IMPLEMENTANDO SEGURIDAD EN GNU/LINUX

Carlos Andrés Babativa Linares
e-mail: cababatival@unadvirtual.edu.co
Ciro Andrés Morales Castro
e-mail: camoralescast@unadvirtual.edu.co
Pedro Pablo Porras Valencia
e-mail: ppporrasv@unadvirtual.edu.co
Sergio Aldana Gómez
e-mail: saldanago@unadvirtual.edu.co
Wilson Camilo Estupiñán Rey
e-mail: wcestupinanr@unadvirtual.edu.co

RESUMEN: *Este trabajo presenta la implementación de un entorno de red seguro en GNU/Linux usando Endian UTM, incluyendo configuración de zonas LAN (verde), DMZ (naranja) y WAN (roja), reglas de NAT, control de acceso HTTP/FTP y un proxy con políticas de autenticación. Se describe la creación de la máquina virtual, la asignación de interfaces de red, el establecimiento de reglas de firewall y reenvío de puertos. Además, se valida la conectividad y se analiza el uso de políticas de listas negras y autenticación en navegación HTTP. Los resultados muestran una topología segura y funcional que refuerza la protección de servidores y usuarios en un entorno de prueba.*

PALABRAS CLAVE: DMZ, Endian, Proxy, Ubuntu, VirtualBox.

1 INTRODUCCIÓN

En la actualidad, la seguridad informática se ha convertido en una prioridad fundamental para cualquier organización que maneje datos sensibles y sistemas de información críticos, la implementación de zonas desmilitarizadas (DMZ) representa una estrategia crucial para proteger la infraestructura interna mientras se permite el acceso controlado a ciertos servicios desde el exterior, este enfoque de seguridad por capas es particularmente importante en entornos donde se requiere exponer algunos servicios a Internet mientras se mantiene protegida la red interna.

El presente artículo documenta la implementación de una arquitectura de seguridad robusta utilizando GNU/Linux Endian Firewall (EFW) como plataforma principal, se detalla la configuración de una zona DMZ para la protección de servidores que contienen bases de datos y aplicaciones críticas bajo plataformas GNU/Linux, el proyecto abarca desde la configuración básica de las interfaces de red hasta el establecimiento de reglas avanzadas de firewall que garantizan la comunicación segura entre las diferentes zonas de la red.

La solución implementada divide la red en tres zonas claramente diferenciadas: la zona verde (LAN interna), la zona naranja (DMZ) y la zona roja (WAN/Internet), esta segmentación permite aplicar políticas de seguridad específicas a cada zona, controlando meticulosamente el tráfico que fluye entre ellas y garantizando así la integridad y confidencialidad de la información.

2 DESARROLLO TEMÁTICAS

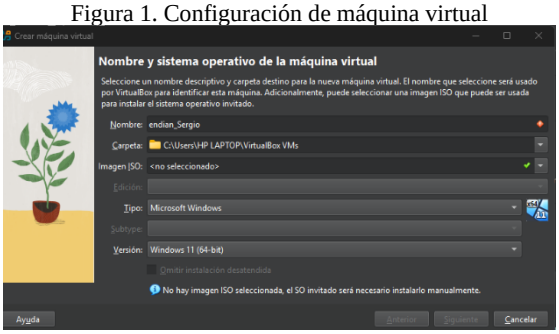
A continuación, se mostrará el desarrollo de cada una de las temáticas desde la instalación y configuración de un entorno de red seguro.

2.1 CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX (TARJETAS DE RED) E INSTALACIÓN EFECTIVA DEL MISMO

2.1.1 CREACIÓN Y PREPARACIÓN DE LA MÁQUINA VIRTUAL ENDIAN

Como aspecto principal se procedió a crear la máquina virtual destinada a implementar el sistema operativo Endian, la imagen iso correspondiente al sistema operativo fue tomada de la biblioteca oficial del fabricante, en este procedimiento se asignaron valores y características requeridas para su instauración según lo ilustrado en la Fig. 1.

Figura 1. Configuración de máquina virtual



Fuente: Autoría Propia

2.1.2 CONFIGURACIÓN DE INTERFACES DE RED EN ENDIAN.

Para la implementación de procesos de red segmentaba y gestión de tráficos seguros se configuraron tres adaptadores de red en el sistema operativo de Endian, las cuales fueron:

- Adaptador 1: (LAN-ZONA VERDE) red interna
- Adaptador 2: (DMZ-ZONA NARANJA) red interna del servidor
- Adaptador 3: (WAN-ZONA ROJA) Configuración NAT en acceso a internet según lo mostrado en la Fig. 2.

Figura 2. Configuración de interfaces de red.

Fuente: Autoría Propia

2.1.1 CREACIÓN Y PREPARACIÓN DE LAS MÁQUINAS VIRTUALES PARA CLIENTES Y SERVIDORES

Con el propósito de simular un entorno de red seguro, se configuraron dos máquinas virtuales adicionales para Linux Mint (ZONA VERDE) y Ubuntu server como (ZONA NARANJA) implementando los protocolos de instalación, configuración para red interna “IP”, mascara de subred, puerta de enlace y DNS según se presenta en la Fig. 3.

