CONFIGURACIÓN Y VERIFICACIÓN DEL MECANISMO NAT EN ENDIAN FIREWALL PARA LA COMUNICACIÓN ENTRE LAN, DMZ Y WAN

Andrés Felipe Ortiz Lozano
e-mail: afortizlo@unadvirtual.edu.co

RESUMEN: *Este artículo presenta el desarrollo de la Temática 2 correspondiente a la Etapa 7 del Diplomado en Sistemas Operativos. El trabajo se centró en la verificación del funcionamiento del mecanismo de traducción de direcciones (NAT) dentro del firewall Endian, con el propósito de permitir la salida a la WAN desde dos segmentos internos: la zona LAN y la zona DMZ. Para ello se realizaron pruebas de conectividad, revisión de interfaces de red y confirmación de las reglas internas de enmascaramiento mediante comandos de consola. Los resultados obtenidos demostraron que Endian gestiona adecuadamente el tráfico entre zonas, garantizando seguridad perimetral y control del flujo de datos. El proceso permitió evidenciar de forma práctica el funcionamiento del NAT dentro de un entorno real de firewall.*

PALABRAS CLAVE: Endian Firewall, NAT, LAN, DMZ, Seguridad perimetral.

1 INTRODUCCIÓN

El presente artículo expone el trabajo individual desarrollado en la Temática 2, cuyo propósito fue validar el funcionamiento del mecanismo NAT en Endian Firewall. La actividad consistió en verificar la comunicación desde dos segmentos de red internos —la zona verde (LAN) y la zona naranja (DMZ)— hacia la zona roja (WAN), confirmando que el firewall realiza el enmascaramiento necesario para permitir el acceso externo de forma segura.

Para ello se emplearon dos máquinas virtuales adicionales: un equipo con Debian Desktop conectado a la LAN y un servidor Ubuntu conectado a la DMZ. Mediante pruebas de red, comandos de verificación y análisis de las reglas establecidas dentro del firewall, fue posible identificar el comportamiento del sistema y comprobar su correcta operación. Esta temática permitió comprender de manera práctica la importancia del NAT dentro de la seguridad perimetral y su papel en el tránsito de información entre redes internas y externas.

2 DESARROLLO DE LA TEMÁTICA 2

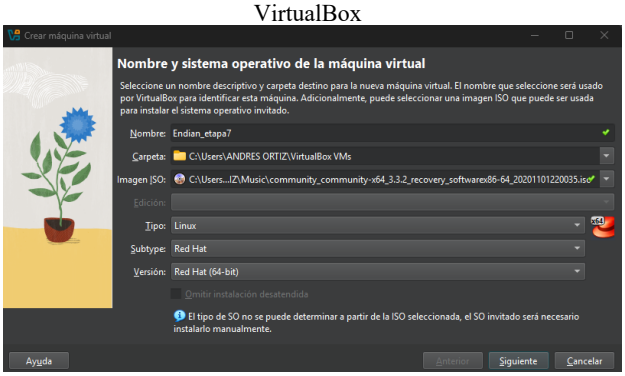
2.1 TEMATICA 2: CONFIGURACIÓN NAT

Instalación y configuración de Endian Firewall en GNU/Linux lo cual es una solución de seguridad todo en uno que se instala como sistema operativo dedicado, ofreciendo una plataforma robusta basada en GNU/Linux para la gestión unificada de amenazas.

Figura 1. Página de Descarga de Endian Firewall Community

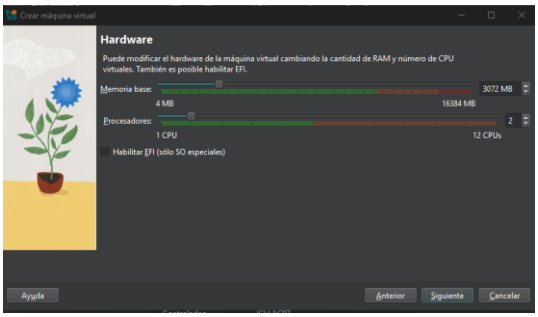
Nota. Captura de pantalla del proceso de descarga desde el sitio oficial. Fuente: Elaboración propia

