IMPLEMENTACIÓN DE SEGURIDAD PERIMETRAL CON ENDIAN EN ENTORNOS VIRTUALIZADOS

Gutierrez Polanco, Bleidy Yurani
e-mail: bygutierrezp@unadvirtual.edu.co
López Quintana, Silvio Marino
slopezq@unadvirtual.edu.co
López Chaves, Jaime Andrés
jalopezchave@unadvirtual.edu.co
Muse Ule, Guillermo
gmuseu@unadvirtual.edu.co
Ordoñez Martínez, Jhon Edisson
jeordonezma@unadvirtual.edu.co

RESUMEN: *Se presenta la instalación y configuración de Endian Firewall en una arquitectura de red segmentada, donde se implementan reglas NAT para gestionar la comunicación entre zonas internas y externas y se habilitan servicios controlados dentro de la DMZ, como HTTP y FTP, restringiendo protocolos no autorizados. Paralelamente, se establecen políticas de acceso entre zonas mediante reglas de firewall, validando su funcionamiento mediante análisis del tráfico y pruebas de conectividad. Asimismo, se incorpora un proxy HTTP no transparente con autenticación y filtrado por listas negras para reforzar el control de navegación desde la LAN. La integración de estos mecanismos consolida una infraestructura más segura, funcional y alineada con las buenas prácticas de protección perimetral en redes virtualizadas.*

PALABRAS CLAVE: Endian Firewall, NAT, DMZ, Seguridad Perimetral, Proxy HTTP.

ABSTRACT

This work describes the installation and configuration of Endian Firewall within a segmented network architecture, where NAT rules are implemented to manage communication between internal and external zones and to enable controlled services within the DMZ, such as HTTP and FTP, while blocking unauthorized protocols. Access policies between zones are defined through firewall rules and validated through traffic analysis and connectivity testing. Additionally, a non-transparent HTTP proxy with user authentication and blacklist filtering is deployed to enhance browsing control within the LAN. The combination of these mechanisms results in a more secure and functional infrastructure, aligned with best practices for perimeter protection in virtualized network environments.

KEYWORDS: Endian Firewall, NAT, DMZ, Perimeter Security, HTTP Proxy.

1. INTRODUCCIÓN

Este documento presenta el proceso de implementación y gestión de una solución de seguridad perimetral basada en GNU/Linux Endian, desplegada en un entorno virtual mediante VirtualBox. Se describe la instalación del sistema y la configuración de sus interfaces de red, junto con la activación de mecanismos NAT que permiten el enlace controlado con redes externas. También se desarrolla la creación de una zona DMZ destinada a la publicación segura de servicios y la definición de reglas de acceso que regulan el tráfico de acuerdo con las políticas establecidas. Finalmente, se incorpora un proxy HTTP no transparente con autenticación de usuarios para supervisar y restringir la navegación hacia Internet. Todo este conjunto de actividades contribuye al fortalecimiento de las competencias prácticas en administración de redes y en la implementación de medidas de seguridad perimetral.

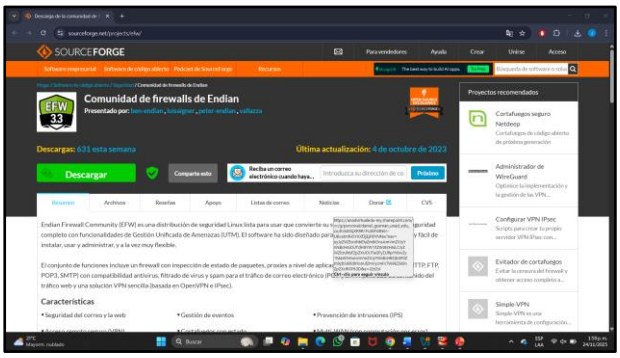
2. INSTALACIÓN ENDIAN

2.1 ARQUITECTURA DE RED Y ESCENARIO

El Endian Firewall es una plataforma de seguridad perimetral de código abierto que reúne diversas herramientas para proteger la red frente a amenazas. Su diseño permite integrar controles de acceso, filtrado avanzado y mecanismos de defensa ante ataques. En este proyecto se configuraron servicios como NAT, firewall y proxy, ajustados a las necesidades del entorno para mejorar la segmentación, regular el tráfico y asegurar una navegación supervisada. Además, se aprovecharon sus funciones de registro y monitoreo para mantener un seguimiento constante de la actividad de la red y facilitar la detección temprana de incidentes, fortaleciendo así la administración y la protección del sistema.

