IMPLEMENTACIÓN DE SEGURIDAD PERIMETRAL EN RED CON ENDIAN UTM Y VIRTUALIZACIÓN EN GNU/LINUX

Edison Estiven Salguero Enciso
e-mail: eesalgueroe@unadvirtual.edu.co
Germán Ricardo Correa Amaya
e-mail: grcorreaa@unadvirtual.edu.co
Richard Alexander Ramirez basto
e-mail: raramirezba@unadvirtual.edu.co
Segundo Enrique Pantoja Diaz
e-mail: sepantojad@unadvirtual.edu.co
Brandon Felipe Tauta Lesmes
e-mail: bftautal@unadvirtual.edu.co

RESUMEN: *La seguridad perimetral de redes es un aspecto crucial en la protección de infraestructuras IT. Este proyecto tiene como objetivo garantizar la protección de servidores dentro de una intranet (LAN) y extranet (WAN) mediante la configuración de una zona DMZ utilizando Endian UTM. La implementación de un firewall Endian, junto con la gestión de acceso mediante políticas, garantiza una comunicación segura entre las zonas de la red. Los pasos incluyen la configuración de NAT, la habilitación de servicios en la zona DMZ, y la implementación de un proxy HTTP con autenticación para filtrar el tráfico hacia la web.*

PALABRAS CLAVE: Seguridad perimetral, Red DMZ, Endian, Firewall, GNU/Linux.

ABSTRACT: *Network perimeter security is a crucial aspect of IT infrastructure protection. This project aims to ensure the protection of servers within an intranet (LAN) and extranet (WAN) by configuring a DMZ zone using Endian UTM. The implementation of an Endian firewall, together with policy-based access management, ensures secure communication between network zones. Steps include configuring NAT, enabling services in the DMZ, and implementing an HTTP proxy with authentication to filter traffic to the web.*

KEY WORDS: Perimeter Security, DMZ Network, Endian, Firewall, GNU/Linux.

1. INTRODUCCIÓN

En el contexto de la seguridad de redes, la protección de los servidores que conforman la intranet y extranet de una organización es fundamental. Este proyecto busca la implementación de una solución de seguridad integral utilizando Endian UTM, una plataforma basada en GNU/Linux que permite configurar y gestionar un firewall de manera eficiente. La propuesta abarca la segmentación de la red en zonas seguras, la configuración de acceso mediante políticas, y la implementación de un proxy HTTP que permita controlar el tráfico hacia la web. Este enfoque mejora la seguridad y la integridad de las bases de datos y aplicaciones de la red.

2. INSTALACIÓN ENDIAN 3.3.2

2.1 CARACTERÍSTICAS GENERALES

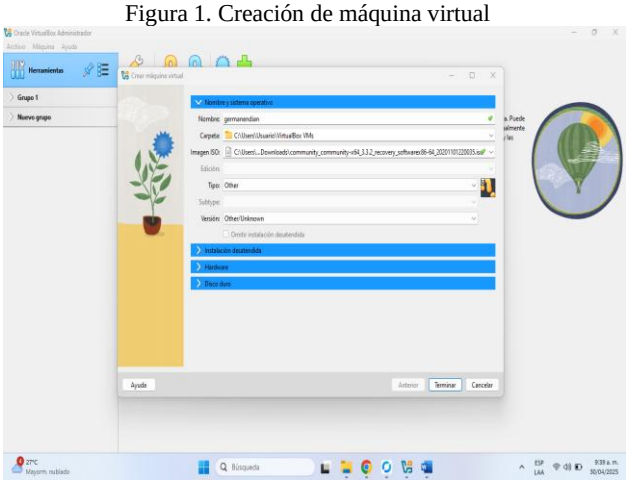
En primer lugar se descarga la distribución de Endian UTM desde su sitio oficial y se instala en plataformas como VirtualBox o en hardware físico como se observa en la figura 1. Es compatible con arquitecturas x86.

Se utiliza el programa Oracle VM VirtualBox para la creación de una máquina virtual con las siguientes configuraciones:

- Tipo: Linux
- Versión: Oracle Linux (64 bit)
- Unidad óptica virtual: ISO

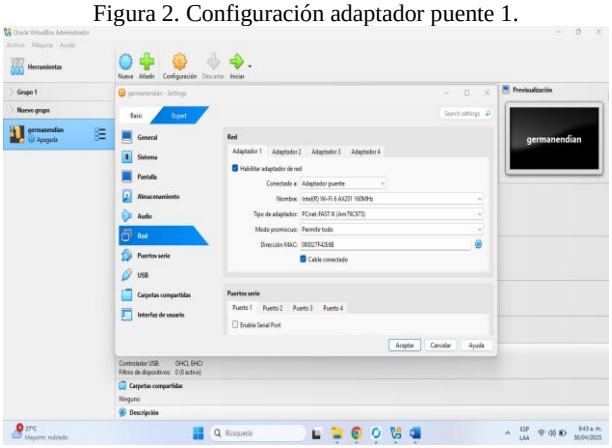
2.2 INSTALACIÓN

Figura 1. Creación de máquina virtual



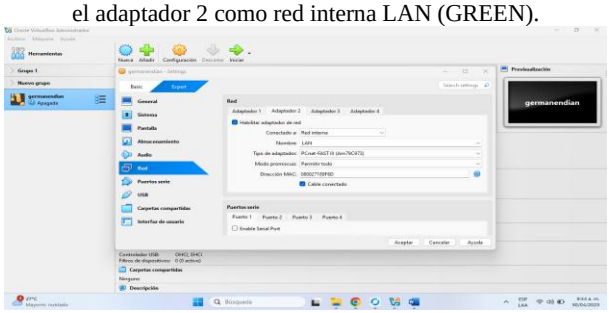
Fuente: Imagen de Autoría propia

Figura 2. Configuración adaptador puente 1.



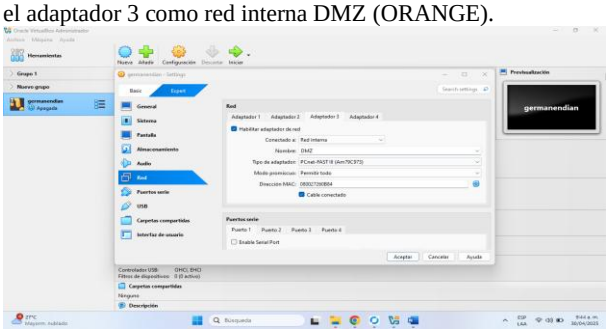
Fuente: Imagen de Autoría propia

Figura 3. Configuración de adaptador puente 2. Configuramos el adaptador 2 como red interna LAN (GREEN).



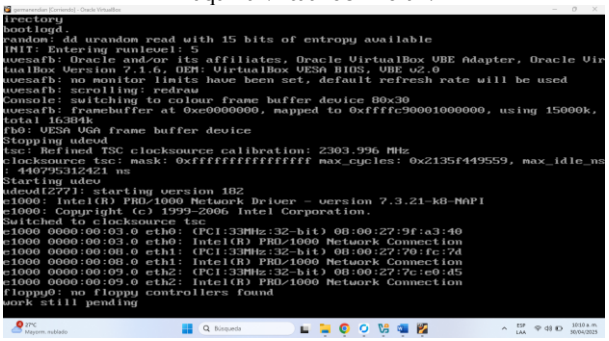
Fuente: Imagen de Autoría propia

Figura 4. Configuración de adaptador puente 3. Configuramos el adaptador 3 como red interna DMZ (ORANGE).