Figura 2. Configuración Inicial de Máquina Virtual en Oracle VirtualBox



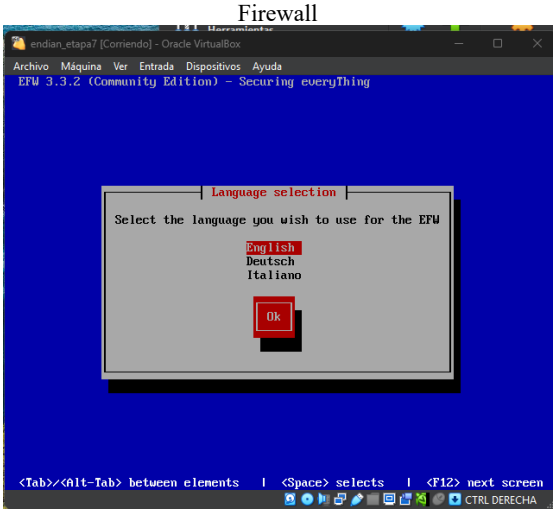
Fuente: Elaboración Propia

Figura 3. Configuración de recursos de hardware en VirtualBox



Fuente: Elaboración Propia

Figura 4. Pantalla de Inicio y Selección de Idioma en Endian Firewall

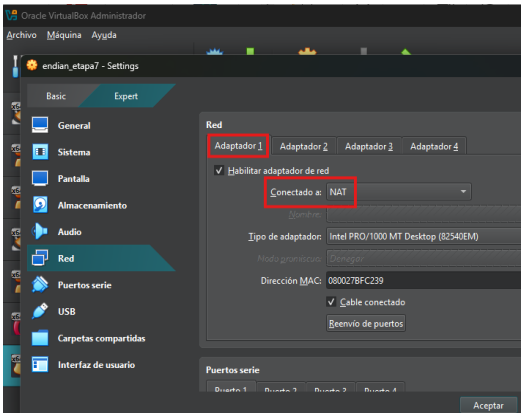


Fuente: Elaboración Propia.

Figura 5. Configuración de Dirección IP Estática

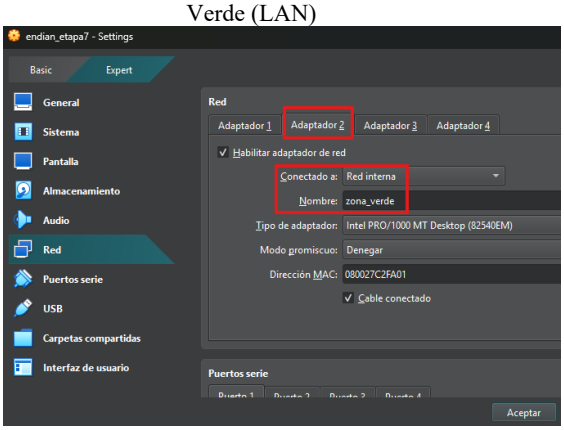
Nota. Asignación de dirección IP y máscara de red durante la instalación. Fuente: Elaboración propia

Figura 6. Configuración del Adaptador de Red NAT en VirtualBox



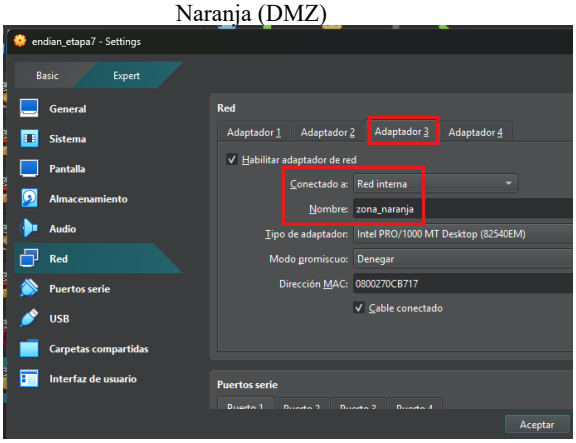
Fuente: Elaboración Propia

Figura 7. Configuración del Adaptador de Red para Zona Verde (LAN)



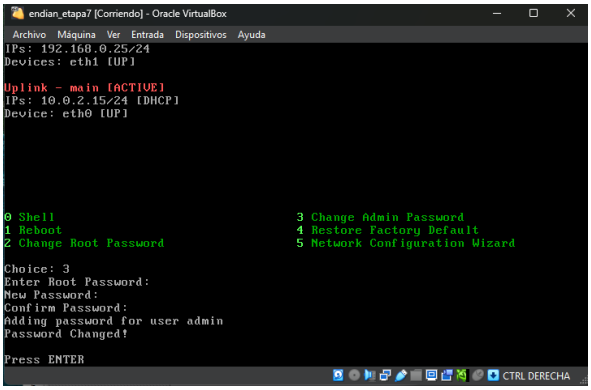
Fuente: Elaboración Propia

Figura 8. Configuración del Adaptador de Red para Zona Naranja (DMZ)