Figura 3. Creación de MV para clientes y servidores.

Fuente: Autoría Propia

2.1.2 CONFIGURACIÓN Y VERIFICACIÓN DE CONECTIVIDAD

En este proceso se llevaron a cabo pruebas de conectividad y diagnósticos de red para el servidor de Ubuntu, posteriormente se estableció una conexión por la IP para administración del firewall desde el navegador, realizando los procesos de configuración conforme con la Fig. 4

Figura 4. Configuración interfaces de red.

Fuente: Autoría Propia

2.1.3 VERIFICACIÓN DE INTERFACES DE RED

Tras la validación y configuración del entorno de Endian se procedió a verificar que el sistema reconociera cada una de las interfaces asignadas en las zonas “VERDE”, “NARANJA” y “ROJA” identificando que las “MAC” (Media Access Control) coincidieran con las establecidas en la máquina virtual, garantizando que cada una de las interfaces de red estén correctamente enlazadas a su zona como se representa en la Fig. 5.

Figura 5. Verificación de enrutamiento interfaces de red.

Fuente: Autoría Propia

2.1.4 CONFIGURACIÓN DE LAS ZONAS Y VERIFICACIÓN FINAL

Luego de la verificación de conectividad de cada una de las zonas se procedió a asignar cada una de las interfaces, verificando el enrutamiento y el DHCP, por otro lado, se realizaron pruebas de conectividad de la (ZONA VERDE) verificando la conexión entre clientes y servidor, así como el aislamiento de la zona roja, verificación de la conexión exitosa del firewall según lo ilustrado en la Fig. 6

Figura 6. Confirmación y verificación del estado de conectividad

Fuente: Autoría Propia

2.2 CONFIGURACIÓN NAT

La implementación se realizó en un entorno virtual utilizando:

- Endian Firewall como cortafuegos y gestor de NAT.
- VirtualBox para la virtualización de las redes LAN, DMZ y WAN.
- Ubuntu Desktop para simular clientes de red interna.
- Ubuntu Server para alojar servicios expuestos en la DMZ.

Se configuraron tres zonas de red en Endian Firewall:

- Green (LAN): red interna de usuarios.
- Orange (DMZ): red segura para servidores públicos.
- Red (WAN): conexión simulada a Internet.
- Se inicia sesión en la interfaz gráfica de Endian. Fig. 7.

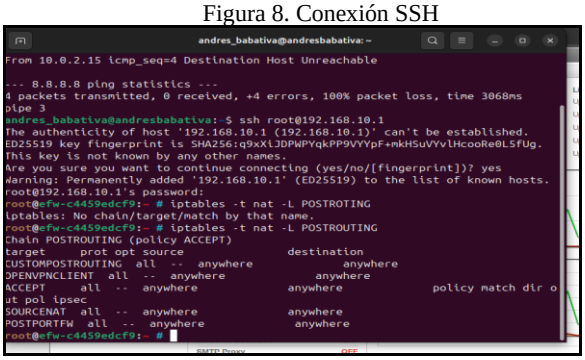
Figura 7. Interfaz gráfica Endian

Fuente: Autoría Propia

Las reglas de NAT se definieron utilizando la interfaz web de EFW y validando su persistencia, Fig. 8. Las pruebas de funcionamiento incluyeron:

- Ping entre zonas para verificar conectividad.
- Curl y navegador web para probar acceso a servicios web.
- SSH para acceso remoto al firewall y servidores.

Figura 8. Conexión SSH



Fuente: Autoría Propia

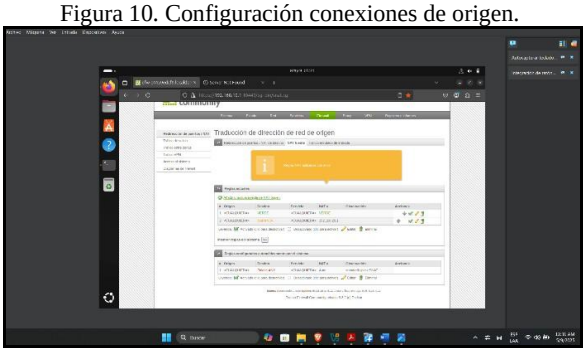
2.2.1 ACCESO DE LAN A WAN MEDIANTE NAT

Se configura una regla de NAT dinámico (masquerading) para permitir que los clientes de la red LAN accedan a Internet. Con conexión exitosa, como se verifica mediante respuestas a ping hacia direcciones públicas y carga de páginas web como se puede validar en las Fig. 9 y Fig. 10.

Figura 9. Configuración reglas

Fuente: Autoría Propia

Figura 10. Configuración conexiones de origen.

