Implementación de Seguridad en GNU/Linux con instalación de firewall Linux Endian y pruebas en Linux Mint y Ubuntu Server bajo máquinas virtuales en Virtual Box
Temática 3: Permitir servicios de la Zona DMZ para la red.

Autor, *Fabián Figueroa Flórez, email: ffigueroaf@unadvirtual.edu.co*

Resumen **— Este artículo documenta el proceso de implementación y configuración de un Firewall GNU/Linux Endian como elemento de seguridad perimetral, utilizando Oracle VirtualBox. La arquitectura de red fue diseñada bajo el esquema de tres zonas de seguridad (Verde, Naranja y Roja), emulando un entorno corporativo de LAN, DMZ y WAN. Se detallan los pasos para la asignación de interfaces de red virtuales (Network Interfaces Cards - NIC) para cada zona. El resultado principal de esta implementación se enfoca en la aplicación de políticas de seguridad Inter-Zona mediante reglas explícitas: se habilitó el acceso a los servicios HTTP (Puerto 80) y FTP (Puerto 21) desde la Red Interna (Zona Verde) hacia el Servidor de Servicios (Zona Naranja), y se implementó la denegación total del protocolo ICMP (Ping) para garantizar el ocultamiento de la infraestructura de red. Este ejercicio valida la comprensión práctica de la segmentación de red y la gestión básica de políticas de firewall.**

PALABRAS CLAVE: Linux, Endian, DMZ, Firewall, LAN, NAT, Red, Segmentación, Seguridad, WAN, Zonas.

I. INTRODUCCIÓN

La seguridad de la información en entornos de red es crucial, y el uso de firewalls de inspección de estado es la primera línea de defensa. Este proyecto se centra en la implementación del software de firewall GNU/Linux Endian, elegido por su robustez y su facilidad para gestionar arquitecturas de múltiples zonas. El objetivo primordial fue establecer un entorno de red segmentado para separar la Red de Área Local (Zona Verde) de los Servidores Públicos (Zona Naranja o DMZ) y el acceso externo (Zona Roja o WAN). La implementación se realizó sobre un entorno de virtualización, utilizando Oracle VirtualBox para simular la conectividad física de cada interfaz de red. Los objetivos específicos se centraron en la gestión de políticas de acceso, permitiendo servicios esenciales (HTTP y FTP) y, simultáneamente, fortaleciendo la seguridad mediante la prohibición del tráfico de diagnóstico (ICMP), práctica fundamental en la ingeniería de sistemas para mitigar ataques de reconocimiento. documento

Fig. 1. Logo de Endian Firewall, Fuente: Wikipedia.

RESULTADOS Y CONFIGURACIÓN DETALLADA (SECCIONES DEL ARTÍCULO)

II. METODOLOGÍA Y CONFIGURACIÓN DE ZONAS

EL ENTORNO VIRTUAL CONSTA DE TRES MÁQUINAS VIRTUALES LINUX: ENDIAN FIREWALL, UN SERVIDOR UBUNTU SERVER Y UN CLIENTE LINUX MINT. LA INTERCONEXIÓN SE LOGRÓ MEDIANTE LA ASIGNACIÓN DE TRES ADAPTADORES DE RED AL ENDIAN, CADA UNO ASOCIADO A UN SEGMENTO DE RED VIRTUAL DISTINTO EN VIRTUALBOX, TAL COMO SE MUESTRA EN LAS SIGUIENTES FIGURAS

1. Evidencia de las 3 instalaciones de las distros Linux en mi Oracle Virtual Box

La Figura 2 muestra la vista de las tres máquinas virtuales esenciales para la implementación: Endian Firewall, Ubuntu Server (DMZ) y Linux Mint (Cliente LAN), todas operando sobre VirtualBox para emular el entorno de tres zonas.

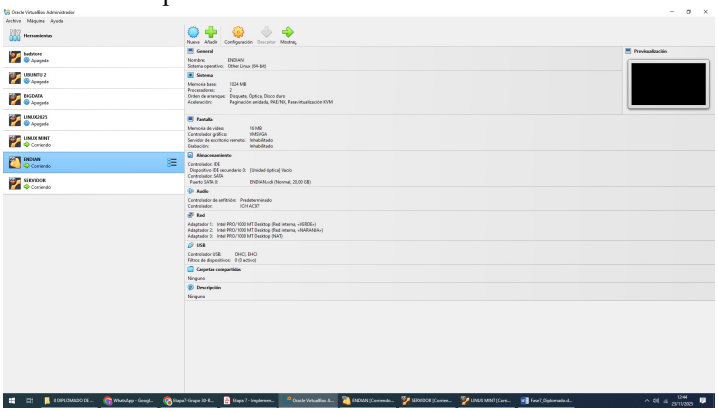

Fig. 2. Autoría Propia.

