DISEÑO E IMPLEMENTACIÓN DE UNA ZONA DESMILITARIZADA (DMZ) UTILIZANDO GNU/LINUX ENDIAN FIREWALL

Jose Vicente Salguero Ramirez
e-mail: jvsalgueros@unadvirtual.edu.co

RESUMEN: *Este trabajo presenta el diseño e implementación de una Zona Desmilitarizada (DMZ) como una estrategia fundamental para la protección de servidores que alojan servicios y bases de datos dentro de una red interna (LAN) con conexión a una red externa (WAN). La solución se basa en la distribución GNU/Linux Endian Firewall, configurada para segmentar la red en zonas diferenciadas: verde (LAN), roja (WAN) y naranja (DMZ). Se detallan los pasos para la configuración de las interfaces de red, el establecimiento de reglas de Network Address Translation (NAT) para permitir la comunicación controlada entre las zonas, la gestión del acceso a servicios específicos alojados en la DMZ, y la implementación de políticas de control de tráfico para asegurar el perímetro de la red. Los resultados demuestran la viabilidad de Endian Firewall como una plataforma robusta para la implementación de arquitecturas de seguridad perimetral efectivas en entornos GNU/Linux.*

PALABRAS CLAVE: Seguridad Perimetral, Zona Desmilitarizada (DMZ), GNU/Linux Endian Firewall, Network Address Translation (NAT).

1 INTRODUCCIÓN

La protección de infraestructuras de red contra las crecientes amenazas cibernéticas demanda la implementación de estrategias de seguridad perimetral robustas y efectivas. Una técnica esencial para mitigar riesgos y controlar el acceso a recursos críticos es la creación de una Zona Desmilitarizada (DMZ), que aísla los servicios expuestos de la red interna. Este trabajo se centra en el diseño e implementación de una DMZ utilizando la distribución GNU/Linux Endian Firewall. Se describe detalladamente la configuración de una arquitectura de red segmentada en las zonas verde (LAN), roja (WAN) y naranja (DMZ), así como el establecimiento de reglas de Network Address Translation (NAT) para gestionar la comunicación entre estas zonas. Adicionalmente, se aborda la definición de políticas de control de acceso para asegurar los servicios alojados en la DMZ. La metodología empleada consistió en la implementación práctica y la configuración detallada de Endian Firewall en un entorno virtualizado. Los resultados obtenidos demuestran la viabilidad y la eficacia de Endian Firewall como una solución de código abierto para la implementación de una DMZ y el fortalecimiento de la seguridad perimetral en entornos

2 OBJETIVOS

Configurar Endian Firewall en un entorno virtual dentro de VirtualBox, asegurando la correcta segmentación de las zonas de red (Zona Verde, Zona Roja y Zona Naranja) para un control efectivo del tráfico.

Establecer el Proxy HTTP No Transparente, activando la autenticación por usuario y aplicando políticas de acceso que restrinjan la navegación según reglas específicas.

Implementar un filtro web con lista negra personalizada, bloqueando sitios como Hotmail, YouTube y El Nuevo Día, y verificar la correcta aplicación de las restricciones desde un navegador en la LAN.

3 CONFIGURACION POR ZONAS

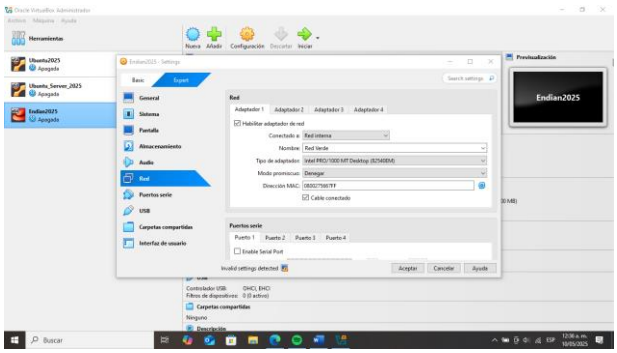
2.1 Configuración:

Para esta práctica se configuraron las máquinas virtuales de la siguiente manera:

Máquina virtual Endian

La Fig. 1 muestra la configuración del adaptador 1 en la zona verde de la red interna.

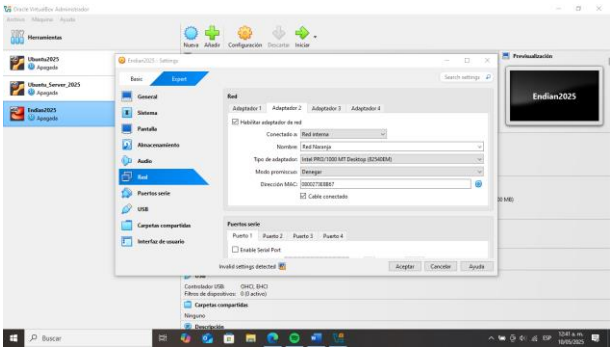
Figura 1. Configuración de la red verde en Endian Firewall



Fuente: Autoria propia

La Fig. 2 muestra la configuración del adaptador 2 en la red interna (zona naranja).

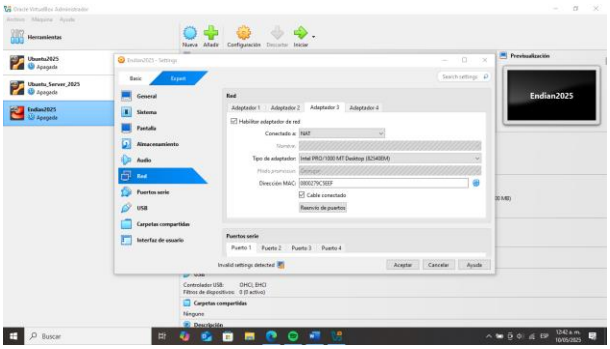
Figura 2. Configuración de la red naranja en Endian Firewall



Fuente: Autoria propia

La Fig. 3 muestra que el adaptador 3 fue configurado en la red NAT.