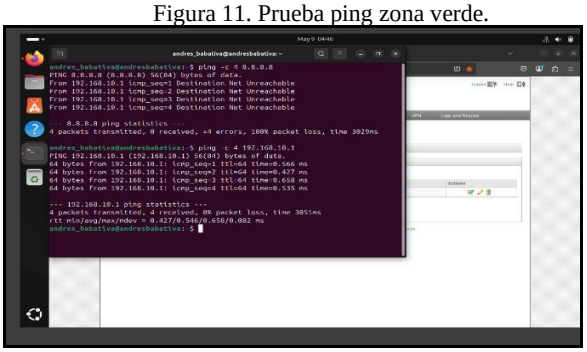


Fuente: Autoría Propia

2.2.2 ACCESO DESDE DMZ A INTERNET

Se configuró una regla que permite el acceso a Internet desde servidores ubicados en la DMZ, respetando el aislamiento respecto a la LAN. La conectividad fue verificada mediante ping y curl desde el servidor en la DMZ hacia destinos públicos, como lo muestra la Fig. 11.

Figura 11. Prueba ping zona verde.

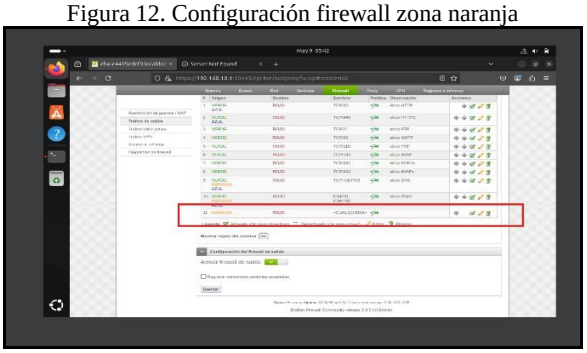


Fuente: Autoría Propia

2.2.3 REENVÍO DE PUERTOS DESDE WAN HACIA DMZ

Se establecieron reglas de port forwarding para publicar servicios web y FTP alojados en un servidor Ubuntu en la DMZ. Se verifica que, desde la red WAN, sea posible acceder correctamente a los servicios configurados, según la Fig. 12.

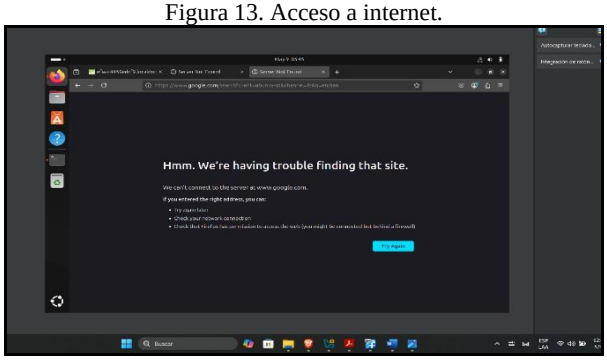
Figura 12. Configuración firewall zona naranja



Fuente: Autoría Propia

En el proceso de configuración de las reglas con Endian Linux, se realizaron correctamente las definiciones para las zonas verde, naranja y roja. Sin embargo, al intentar acceder a internet desde la zona verde, no fue posible establecer la conexión, Fig. 13, lo que sugiere que aún es necesario ajustar algunos parámetros de red o reglas del firewall.

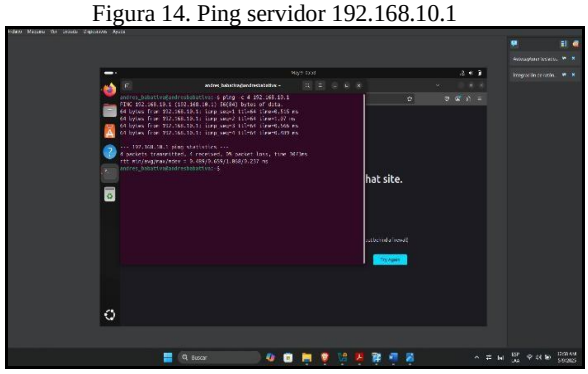
Figura 13. Acceso a internet.



Fuente: Autoría Propia

Las peticiones al servidor si tienen respuesta al validarlo por medio de un ping a la red verde: 192.168.10.1, donde no se registraron errores en las peticiones, según la Fig. 14.

Figura 14. Ping servidor 192.168.10.1



Fuente: Autoría Propia

La configuración realizada permite segmentar las zonas de red, asegurando que el tráfico solo fluya de manera controlada según las reglas establecidas, validar Fig. 15. El NAT dinámico oculta las direcciones privadas, reduciendo riesgos de exposición directa. A su vez, el reenvío de puertos brinda acceso controlado a servicios públicos en la DMZ, cumpliendo con las buenas prácticas de seguridad.

Figura 15. Ping servidor Ubuntu

Fuente: Autoría Propia

2.3 PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

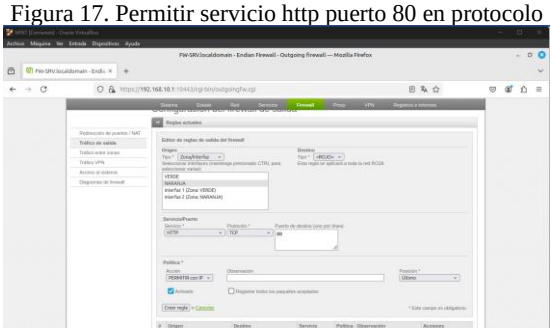
Una vez configuradas las zonas roja, naranja y verde, es posible acceder a la interfaz web de Endian desde un equipo cliente como se muestra en la Fig. 16.