2. Evidencia de los 3 accesos por máquina virtual a las 3 distros

Se confirma el correcto funcionamiento y accesibilidad a las consolas de cada una de las distribuciones instaladas, verificando la carga efectiva del sistema operativo en el entorno virtual.

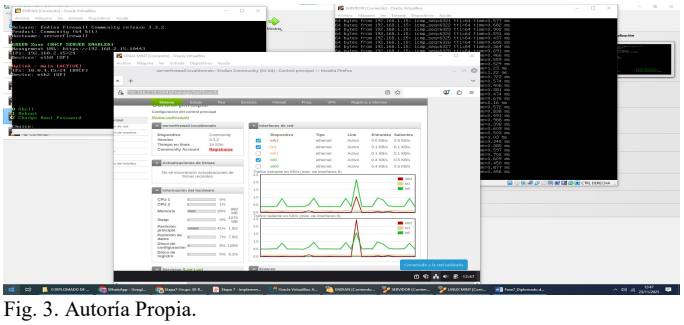

Fig. 3. Autoría Propia.

3. Evidencia de acceso por ambiente web a la configuración del Endian

El acceso a la consola de administración se realiza a través del protocolo HTTPS y el puerto no estándar 10443 (ej. https://192.168.2.15:10443/), accediendo desde el cliente Linux Mint (Zona Verde) hacia la interfaz de gestión del Firewall.

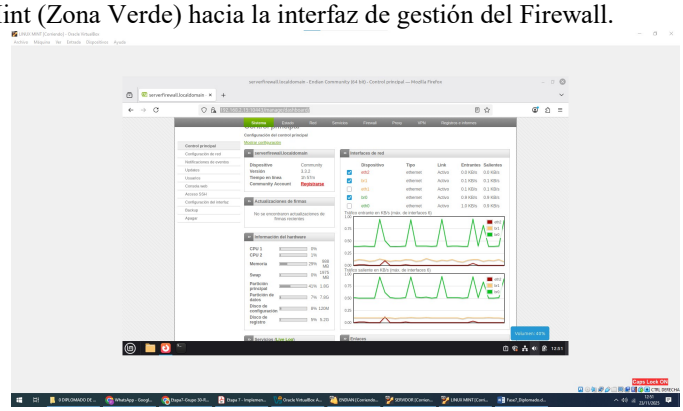

Fig. 4. Autoría Propia.

III. Pruebas Iniciales de Conectividad (ICMP)

Antes de aplicar cualquier política de denegación, se verifica el estado de la conectividad por defecto entre las zonas mediante el protocolo ICMP (Ping).

4. Respuesta de ping zona verde desde el Linux Mint

Se realiza una prueba de ping desde el cliente (Zona Verde) hacia la IP del servidor Ubuntu (Zona Naranja). La respuesta exitosa indica que, por defecto, el tráfico ICMP es permitido por las políticas predeterminadas del firewall en esta dirección.

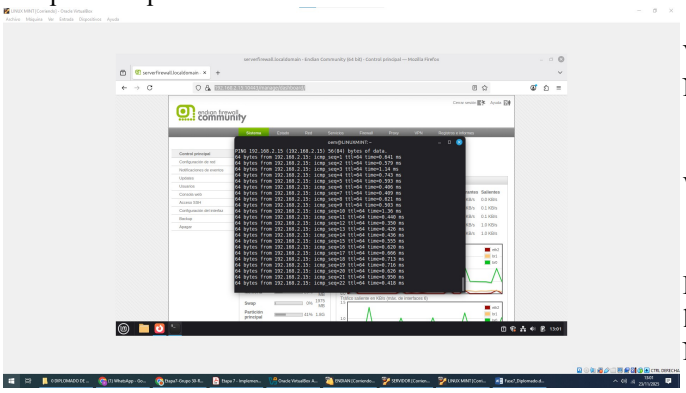

Fig. 5. Autoría Propia.

5. Respuesta de ping zona naranja desde el servidor Ubuntu

De manera recíproca, se verifica la conectividad desde el servidor (Zona Naranja) hacia la IP del cliente (Zona Verde), confirmando que el tráfico ICMP fluye libremente en ambas direcciones antes de aplicar las reglas restrictivas.