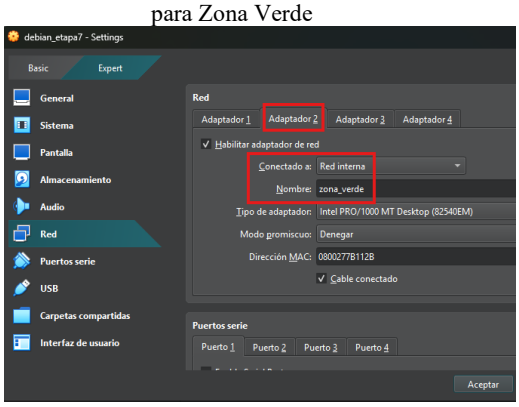
Fuente: Elaboración Propia

Figura 9. Cambio de Contraseña del Usuario Root en Endian Firewall



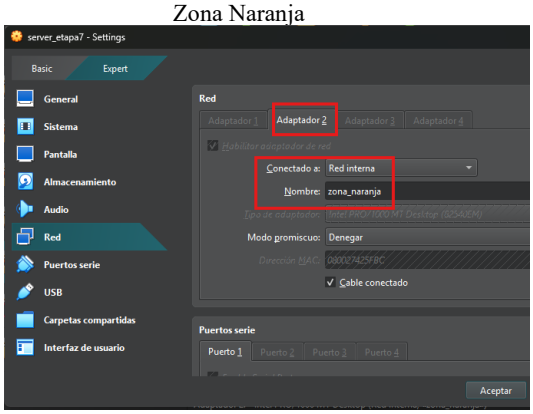
Nota. Proceso de modificación de credenciales de administrador. Fuente: Elaboración propia.

Figura 10. Configuración de Red en Debian Desktop para Zona Verde



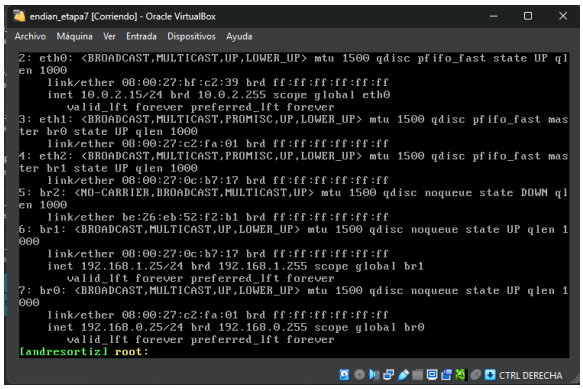
Fuente: Elaboración Propia

Figura 11. Configuración de Red en Ubuntu Server para Zona Naranja



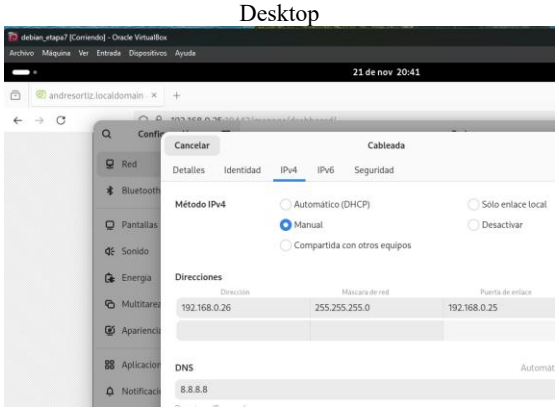
Fuente: Elaboración Propia

Figura 12. Resumen de la configuración de Interfaces de Red en Endian Firewall



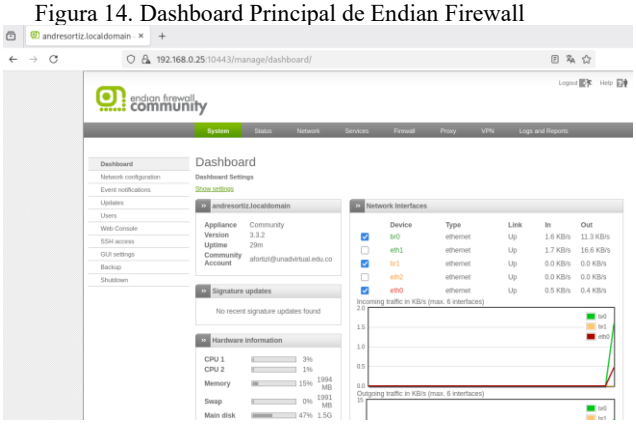
Nota. Asignación de puertos de red a zonas de seguridad específicas. Fuente: Elaboración Propia

