TÍTULO “IMPLEMENTACIÓN DE FIREWALL PERIMETRAL CON ENDIAN COMMUNITY PARA LA SEGURIDAD DE REDES LAN, WAN Y DMZ “

Integrante 1 Jose Fabian Triana Acosta
e-mail: jftrianaa@unadvirtual.edu.co

RESUMEN: *La actividad se centra en una solución de seguridad perimetral con GNU/Linux Endian Firewall en una virtualización. El objetivo general consiste en proteger la infraestructura de red a través de la segmentación en zonas verde (LAN), roja (WAN) y naranja (DMZ) y en controlar adecuadamente el tráfico y la seguridad de los servicios alojados en servidores Linux. En el desarrollo se llevan a cabo tareas de (1) instalación y configuración de Endian Firewall en VirtualBox; (2) reglas NAT para comunicar las redes; (3) habilitar los servicios HTTP y FTP en la DMZ; (4) crear reglas de acceso para permitir o denegar tráfico entre zonas; (5) validar la conectividad mediante las pruebas de navegación y transferencia de archivos.*
Además, se implementa un proxy HTTP no transparente con autenticación de usuarios y políticas de filtrado web, listas negras para denegar el acceso a determinados sitios de Internet, lo que permite aplicar los conceptos básicos de seguridad informática, administración de redes y control de acceso que favorecen la práctica de un aprendizaje más significativo de la protección perimetral en el medio GNU/Linux.

PALABRAS CLAVE: DMZ, Endian Firewall, Firewall perimetral, Segmentación de redes.

INTRODUCCIÓN

La seguridad perimetral representa uno de los pilares centrales de la salvaguarda de la infraestructura tecnológica contemporánea, en especial en entornos corporativos donde se desarrollan servicios, aplicaciones Web y bases de datos emparejadas a redes tanto internas como externas. En este sentido, la puesta en marcha de métodos de control y filtrado del tráfico permite multiplicar las posibilidades de reducir el riesgo de acceso no autorizado, ataques informáticos y de las actuales vulnerabilidades que pueden amenazar la disponibilidad, la confidencialidad y la integridad de la información.

Con la realización de esta actividad se pretende crear e implementar un entorno de seguridad con GNU/Linux donde se utilice la distribución Endian Firewall Community (EFW) como plataforma de protección perimetral. De este modo se plantea implementar una correcta arquitectura de red segmentada en zonas LAN, WAN y DMZ y de este modo controlar el tráfico entre usuarios, servidores y el acceso a Internet. Se quiere también realizar configuraciones vinculadas a NAT, reglas de acceso, publicación de servicios Web y FTP, políticas de filtrado y autenticación mediante proxy HTTP.

La práctica de esta actividad fomenta las competencias en administración de redes y seguridad informática, elaborando un claro entendimiento del funcionamiento de los firewalls, segmentación de redes, traducción de direcciones, control de servicios y políticas de acceso en entornos virtualizados mediante VirtualBox y plataformas GNU.

METODOLOGÍA

Configuración de la Infraestructura Virtual

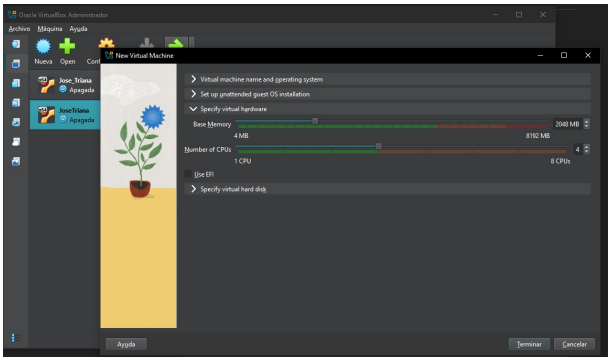
La implementación se realizó sobre Oracle VirtualBox, creando una máquina virtual para Endian Firewall con las siguientes características:

Memoria RAM: 2048 MB
Núcleos de CPU: 4
Almacenamiento: 40.67 GB
Adaptadores de red: 3 (GREEN, RED y ORANGE)