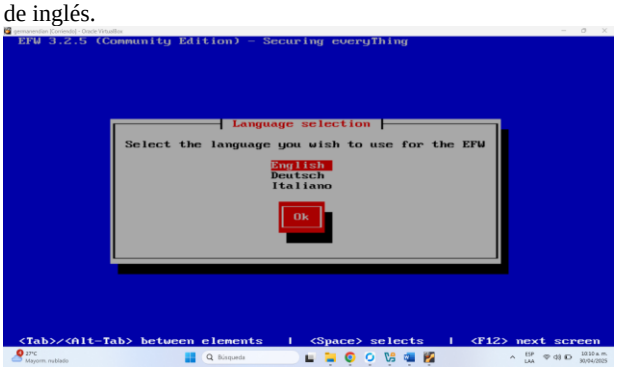
Fuente: Imagen de Autoría propia

Figura 5. Iniciamos la máquina virtual de Endian. Iniciamos la máquina virtual de Endian.



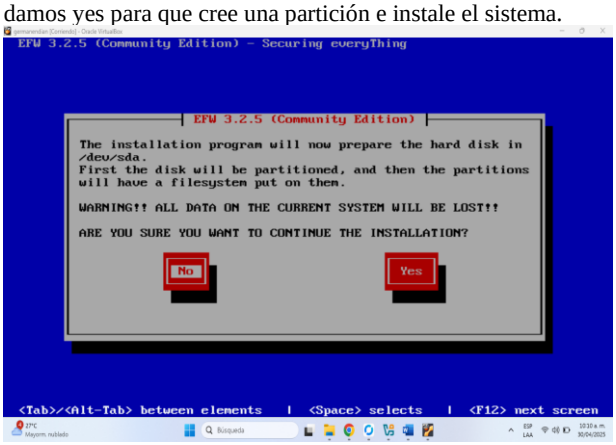
Fuente: Imagen de Autoría propia

Figura 6. Escogemos el idioma de inglés. Escogemos el idioma de inglés.



Fuente: Imagen de Autoría propia

Figura 7. Creamos partición para instalación del sistema le damos yes para que cree una partición e instale el sistema.



Fuente: Imagen de Autoría propia

Figura 8. Negamos la habilitación de puerto serial. Seleccionamos "No" porque no necesitamos habilitar el acceso al firewall a través de un puerto serial.

Fuente: Imagen de Autoría propia

Figura 9. Establecimiento de ip GREEN.Establecemos la ip y la máscara de (GREEN)

Fuente: Imagen de Autoría propia

Figura 10. Evidencia de inicio de Endian. De forma exitosa pudimos iniciar Endian, donde nos muestra la ip de (GREEN)

Fuente: Imagen de Autoría propia

3. DESARROLLO TEMATICAS

3.1 TEMÁTICA 1.

La temática desarrollada aborda la configuración e implementación de GNU/Linux Endian Firewall en un entorno virtualizado utilizando VirtualBox, orientada a establecer una infraestructura de red segura con segmentación adecuada. Se configuraron las tres zonas fundamentales: Verde (LAN), Roja (WAN) y Naranja (DMZ), asignando a cada una un rango IP específico y adaptadores de red virtuales según las buenas prácticas de seguridad perimetral.

El proceso incluyó la descarga y preparación de la ISO, instalación del sistema, asignación de las interfaces de red, y puesta en marcha de los servicios esenciales del firewall. Asimismo, se realizaron pruebas de conectividad y validación del flujo de tráfico entre las distintas zonas y hacia Internet, garantizando la correcta operatividad y segmentación.

Como parte del proceso, se configuraron reglas específicas para permitir el tráfico HTTP desde la zona verde hacia la zona naranja, como se muestra en la Figura 11. Esta configuración es clave para controlar el acceso entre zonas y aplicar políticas de seguridad granular.

Esta experiencia proporciona una base práctica para fortalecer el conocimiento en administración de redes y seguridad informática en entornos controlados.

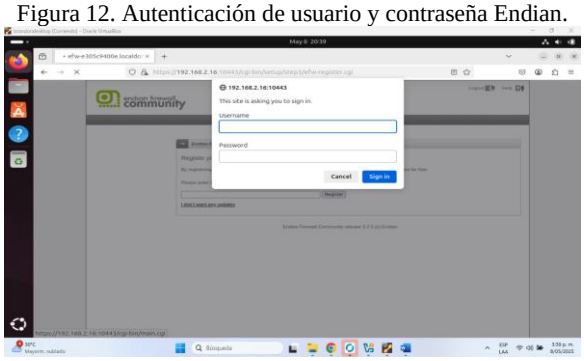
Figura 11 Configuración reglas zona verde a naranja HTTP

Fuente: Imagen de Autoría propia

3.2 TEMÁTICA 2: CONFIGURACIÓN NAT.

La temática desarrollada muestra cómo configurar adecuadamente las reglas de NAT (Traducción de Direcciones de Red) en el firewall Endian asegurándose de que las máquinas en la red puedan acceder a Internet de manera controlada. Esto incluye la configuración de direcciones IP estáticas y la creación de reglas de Source NAT para que el tráfico desde la red interna pueda salir a la red externa.

Figura 12. Autenticación de usuario y contraseña Endian.



Fuente: Autoría propia

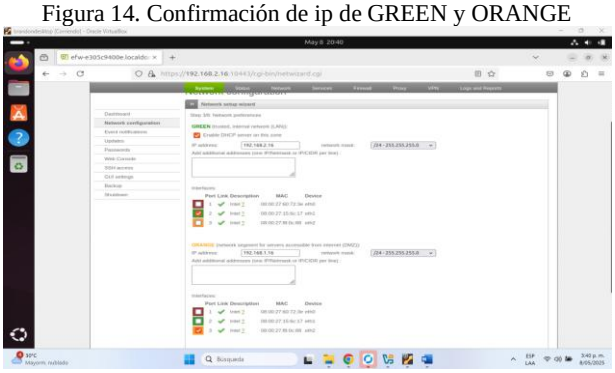
Abrimos Firefox y colocamos https://192.168.2.16:10443 para acceder a Endian, ver figura 12.

Figura 13. Configuración de RED en modo DHCP.

Fuente: Autoría propia

Confirmamos la configuración de RED (WAN) como se observa en la figura 13.

Figura 14. Confirmación de ip de GREEN y ORANGE



Fuente: Autoría propia

Igualmente, para LAN y DMZ que tengan las ip correctamente configuradas, ver figura 14.

Figura 15. Confirmación de configuración de RED en DHCP.

