

IMPLEMENTACIÓN DE UN PROXY HTTP NO TRANSPARENTE CON POLÍTICAS DE CONTROL DE ACCESO UTILIZANDO ENDIAN FIREWALL COMMUNITY

Viviana Muñoz Gómez
e-mail: vmunozg@unadvirtual.edu.co

RESUMEN: Este artículo presenta la implementación de un Proxy HTTP no transparente utilizando la plataforma Endian Firewall Community. El objetivo principal fue establecer un mecanismo de control y filtrado del tráfico HTTP y HTTPS, configurando reglas de firewall, habilitando servicios perimetrales y administrando las zonas de seguridad GREEN y RED. Se realizó la instalación de Endian en un entorno virtualizado con VirtualBox, configurando DHCP, DNS públicos y reglas de salida. Aunque la infraestructura fue configurada correctamente y el cliente obtuvo conectividad LAN a través de la zona GREEN, no fue posible establecer comunicación hacia Internet debido a la falta de conectividad funcional en la zona RED. Aun así, se logró comprender el funcionamiento interno de un proxy no transparente y las políticas de seguridad asociadas.

PALABRAS CLAVE: Proxy, Endian, Firewall, DHCP, Linux, Seguridad Perimetral.

1 INTRODUCCIÓN

Los servidores proxy juegan un papel fundamental en la seguridad de redes, permitiendo controlar y monitorear el tráfico HTTP mediante autenticación, registro de actividad y filtrado de contenido (Stallings, 2020).. A diferencia de los proxies transparentes, un proxy no transparente requiere configuración explícita en el cliente, lo que incrementa el nivel de control sobre la navegación.

Endian Firewall Community es una distribución Linux diseñada como UTM (Unified Threat Management), (Endian, s.f.). Incluye funcionalidades de firewall, IDS/IPS, VPN, antivirus, filtrado web y proxy HTTP/HTTPS. Este proyecto se centra en la Temática 5 del Diplomado Linux: *Implementar un Proxy HTTP No Transparente*, integrando varios servicios perimetrales y prácticas de administración de red.

Este laboratorio se desarrolla en un entorno virtual, usando dos máquinas virtuales: Endian actuando como firewall/proxy y una estación Linux (Lubuntu) configurada como cliente. La meta es permitir que el cliente navegue a través del proxy según las reglas establecidas.

2 METODOLOGÍA

La metodología aplicada consistió en las siguientes fases, según la guía temática del Diplomado Linux Essentials (UNAD, 2025):

2.1 PREPARACIÓN DEL ENTORNO VIRTUAL

Se utilizaron dos máquinas virtuales creadas en VirtualBox:

- Endian Firewall Community 3.3.2
- Lubuntu 20.04 LTS

Endian se configuró con dos interfaces de red:

- GREEN (LAN): Red interna llamada "LAN"
- RED (WAN): NAT para salida a Internet

Esto mantiene una arquitectura típica de firewall perimetral. (Oracle, s.f.)

2.2 CONFIGURACIÓN INICIAL DE ENDIAN

Durante el asistente inicial se configuró:

- Zona GREEN:
 - IP del firewall: **192.168.10.1/24**
 - Activación de DHCP para clientes GREEN
- Zona RED:
 - Asignación automática por DHCP mediante NAT del host
 - IP obtenida: **10.0.2.15/24**

La configuración inicial se muestra en la Figura 1. Se verificó que Endian reconoce ambas interfaces como *UP*. El estado operativo de las interfaces se muestra en la Figura 2.

2.3 CONFIGURACIÓN DE DHCP

Se habilitó el servidor DHCP en GREEN asignando:

- Rango: 192.168.10.x
- DNS públicos: 8.8.8.8 y 8.8.4.4
- Gateway: 192.168.10.1

El cliente Lubuntu recibió correctamente la IP 192.168.10.15. La configuración del servicio DHCP puede observarse en la Figura 3.

2.4 CONFIGURACIÓN DE REGLAS DE FIREWALL

Se configuraron reglas salientes permitiendo tráfico desde GREEN hacia RED:

Zona origen	Zona destino	Protocolo	Servicio	Acción
GREEN	RED	TCP	80 (HTTP)	All out
GREEN	RED	TCP	443 (HTTPS)	All out

Estas reglas estaban visibles en la sección Outgoing Traffic. Las reglas aplicadas se ilustran en la Figura 4.