Figura 3. Configuración de la red roja en Endian Firewall

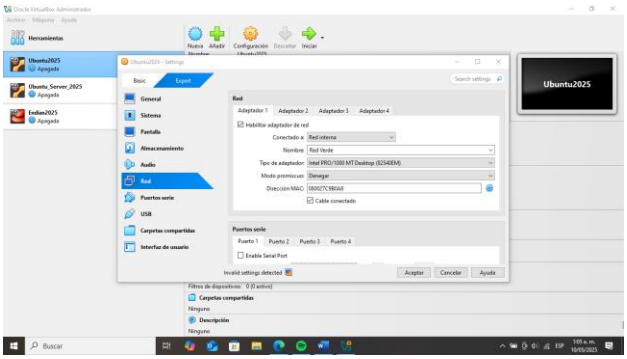


Fuente: Autoria propia

Configuracion adaptador de ubuntu desktop

El adaptador 1 se deja en la zona verde, de esta manera quedaría como un usuario que accede a internet por medio del firewall Endian, como se muestra en la fig. 4.

Figura 4.adaptador ubuntu desktop

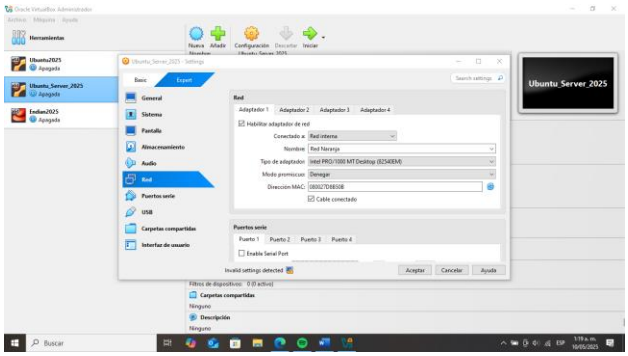


Fuente: Autoria propia

Configuracion ubuntu server

La Fig. 5 muestra la asignación del adaptador 1 a la red interna naranja, correspondiente al servidor web.

Figura 5. Adaptador ubuntu server



Fuente: Autoria propia

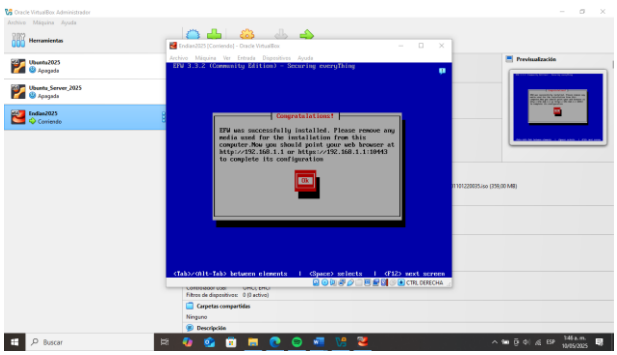
2.2 Instalación

2.2.1 Instalación del sistema operativo

Se realiza la instalacion de la maquinas virtuales endian, ubuntu desktop y ubuntu server, se muestra solo la instalacion de endian.

La Fig. 6 presenta la finalización del proceso de instalación del firewall Endian.

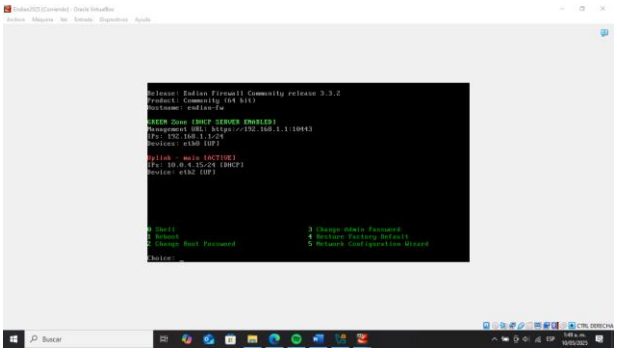
Figura 6. Finalización instalación endian



Fuente: Autoria propia

La fig. 7 muestra el sistema operativo endian instalado y funcionando adecuadamente, se coloca ip 192.168.1.1.

Figura 7.Endian operativo



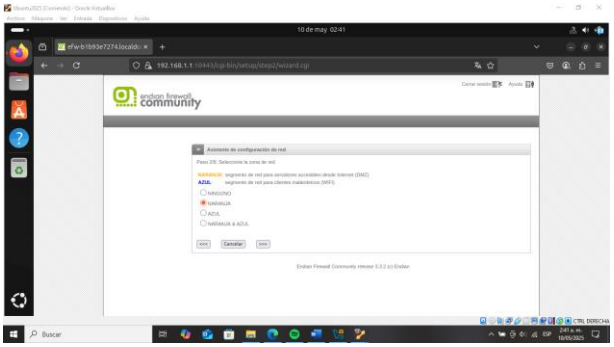
Fuente: Autoria propia

2.2.2 Configuración inicial de Endian Firewall

Se configura las zonas en endian

Luego de esto se realizaron ajustes basicos de inicio como aceptar licencia, cambios de claves admin y root. En la fig.8 se seleccciona la zona de red naranja.