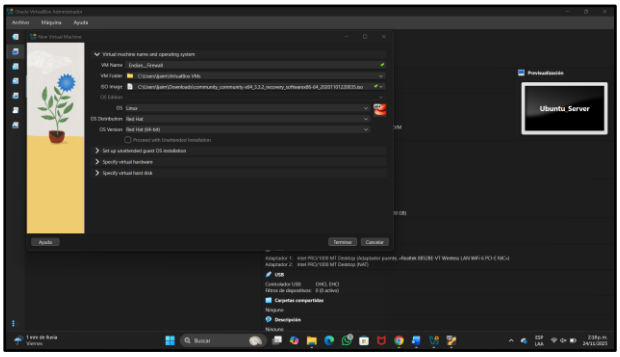
La implementación de Endian (UTM) se realizó en un entorno virtualizado con el propósito de simular una infraestructura empresarial básica. El firewall se configuró como componente perimetral encargado del filtrado y control del tráfico entre las zonas LAN, WAN y DMZ. Para complementar el escenario, se incorporaron dos máquinas Linux adicionales: una como servidor y otra como equipo cliente, ambas conectadas a la red interna. La instalación incluyó la asignación de interfaces de red para cada zona y la configuración estática de la dirección destinada a la administración del sistema, garantizando la comunicación adecuada entre los distintos elementos del entorno.