Figura 16. Ingreso a la plataforma web del FW Endian

Fuente: Autoría Propia

Inicialmente, se accede al módulo Firewall, luego Servicios de salida, donde se procede a crear una regla. En esta configuración, se selecciona la interfaz naranja, el servicio HTTP, el protocolo TCP y el puerto 80.nte se ingresa al Firewall, servicios de salida, y se crea la regla, selecciona la interfaz naranja, en servicio selecciona http, en protocolo selecciona TCP y en puerto selecciona 80, como se observa en la Fig. 17.

Figura 17. Permitir servicio http puerto 80 en protocolo



Fuente: Autoría Propia

Posteriormente, se configura el servicio FTP para el servidor Ubuntu, utilizando el protocolo TCP y el puerto 21, como se ve en la Fig. 18.

Figura 18. Permitir servicio FTP en puerto 21 con protocolo TCP

Fuente: Autoría Propia

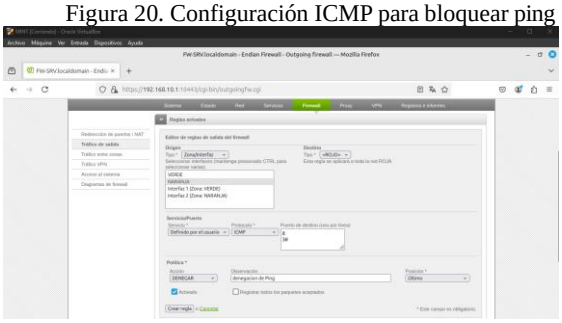
Los cambios realizados en el firewall son guardados para aplicar la configuración establecida según se aprecia en la Fig. 19.

Figura 19. Aplicación de cambios en el FW

Fuente: Autoría Propia

Mediante la siguiente regla, se deniega el protocolo ICMP, específicamente los puertos 8 y 30, con el fin de bloquear las solicitudes de ping en la red de acuerdo con la Fig. 20.

Figura 20. Configuración ICMP para bloquear ping



Fuente: Autoría Propia

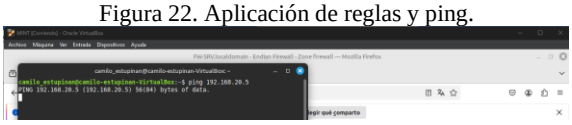
Antes de aplicar la configuración, se observa que el equipo de usuario puede realizar ping al servidor con dirección IP 192.168.20.5, según lo ilustrado en la Fig. 21.

Figura 21. Ping desde el equipo cliente al servidor.

Fuente: Autoría Propia

Una vez aplicada la configuración, se observa que ya no es posible realizar ping al servidor con la misma dirección IP, como se visualiza en la Fig. 22.

Figura 22. Aplicación de reglas y ping.



Fuente: Autoría Propia

2.4 REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO

Se configuró una VM en VirtualBox con tres interfaces: interna (verde/LAN), DMZ (naranja) y DHCP (roja/WAN). Durante la instalación de Endian UTM, el sistema detectó automáticamente las tres tarjetas de red Fig. 23.

Figura 23. Detección de adaptadores de red

Fuente: Autoría Propia

Como se observa Endian reconoce las interfaces en el orden configurado, lo que permite asignarles zonas de seguridad específicas.

2.4.1 CONFIGURACIÓN DE ZONAS DE RED

Posterior a la instalación, se accedió al portal web de administración en https://192.168.10.1:10443. Se configuraron:

- Zona verde (LAN): 192.168.10.1/24
- Zona naranja (DMZ): 192.168.20.1/24
- Zona roja (WAN): DHCP

2.4.2 REGLAS DE ACCESO HTTP Y FTP ENTRE ZONAS VERDE Y NARANJA

Para permitir HTTP (puerto 80) y FTP (puerto 21) desde LAN hacia DMZ, se creó una regla en Firewalls → Policy, seleccionando origen VERDE, destino NARANJA, y servicio HTTP. A continuación, se replicó para FTP. La Fig. 24 muestra la regla HTTP activa, según la Fig. 24.

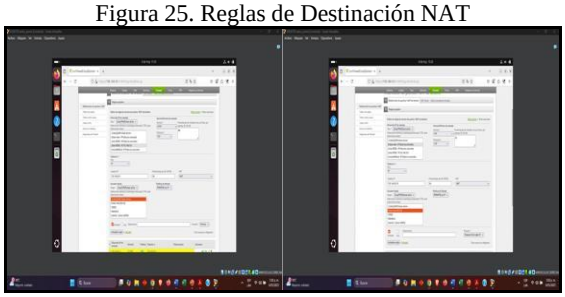
Figura 24. creación de regla de firewall

Fuente: Autoría Propia

2.4.3 DESTINACIÓN NAT

En Firewalls → Port Forwarding, se expusieron servicios internos al Internet (zona roja). Se añadieron dos reglas: HTTP entrante al servidor DMZ y FTP entrante, según la Fig. 25.