Fuente: Autoría propia

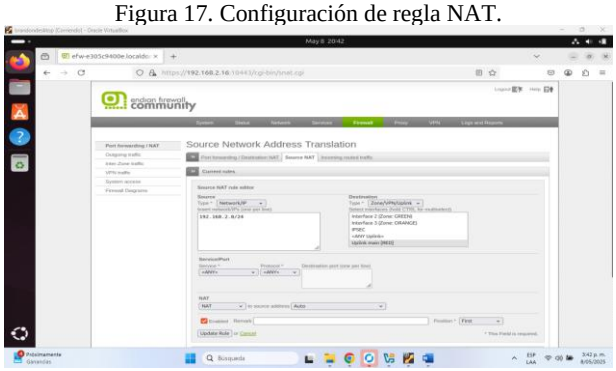
Igualmente, que WAN está en el puerto eth0, ver figura 15.

Figura 16. Ingresamos al módulo firewall.

Fuente: Autoría propia (Brandon)

Nos vamos al módulo de Firewall – Source NAT (figura 16) y le damos en el botón de añadir un nuevo NAT

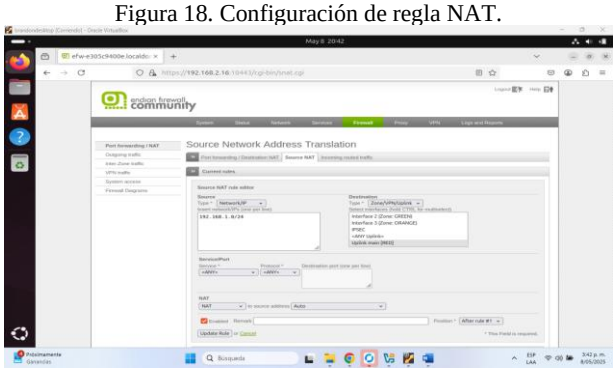
Figura 17. Configuración de regla NAT.



Fuente: Autoría propia

Se configuró una regla de Source NAT(figura 17) para permitir que el tráfico de la red GREEN (LAN) acceda a Internet a través de la red RED (WAN).

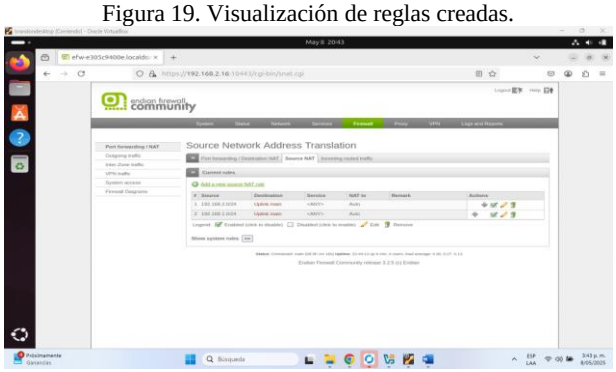
Figura 18. Configuración de regla NAT.



Fuente: Autoría propia

Se configuró una regla de Source NAT para la red ORANGE (DMZ)(figura18), permitiendo que el tráfico de la red 192.168.1.0/24 se enmascare y salga hacia la interfaz RED (WAN). Esto habilita que la red DMZ tenga acceso a Internet a través de la red externa.

Figura 19. Visualización de reglas creadas.



Fuente: Autoría propia

De manera correcta visualizamos que las creaciones fueron exitosas y están guardadas como se observa en la figura 19.

Figura 20. Visualización de ping exitoso desde GREEN.

Fuente: Autoría propia

Se muestra que Desktop ha realizado con éxito un ping a 8.8.8.8, lo que significa que la máquina tiene acceso a Internet y la configuración de NAT en Endian para permitir la salida a la WAN desde la red GREEN está funcionando correctamente, ver figura20.

3.3 TEMÁTICA 3: PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED.

El desarrollo de la temática a presentar aborda la implementación de políticas de filtrado en GNU/Linux Endian Firewall para optimizar la seguridad y garantizar la disponibilidad de servicios críticos en la zona DMZ. Se establecieron reglas específicas para permitir el acceso a HTTP (Puerto 80) y FTP (Puerto 21) en un servidor Web basado en Ubuntu, asegurando un tráfico controlado. A la vez, se bloqueó el tráfico ICMP (Eco – Tipo 8 y Tipo 30) con el fin de impedir intentos de reconocimiento y posibles ataques, lo cual se verificó mediante pruebas de ping con 100% de pérdida desde la zona Verde. La validación se llevó a cabo analizando los contadores de iptables y monitoreando el tráfico, lo que confirmó la efectividad de las reglas aplicadas. Esta experiencia resalta la relevancia de un filtrado granular y coherente en entornos virtualizados para fortalecer la resiliencia y seguridad de la infraestructura de red.

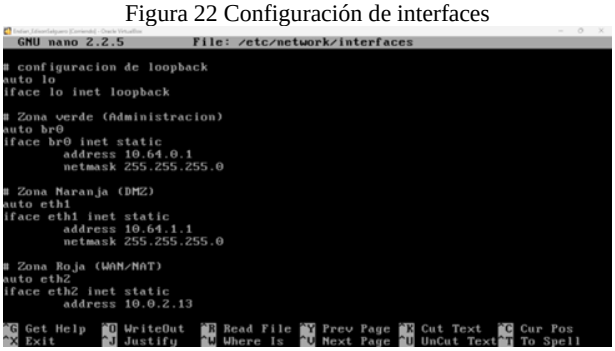
Instalación correcta e inicio de Endian, (ver figura 21) se puede ver la configuración de la ip de (GREEN)

Figura 21 Evidencia de instalación

Fuente: Imagen de Autoría propia

Se realiza la configuración de Interfaces en Endian, para gestionar las zonas (ver figura 22) dependiendo del rango de direcciones seleccionadas.

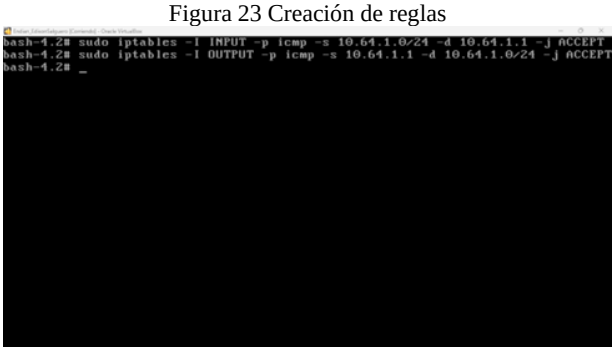
Figura 22 Configuración de interfaces



Fuente: Imagen de Autoría propia

Existe una regla que bloquea ICMP, por lo que se debe crear una excepción para que el tráfico ICMP desde la red DMZ pueda ser procesado, permitiendo ICMP entrante desde DMZ y saliente hacia la DMZ (ver figura 23).

Figura 23 Creación de reglas



Fuente: Imagen de Autoría propia

Ahora, para permitir los servicios HTTP (Puerto 80) y FTP (Puerto 21) desde el servidor Web bajo Ubuntu Server vamos a aplicar las reglas de firewall en Endian, el cual actúa como firewall y router para la infraestructura y eso lo aplicaremos con iptables para definir las reglas en la cadena FORWARD la cual se encarga del tráfico que atraviesa el firewall (ver figura 24).