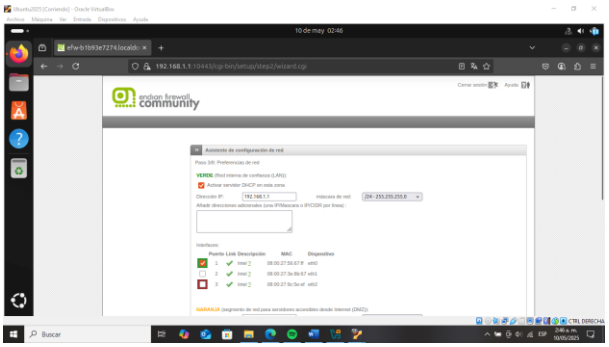
Figura 8. Zona red



Fuente: Autoria propia

La Fig. 9 muestra la configuración de la zona verde, manteniendo la IP previamente asignada.

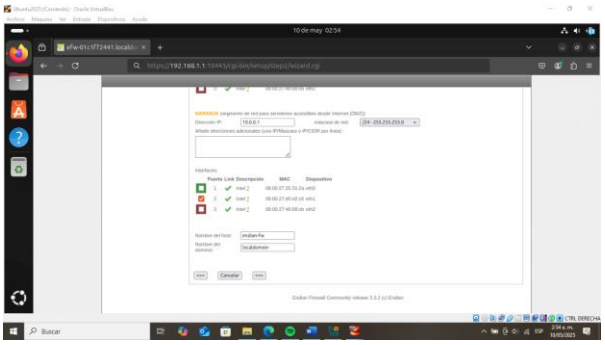
Figura 9.Zona verde



Fuente: Autoria propia

La Fig. 10 muestra la configuración de la zona naranja y dejamos la ip 10.0.0.1 seleccionamos el puerto 2 y hostname endian-fw.

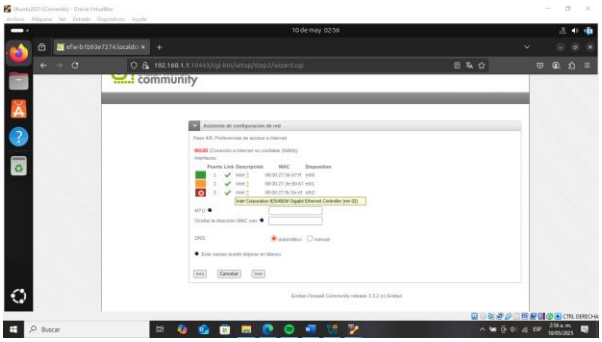
Figura 10.Zona naranja



Fuente: Autoria propia

La fig. 11 muestra como configuramos la zona roja pero la dejamos como esta, despues de esto siguen configuraciones basicas.

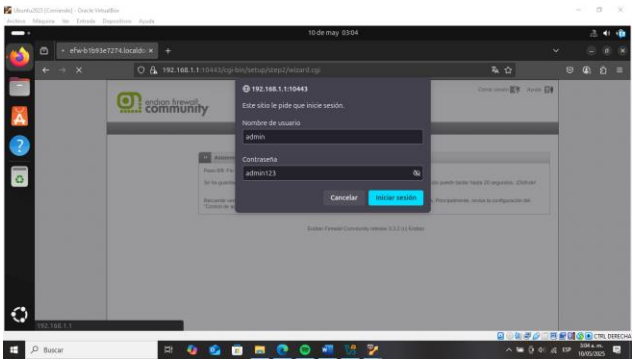
Figura 11.Zona roja



Fuente: Autoria propia

La Fig. 12 muestra el acceso a la interfaz web de Endian desde Ubuntu Desktop con su clave y usuario respectivo.

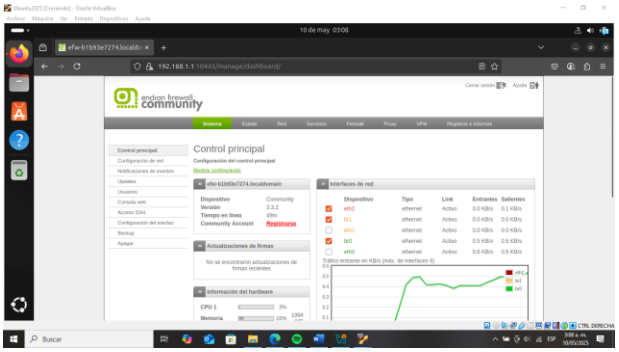
Figura 12. Explorador ubuntu



Fuente: Autoria propia

La Fig. 13 presenta la página principal de Endian, evidenciando su correcto funcionamiento.

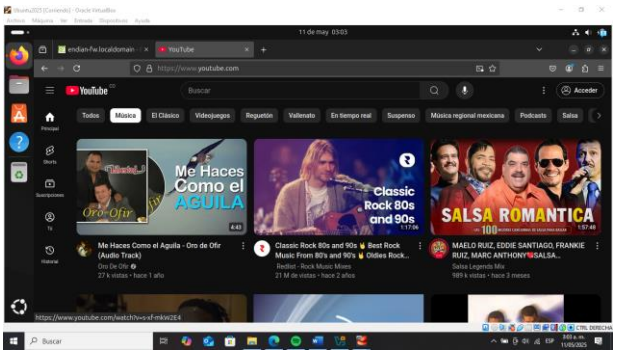
Figura 13.Pagina prinncipal endian



Fuente: Autoria propia

La Fig. 14 muestra que Ubuntu Desktop tiene acceso a Internet.

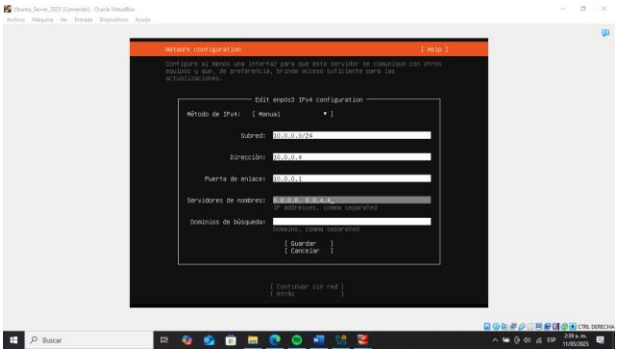
Figura 14 Navegacion Ubuntu



Fuente: Autoria propia

La fig. 15 nos muestra que el server se configuro para que quede bajo el control del endian y se coloca la ip 10.0.0.1 en puerta de enlace para que lo gobierne.