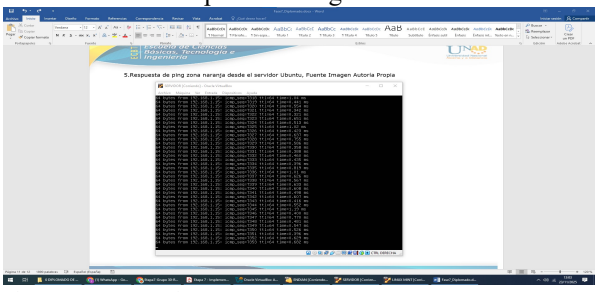

Fig. 6. Autoría Propia.

6. Configuración por consola del firewall Endian

Se accede a la consola del Endian para confirmar la configuración de red de las interfaces (Green: 192.168.2.15, Orange: 192.168.1.15, Red: DHCP), paso previo a la administración de reglas por interfaz web.

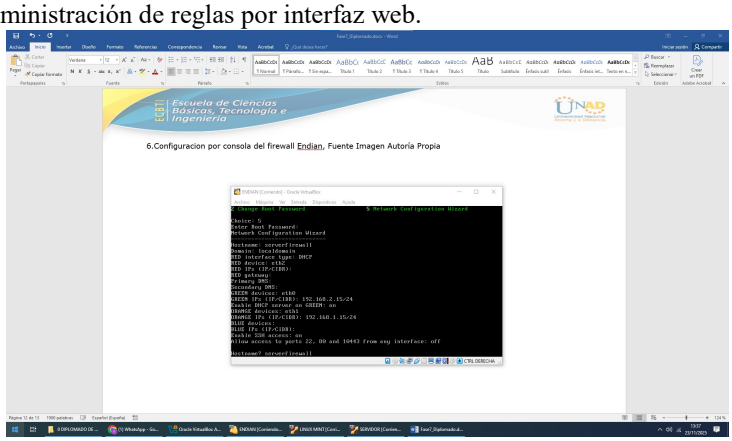

Fig. 7. Autoría Propia.

IV. Aplicación de Políticas de Acceso Inter-Zona

Las siguientes subsecciones detallan la creación de reglas de tipo Inter-Zone Policy dentro del panel de administración web del Endian. La metodología implica la creación de reglas específicas de ALLOW (Permitir) y DENY (Denegar), respetando el principio de orden de procesamiento (las reglas más específicas deben ir primero).

A. Habilitación de Servicios (HTTP y FTP)

El tráfico de servicio debe ser permitido desde la Zona Verde (LAN) hacia el servidor con IP 192.168.1.20 en la Zona Naranja (DMZ).

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

Se crea la primera regla de tipo ALLOW especificando el Protocolo TCP y el Puerto de Destino 80 (HTTP). El Origen es la Zona Verde y el Destino es la IP del servidor en la Zona Naranja.

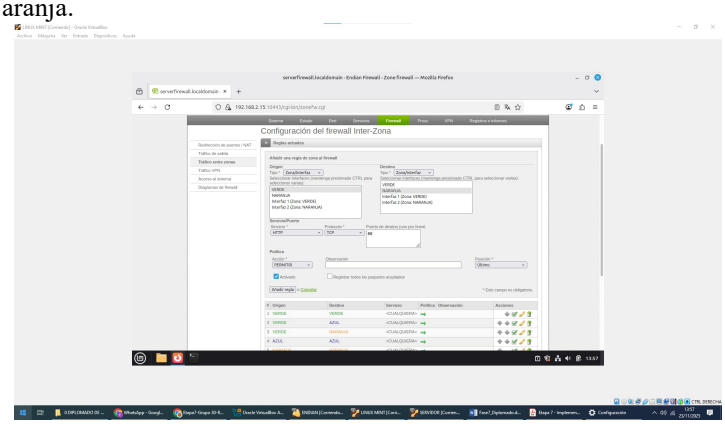

Fig. 8. Autoría Propia.

8. Regla del firewall modificada

Se visualiza la regla creada en la lista de políticas, pendiente de aplicación, asegurando que se cumplan los parámetros definidos.

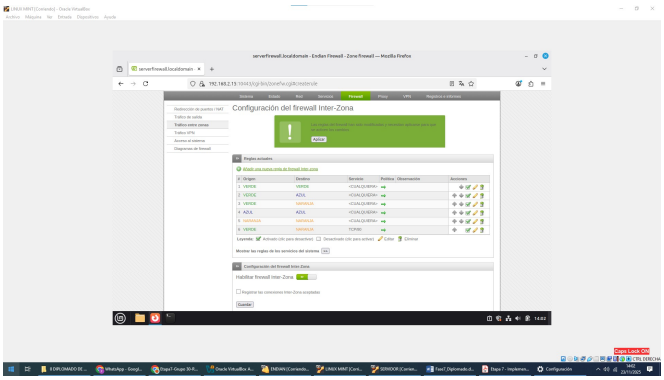

Fig. 9. Autoría Propia.