Figura 25. Reglas de Destinación NAT



Fuente: Autoría Propia

2.4.4 VERIFICACIÓN DE CONECTIVIDAD INTERZONA

Se probó el ping y acceso HTTP/FTP en varias direcciones.

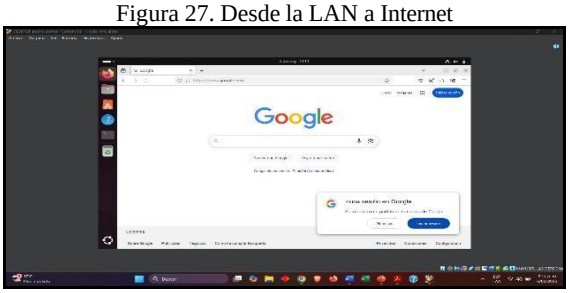
Desde LAN a DMZ: http://192.168.20.1, según la Fig. 26.

Figura 26. Detección de adaptadores de red Endian

Fuente: Autoría Propia

Desde LAN a Internet: https://www.google.com, según la Fig. 27.

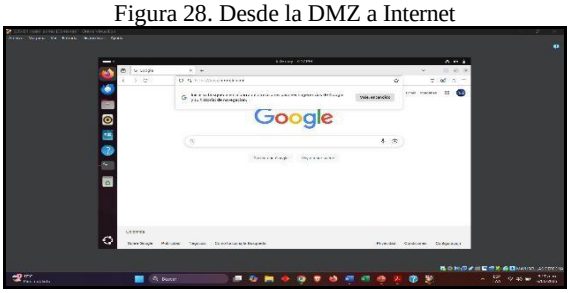
Figura 27. Desde la LAN a Internet



Fuente: Autoría Propia

Desde DMZ a Internet: https://www.google.com, según la Fig. 28.

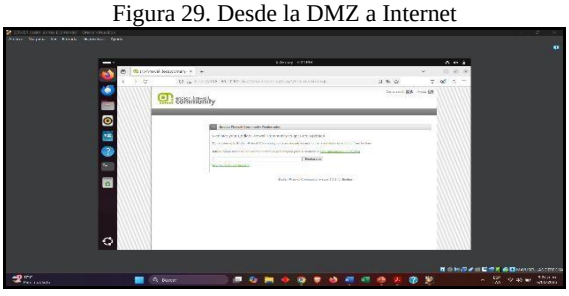
Figura 28. Desde la DMZ a Internet



Fuente: Autoría Propia

Desde WAN a DMZ: http://192.168.17.52 (IP pública asignada a WAN), según la Fig. 29.

Figura 29. Desde la DMZ a Internet



Fuente: Autoría Propia

En la LAN, se abre una terminal se ejecuta ftp ftp.gnu.org, y la conexión FTP saliente funcionara, según la Fig. 30.

Figura 30. Servicio FTP desde la LAN hacia la WAN

Fuente: Autoría Propia

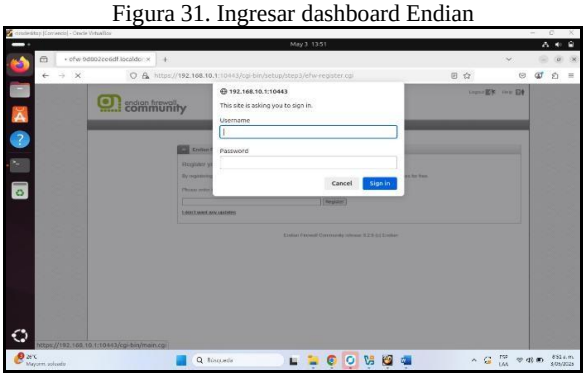
2.5 IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE) CON POLÍTICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET.

Se busca crear un perfil y establecer una lista negra que bloquee los sitios www.hotmail.com, www.youtube.com y www.elnuevodia.com.co. Además, se debe implementar la autenticación por usuario, creando un usuario y asignándolo a un grupo, estableciendo una política de acceso y vinculando esta política con el perfil creado. Finalmente, se debe probar el acceso a los sitios bloqueados desde la LAN utilizando un navegador web.

2.5.1 CONFIGURACION RED – DHCP

Posterior a la configuración de las zonas ingresamos a Endian desde Ubuntu con el navegador Firefox a la ip 192.168.10.1:10443 con el usuario y contraseña configurada en Endian Fig. 31.

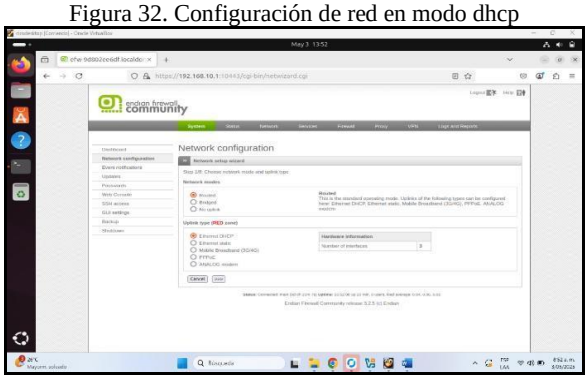
Figura 31. Ingresar dashboard Endian



Fuente: Autoría Propia

En el módulo de Network configuration y se procede a configurar RED de manera DHCP Fig. 32.