Figura 1
Creación Máquina Virtual Endian

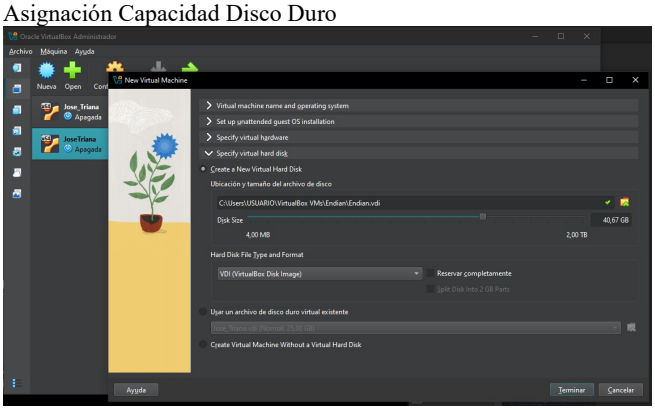
Fuente: Autoria Propia
Selección Nombre, Ubicación , ISO y version.

Figura 2
Asignacion Memoria



Fuente: Autoria Propia
Se elige memoria 2048 mb y 4 nucleos.

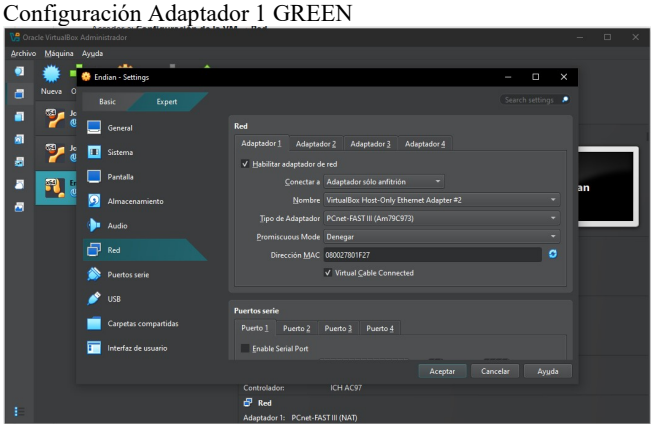
Figura 3
Asignación Capacidad Disco Duro



Fuente: Autoria Propia
Se elegie 40.67 GB de espacio en Disco Duro

En la Fig. 4 se muestra la configuración del primer adaptador, correspondiente a la zona GREEN (LAN), configurado como Adaptador solo anfitrión con dirección IP 192.168.1.1/24.

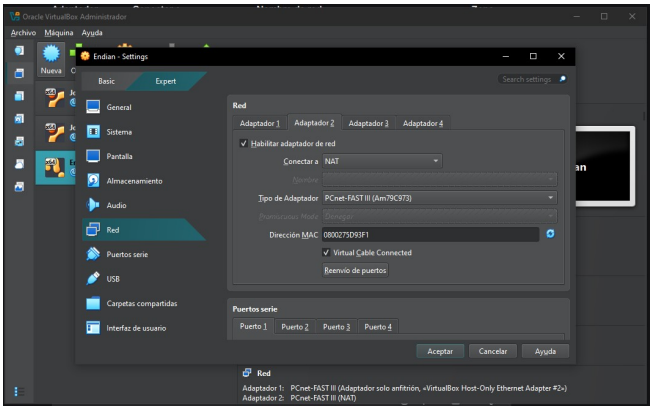
Figura 4
Configuración Adaptador 1 GREEN



Fuente: Autoria Propia

De acuerdo con la Fig. 5, el segundo adaptador correspondiente a la zona RED (WAN) se configuró en modo NAT para permitir la salida a Internet mediante DHCP.

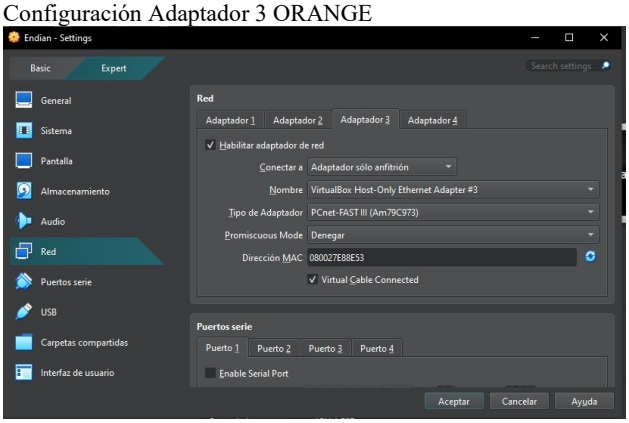
Figura 5
Configuracion Adaptador 2 RED



Fuente: Autoria Propia

La Fig. 6 presenta la configuración del tercer adaptador para la zona ORANGE (DMZ), configurado como Adaptador solo anfitrión con dirección IP 172.16.1.1/24.