Figura 13. Configuración de IP Estática en Debian Desktop



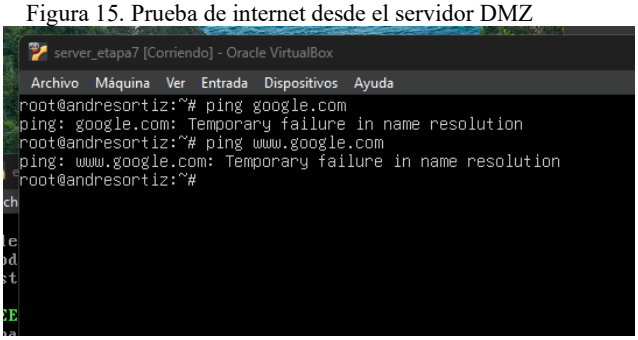
Nota. Asignación manual de dirección IP en el cliente Debian. Fuente: Elaboración Propia

Figura 14. Dashboard Principal de Endian Firewall



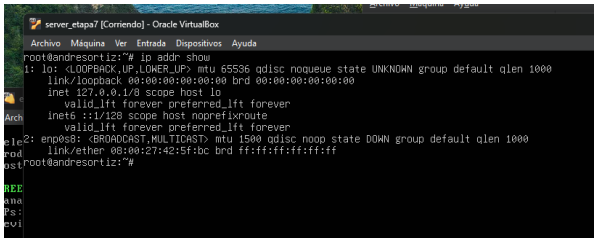
Nota. Interfaz principal administrativa después del inicio de sesión. Fuente: Elaboración Propia

Figura 15. Prueba de internet desde el servidor DMZ



Nota. Asignación manual de dirección IP en el servidor Ubuntu. Fuente: Elaboración Propia

Figura 16. Verificación de Configuración de Red con ip addr show

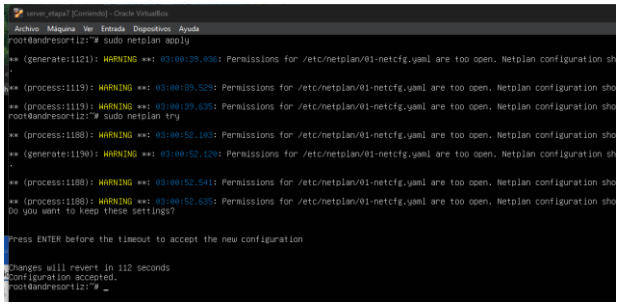


Fuente: Elaboración Propia

Figura 17. Edición de Configuración de Red en Netplan

Nota. Modificación del archivo de configuración de red en Ubuntu Server. Fuente: Elaboración Propia

Figura 18. Aplicación de Cambios de Configuración de Red



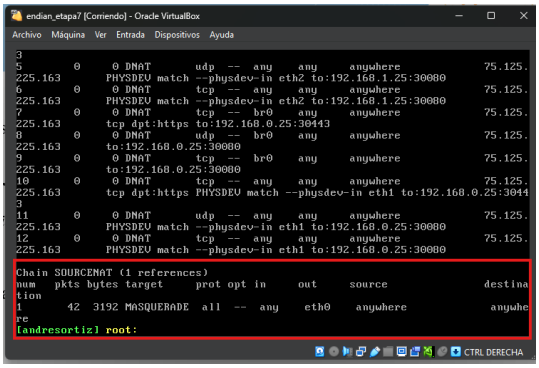
Fuente: Elaboración Propia

Figura 19. Monitoreo de Actividad en Zonas de Red

Fuente: Elaboración Propia

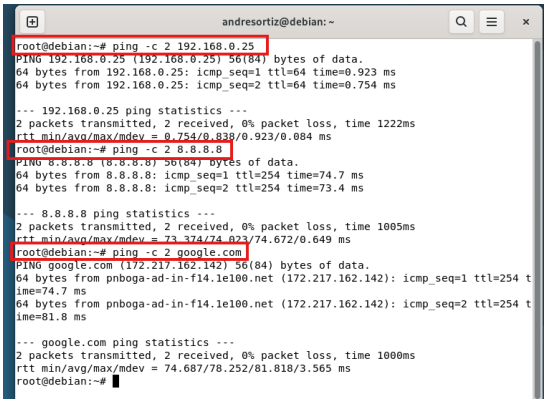
2.2 CONFIGURAR NAT PARA DEMOSTRAR COMUNICACIÓN LAN – WAN

