IMPLEMENTACIÓN PROTOCOLOS DE SEGURIDAD GNU/LINUX MEDIANTE ENDIAN

Luis David Buitrago Castaño
ldbuitragoca@unadvirtual.edu.co

Resumen—Este informe presenta un laboratorio de seguridad perimetral implementado con Endian Firewall (GNU/Linux) en un entorno virtualizado con Oracle VirtualBox. La solución se organiza por zonas de confanza —VERDE (LAN), ROJA (WAN) y NARANJA (DMZ)— y aplica controles progresivos: confguración de interfaces y direccionamiento, activación de NAT para salida, reglas de fltrado por servicio (HTTP, FTP e ICMP) y despliegue de un proxy HTTP no transparente con autenticación y una política de lista negra. Se anexan evidencias y pruebas para sustentar la segmentación, el mínimo privilegio y el control de navegación.

PALABRAS CLAVE—Endian, frewall, seguridad perimetral, NAT, SNAT, DMZ, proxy HTTP, segmentación, VirtualBox, GNU/Linux.

I. INTRODUCCIÓN

La seguridad perimetral se basa en separar dominios de confanza y aplicar políticas explícitas sobre el tráfco que cruza el borde de red. Un enfoque práctico consiste en segmentar por zonas (LAN, DMZ y WAN) y aplicar contro- les por capas: conectividad mínima necesaria, traducción de direcciones para salida, fltrado por servicio y restricciones a nivel de aplicación. Endian integra capacidades UTM y facilita la operación de reglas, servicios y registros en escenarios de laboratorio [1].

Para aproximar un escenario realista sin infraestructura física, el despliegue se realiza en VirtualBox, defniendo adaptadores internos para LAN/DMZ y un adaptador NAT para emular salida a Internet (WAN) [2]. Los hosts GNU/Linux pueden apoyarse en guías ofciales para instalación/gestión de servicios y verifcación [3], [4].

II. OBJETIVOS

II-A. Objetivo general

Confgurar y validar un frewall perimetral basado en GNU/Linux Endian que integre NAT, fltrado de tráfco, segmentación por zonas (LAN, WAN y DMZ) y proxy HTTP, para fortalecer el control de acceso y navegación en un entorno virtualizado.

II-B. Objetivos específcos

- Defnir una topología por zonas en VirtualBox e instalar Endian como punto central de control.
- Implementar NAT y reglas de frewall para permitir y/o restringir tráfco entre zonas (HTTP, FTP e ICMP).
- Confgurar proxy HTTP no transparente con autentica- ción y lista negra para control de navegación.

III. DISEÑO DEL LABORATORIO

III-A. Topología y segmentación

La topología separa la red en tres zonas: VERDE (LAN), NARANJA (DMZ) y ROJA (WAN). Esta separación reduce el blast radius ante fallas o compromisos, y permite aplicar reglas específcas por zona.

Cuadro I
ZONAS Y PROPÓSITO DE SEGURIDAD EN EL LABORATORIO

Zona	Rol	Riesgo esperado / control
Verde (LAN)	Red interna de adminis- tración y usuarios.	Riesgo bajo; acceso a servicios y salida con- trolada.
Naranja (DMZ)	Servicios expuestos (p. ej., web/FTP).	Riesgo medio; reglas explícitas desde/hacia otras zonas.
Roja (WAN)	Enlace a Internet (NAT).	Riesgo alto; se mi- nimiza exposición de puertos y se audita.

III-B. Confguración en VirtualBox

Se recomienda utilizar dos Internal Network para LAN y DMZ, y un adaptador en modo NAT para la WAN. Esto permite que Endian enrute y fltre tráfco entre segmentos internos, y realice SNAT para la salida a Internet.