Figura 1. Descarga del archivo ISO de Endian Firewall desde el sitio oficial



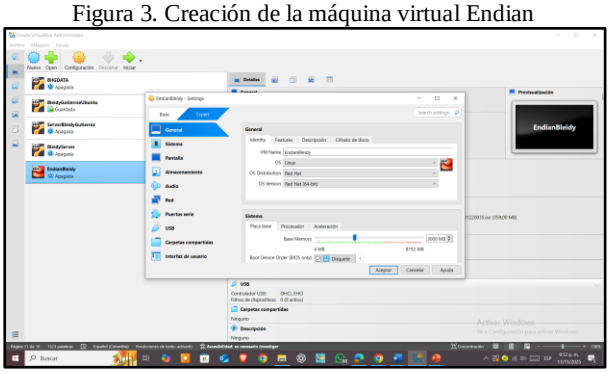
Fuente: Autoría Propia

Figura 2. Pantalla inicial de creación de la máquina virtual Endian



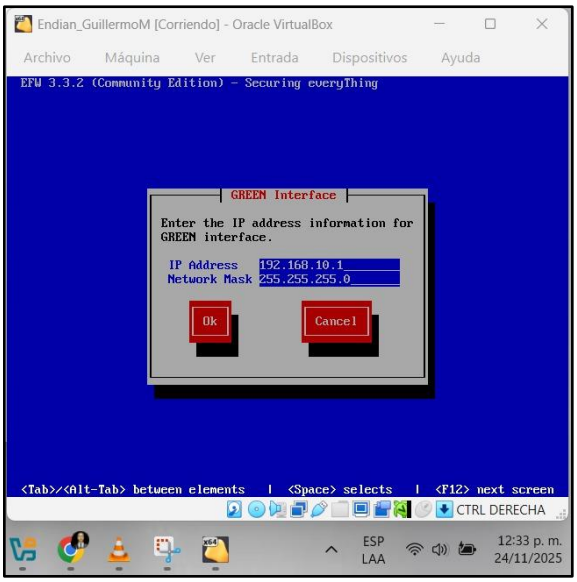
Fuente: Autoría Propia

Figura 3. Creación de la máquina virtual Endian



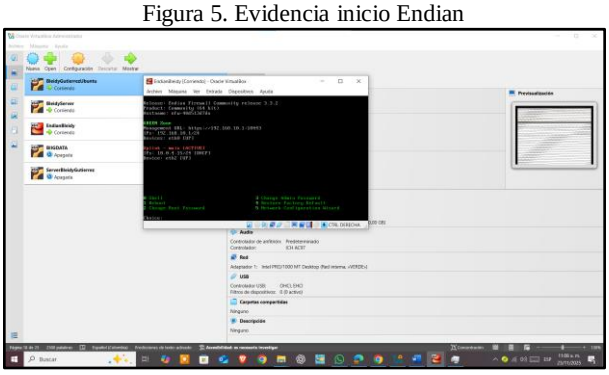
Fuente: Autoría propia

Figura 4. Establecimiento de ip GREEN.



Fuente: Autoría propia

Figura 5. Evidencia inicio Endian



Fuente: Autoría propia

3 DESARROLLO TEMATICAS

3.1 TEMÁTICA 1: CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX (TARJETAS DE RED) E INSTALACIÓN EFECTIVA DEL MISMO

Se expone la implementación de una red segmentada empleando Endian Firewall como herramienta central para reforzar la seguridad y optimizar el flujo de comunicación entre distintos niveles de la infraestructura. El proceso incluye la configuración de los adaptadores de red, la asignación de parámetros de direccionamiento y la definición de reglas de control de tráfico. La segmentación en zonas LAN, DMZ y WAN demuestra ser efectiva para organizar los servicios y reducir posibles riesgos, ofreciendo un esquema aplicable a otros entornos. Endian 3.3.2, instalado sobre una máquina con Linux, actúa como el componente encargado de la gestión perimetral y del filtrado necesario para mantener protegidos los recursos críticos.

El adaptador LAN utiliza el segmento 192.168.2.0/24, donde Endian funciona como la puerta de enlace. La red asigna direcciones IP mediante DHCP, reservando algunas para equipos que requieren disponibilidad constante. Además,

se aplica una política estricta de firewall que bloquea accesos no autorizados, garantizando seguridad sin afectar la gestión dinámica de la red.

La interfaz WAN se configura para obtener su dirección IP mediante DHCP, facilitando la conexión externa. Se emplea NAT overload para que varios equipos internos utilicen la misma IP pública, manteniendo eficiencia en el uso de recursos. Además, se aplican reglas de seguridad que permiten únicamente tráfico originado desde la red interna y se bloquean puertos innecesarios, reduciendo riesgos y fortaleciendo la protección perimetral.

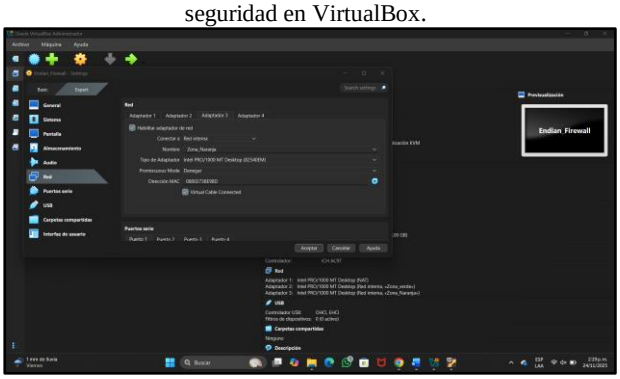
La DMZ se configura como un segmento aislado donde el servidor Ubuntu utiliza una dirección IP fija y una puerta de enlace asociada al firewall. Para proteger los servicios expuestos, se aplican reglas específicas que solo permiten tráfico hacia los puertos necesarios, como HTTP, HTTPS y SMTP. Además, se habilitan mecanismos de supervisión y limitación de conexiones para evitar sobrecargas o intentos de ataque, garantizando así la disponibilidad de los servicios y la seguridad frente a amenazas externas.

Zona verde (LAN): Red interna para dispositivos locales (192.168.10.1).

Zona naranja (DMZ): Servidores accesibles de forma controlada (192.168.20.1).