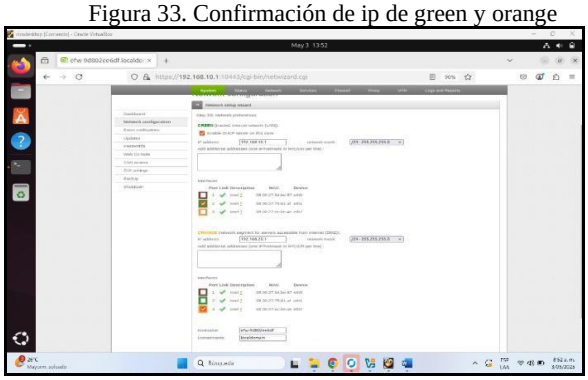
Figura 32. Configuración de red en modo dhcp



Fuente: Autoría Propia

Se realiza configuración del tipo de red para las zonas del firewall. Donde se ha seleccionado ORANGE para definir el segmento de red que será accesible desde Internet DMZ. Confirmamos las ip de GREEN 192.168.10.1 para LAN y ORANGE 192.168.20.1, según la Fig. 33.

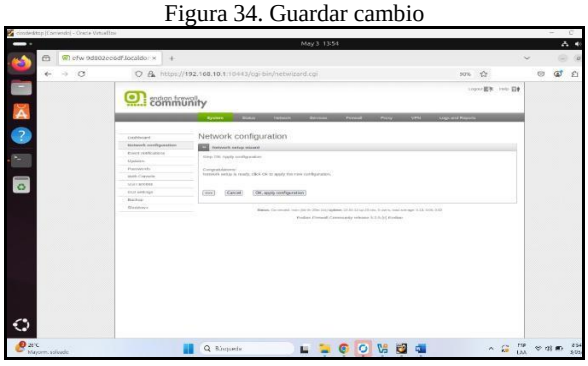
Figura 33. Confirmación de ip de green y orange



Fuente: Autoría Propia

Así mismo se realiza configuración con los DNS de Google 8.8.8.8 y 8.8.4.4 y posterior de se confirma la configuración de RED DHCP, donde se aplican los cambios y se guarda, según la Fig. 34.

Figura 34. Guardar cambio

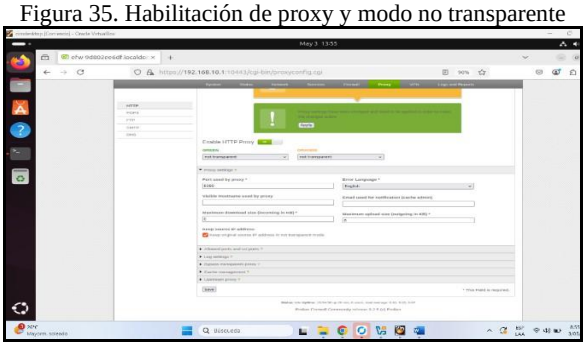


Fuente: Autoría Propia

2.5.2 AUTENTICACIÓN POR USUARIO

Ahora en el módulo de Proxy, en el submódulo de Autenticación, en el botón de manage users. Posterior se habilita el módulo de Proxy y activamos la autenticación por usuario, según la Fig. 35.

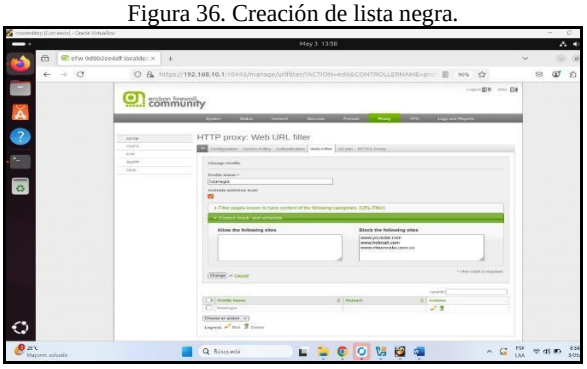
Figura 35. Habilitación de proxy y modo no transparente



Fuente: Autoría Propia

Se crea un nuevo filtro con el nombre listanegra, donde se bloquea 3 páginas, www.hotmail.com, www.youtube.com, www.elnuevodia.com.co se aplica y guardar cambios, según la Fig. 36.

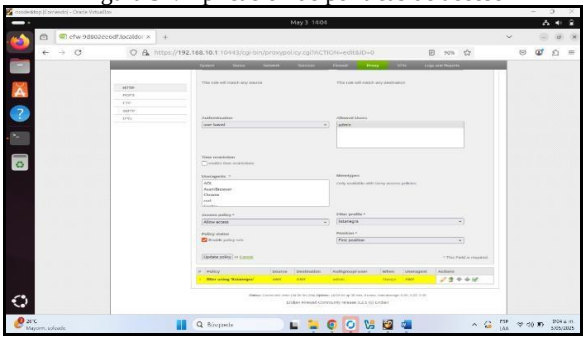
Figura 36. Creación de lista negra.