Figura 24. Permitir HTTP (puerto 80) y Permitir FTP (puerto 21) con iptables.

Fuente: Imagen de Autoría propia

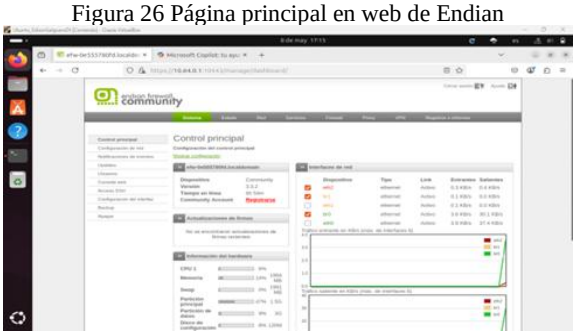
Para denegar el protocolo ICMP (Puerto 8 y puerto 30) para no permitir hacer ping en la red (ver figura 25) y probar a través de una consola o terminal la no respuesta del comando ping hacia una IP de la red, se pueden configurar las reglas de iptables para Bloquear ICMP de Tipo 8 y Tipo 30.

Figura 25.Creacion de reglas

Fuente: Imagen de Autoría propia

Aquí podemos evidenciar la conexión desde la zona verde con ENDIAN después de las configuraciones y se evidencia que la DMZ está activa también (ver figura 26).

Figura 26 Página principal en web de Endian



Fuente: Imagen de Autoría propia

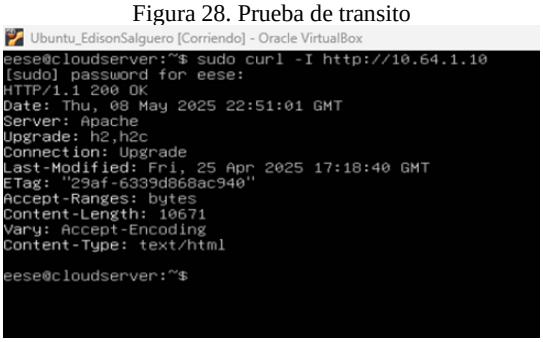
Aunque creamos las reglas desde el BASH de ENDIAN, replicamos estas mismas reglas desde GUI de ENDIAN (ver figura 27) y las aplicamos

Figura 27 Creación de reglas en GUI

Fuente: Imagen de Autoría propia

Desde Ubuntu Server (ver figura 28) se puede ver una respuesta HTTP con código 200 OK en los encabezados, lo que indica que el tráfico HTTP (puerto 80) está permitido.

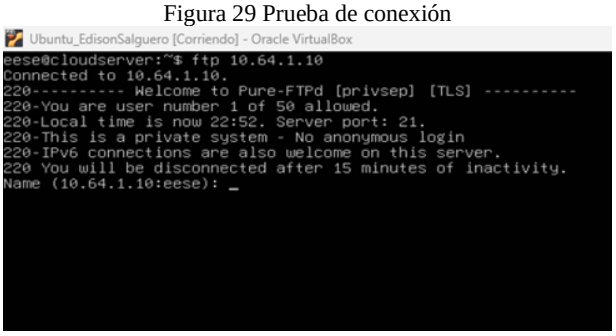
Figura 28. Prueba de transito



Fuente: Imagen de Autoría propia

Desde Ubuntu Server (ver figura 29) se puede ver que la conexión se establece, confirmando que el tráfico FTP en puerto 21 es permitido.

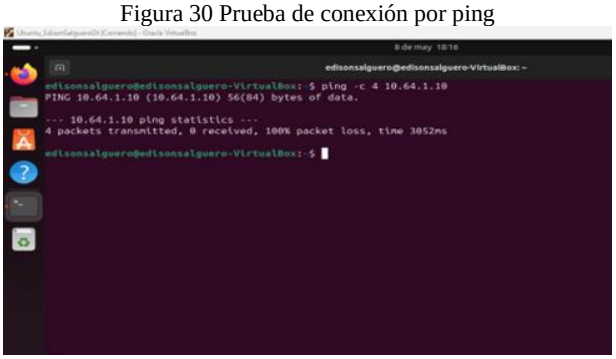
Figura 29 Prueba de conexión



Fuente: Imagen de Autoría propia

Desde el host Ubuntu Desktop (ver figura 30) que se encuentra en la red (zona Verde) se ejecuta un ping a la IP del servidor que se encuentra en la (zona Naranja) la salida muestra el 100% de paquetes perdidos, lo que indica que no hay respuesta a los paquetes de tipo Echo Request (ICMP Tipo 8) y también para (Tipo 30) lo que muestra se está bloqueando el ICMP.

Figura 30 Prueba de conexión por ping



Fuente: Imagen de Autoría propia

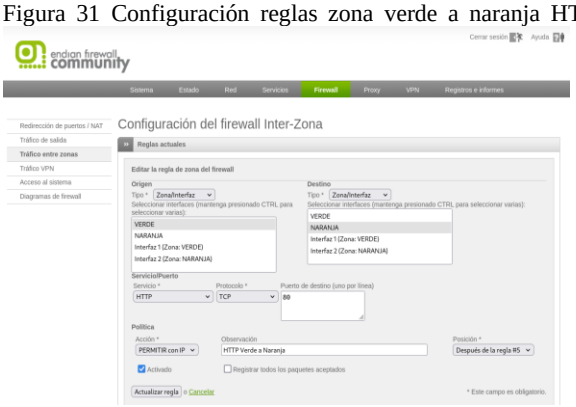
3.4 TEMÁTICA 4: REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO.

En arquitecturas de red segmentadas, como las gestionadas mediante plataformas tipo Endian Firewall, las reglas de acceso son esenciales para definir y controlar el flujo de tráfico entre zonas de seguridad diferenciadas, tales como la

red interna (VERDE), la zona desmilitarizada (DMZ o NARANJA), la red externa (ROJA/WAN) e Internet. Estas reglas permiten establecer políticas de acceso estrictas que aseguran la funcionalidad de los servicios sin comprometer la integridad ni la confidencialidad del sistema.

Por ejemplo, la habilitación del tráfico HTTP desde la zona VERDE hacia la NARANJA se efectúa mediante la definición de reglas que especifican el origen, destino, protocolo y puerto involucrado (TCP/80). Estas reglas se configuran utilizando criterios como "Zona/Interfaz" y acciones de tipo "PERMITIR con IP", con descripciones explícitas como “HTTP Verde a Naranja”, lo que facilita su gestión y auditoría como se muestra en la (Figura 31).