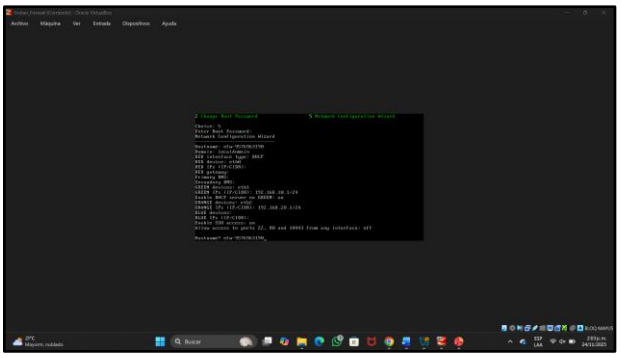
Zona roja (WAN): Conexión a internet mediante NAT.

Figura 6. Configuración de adaptadores de red para zonas de seguridad en VirtualBox.



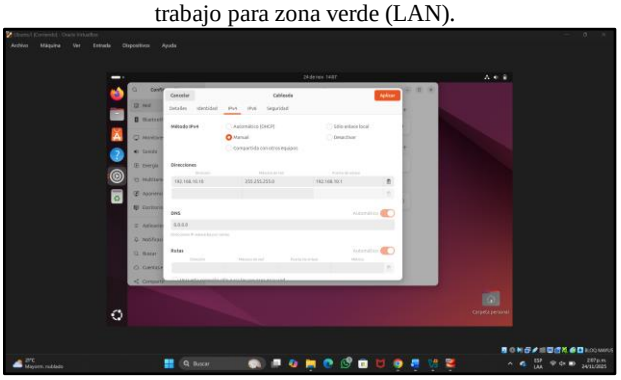
Fuente: Autoría Propia

Figura 7. Configuración final de interfaces y servicios de red en Endian Firewall.



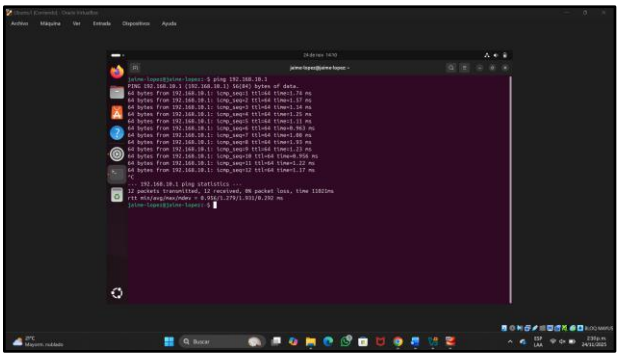
Fuente: Autoría Propia

Figura 8. Configuración manual de red IPv4 en estación de trabajo para zona verde (LAN).



Fuente: Autoría Propia

Figura 9. Prueba de conectividad exitosa hacia Endian Firewall desde estación de trabajo en Ubuntu desktop.



Fuente: Autoría Propia

Configuración de la NAT, LAN, WAN

Se validó que el cliente LAN tuviera acceso a Internet mediante:

- PING a 8.8.8.8
- Navegación exitosa en Google

Esto demuestra que Endian aplicó correctamente el enmascaramiento (MASQUERADE) sobre la interfaz WAN.

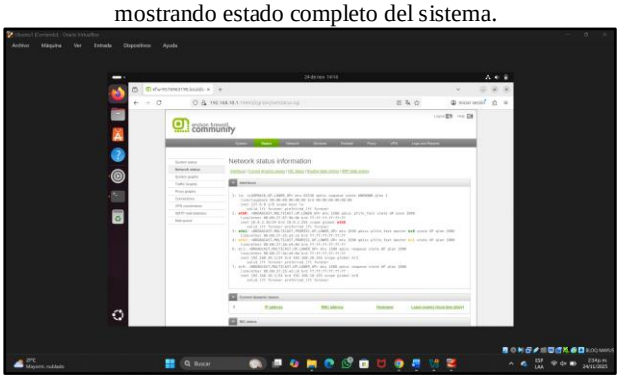
Parámetros:

- Origen: NARANJA
- Servicio: TCP/80
- Traducir a: 192.168.20.2 (Servidor DMZ)

- Estado: Activado

La regla permite que solicitudes externas hacia el puerto 80 sean reenviadas al servidor DMZ.