9. Regla del firewall aplicada satisfactoriamente

Se confirma la aplicación y activación de la regla en el daemon del firewall, haciendo que el tráfico HTTP desde la LAN hacia el DMZ sea permitido.

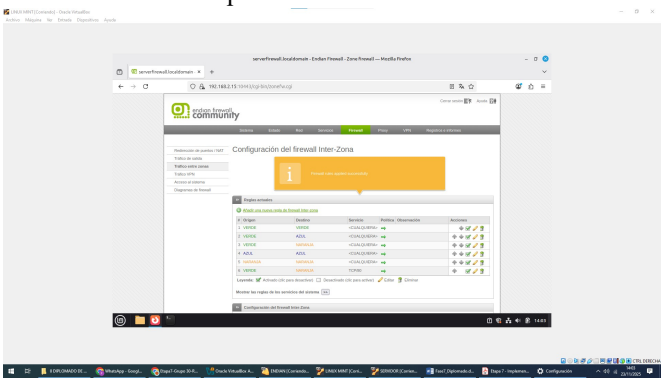

Fig. 10. Autoría Propia.

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

Siguiendo el mismo procedimiento, se crea una regla idéntica, cambiando únicamente el Puerto de Destino a 21 para habilitar el acceso al servicio FTP.

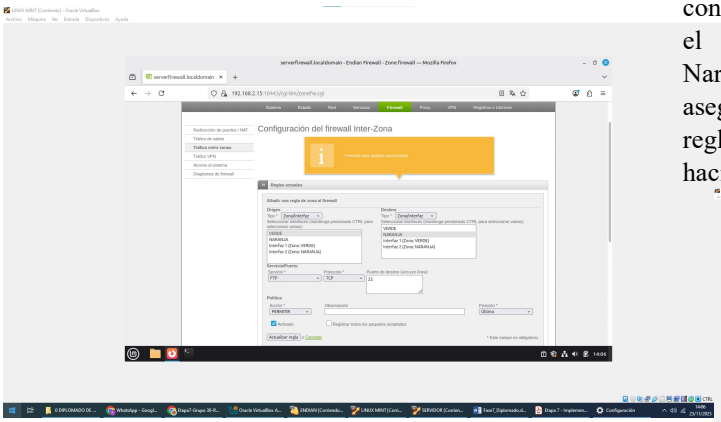

Fig. 11. Autoría Propia.

11. Regla del firewall modificada

Visualización de la nueva regla de ALLOW para FTP en la tabla de políticas.

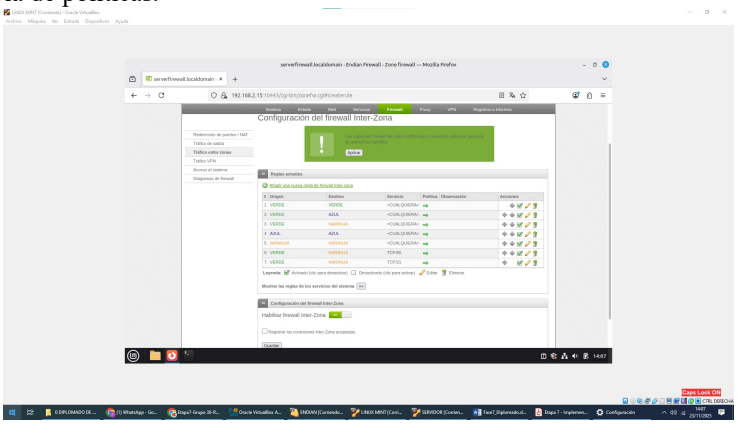

Fig. 12. Autoría Propia.

12. Regla del firewall aplicada satisfactoriamente

Confirmación de la aplicación exitosa de la regla FTP, garantizando el acceso a ambos servicios desde la Zona Verde.