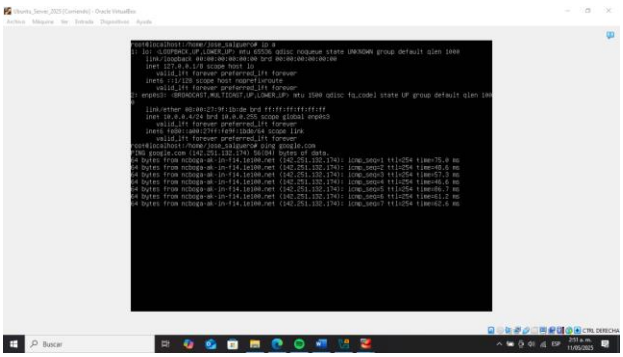
Figura 15.Configuracion ubuntu server



Fuente: Autoria propia

Después de ingresar al servidor, como se observa en la fig. 16, verificamos la conectividad a internet realizando un ping a google.com, confirmando que las zonas están configuradas y listas para trabajar en la temática escogida.

Figura 16.Acceso internet en server



Fuente: Autoria propia

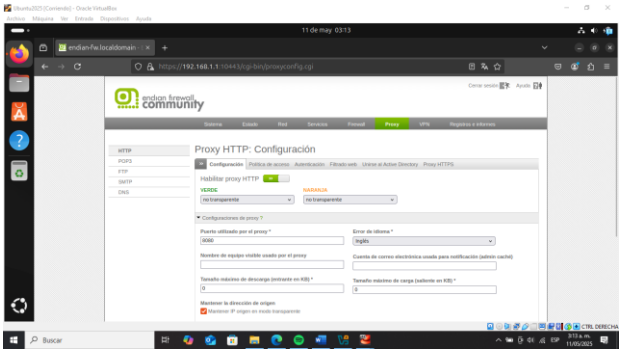
2.3 Tematica escogida # 5

2.3.1 Creación de perfil y lista negra

Crear un perfil y establecer una lista negra bloqueando los siguientes sitios:
www.hotmail.com, www.youtube.com, www.elnuevodia.com.co

Como se observa en la fig. 17 activamos el HTTP proxy y dejamos el puerto 8080.

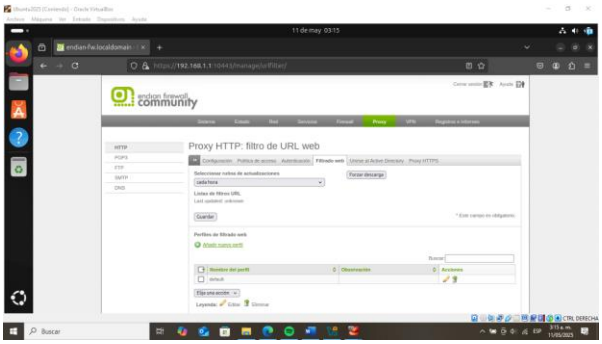
Figura 17.activacion HTTP proxy



Fuente: Autoria propia

Ahora vamos a filtrado web y seleccionamos rutina de actualizaciones cada hora, como nos muestra la fig. 18.

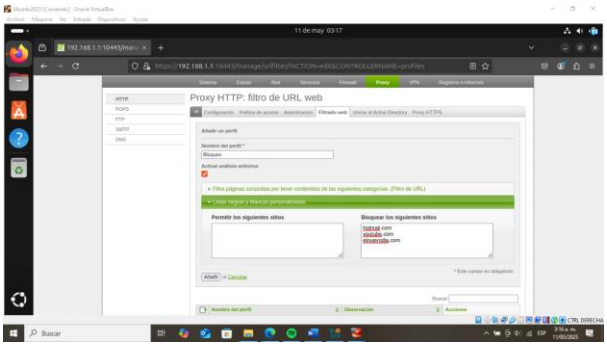
Figura 18.Rutina de actualizaciones



Fuente: Autoria propia

Como se observa en la fig. 19 luego vamos a filtrado web y creamos la lista negra con nombre bloqueo y agregamos las paginas que vamos a bloquear.

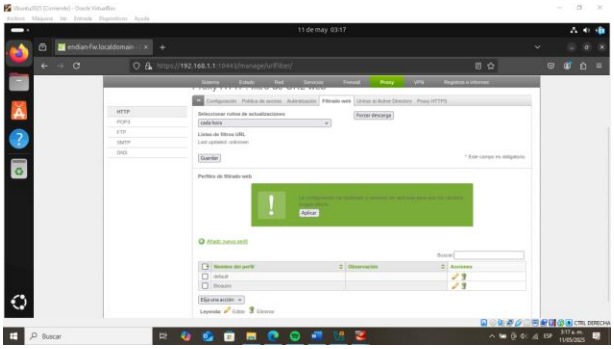
Figura 19.Lista negra



Fuente: Autoria propia

Guardamos y aplicamos los cambios, Como se observa en la fig. 20.