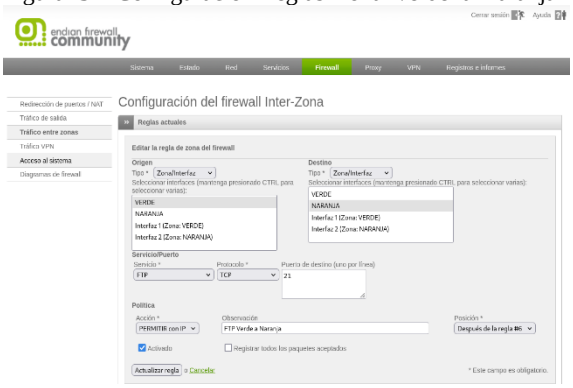
Figura 31 Configuración reglas zona verde a naranja HTTP



Fuente: Imagen de Autoría propia

Del mismo modo, se configura una regla análoga para el tráfico FTP (TCP/21) desde la zona VERDE hacia la NARANJA, siguiendo el principio de segmentación segura y defensa en profundidad. La descripción “FTP Verde a Naranja” permite identificar rápidamente la política implementada como se aprecia en la (Figura 32).

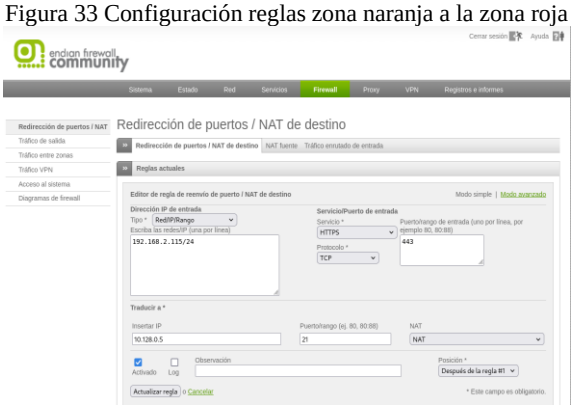
Figura 32 Configuración reglas zona verde a naranja FTP



Fuente: Imagen de Autoría propia

En sentido inverso, se habilita el tráfico saliente desde la zona NARANJA hacia Internet, autorizando únicamente protocolos específicos como HTTPS (TCP/443), con la descripción “Internet con ZONA-NARANJA”. Esta configuración posibilita, por ejemplo, actualizaciones seguras desde los servidores en la DMZ hacia repositorios externos como se observa en la (figura 33).

Figura 33 Configuración reglas zona naranja a la zona roja



Fuente: Imagen de Autoría propia

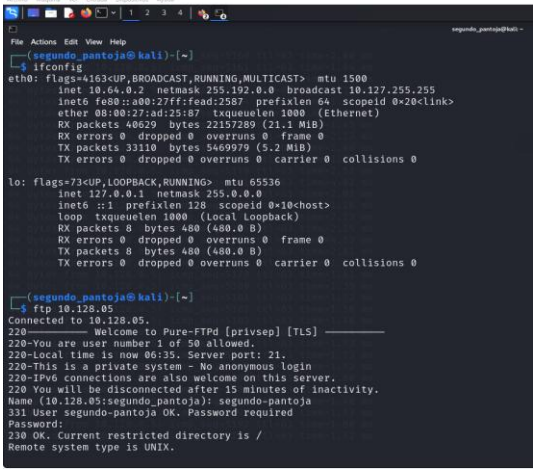
La gestión del tráfico entrante desde la red ROJA hacia la DMZ también se realiza bajo reglas de redirección y NAT, tales como el acceso al puerto 8080 de un servidor web en la DMZ. Esta regla, priorizada en el procesamiento, permite mantener el aislamiento de la zona VERDE mientras se habilita el acceso controlado desde el exterior ver (figura 34).

Figura 34 Configuración reglas zona roja a la zona naranja

Fuente: Imagen de Autoría propia

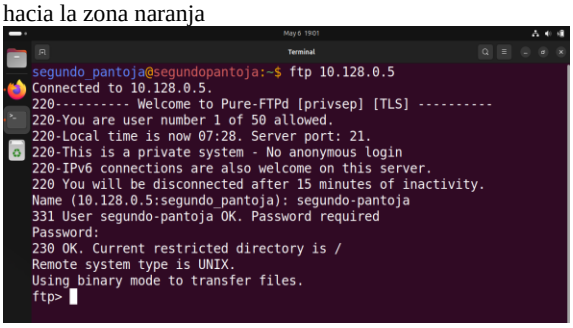
Para validar las reglas del firewall, se realizaron pruebas de conectividad desde distintas zonas utilizando sistemas específicos: Desde un cliente virtual Kali Linux en la zona VERDE (LAN), se verificó el acceso a servicios web en la DMZ mediante comandos curl y ping (Figura 35); Una maquina virtua Ubuntu Focal Fossa en la zona ROJA (WAN) estableció conexión FTP exitosa hacia la DMZ, demostrando la correcta aplicación de las políticas de redirección (Figura 36); y desde el mismo host Ubuntu Focal Fossa se accedió al servicio phpMyAdmin instalado en el servidor Kali Linux de la DMZ mediante HTTP (Figura 37), confirmando que las reglas NAT permiten accesos controlados desde redes externas sin comprometer la seguridad interna. Estas pruebas evidencian que la segmentación de redes opera según lo diseñado, manteniendo el aislamiento de la zona VERDE mientras habilita comunicaciones seguras con la DMZ

Figura 35 Ejecución de comandos ftp y curl desde la zona verde hacia la zona naranja



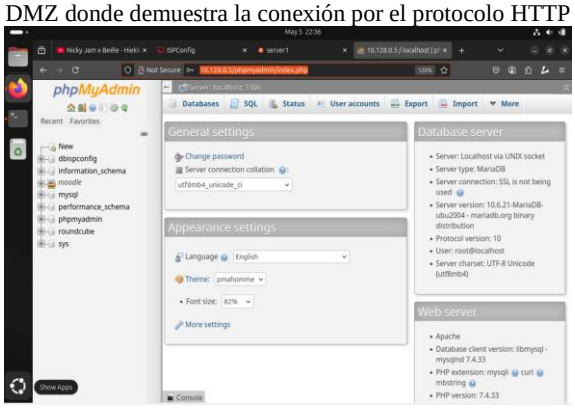
Fuente: Imagen de Autoría propia

Figura 36 Ejecucion del conmandos ftp desde la zona roja hacia la zona naranja



Fuente: Imagen de Autoría propia

Figura 37 Acceso a phpmyadmin desde la zona roja hacia la DMZ donde demuestra la conexión por el protocolo HTTP

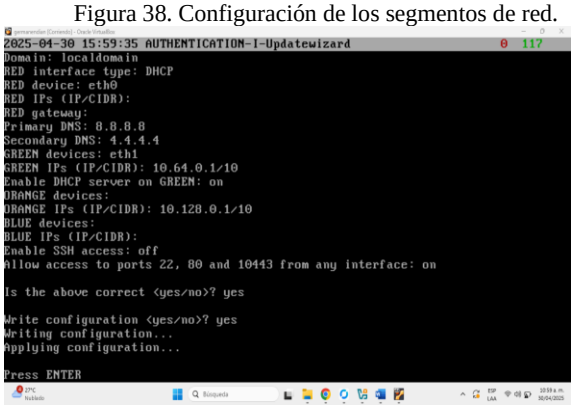


Fuente: Imagen de Autoría propia

3.5 TEMÁTICA 5: IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE) CON POLÍTICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET.

Producto esperado: El producto esperado consiste en 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 asignándole 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.