Figura 10. Interfaz web de administración de Endian Firewall mostrando estado completo del sistema.



Fuente: Autoría Propia

RESULTADOS

Tabla de asignación de zonas

Tabla 1 Asignación de zonas en Endian Firewall

Zona 2	Interfaz	IP	Función
Verde	br0	192.168.10.1/24	Red interna segura
Naranja	br1	192.168.20.1/24	Servidores expuestos
Roja	eth1	DHCP	Salida a internet

- Endian Firewall filtró correctamente el tráfico no autorizado entre zonas.

Seguridad:

● La DMZ aisló los servidores de la red interna, reduciendo riesgos de ataques externos.

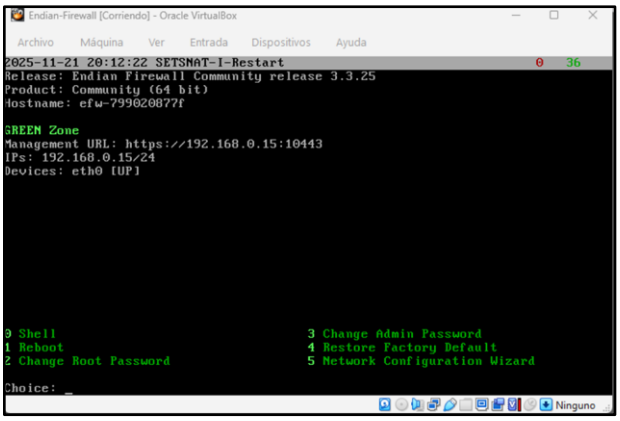
● Las políticas de NAT ocultaron las IPs internas desde la WAN. Limitaciones: ● La configuración inicial requirió ajustes manuales en las tablas de rutas.

● La falta de redundancia en los adaptadores podría ser un punto crítico.

3.2 TEMATICA 2: CONFIGURACIÓN NAT

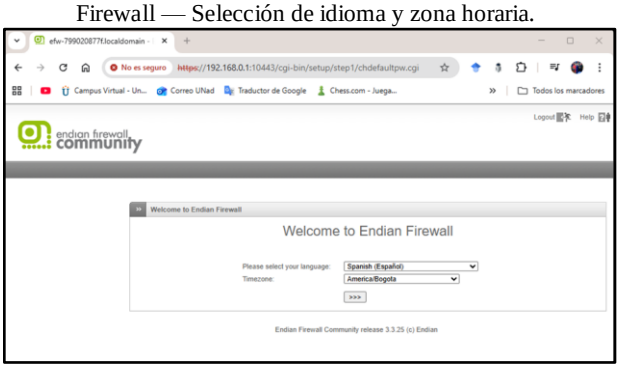
Producto esperado: Configurar la traducción de direcciones de red (NAT) para habilitar el acceso de la red LAN hacia la WAN y permitir que la DMZ se comunique con Internet, comprobando el correcto funcionamiento del reenvío de puertos y la generación adecuada de las reglas asociadas.

Figura 11. Pantalla de arranque del sistema Endian mostrando la URL de administración asignada.



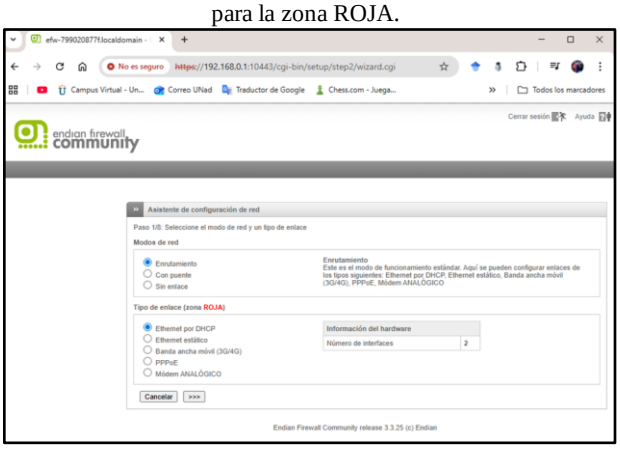
Fuente: Autoría Propia

Figura 12. Asistente de configuración inicial de Endian Firewall — Selección de idioma y zona horaria.