IV. IMPLEMENTACIÓN

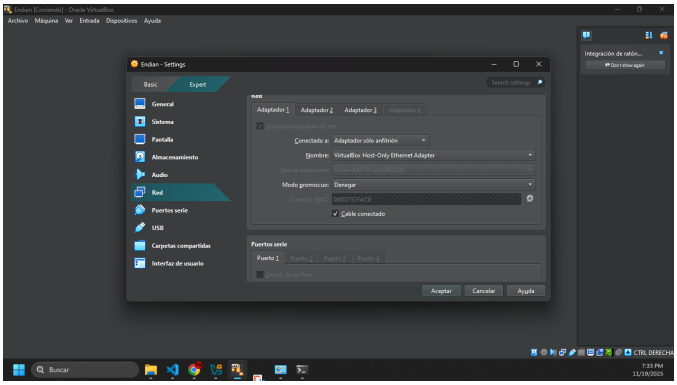
IV-A. Instalación y parametrización inicial

La instalación se completa con el asistente de Endian, defniendo credenciales administrativas, mapeo de interfaces por zona y parámetros de red. Una verifcación importante es asegurar que la interfaz externa (WAN) no quede confgurada como interna, para no alterar el nivel de confanza del perí- metro [1].

IV-B. NAT para salida (LAN y DMZ)

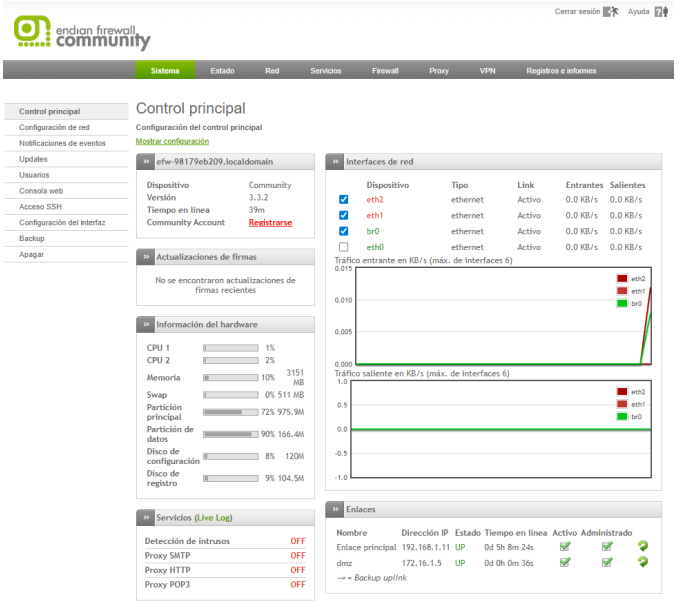
Dado que las redes privadas no son enrutable en Internet, se habilita NAT de salida para permitir consumo de servicios externos desde LAN/DMZ cuando la política lo autoriza. La validación se sustenta con reglas visibles y pruebas documen- tadas.

Ilustración 1. Confguración de adaptadores en VirtualBox: LAN/DMZ como redes internas y WAN como NAT.



Fuente: autoría propia

Ilustración 2. Asignación de interfaces a zonas VERDE, NARANJA y ROJA en Endian.

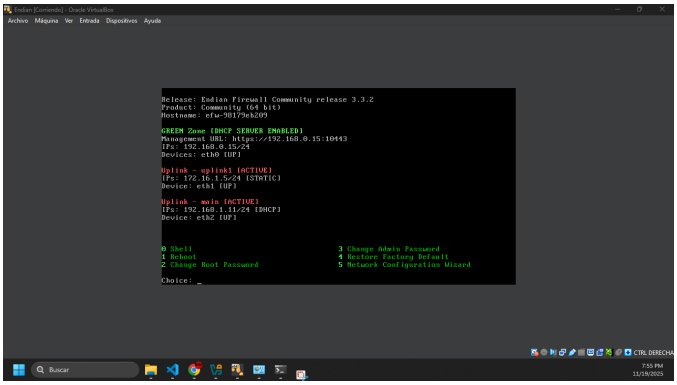


Fuente: autoría propia

Ilustración 3. Regla de NAT de salida (SNAT) para habilitar salida desde LAN/DMZ hacia WAN.