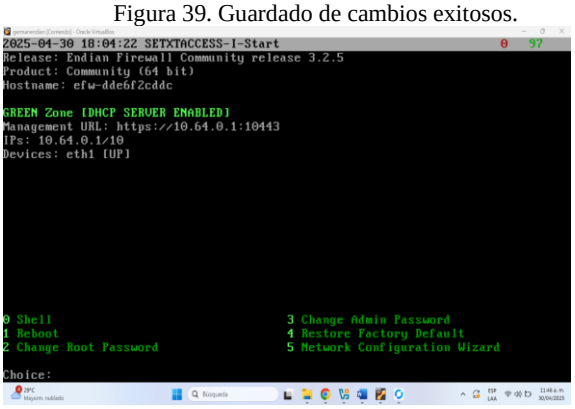
Figura 38. Configuración de los segmentos de red.



Fuente: Imagen de Autoría propia

Como se muestra en la figura 38 configuramos las zonas de manera correcta, teniendo en cuenta que RED = DHCP, GREEN = 10.64.0.1/10 y ORANGE = 10.128.0.1/10

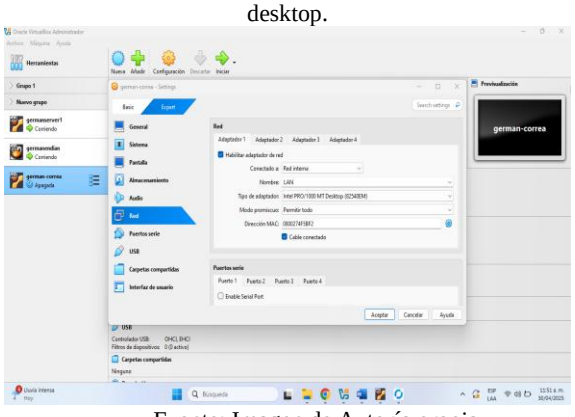
Figura 39. Guardado de cambios exitosos.



Fuente: Imagen de Autoría propia

Como se muestra en la figura 39 guardamos los cambios.

Figura 40. Configuración de adaptador 1, Ubuntu desktop.



Fuente: Imagen de Autoría propia

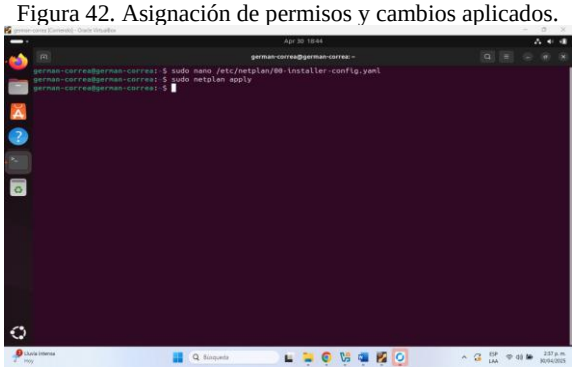
Como se muestra en la figura 40 abrimos la configuración de red de Ubuntu desktop y configuramos en adaptador 1 con red interna y con el nombre LAN (GREEN).

Fuente 41. Configuración de ip estática en Ubuntu desktop.

Fuente: Imagen de Autoría propia

Como se muestra en la figura 41 entramos en desktop y en 00-installer.config.yaml configuramos la ip estática 10.64.0.2/10.

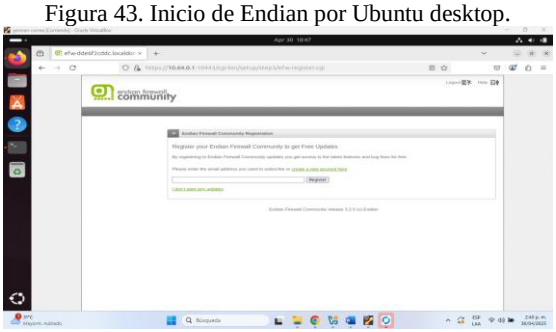
Figura 42. Asignación de permisos y cambios aplicados.



Fuente: Imagen de Autoría propia

Como se muestra en la figura 42 establecemos los permisos 600 al 00-installer-config y aplicamos cambios a Netplan.

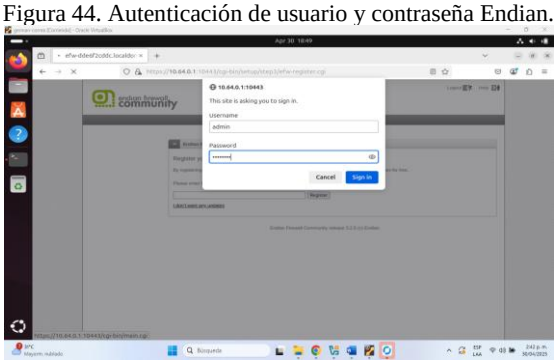
Figura 43. Inicio de Endian por Ubuntu desktop.



Fuente: Imagen de Autoría propia

Como se muestra en la figura 43 entramos en Firefox y con la ip de GREEN https://10.64.0.1:10443 entramos a Endian.

Figura 44. Autenticación de usuario y contraseña Endian.



Fuente: Imagen de Autoría propia

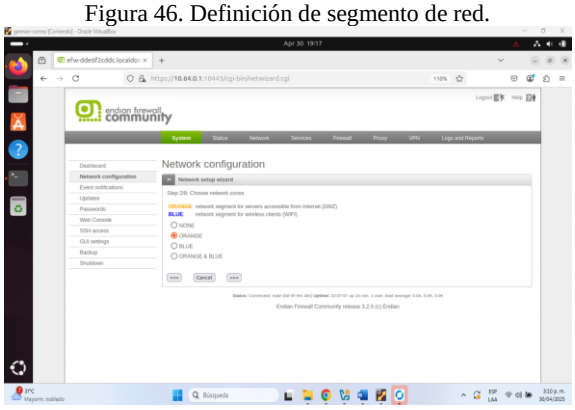
Como se muestra en la figura 44 nos pide usuario y contraseña y le damos en sing in para poder ingresar

Figura 45. Configuración de RED en modo DHCP.

Fuente: Imagen de Autoría propia

Como se muestra en la figura 45 Nos dirigimos al módulo de Network configuración y procedemos a configurar RED de manera DHCP

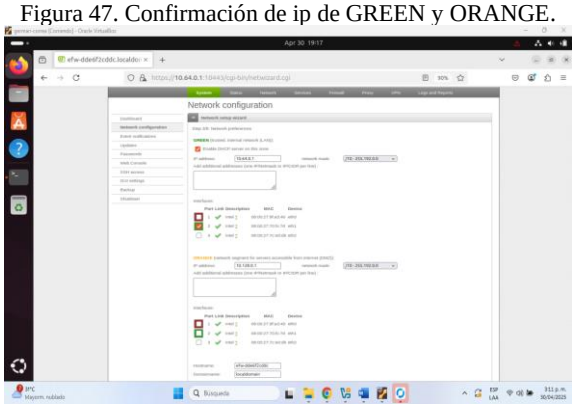
Figura 46. Definición de segmento de red.



Fuente: Imagen de Autoría propia

Como se muestra en la figura 46. En este paso, se está configurando el tipo de red para las zonas del firewall. Se ha seleccionado ORANGE para definir el segmento de red que será accesible desde Internet (DMZ).