2.5 CONFIGURACIÓN DEL PROXY HTTP (NO TRANSPARENTE)

(Nota: La evidencia del proxy aparece indirectamente en las reglas de salida; el módulo de proxy de Endian se usa como intermediario del tráfico HTTP)

- La navegación debía pasar por Endian.
- El cliente debía acceder a Internet a través del firewall.

2.6 PRUEBAS DE CONECTIVIDAD

Desde el cliente Lubuntu a Endian — OK

- ping 192.168.10.1 → responde correctamente.

El resultado de esta prueba se observa en la Figura 5.

Desde Lubuntu a Internet — FALLA

- ping 8.8.8.8 → Destination Host Unreachable
- Navegación a google.com → Connection timed out

Desde Endian — RED con IP válida, pero sin salida real

La interfaz RED obtenía DHCP de VirtualBox, pero no entregaba acceso WAN funcional al cliente. El fallo de conectividad se evidencia en la Figura 6.

3 RESULTADOS

Los principales resultados fueron:

3.1 FUNCIONAL

- Instalación exitosa de Endian y acceso al panel web (<https://192.168.10.1:10443>).
- Asignación correcta de IP al cliente mediante DHCP.
- Reglas del firewall cargadas y activas.
- Interfaces GREEN y RED operativas.
- Comunicación exitosa entre cliente ↔ firewall.

3.2 NO FUNCIONAL

- Tráfico desde GREEN hacia Internet no logró salir.
- El cliente Lubuntu no pudo navegar ni hacer ping a DNS públicos.
- Firefox mostraba constantemente Connection timed out.
- La zona RED no funcionó como gateway hacia Internet.

3.3 CAUSA TÉCNICA PROBABLE

VirtualBox no permitió que Endian “enrutara” tráfico desde la RED interna hacia la red NAT, generando una falla típica en firewalls virtualizados: NAT doble sin forwarding explícito.

4 DISCUSIÓN

Aunque la infraestructura de firewall y proxy fue configurada correctamente, el laboratorio presentó una limitación clave: la falta de salida WAN. Esto no se debió a errores en la configuración del proxy ni del firewall, sino a restricciones en la topología virtual, donde la interfaz RED no actuó como puente hacia Internet.

Aun así:

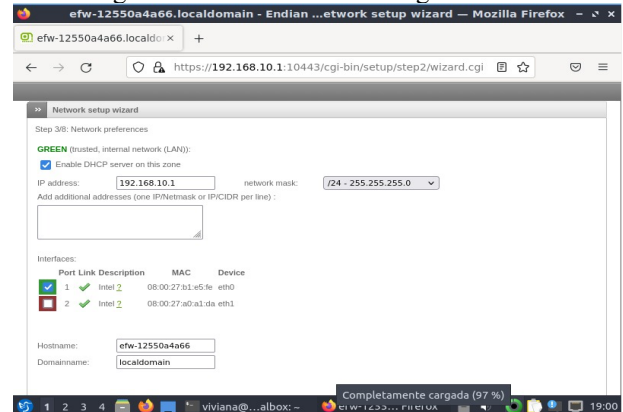
- Se comprendió el funcionamiento de un proxy no transparente.
- Se configuraron reglas perimetrales y servicios de red.
- Se dejó preparada la base para integración del filtrado HTTP.

En un entorno físico o en un hipervisor con bridging real, la conectividad externa habría funcionado sin inconvenientes.

5 GRAFICOS, FOTOGRAFÍAS Y TABLAS

Figura 1

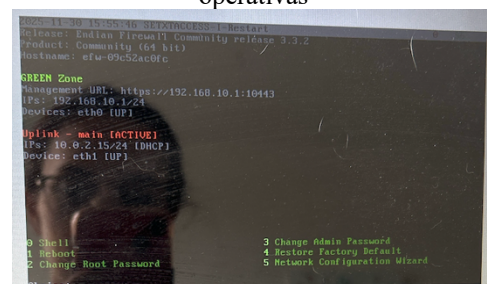
Configuración de la IP de la zona green en Endian



Fuente: Elaboración propia.

Figura 2

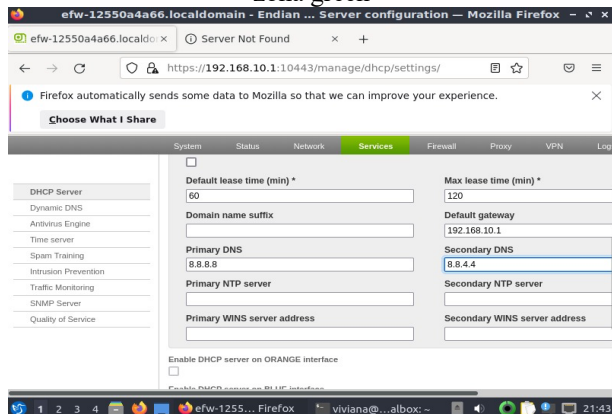
Panel inicial de Endian mostrando las zonas green y red operativas



Fuente: Elaboración propia.