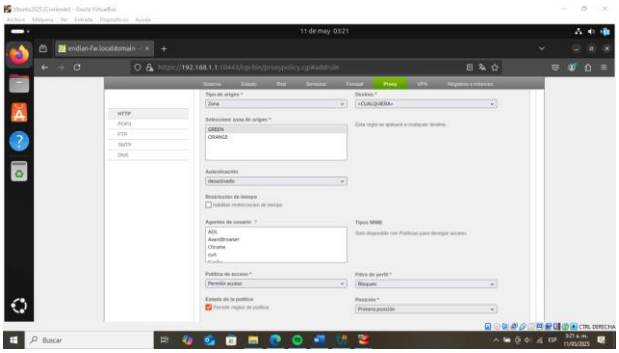
Figura 20.Cambios aplicados filtrado



Fuente: Autoria propia

En la Fig. 21 se muestra el procedimiento de configuración en la pestaña "Política de acceso". En esta sección se selecciona el tipo de origen como "Zona", eligiendo la zona green. En la política de acceso se establece el permiso, y en el filtro de perfil se asocia la lista negra previamente creada con el nombre "bloqueo". Los demás parámetros se mantienen con la configuración predeterminada.

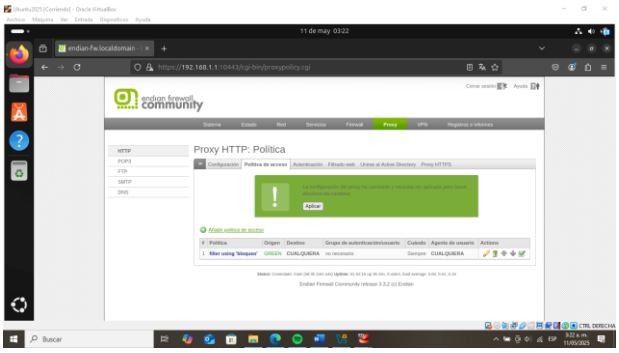
Figura 21.Politica de acceso



Fuente: Autoria propia

La Fig. 22 confirma la aplicación de la política de acceso.

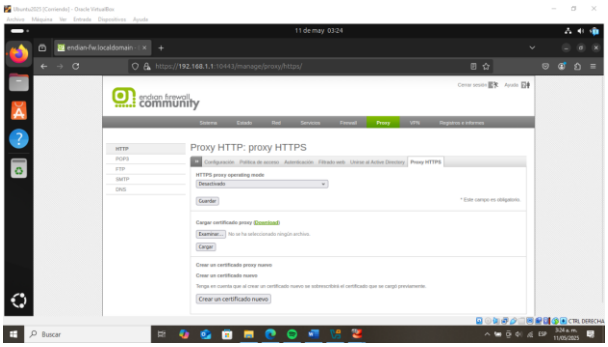
Figura 22.Cambios aplicados politica



Fuente: Autoria propia

Nos dirigimos a proxy HTTPS, esto para crear el certificado que luego vamos a guardar en el explorador del ubuntu desktop, como se observa en la fig. 23.

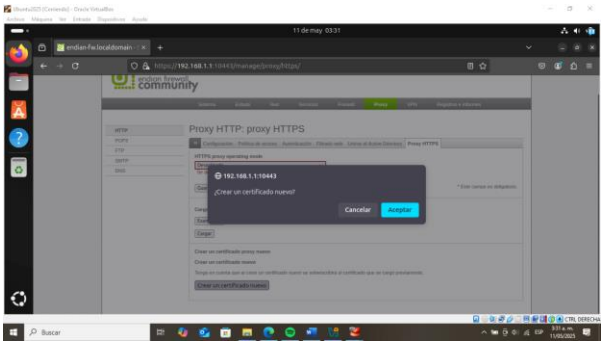
Figura 23.Certificado



Fuente: Autoria propia

Como se observa en la fig. 24 Creamos el certificado.

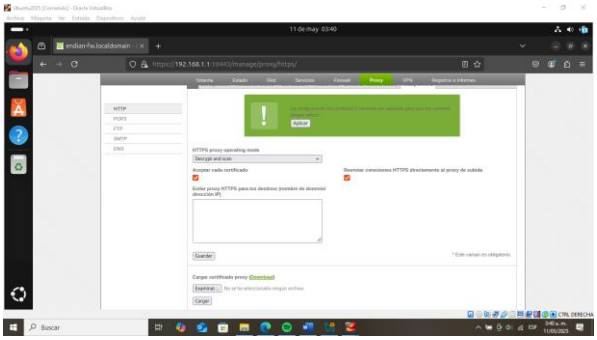
Figura 24. Creacion certificado



Fuente: Autoria propia

Luego en la fig. 25 vemos que escogemos donde dice HTTPS proxy operating mode decrypt and scan y aplicamos cambios.

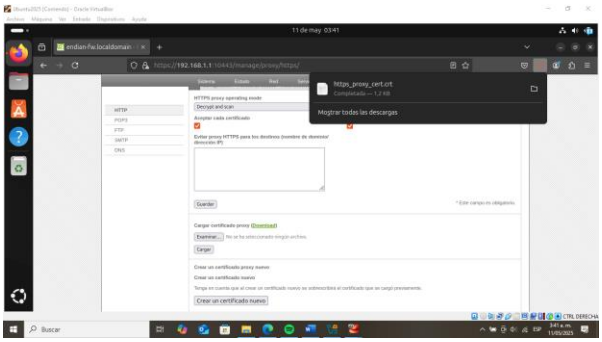
Figura 25.operating mode



Fuente: Autoria propia

La Fig. 26 muestra el proceso de descarga del certificado.

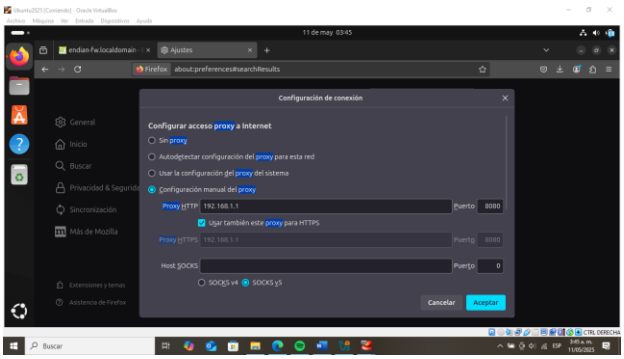
Figura 26.descarga de cerrtificado



Fuente: Autoria propia

Ahora en el navegador del ubuntu dektop configuramos la ip donde se va supervisar todo el trafico que es 192.168.1.1 con puerto 8080, como se observa en la fig. 27.

