Configuración de Seguridad Perimetral y Reglas NAT en Endian Firewall UTM

Luis Miguel Huertas Montaña
lmhuertasm@unadvirtual.edu.co

RESUMEN: *Este documento detalla la implementación técnica de la Temática 2: Configuración NAT. Se presenta el despliegue de un Firewall Endian en un entorno virtualizado para segmentar redes LAN y DMZ. Se validan las reglas de traducción de direcciones (SNAT y DNAT) y se reporta la auditoría de servicios web en servidores GNU/Linux. Los resultados confirman una infraestructura blindada que permite el acceso controlado a internet y la publicación segura de servicios.*

PALABRAS CLAVE: NAT, Endian Firewall, DMZ, Seguridad Perimetral, Apache2, GNU/Linux.

I. INTRODUCCIÓN

La protección de infraestructuras críticas requiere la implementación de firewalls que realicen traducción de direcciones de red (NAT). Este procedimiento permite enmascarar las direcciones privadas de una organización bajo una única IP pública, reduciendo la exposición directa ante posibles ataques desde la WAN.

II. DISEÑO DE LA INFRAESTRUCTURA

Se configuraron tres nodos en VirtualBox. El nodo central (Endian) gestiona tres interfaces lógicas asignadas a adaptadores físicos:

- Red (WAN): Adaptador Puente.
- Green (LAN): Red Interna.
- Orange (DMZ): Red Interna.

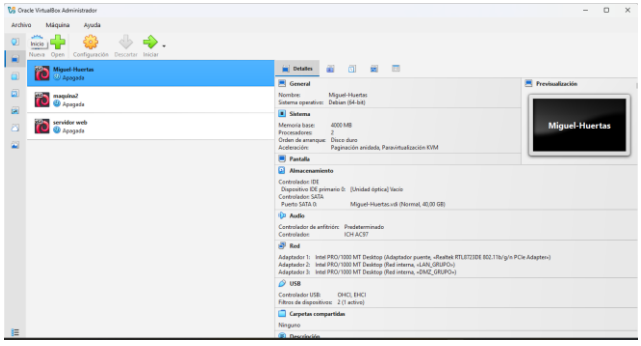

Fig. 1. Segmentación de interfaces físicas en el hipervisor.

III. CONFIGURACIÓN NAT (TEMÁTICA 2)

A. NAT de LAN a WAN

Se activó la regla de salida para la zona Green. Esto permite que el cliente interno acceda a recursos externos. La validación se realizó mediante la resolución de nombres y latencia de red.

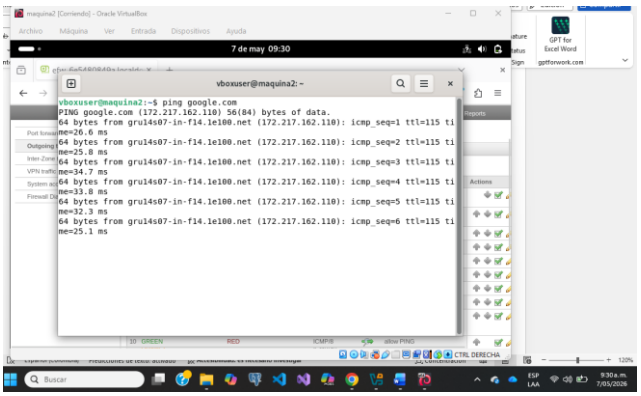

Fig. 2. Validación de conectividad mediante ICMP.

B. Configuración de la DMZ

Para el servidor en la zona Orange, se configuró la IP 192.168.20.1 como gateway. Se aplicaron reglas de tráfico saliente para permitir la instalación de paquetes.

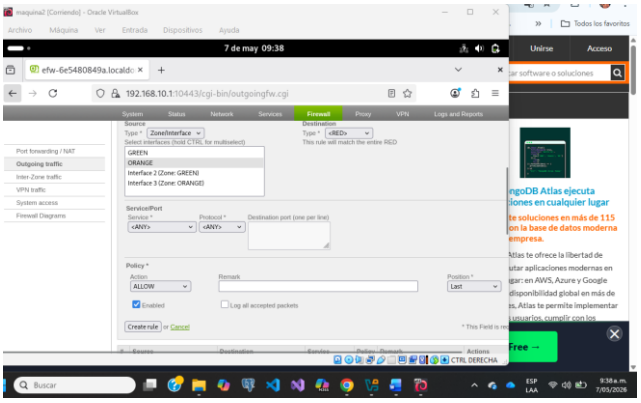

Fig. 3. Creación de reglas de reenvío de puertos (Port Forwarding).

IV. AUDITORÍA DE SERVICIOS

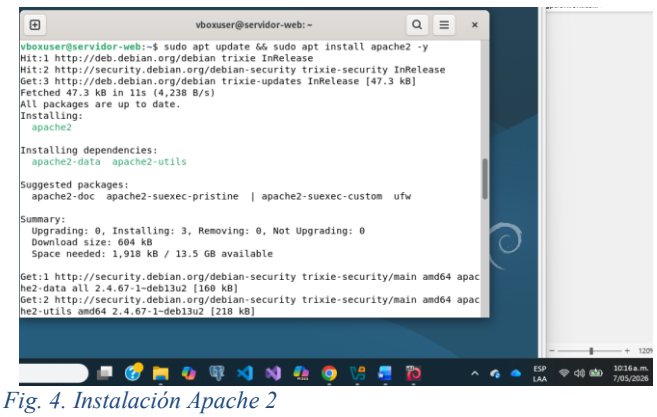

Fig. 4. Instalación Apache 2

En el servidor DMZ se instaló Apache2. Siguiendo el protocolo de la actividad, se verificó su estado integrando el comando date para certificar la vigencia de la prueba.

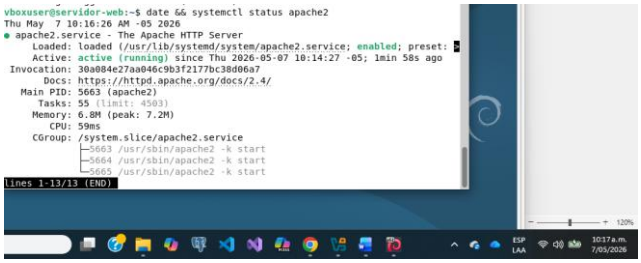

Fig. 5. Evidencia de servicio activo y marcas de tiempo de auditoría.

V. CONCLUSIONES

La implementación de Endian Firewall garantiza un control granular sobre el flujo de datos. La segmentación DMZ asegura que, en caso de compromiso del servidor web, la red LAN permanezca aislada y segura.

REFERENCIAS

[1] UNAD, "Guía de actividades - Seguridad Perimetral," 2026.
[2] Endian UTM Manual, "Network Configuration Guide," 2023.
[3] IEEE Editorial Style Manual, 2024.
[4] Endian UTM 3.3 Community, "Reference Manual for Security Administrators," 2024.
[5] UNAD, "Guía de Actividades Etapa 7: Implementando Seguridad en GNU/Linux," 2026.
[6] IEEE Editorial Style Manual for Authors, IEEE Periodicals, 2023.