comprender cómo la segmentación de red y el uso de un firewall UTM fortalecen la protección de los servicios y reducen los riesgos de acceso no autorizado.

6 REFERENCIAS

[1] G. Obregón-Pulido, B. Castillo-Toledo and A. Loukianov, *"A globally convergent estimator for n frequencies"*, IEEE Trans. On Aut. Control. Vol. 47. No 5. pp 857-863. May 2002.

[2] H. Khalil, *"Nonlinear Systems"*, 2nd. ed., Prentice Hall, NJ, pp. 50-56, 1996.

[3] Francis. B. A. and W. M. Wonham, *"The internal model principle of control theory"*, Automatica. Vol. 12. pp. 457-465. 1976.

[4] E. H. Miller, *"A note on reflector arrays"*, IEEE Trans. Antennas Propagat., Aceptado para su publicación.

[5] *Control Toolbox* (6.0), User´s Guide, The Math Works, 2001, pp. 2-10-2-35.

[6] J. Jones. (2007, Febrero 6). Networks (2nd ed.) [En línea]. Disponible en: http://www.atm.com.

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

[8] Innova Sytrus. (2025, 21 de noviembre). Cómo configurar Endian Firewall con Ubuntu y VirtualBox [Video]. YouTube. https://www.youtube.com/watch?v=gavzDYz8FkE

[9] Camilo. (s.f.). *ENDIAN FIREWALL CONFIGURACION y ADMINISTRACION*. GreenRoot (DonJuanBlog). http://donjuanblogo.blogspot.com/2012/05/endian-firewall-configuracion-y.html

[10] *DMZ: qué es, para qué sirve y cómo configurarlo - RedUSERS*. (n.d.). RedUSERS. https://www.redusers.com/noticias/publicaciones/dmz/

[11] *¿QUE ES ENDIAN? OpenSource UTM (Gestión Unificada de Amenazas), Bogota - Colombia*. (n.d.). https://quasarbi.com/endian.html