Figura 6
Configuración Adaptador 3 ORANGE

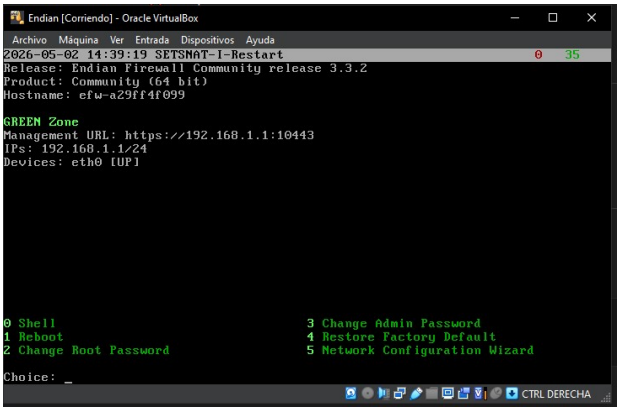


Fuente: Autoria Propia

Instalación y Configuración de Endian Firewall

La instalación de Endian Firewall Community se realizó siguiendo el asistente gráfico. Al finalizar la instalación, se verificó que las zonas GREEN, RED y ORANGE estuvieran correctamente configuradas.

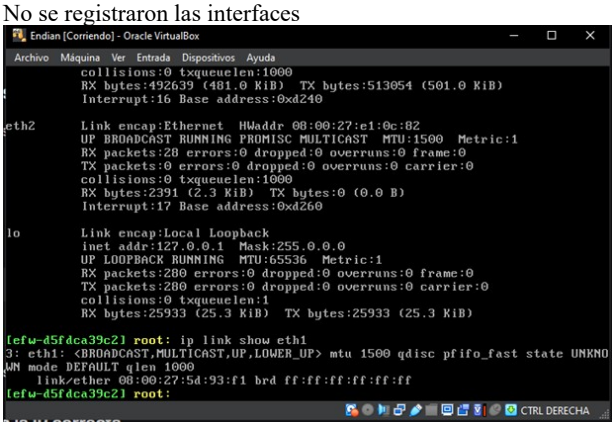
Figura 7
Instalación Endian



Fuente: Autoria Propia

Como se evidencia en la Fig. 8, inicialmente las zonas ORANGE y RED no aparecían configuradas, por lo que fue necesario realizar una configuración manual de las interfaces.

Figura 8
No se registraron las interfaces



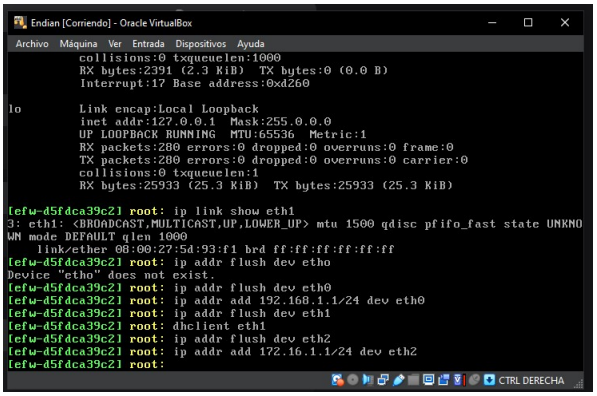
Fuente: Autoria Propia

Configuración Manual de Interfaces en Endian

Mediante el shell de Endian, se procedió a configurar manualmente las interfaces de red con los siguientes comandos:

ip addr add 192.168.1.1/24 dev eth0
ip addr add 172.16.1.1/24 dev eth2
dhclient eth1
ip route add default dev eth1