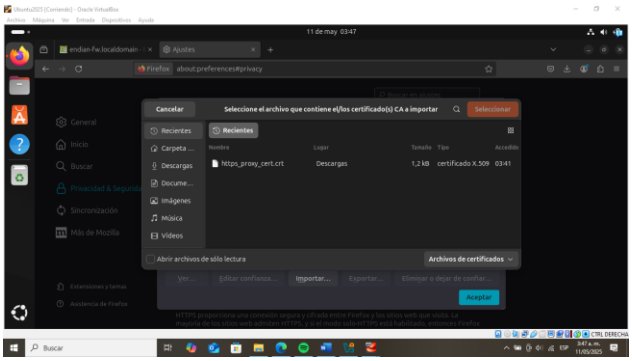
Figura 27.Configuracion IP



Fuente: Autoria propia

La Fig. 28 muestra el proceso de guardado del certificado previamente descargado. Este paso es necesario porque, al configurar manualmente la IP del proxy, el navegador generará advertencias de seguridad al acceder a cualquier sitio web. La instalación del certificado permite evitar dichas advertencias y establecer una navegación segura desde el cliente.

Figura 28.Guardado de certificado



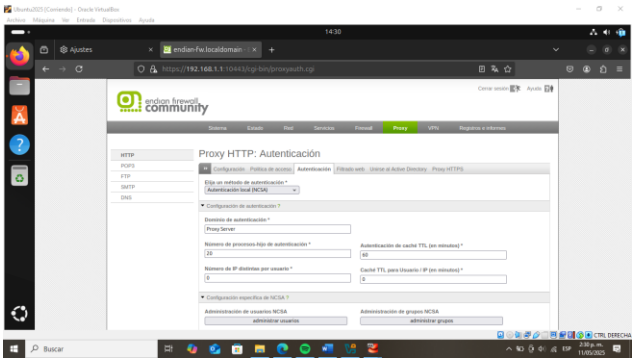
Fuente: Autoria propia

2.3.2 Configuración de autenticación

Autenticación por usuario: A través de la opción proxy cree un usuario y asócielo a un grupo. Establezca una política de acceso y vincule el perfil creado en el punto anterior y relaciónelo también con la política de autenticación.

Como se observa en la figura 29 Ahora nos dirigimos a la pestaña autenticacion y dejamos autencion local NSCA.

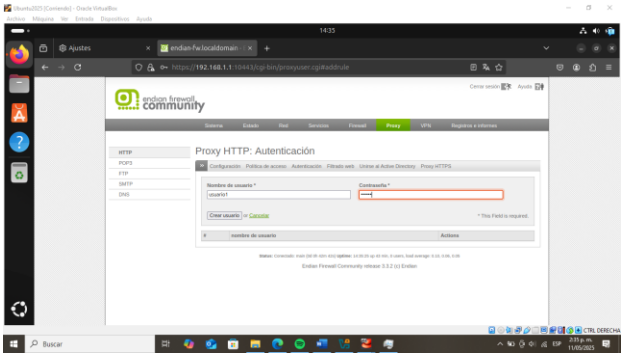
Figura 29.Autenticación



Fuente: Autoria propia

Ahora ingresamos donde dice administrar usuarios y creamos el usuario1 con contraseña 123456, Como se observa en la fig. 30.

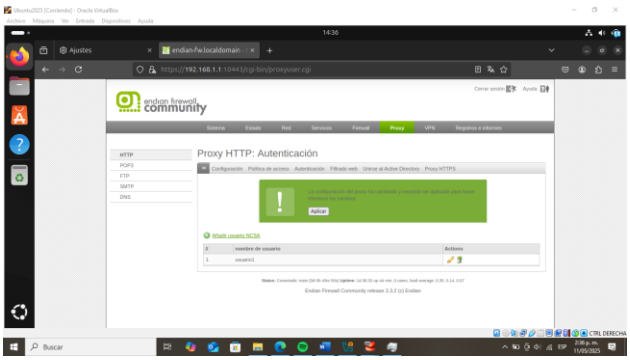
Figura 30.Administrar usuarios



Fuente: Autoria propia

Aplicamos cambios y queda guardado el usuario1, Como se muestra en la fig. 31.

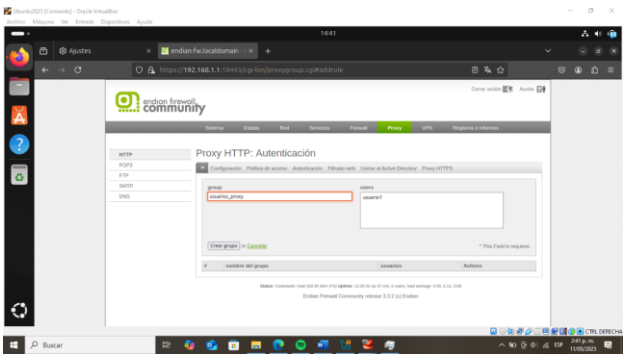
Figura 31.usuario1



Fuente: Autoria propia

Ahora vamos en donde dice administrar de grupos y creamos el grupo usuarios_proxy y ligamos el usuario1, Como se observa en la fig. 32.