Figura 47. Confirmación de ip de GREEN y ORANGE.



Fuente: Imagen de Autoría propia

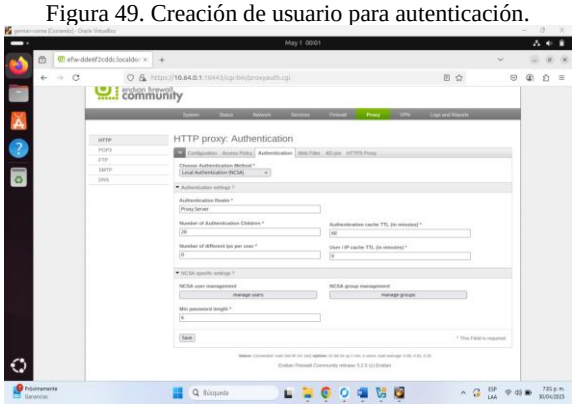
Como se muestra en la figura 47 Confirmamos las ip de GREEN (10.64.0.1 (eth1)) y ORANGE (10.128.0.1(eth2)).

Figura 48. Confirmación de configuración de RED en DHCP.

Fuente: Imagen de Autoría propia

Como se muestra en la figura 48. Confirmamos RED (DHCP (eth0)).

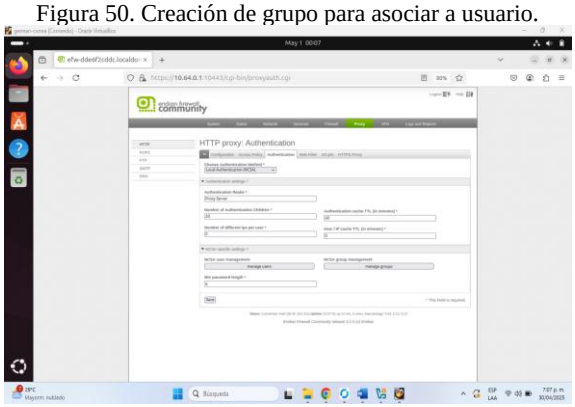
Figura 49. Creación de usuario para autenticación.



Fuente: Imagen de Autoría propia

Como se muestra en la figura 49. Nos dirigimos al módulo de Proxy, en el submódulo de Autenticación y le damos en el botón de manage users, para crear un usuario para autenticarse.

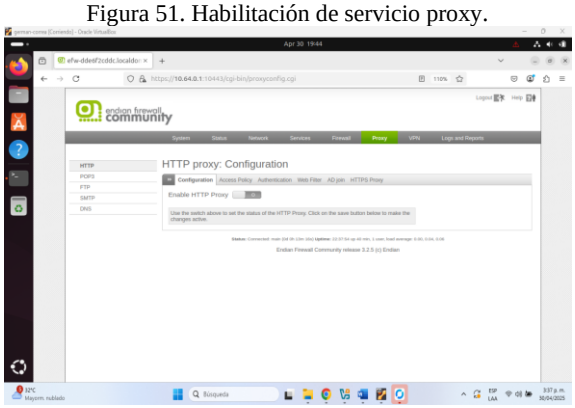
Figura 50. Creación de grupo para asociar a usuario.



Fuente: Imagen de Autoría propia

Como se muestra en la figura 50. De igual forma en el módulo de autenticación le damos en el botón de manage Groups.

Figura 51. Habilitación de servicio proxy.



Fuente: Imagen de Autoría propia

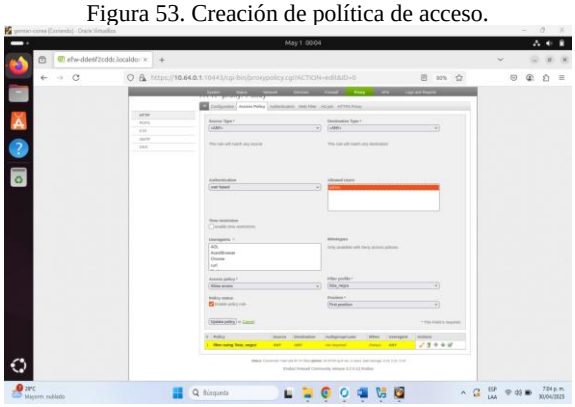
Como se muestra en la figura 51. Nos dirigimos al módulo Configuración y habilitamos el servicio de Proxy por medio de Enable HTTP Proxy.

Figura 52. Configuración de no transparente.

Fuente: Imagen de Autoría propia

Como se muestra en la figura 52. Colocamos las redes en tipo no transparente, puerto 8080 y demás configuración.

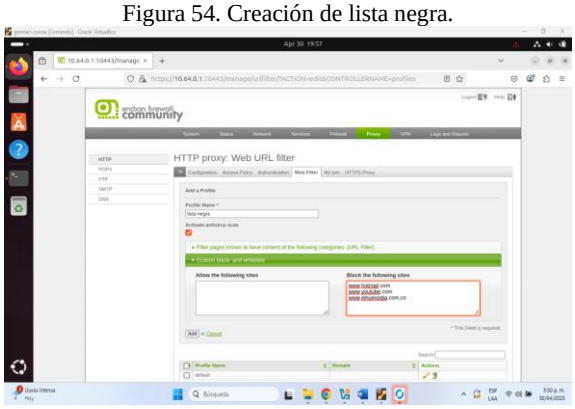
Figura 53. Creación de política de acceso.



Fuente: Imagen de Autoría propia

Como se muestra en la figura 53. Creamos una política de acceso donde asociamos nuestro usuario admin, le damos que apruebe la regla que se creó llamada lista negra y llenamos la demás configuración.

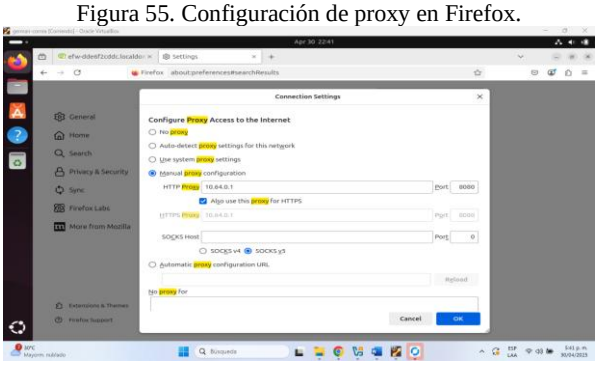
Figura 54. Creación de lista negra.



Fuente: Imagen de Autoría propia

Como se muestra en la figura 54. Creamos un nuevo filtro con el nombre lista negra, donde bloqueamos 3 páginas, www.hotmail.com, www.youtube.com, www.elnuevodia.com.co.