Figura 9
Se configuran de manera manual las interfaces



Fuente: Autoria Propia

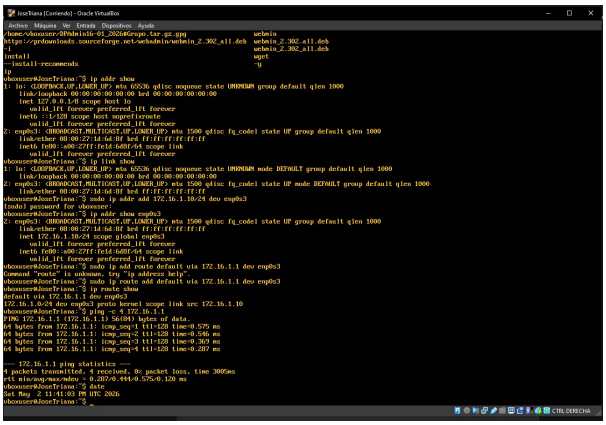
Configuración del Servidor en Zona DMZ

Para el servidor ubicado en la zona DMZ, se asignó la dirección IP 172.16.1.10/24 sobre la interfaz enp0s3. Se ejecutaron los siguientes comandos:

sudo ip addr add 172.16.1.10/24 dev enp0s3
sudo ip route add default via 172.16.1.1 dev enp0s3

La Fig. 10 muestra la verificación de conectividad mediante el comando ping -c 4 172.16.1.1, confirmando la comunicación con el firewall.

Figura 10
Configuracion IP Server



Fuente: Autoria Propia

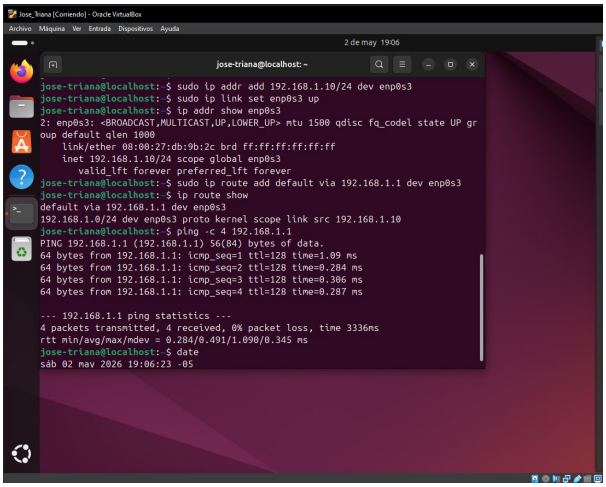
Configuración del Cliente en Zona GREEN

Para el equipo cliente en la zona GREEN (LAN), se asignó la dirección IP 192.168.1.10/24 sobre la interfaz enp0s3:

sudo ip addr add 192.168.1.10/24 dev enp0s3
sudo ip route add default via 192.168.1.1 dev enp0s3

La Fig. 11 muestra la prueba de conectividad exitosa mediante ping -c 4 192.168.1.1.

Figura 11
Configuracion Interfaz Desktop



Fuente: Autoria Propia

CONCLUSIONES

La instalación e implementación del sistema GNU/Linux Endian Firewall en el entorno virtual VirtualBox tuvo como resultado la creación de una infraestructura base de seguridad de perímetro al generar la segmentación de la red mediante las zonas verde (LAN), roja (WAN) y naranja (DMZ), y fue realmente didáctica para la comprensión de la importancia de que se debe realizar una buena asignación de interfaces de red y los direccionamientos IP para garantizar que se mantenga el orden y la seguridad entre las diferentes zonas.

También se vio soporte en el fortalecimiento de habilidades en virtualización, administración de sistemas GNU/Linux, configuración inicial de firewalls impactando claramente en cómo una correcta implantación de Endian Firewall ayuda a mejorar la protección de los servicios y recursos de red y su acceso no autorizado. Por último, la temática propició el entendimiento de la importancia de la segmentación de redes como base para la seguridad de la informática en las empresas.

REFERENCIAS

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

[2] Linux Professional Institute. (2022). LPIC-1 Exam 101 – Tema 101: Determinar y configurar los ajustes de hardware. LPI. https://learning.lpi.org/es/learning-materials/101-500/101/101.1/

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

[4] Canonical. (2023). Guía del Ubuntu desktop 20.04 LTS. Help Ubuntu. https://help.ubuntu.com/

[5] Debian. (2023). El manual del administrador de Debian 12.5.0. Debian. https://www.debian.org/releases/stable/amd64/index.es.html