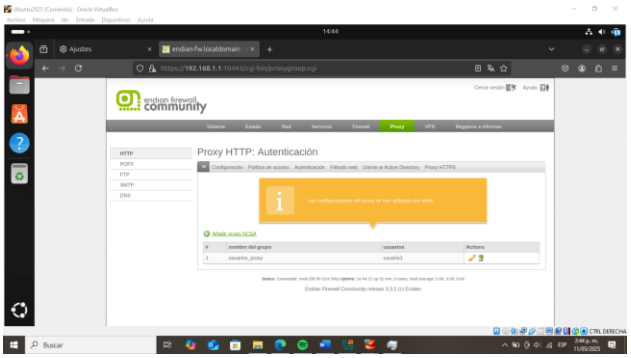
Figura 32.Grupos



Fuente: Autoria propia

Aplicamos los cambios, como se observa en la fig. 33.

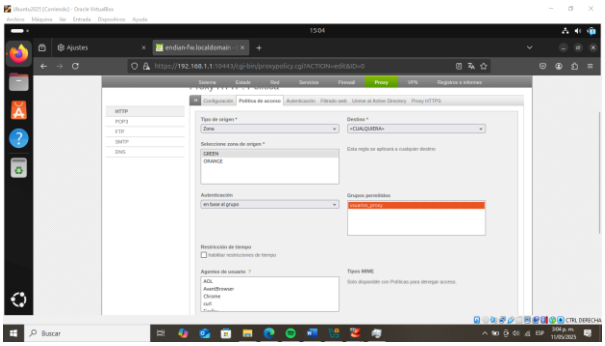
Figura 33.Cambios aplicados grupos



Fuente: Autoria propia

Ahora nos dirgimos a politica de acceso y hacemos una modificacion a la politica ya habiamos realizado anteriormente, consiste en cambiar autenticacion en base al grupo y seleccionamos el grupo, Como se aprecia en la fig. 34.

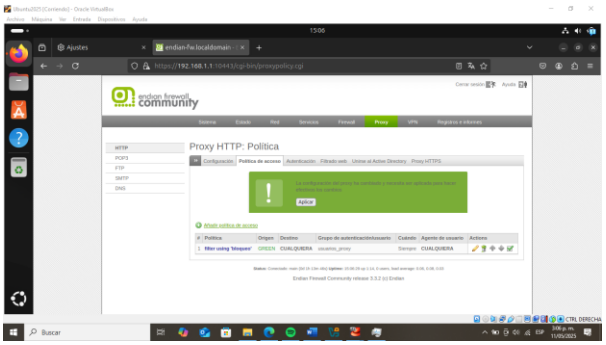
Figura 34.politica de acceso grupo



Fuente: Autoria propia

Actualizamos la politica y aplicamos cambios, Como se observa en la fig. 35.

Figura 35.Aplicar cambios politica



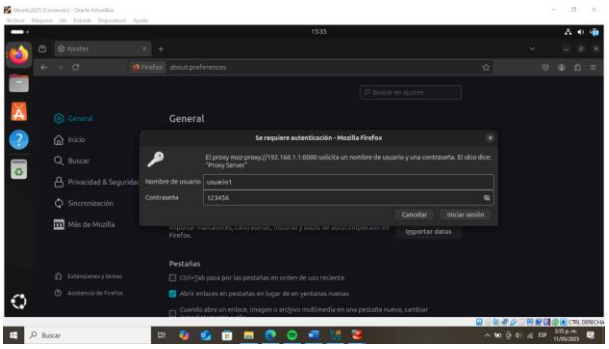
Fuente: Autoria propia

2.3.3 Pruebas de acceso y restricción

Probar desde la LAN a través de un navegador Web, el acceso a los portales referenciados en la lista negra.

Vamos al navegador y nos va pedir el usuario y la contraseña y colocamos los datos para acceder, Como se muestra en la fig. 36.

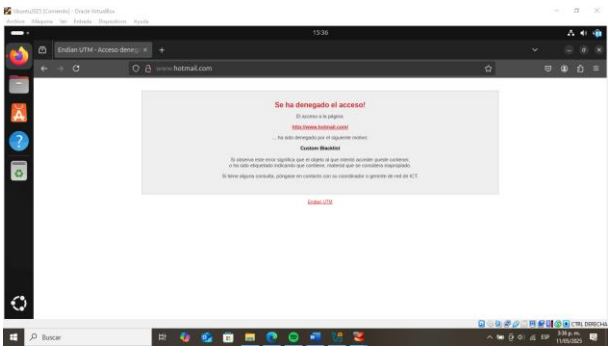
Figura 36. Datos usuario1



Fuente: Autoria propia

La Fig. 37 muestra la verificación de acceso restringido a los sitios definidos en la lista negra.
www.hotmail.com restringido por blacklist.

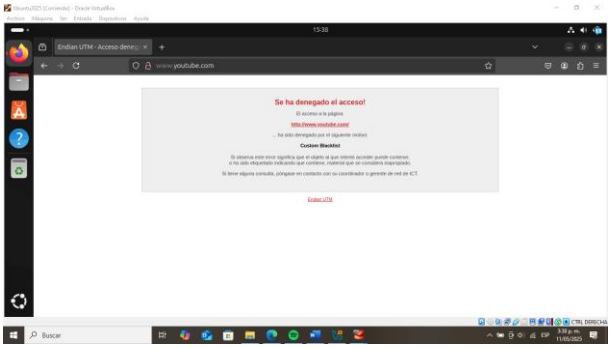
Figura 37.Hotmail restringido



Fuente: Autoria propia

En la fig 38 vemos la pagina www.youtube.com restringida por blacklist.