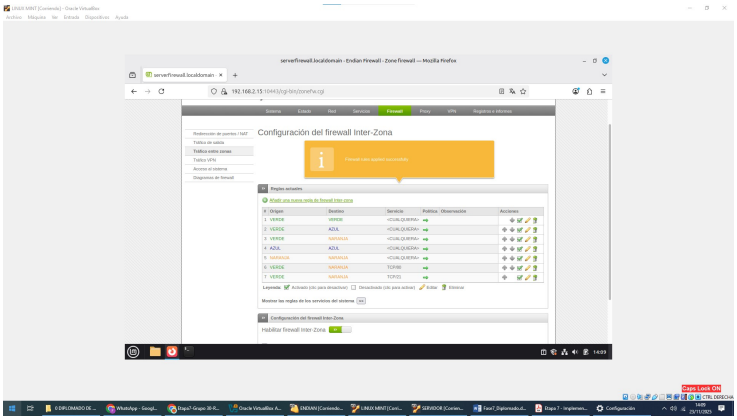

Fig. 13. Autoría Propia.

B. Denegación del Protocolo de Diagnóstico (ICMP)

Para mitigar la huella de red (fingerprinting) y los ataques de reconocimiento, se implementa una política explícita de denegación de ICMP, la cual debe estar ubicada antes de cualquier regla general de permiso.

13. Denegar el protocolo ICMP (Puerto 8 y 30) para no permitir hacer ping en la redSe crea una regla de tipo DENY con el Protocolo ICMP. Esta regla se configura para bloquear el tráfico en ambas direcciones (Verde $\leftrightarrow$ Naranja) y se posiciona en las primeras líneas de la tabla para asegurar su prioridad. El resultado esperado, tras aplicar la regla, es la falla total del comando ping desde el Linux Mint hacia el servidor Ubuntu, probando la efectividad del bloqueo.

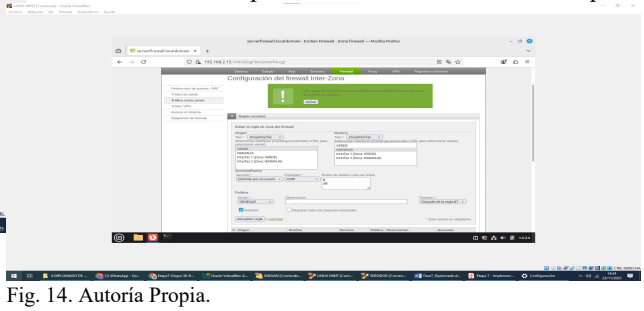

Fig. 14. Autoría Propia.

14. Evidencia final de las 3 reglas creadas

Se presenta la tabla final de políticas, destacando las tres reglas implementadas: las dos reglas de ALLOW (HTTP y FTP) y la regla prioritaria de DENY (ICMP), verificando su orden y activación satisfactoria.

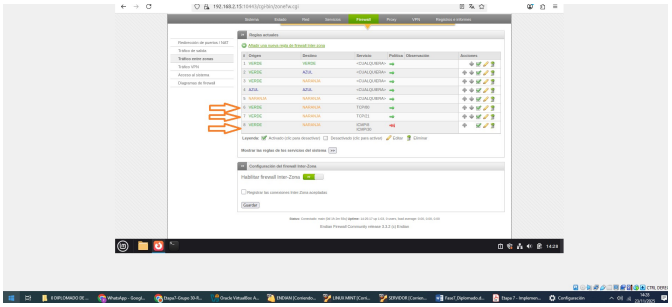

Fig. 15. Autoría Propia.

4. Conclusiones

La implementación del firewall GNU/Linux Endian en VirtualBox demostró la capacidad para segmentar una red en zonas de seguridad críticas (LAN, DMZ, WAN). El ejercicio de configuración de políticas de acceso confirmó un principio fundamental en la seguridad de redes: el orden de las reglas es determinante para la efectividad del firewall. La aplicación exitosa de las reglas para permitir el tráfico HTTP (80) y FTP (21) valida la capacidad de controlar el acceso a servicios específicos en la DMZ. Más importante aún, la denegación explícita del protocolo ICMP (Ping), priorizando las reglas de DENY sobre cualquier política de ALLOW predeterminada, cumple con el objetivo de ocultar la infraestructura, fortaleciendo la postura de seguridad de la red implementada. Este proyecto establece una base sólida para futuros estudios sobre NAT, VPN y sistemas de detección de intrusiones (IDS/IPS) dentro del entorno Endian.

RECONOCIMIENTOS

Al señor tutor, Ingeniero Iván Guillermo Duarte Pacheco, por su dedicación, apoyo y esfuerzo con todos los alumnos, esforzándonos a la excelencia académica en este diplomado, DIOS le continúe bendiciendo con sabiduría y entendimiento.

REFERENCIAS

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

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

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

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

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