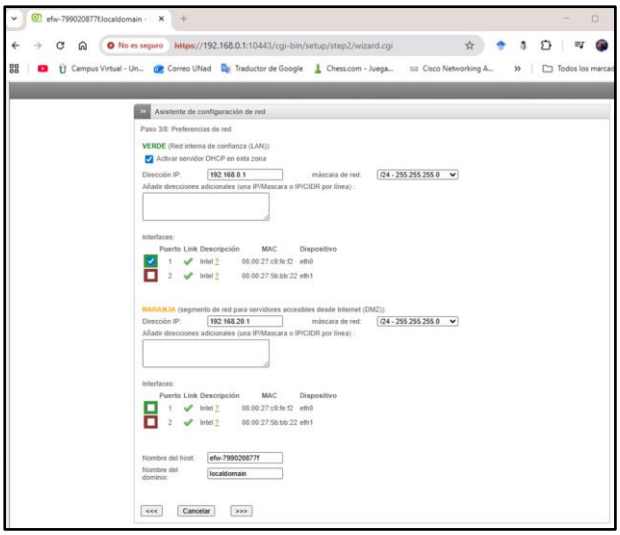
Fuente: Autoría Propia

Figura 13. Configuración del modo de red y tipo de enlace para la zona ROJA.



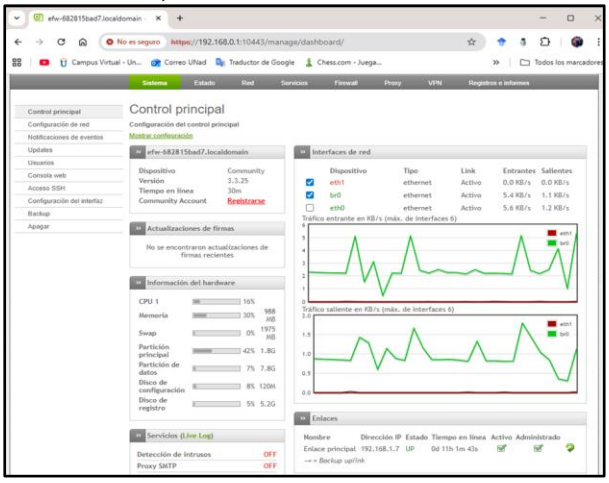
Fuente: Autoría Propia

Figura 14. Asignación de direcciones IP para las zonas GREEN (LAN) y ORANGE (DMZ).



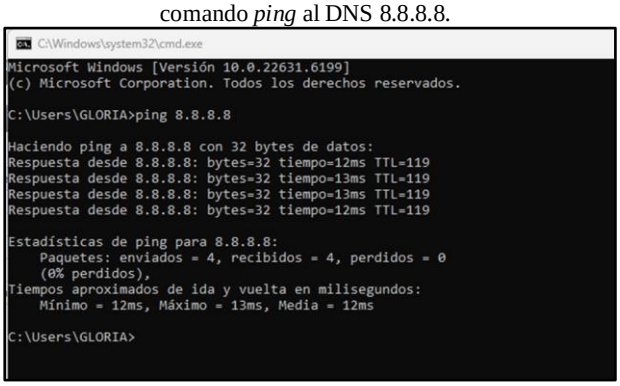
Fuente: Autoría Propia

Figura 15. Panel de control principal tras la configuración de red, mostrando estado de interfaces.