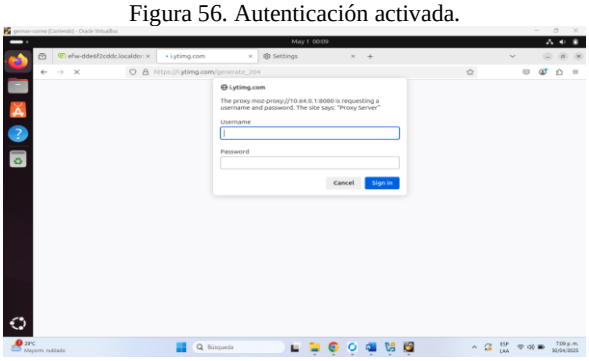
Figura 55. Configuración de proxy en Firefox.



Fuente: Imagen de Autoría propia

Como se muestra en la figura 55. Vamos a la configuración de proxy en nuestro buscador Firefox y manualmente configuramos el Proxy donde colocamos 10.64.0.1 y le decimos que usemos el mismo proxy en HTTPS también.

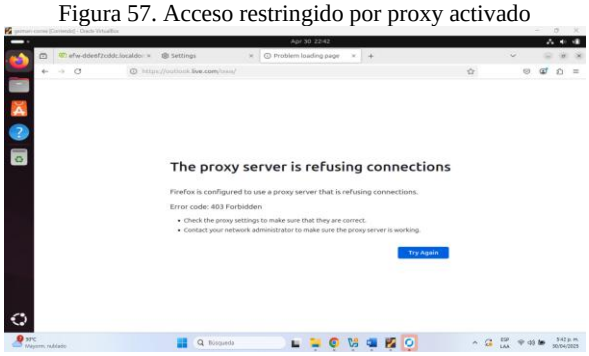
Figura 56. Autenticación activada.



Fuente: Imagen de Autoría propia

Como se muestra en la figura 56. Intentamos ingresar a las páginas bloqueadas y nos piden autenticación de usuario.

Figura 57. Acceso restringido por proxy activado



Fuente: Imagen de Autoría propia

Como se muestra en la figura 57. Luego de colocar la autenticación nos muestra el siguiente mensaje.

4. CONCLUSIONES

El proyecto implementó una solución de seguridad perimetral eficiente mediante Endian UTM, segmentando la red y protegiendo los recursos críticos. Configuraciones como NAT, servicios en la DMZ y un proxy HTTP con autenticación reforzaron la integridad de los servidores y aplicaciones, minimizando riesgos.

Esta estrategia modular, basada en control de acceso y filtrado de tráfico, optimizó la seguridad de la red corporativa. El resultado fue un entorno más estable y protegido, adaptado a las necesidades de defensa en profundidad.

La implementación de políticas de acceso en entornos segmentados es fundamental para garantizar el tráfico interzonal, tanto funcionalmente como dentro de una estrategia de defensa en profundidad.

Una configuración adecuada de reglas de firewall —definiendo origen, destino, protocolo y acción— permite controlar los servicios disponibles, reduciendo vectores de ataque y manteniendo la estabilidad de la red.

Las técnicas NAT, redirección de puertos y validación mediante terminal fortalecen la auditoría y el monitoreo del tráfico. Esto asegura que servicios críticos (HTTP, FTP) operen

entre zonas sin comprometer la seguridad interna, alineándose con principios de segmentación lógica y gobernanza de

5 REFERENCIAS

[1] Canonical, "Guía del Ubuntu desktop 20.04 LTS," Help Ubuntu, 2023. [Online]. Available: https://help.ubuntu.com/20.04/ubuntu-help/index.html.
[2] Debian, "El manual del administrador de Debian 12.5.0," 2023. [Online]. Available: https://www.debian.org/releases/stable/amd64/index.es.html.
[3] Guest, "Endian Firewall," PDFCoffee, n.d. [Online]. Available: https://pdfcoffee.com/endian-firewall-2-pdf-free.html. [Accessed: May 24, 2025].
[4] I. Gómez-Marí and A. Pedrosa-Sáez, "La educación en la era del metaverso: ¿Está la comunidad educativa preparada?," *EducaT: Educación Virtual, Innovación y Tecnologías*, vol. 4, no. 1, pp. 3–44, 2023. [Online]. Available: https://hemeroteca.unad.edu.co/index.php/educat/article/view/6571/6473.
[5] 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.
[6] Kali Linux, "Kali Linux Documentation," Offensive Security, 2023. [Online]. Available: https://www.kali.org/docs/.
[7] Linux Hint, "How to Install and Configure Endian Firewall," 2022. [Online]. Available: https://linuxhint.com/install-configure-endian-firewall/.
[8] LPI, *Linux Essentials: Tema 1 - La Comunidad Linux y una carrera en el mundo del código abierto*, 2022. [Online]. Available: https://learning.lpi.org/es/learning-materials/010-160/1/.
[9] LPI, *Linux Essentials: Tema 2 - Encontrando el camino en un sistema Linux*, 2022. [Online]. Available: https://learning.lpi.org/es/learning-materials/010-160/2/.
[10] LPI, *Linux Essentials: Tema 3 - El poder de la línea de comandos*, 2022. [Online]. Available: https://learning.lpi.org/es/learning-materials/010-160/3/.
[11] LPI, *Linux Essentials: Tema 4 - El sistema operativo Linux*, 2022. [Online]. Available: https://learning.lpi.org/es/learning-materials/010-160/4/.
[12] LPI, *Linux Essentials: Tema 5 - Seguridad y sistema de permisos de archivos*, 2022. [Online]. Available: https://learning.lpi.org/es/learning-materials/010-160/5/.
[13] LPI, *LPIC-1 Exam 101: Tema 101 - Arquitectura del Sistema*, 2022. [Online]. Available: https://learning.lpi.org/es/learning-materials/101-500/101/.
[14] LPI, *LPIC-1 Exam 101: Tema 102 - Comandos GNU y Unix*, 2022. [Online]. Available: https://learning.lpi.org/es/learning-materials/101-500/102/.
[15] J. A. Moral, "Debian GNU/Linux y la Línea de Comandos," Unpublished manual, n.d. [Online]. Available: https://www.academia.edu/download/69665786/DebianGNULinuxYLaLineaDeComandos.pdf.
[16] Oracle, "Manual de usuario VirtualBox," 2020. [Online]. Available: https://www.virtualbox.org/manual/.
[17] Oracle, "Oracle VM VirtualBox User Manual (Version 7.0)," 2024. [Online]. Available: https://www.virtualbox.org/manual/UserManual.html.
[18] phpMyAdmin, "Documentation," n.d. [Online]. Available: https://www.phpmyadmin.net/docs/. [Accessed: May 24, 2025].
[19] Universidad Nacional Abierta y a Distancia (UNAD), "Instalación y configuración del Servidor Zentyal en zona DMZ del cortafuegos Endian," n.d. [Online]. Available: https://repository.unad.edu.co/handle/10596/38552.
[20] Universidad Señor de Sipán, "Implementación de un sistema de control y seguridad Informático ENDIAN FIREWALL," *INGENIERÍA: Ciencia, Tecnología e Innovación*, n.d. [Online]. Available: https://revistas.uss.edu.pe/index.php/ING/article/view/2401.
[21] Ubuntu, "Ubuntu 20.04 LTS (Focal Fossa) release notes," Canonical Ltd., 2020. [Online]. Available: https://releases.ubuntu.com/focal/.