Implementando Seguridad en GNU/Linux

Oscar Felipe Campuzano Torres
e-mail: ofcampuzanot@unadvirtual.edu.co

RESUMEN: *Se implementó y validó un Proxy HTTP no transparente sobre la distribución Endian Firewall Community en un entorno virtualizado que simuló una red corporativa con zonas GREEN (LAN) y RED (WAN). Se configuraron perfiles de filtrado web, listas negras de dominios, autenticación de usuarios locales y políticas de acceso asociadas a grupos. Las pruebas desde estaciones cliente Linux comprobaron que las URLs HTTP incluidas en la blacklist quedaban bloqueadas según la política aplicada. Se discuten las limitaciones frente a sitios HTTPS y alternativas como inspección SSL o bloqueo por DNS. El trabajo ilustra capacidades de control de acceso, trazabilidad y gestión de navegación en soluciones GNU/Linux orientadas a perímetros de red.*

PALABRAS CLAVE: Proxy HTTP, firewall, filtrado web, seguridad de red.

1 INTRODUCCIÓN

El acceso a Internet dentro de organizaciones requiere mecanismos de control que permitan proteger los recursos tecnológicos y garantizar el cumplimiento de políticas internas. Los servidores proxy son una herramienta fundamental para este propósito, ya que permiten filtrar tráfico, autenticar usuarios y registrar actividades de navegación.

Endian Firewall Community es una distribución GNU/Linux orientada a la seguridad perimetral que integra servicios de firewall, proxy, filtrado web y control de acceso. Este trabajo describe la implementación de un proxy HTTP no transparente con autenticación de usuarios y bloqueo de dominios mediante listas negras, desplegado en un entorno virtualizado que simula una red empresarial real.

2 OBJETIVOS

A. Objetivo general

Implementar un servidor proxy HTTP no transparente utilizando Endian Firewall Community que permita autenticación de usuarios y control de navegación mediante listas negras.

B. Objetivos específicos

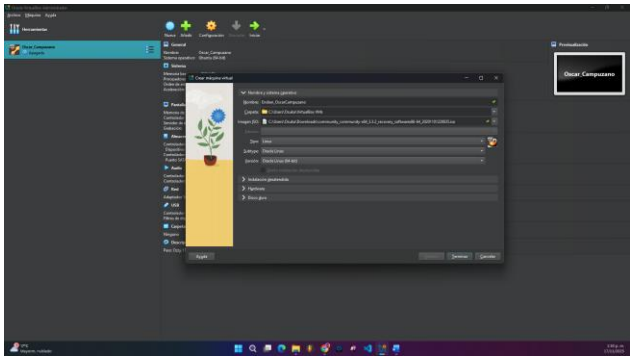
- Configurar la infraestructura virtual de red con zonas LAN y WAN.
- Habilitar el servicio proxy HTTP y definir perfiles de filtrado.
- Crear usuarios locales y grupos de acceso.
- Implementar listas negras de dominios restringidos.
- Validar el funcionamiento mediante pruebas desde un cliente Linux.

3 ENTORNO DE IMPLEMENTACIÓN

3.1 Plataforma de virtualización

Se utilizó Oracle VirtualBox para desplegar la máquina virtual con Endian Firewall Community, permitiendo simular un entorno de red controlado.

Figura 1. Creación de VM en VirtualBox



Fuente: Autoría Propia

3.2 Configuración de red

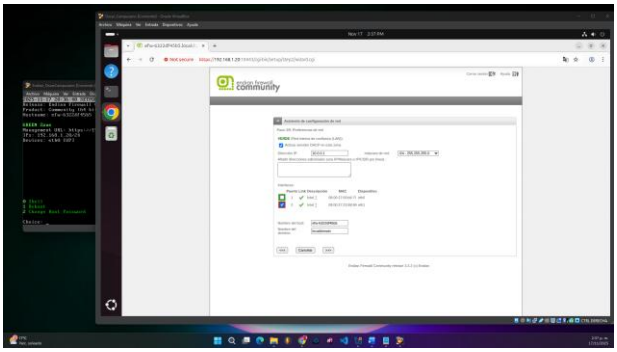
Se definieron dos interfaces:

Tabla 1. Configuración de interfaces

Zona	Función	Dirección IP	Descripción
GREEN	LAN	10.0.0.1/24	Red interna
RED	WAN	DHCP / Bridge	Acceso a Internet

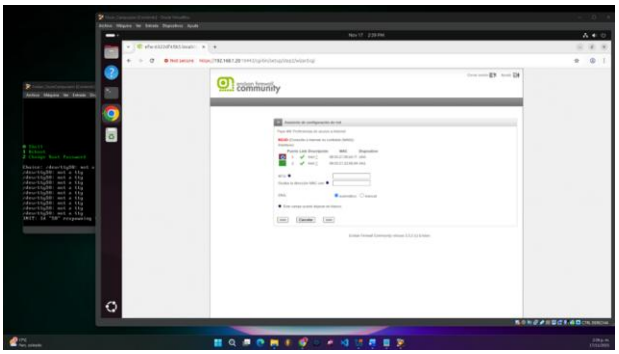
Fuente: Autoría Propia

Figura 2. Creación de GREEN Zone



Fuente: Autoría Propia

Figura 3. Creación de VM en VirtualBox

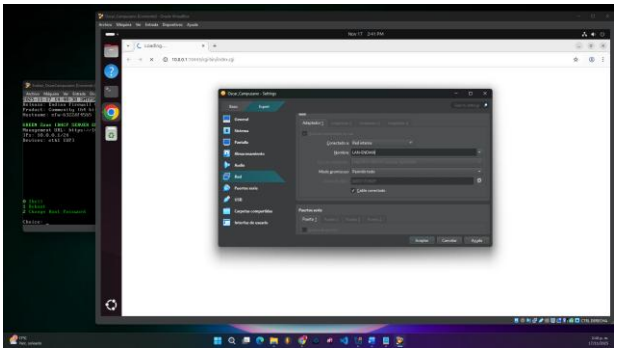


Fuente: Autoría Propia

3.3 Sistema cliente

Se utilizó un equipo Linux como cliente para configurar manualmente el proxy y validar las políticas de acceso.

Figura 4. Uso de otra VM como host del FW



Fuente: Autoría Propia

4 IMPLEMENTACIÓN DEL PROXY

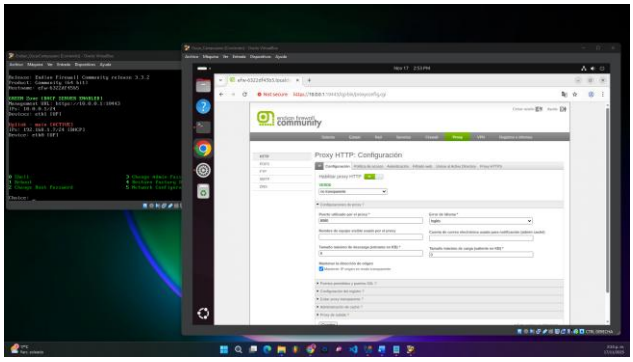
4.1 Instalación de Endian Firewall

Se descargó la imagen ISO oficial y se instaló en la máquina virtual. Posteriormente se configuraron las interfaces GREEN y RED y se accedió a la consola web de administración.

4.2 Activación del proxy HTTP

Desde la interfaz web se habilitó el servicio HTTP Proxy, seleccionando el modo no transparente para requerir configuración manual en los clientes.

Figura 5. Activación del proxy HTTP



Fuente: Autoría Propia

4.3 Creación de usuarios y grupos

Se crearon usuarios locales dentro del sistema y se asignaron a grupos, permitiendo aplicar políticas específicas según el perfil.

Tabla 2. Ejemplo de usuario creado

Usuario	Grupo	Descripción
usuario1	proxy_users	Usuario de pruebas

Fuente: Autoría Propia

4.4 Configuración de lista negra

Se creó un perfil de filtrado que incluyó dominios restringidos.