Fuente: Autoría Propia

Se configura una política de acceso donde se asocia el usuario admin, se aprueba la regla que se crea llamada listanegra y se termina la demás configuración, según la Fig. 37.

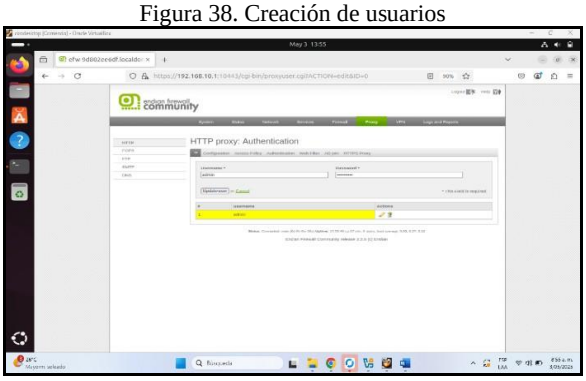
Figura 37. Aplicación de políticas de acceso



Fuente: Autoría Propia

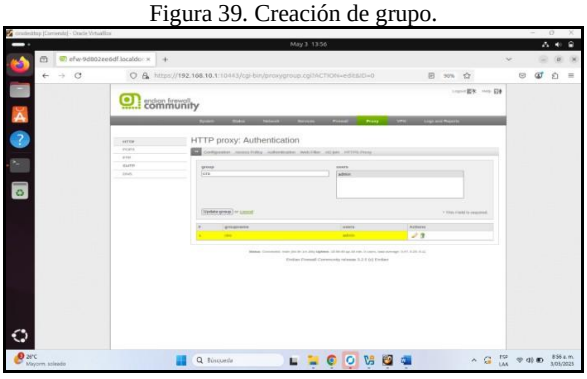
Se crea un usuario llamado admin Fig. 38 y un grupo personalizado llamado "ciro", asociando ese usuario al grupo. Esto permite aplicar filtros y reglas específicas a los usuarios autenticados, según la Fig. 39.

Figura 38. Creación de usuarios



Fuente: Autoría Propia

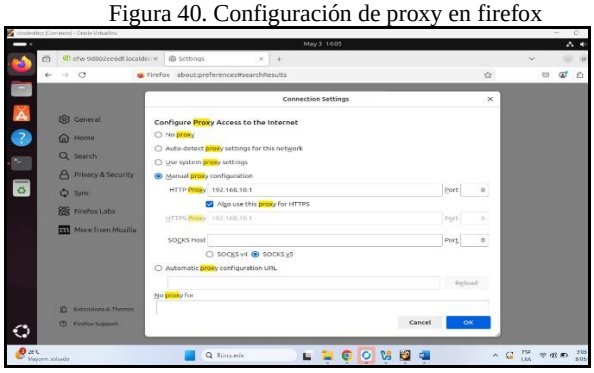
Figura 39. Creación de grupo.



Fuente: Autoría Propia

Ahora en la configuración de proxy en el navegador Firefox y manualmente se configura el Proxy donde se coloca 192.168.10.1 y se configura para usar el mismo proxy en HTTPS, como se observa en la Fig. 40.

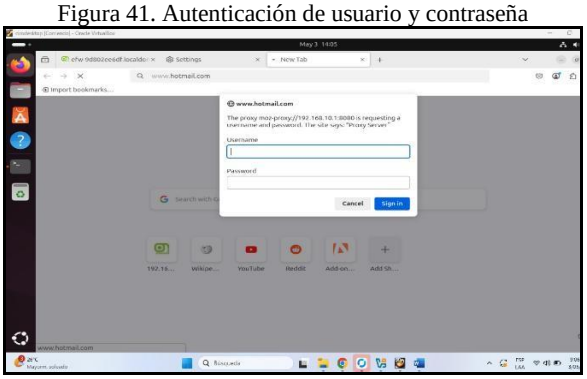
Figura 40. Configuración de proxy en firefox



Fuente: Autoría Propia

Se intenta ingresar a www.hotmail.com y pide autenticación de usuario, según la Fig. 41

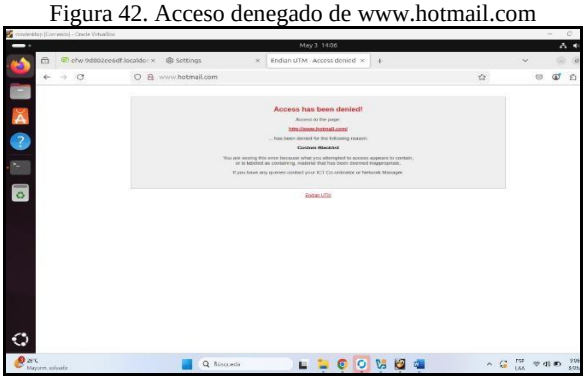
Figura 41. Autenticación de usuario y contraseña



Fuente: Autoría Propia

Posterior muestra un mensaje de acceso denegado, según la Fig. 42.