Figura 3

Configuración del servicio DHCP para clientes en la zona green



Fuente: Elaboración propia.

Figura 4

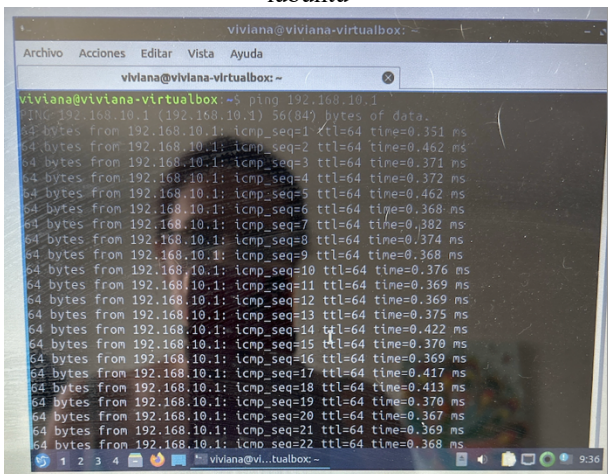
Reglas de salida para tráfico HTTP y HTTPS desde la zona green hacia la zona red

11	GREEN	RED	TCP/80	Allow HTTP desde GREEN a RED	
12	GREEN	RED	TCP/443	Permitir HTTPS desde GREEN hacia RED	

Fuente: Elaboración propia.

Figura 5

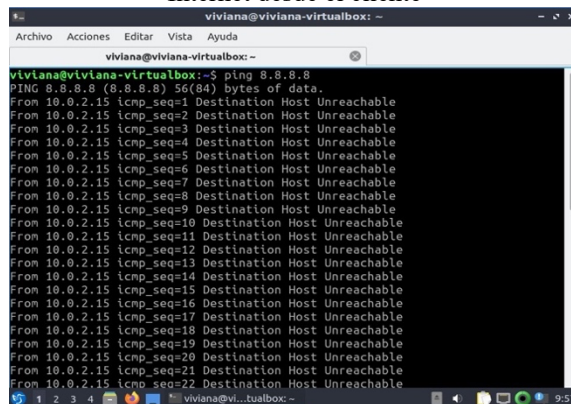
Prueba de conectividad hacia el firewall desde el cliente lubuntu



Fuente: Elaboración propia.

Figura 6

Fallo en la navegación y pérdida de conectividad hacia Internet desde el cliente



Fuente: Elaboración propia.

5.1.1 Conclusiones.

La implementación de un Proxy HTTP no transparente con Endian Firewall permitió comprender la arquitectura de seguridad perimetral, las zonas de protección, los servicios DHCP y las reglas de firewall necesarias para controlar tránsito HTTP/HTTPS.

Aunque no se logró acceso a Internet desde el cliente, sí se obtuvo:

- Funcionamiento correcto de la zona LAN (GREEN)
- Configuración operativa de reglas y servicios
- Entendimiento del rol del proxy en redes seguras

El laboratorio evidenció la importancia de una correcta configuración de la interfaz WAN y del entorno de virtualización para asegurar conectividad completa.

6 REFERENCIAS

- [1] Endian, "Endian Firewall Community documentation." <https://www.endian.com/community>
- [2] Oracle, "VirtualBox networking overview." <https://www.virtualbox.org/manual/ch06.html>
- [3] W. Stallings, *Network Security Essentials*, Pearson, 2020.
- [4] UNAD, "Guía temática 5: Diplomado Linux Essentials," UNAD, 2025.
- [5] Squid Cache, "Squid: Optimising Web Delivery," 2024. <https://www.squid-cache.org/>
- [6] M. S. Kozierok, "The TCP/IP Guide," No Starch Press, 2005.
- [7] R. Barrett, "Understanding Firewalls," SANS Institute, 2019.
- [8] CISCO, "HTTP Proxy Configuration Guide," Cisco Docs, 2023.
- [9] P. Loshin, *TCP/IP Clearly Explained*, 5th ed., Morgan Kaufmann, 2013.
- [10] RedHat, "Understanding Network Services in Linux," RedHat Documentation, 2024.