Figura 20. Verificación de Configuración NAT en Firewall



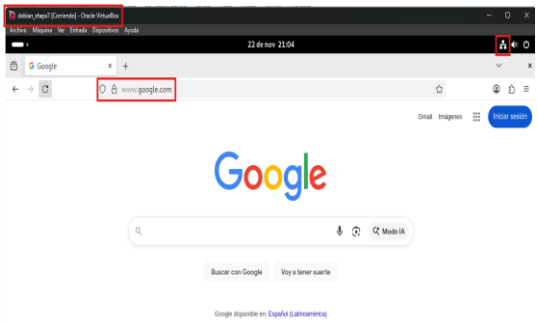
Fuente: Autoría Propia

Figura 21. Prueba de Conectividad desde LAN hacia WAN



Nota. Verificación de comunicación desde la zona verde hacia internet externa. Fuente: Elaboración Propia

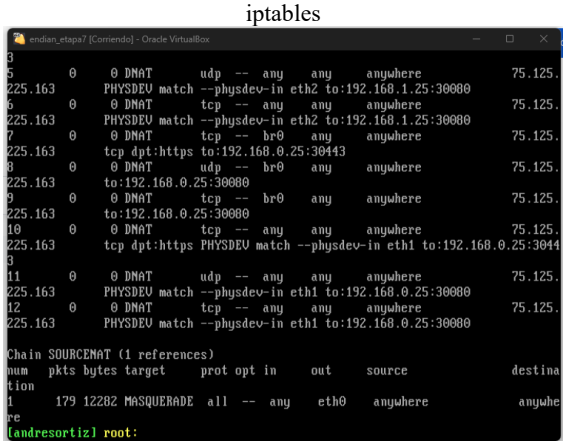
Figura 22. Navegación Web desde Debian Desktop a través de NAT



Nota. Acceso a sitios web externos desde el navegador del cliente LAN. Fuente: Elaboración Propia

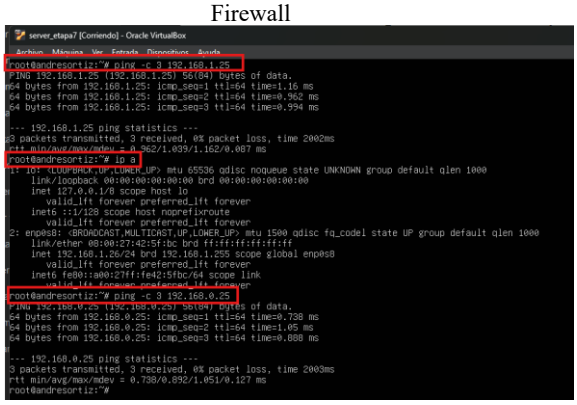
2.3 CONFIGURAR NAT PARA DEMOSTRAR COMUNICACIÓN DMZ – WAN

Figura 23. Verificación de Reglas NAT con iptables



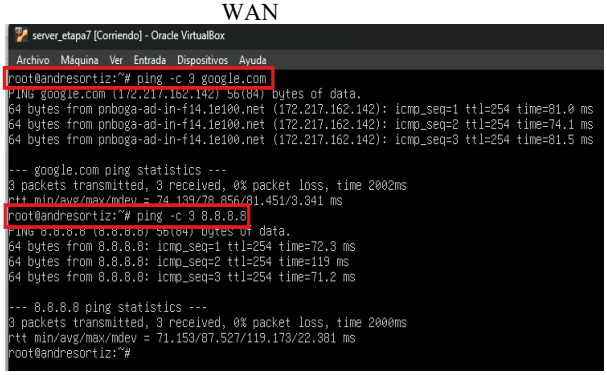
Nota. Comprobación de reglas de traducción de direcciones para la zona DMZ. Fuente: Elaboración Propia

Figura 24. Prueba de Conectividad desde DMZ hacia Firewall



Nota. Verificación de comunicación desde la zona naranja hacia el firewall. Fuente: Elaboración Propia

Figura 25. Prueba de Conectividad desde DMZ hacia WAN



Nota. Verificación de comunicación desde la zona naranja hacia internet externa. Fuente: Elaboración Propia

3 CONCLUSIONES.

Las pruebas realizadas desde la LAN y la DMZ permitieron confirmar que Endian Firewall aplica correctamente el mecanismo NAT, permitiendo la salida a la red WAN mediante el enmascaramiento de direcciones internas.

La revisión de las reglas internas mediante iptables evidenció el funcionamiento del firewall en la gestión del tráfico, destacando la presencia de reglas MASQUERADE que garantizan la correcta traducción entre redes.

La integración de las pruebas en ambas zonas internas mostró el comportamiento estable y coherente del firewall, reforzando la importancia del NAT dentro de la seguridad perimetral y el control del tránsito entre redes segmentadas.

4 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

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