Fuente: autoría propia

Ilustración 4. Políticas de tráfco entre zonas: habilitación selectiva de servicios requeridos.



Fuente: autoría propia

IV-C. Tráfco entre zonas y mínimo privilegio

El fltrado entre zonas se estructura con permisos explícitos por servicio, manteniendo bloqueos por defecto y habilitando únicamente lo requerido (por ejemplo, HTTP/FTP según necesidad del escenario).

IV-D. Servicios en DMZ y endurecimiento (ICMP)

Para simular un entorno típico, la DMZ aloja servicios como HTTP/FTP. Como endurecimiento, se defne una regla que niegue ICMP (ping) desde la LAN hacia la DMZ para reducir reconocimiento básico del segmento expuesto.

V VALIDACIÓN (PRUEBAS Y RESULTADOS)

Las pruebas se documentan según el objetivo: conectividad interna hacia gateway, salida a Internet con NAT bajo política, acceso controlado a servicios en DMZ y validación del proxy Autenticación y bloqueo por lista negra. Se recomienda anexar capturas de verifcación (interfaces, rutas, DNS y pruebas de conectividad) para sustentar resultados.

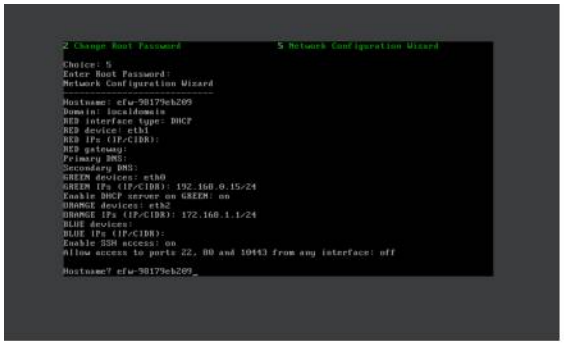
VI. EVIDENCIAS FINALES: FILTRADO, PROXY Y VERIFICACIÓN EN GNU/LINUX

En esta sección se consolidan evidencias representativas del control entre zonas, las políticas de proxy y la verifcación de conectividad y servicios desde GNU/Linux (cliente/servidor).

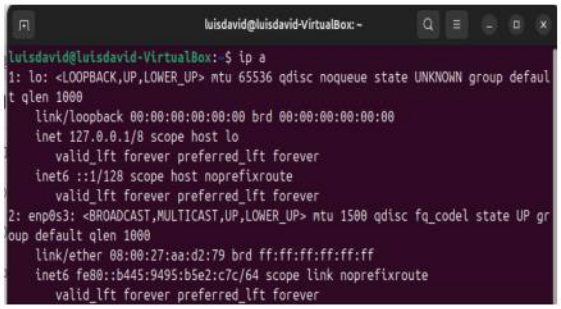
VII. CONCLUSIONES

La segmentación por zonas (LAN/DMZ/WAN) y la aplicación de NAT, reglas inter-zona y proxy con autenticación permiten implementar un esquema de seguridad perimetral completo en un entorno virtualizado. Como buena práctica, se recomienda mantener políticas por defecto restrictivas,

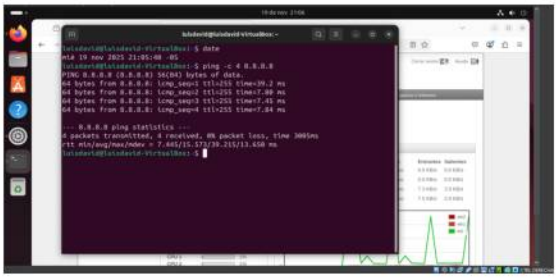
Ilustración 5. Evidencias consolidadas: verifcación en GNU/Linux (interfaces, rutas, DNS y conectividad) y controles en Endian (fltrado, proxy, autenticación y blacklist).