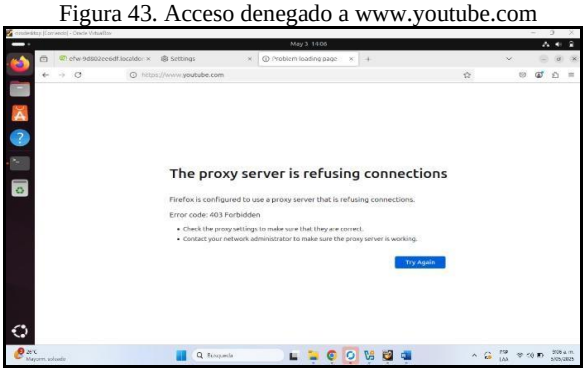
Figura 42. Acceso denegado de www.hotmail.com



Fuente: Autoría Propia

De igual forma se intenta ingresar a www.youtube.com y muestra el siguiente mensaje, según la Fig. 43.

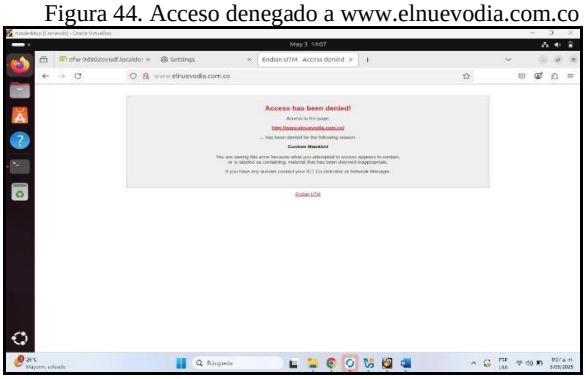
Figura 43. Acceso denegado a www.youtube.com



Fuente: Autoría Propia

Por último, se intenta ingresar a www.elnuevodia.com.co y sale el mensaje también, según la Fig. 44.

Figura 44. Acceso denegado a www.elnuevodia.com.co



Fuente: Autoría Propia

3 CONCLUSIONES.

La segmentación de red con UTM Endian y VirtualBox facilita la gestión de políticas de seguridad. La implementación demostró eficacia en el control de servicios y autenticación de usuarios, reforzando la protección de infraestructuras en entornos GNU/Linux

Dividir una infraestructura de red en segmentos distintos es clave para garantizar su seguridad y eficiencia operativa. Organizar la red en áreas específicas, tales como LAN y DMZ, y aplicar políticas de acceso detalladas, asegura que los sistemas internos estén resguardados contra accesos no autorizados, mientras que permite un acceso controlado a servicios externos, como los servidores web.

La configuración de NAT y servicios de red en Linux es fundamental para garantizar la conectividad y seguridad en entornos de red. A través de este trabajo, se evidenció la importancia de definir correctamente las reglas de NAT para permitir la comunicación entre redes (LAN, WAN y DMZ), así como los desafíos que surgen cuando las configuraciones no son precisas, como la pérdida de paquetes o la imposibilidad de acceder a Internet. Este ejercicio reforzó el manejo de herramientas como iptables y la necesidad de validar cada paso para asegurar el correcto enrutamiento del tráfico.

Los errores en la configuración de NAT y firewall son oportunidades de aprendizaje. Durante el ejercicio, la imposibilidad de acceder a Internet desde la red LAN (pese a la configuración de NAT) evidenció la importancia de revisar meticulosamente cada componente: desde las reglas de iptables hasta las políticas del firewall (como se observó en Endian Firewall). Este fallo permitió identificar que, más allá de aplicar las reglas correctamente, es crucial verificar:

- El enrutamiento entre interfaces (LAN, WAN y DMZ).
- Las políticas de firewall que podrían estar bloqueando el tráfico de salida.
- La asignación de direcciones IP y puertos en el reenvío NAT.

4 REFERENCIAS

[1] Canonical. (2023). Guía del Ubuntu Desktop 20.04 LTS. Disponible en: https://help.ubuntu.com/20.04/ubuntu-help/index.html

[2] Debian (2023). El manual del administrador de Debian 12.5.0. Disponible en: https://www.debian.org/releases/stable/amd64/index.es.html

[3] Endian. (2016). Endian UTM 3.2 manual referencia. Disponible en: http://docs.endian.com/3.2/utm/index.html

[4] LaCroix, J. (2016). Mastering Ubuntu Server. Packt Publishing Ltd.

[5] Linux Professional Institute (LPI). (2022). Tema 102: Comandos GNU y Unix. Disponible en: https://learning.lpi.org/es/learning-materials/101- 500/102/

[6] Oracle. (2020). Manual de usuario VirtualBox. Disponible en: https://www.virtualbox.org/manual/

[7] Stover, S. (2021). Network security with depth. Journal of Information Security, 8(3), 15–27.

[8] Rodriguez, A. (2019). Configuring DMZ for secure web services. En Proceedings of the International Conference on Network Security (pp. 102–108).

[9] Smith, B. (2018). Implementing NAT in enterprise networks. IEEE Communications Magazine, 57(4), 34–40.

[10] Johnson, C. (2017). Proxy authentication techniques. ACM Transactions on Internet Technology, 18(1), 1–12.