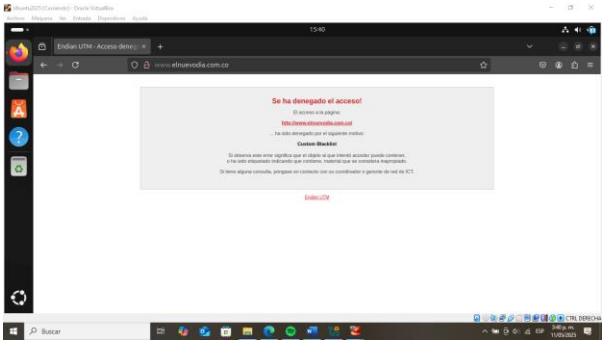
Figura 38.Youtube restringido



Fuente: Autoria propia

www.elnuevodia.com.co restringido por blacklist como se ve en la fig. 39.

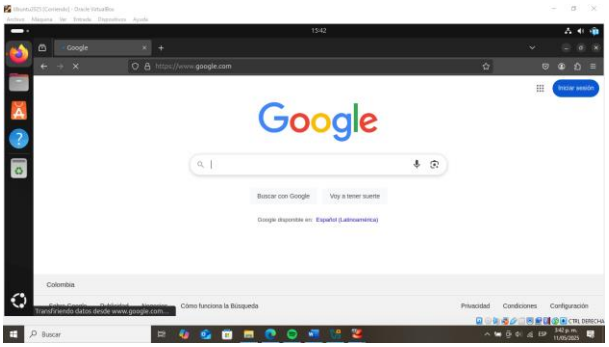
Figura 39.Elnuevodia restringido



Fuente: Autoria propia

Los demas sitios funcionan correctamente como vemos en la fig.40 con google.

Figura 40. Google funcionando



Fuente: Autoria propia

4 ENLACE DEL VIDEO

https://youtu.be/4W7lzFS0gzk

5 CONCLUSIONES

La implementación de GNU/Linux Endian Firewall con las zonas verde, roja y naranja demostró la capacidad de establecer una segmentación de red lógica y efectiva, aislando la red interna de la externa y creando una zona segura para los servidores expuestos (DMZ), tal como lo fundamentan los principios de seguridad perimetral.

La correcta configuración de reglas de Network Address Translation (NAT) en Endian Firewall permitió establecer la comunicación bidireccional controlada entre la LAN, la DMZ y la WAN, validando la teoría de que NAT es esencial para enmascarar direcciones privadas y permitir el acceso a redes externas de forma segura.

La apertura selectiva de puertos para los servicios HTTP (80) y FTP (21) hacia la DMZ, combinada con el bloqueo del protocolo ICMP, evidenció la importancia de aplicar el principio de mínimo privilegio y la deshabilitación de servicios innecesarios para reducir la superficie de ataque, un concepto clave en la seguridad de servidores.

La definición de reglas de acceso específicas entre las zonas (verde-naranja, internet-DMZ) y la verificación del tráfico a través de pruebas de conectividad confirmaron la efectividad de las listas de control de acceso (ACLs) en la gestión del flujo de información y la aplicación de políticas de seguridad personalizadas entre segmentos de la red.

La implementación de un proxy HTTP no transparente con políticas de autenticación y listas negras demostró la capacidad de Endian Firewall para controlar y restringir el acceso a contenidos web desde la LAN, reforzando la seguridad y la productividad de los usuarios mediante la aplicación de políticas de uso aceptable basadas en la teoría de filtrado de contenido y control de acceso a nivel de aplicación.

5.1.1 CITAS Y/O REFERENCIAS

6 REFERENCIAS

[1] LPI, "LPIC-1 Exam 101, Tema 102: Comandos GNU y Unix," 2022. [Online]. Available: https://learning.lpi.org/es/learning-materials/101-500/102/. [Accessed May 2025].

[2] Canonical, "Guía del Ubuntu Desktop 20.04 LTS," Help Ubuntu, 2023. [Online]. Available: https://help.ubuntu.com/20.04/ubuntu-help/index.html. [Accessed May 2025].

[3] Debian, "El manual del administrador de Debian 12.5.0," 2023. [Online]. Available: https://www.debian.org/releases/stable/amd64/index.es.html. [Accessed May 2025].

[4] Oracle, "Manual de usuario VirtualBox," 2020. [Online]. Available: https://www.virtualbox.org/manual/. [Accessed May 2025].

[5] Endian, "Endian UTM 3.2 Manual referencia," 2016. [Online]. Available: http://docs.endian.com/3.2/utm/index.html. [Accessed May 2025].

[6] J. LaCroix, _Mastering Ubuntu Server: *Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting Ubuntu Server*_, Packt Publishing, 2020. [Online]. Available: https://research-ebsco-com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b41952. [Accessed May 2025].

[7] Free Software Foundation, “Software libre y educación. El sistema operativo GNU,” 2016. [Online]. Available: http://www.gnu.org/education/education.html. [Accessed May 2025].

[8] P. F. Hernandez and J. Sánchez, “Monitoreo y administración de sistemas Linux”, Repositorio Institucional UNAD, 2022. [Online]. Available: https://repository.unad.edu.co/handle/10596/53211. [Accessed May 2025].

[9] P. F. Hernández and J. Sánchez, “Servidores para administración remota y compartir recursos”, Repositorio Institucional UNAD, 2022. [Online]. Available: https://repository.unad.edu.co/handle/10596/53212. [Accessed May 2025].

[10] J. H. Jiménez, “Shell Script para Bash”, Repositorio Institucional UNAD, 2016. [Online]. Available: https://repository.unad.edu.co/handle/10596/9758. [Accessed May 2025].

Notas:

1. Todas las configuraciones descritas en este documento fueron implementadas en un entorno de máquinas virtuales utilizando Oracle VirtualBox. Las IPs asignadas fueron gestionadas de forma estática con fines didácticos y podrían variar en un entorno real.