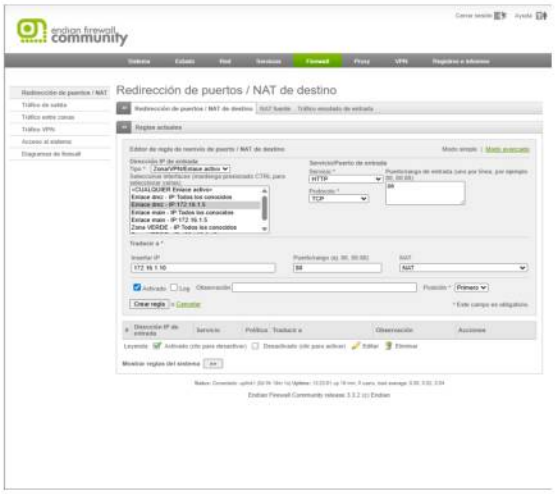
(a) Verificación de interfaces (ip a).



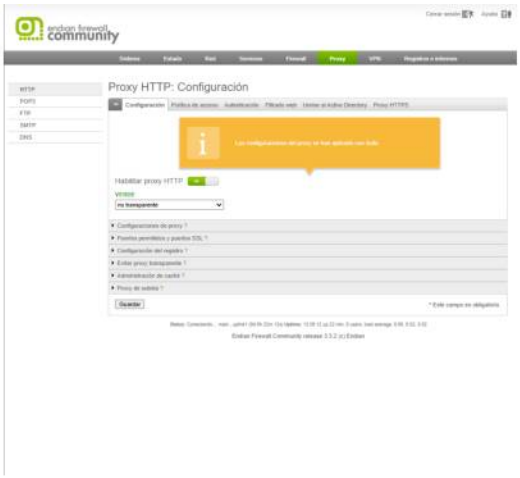
(b) Ruta por defecto y gateway.



(c) Pruebas DNS/salida.

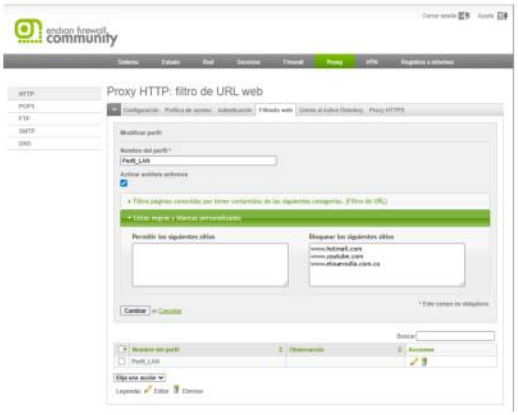


(d) Bloqueo ICMP.



(e) Proxy HTTP.

(f) Autenticación.



(g) Lista negra.

Fuente: autoría propia

habilitar únicamente servicios necesarios, auditar reglas (logs) y validar cada requisito con pruebas reproducibles.

REFERENCIAS

Endian, "Endian UTM 3.2 – manual de referencia," http://docs.endian. com/3.2/utm/index.html, 2016, accedido: 2025-11-19.

Oracle Corporation, "VirtualBox user manual," https://www.virtualbox. org/manual/, 2020, accedido: 2025-11-19.

Canonical, "Guía del escritorio Ubuntu 20.04 LTS," https://help.ubuntu. com/20.04/ubuntu-help/index.html, 2023, accedido: 2025-11-19.

Debian Project, "Debian 12.5 "Bookworm" – manual del administrador," https://www.debian.org/releases/stable/amd64/index.es.html, 2023, acce- dido: 2025-11-19.

Jay LaCroix. (2020). Mastering Ubuntu Server : Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting Ubuntu Server . Packt Publishing. https://research-ebsco-com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b4195

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

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

Debian (2023). El manual del administrador de Debian 12.5.0

Debian https://www.debian.org/releases/stable/amd64/index.es. html