Tabla 3. Dominios bloqueados

Dominio
elnuevodia.com
hotmail.com
youtube.com

}

Fuente: Autoría Propia

5 CONFIGURACIÓN DEL CLIENTE

En el sistema Linux cliente se configuró manualmente el proxy especificando:

Tabla 4. Configuración del proxy

Parámetro	Valor
Dirección proxy	10.0.0.1

Puerto	8080
Autenticación	Usuario local

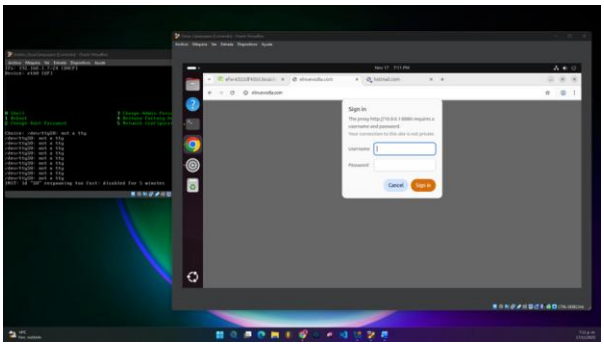
Fuente: Autoría Propia

6 RESULTADOS

Las pruebas realizadas permitieron observar:

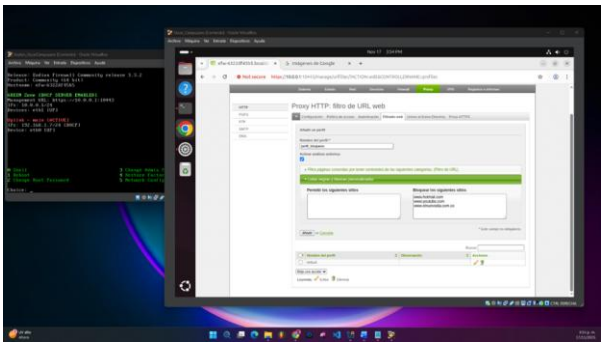
- Bloqueo exitoso de sitios HTTP incluidos en la blacklist.
- Solicitud de autenticación antes de permitir navegación.
- Registro de actividad por usuario.
- Limitaciones en bloqueo de sitios HTTPS sin inspección SSL.

Figura 6. Ejemplo de bloqueo de sitio web mediante proxy.



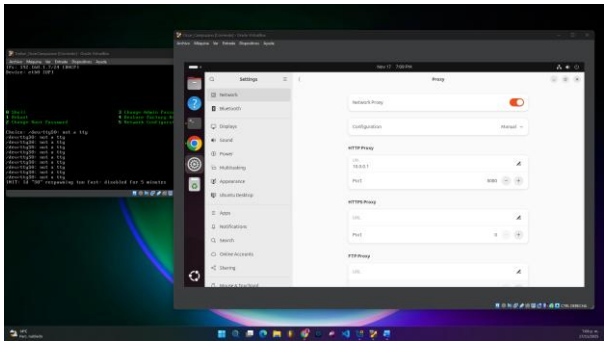
Fuente: Autoría Propia

Figura 7. Configuración de perfil de filtrado en Endian.



Fuente: Autoría Propia

Figura 8. Configuración manual de proxy en cliente Linux.



Fuente: Autoría Propia

7 CONCLUSIONES

- Se logró implementar un proxy HTTP funcional con autenticación de usuarios.
- Las listas negras permiten controlar el acceso a sitios específicos.
- El sistema permite registrar y auditar la navegación.
- Endian Firewall es una alternativa eficiente y de bajo costo.

8 TRABAJO FUTURO

- Implementar inspección SSL.
- Automatizar configuración en clientes.
- Evaluar rendimiento en entornos reales.

9 REFERENCIAS

[[1] Linux Professional Institute. (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. https://help.ubuntu.com/20.04/ubuntu-help/index.html

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

[4] Oracle Corporation. (2020). Oracle VM VirtualBox User Manual. https://www.virtualbox.org/manual/

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