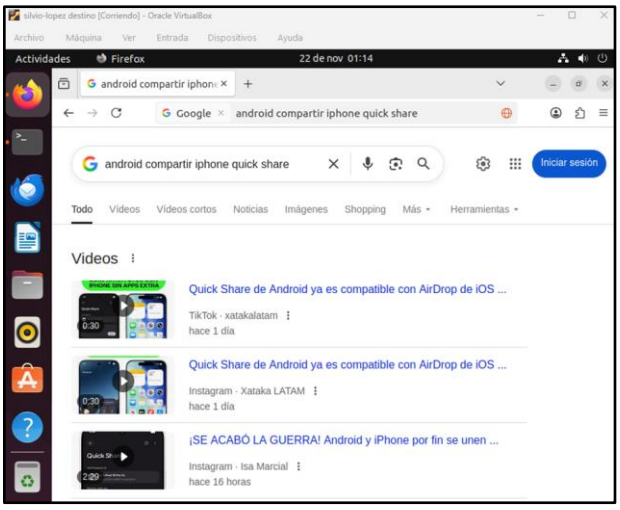
Fuente: Autoría Propia

Figura 16. Prueba de conectividad LAN → WAN mediante comando *ping* al DNS 8.8.8.8.



Fuente: Autoría Propia

Figura 17. Prueba de navegación en la máquina cliente de la LAN, demostrando acceso a Internet.



Fuente: Autoría Propia

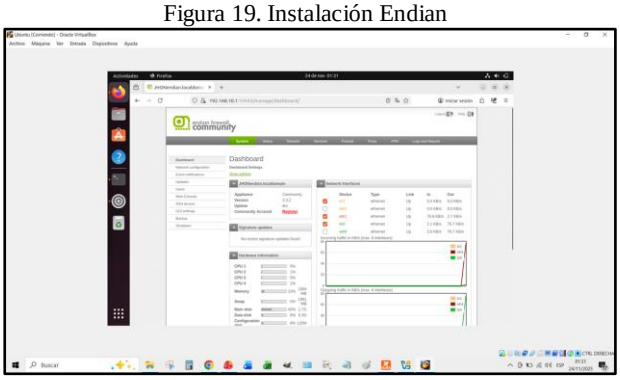
Figura 18. Configuración de una regla de NAT de destino (DNAT) desde la zona ORANGE hacía servidor interno.

Fuente: Autoría Propia

Server también ha realizado con éxito un ping a 8.8.8.8, lo que indica que la máquina también tiene acceso a Internet. Esto muestra que la configuración de red y NAT en Endian y el servidor están funcionando correctamente, permitiendo que ambas máquinas puedan comunicarse con el exterior.

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

Figura 19. Instalación Endian

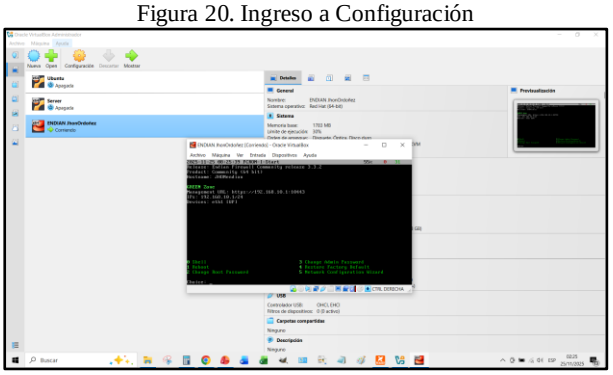


Fuente: Autoría Propia

En el programa de virtualización VirtualBox, se realiza la instalación y configuración de Endian, con las zonas y segmentos de red acordados.

Acceso a la Interfaz gráfica

Figura 20. Ingreso a Configuración

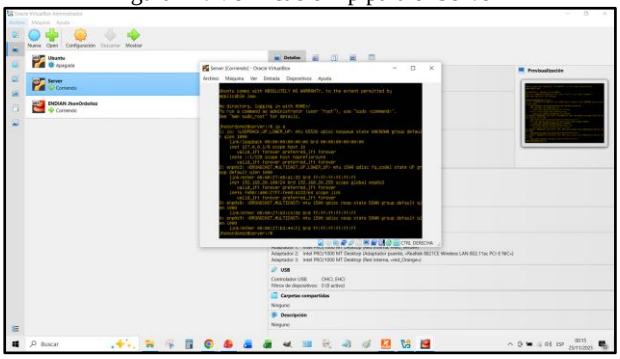


Fuente: Autoría Propia

Por medio de la Ip asignada a los clientes de la zona verde 192.168.10.1 se ingresa al entorno gráfico de Endian

Verificación Ip Server

Figura 21. Verificación ip para el Server

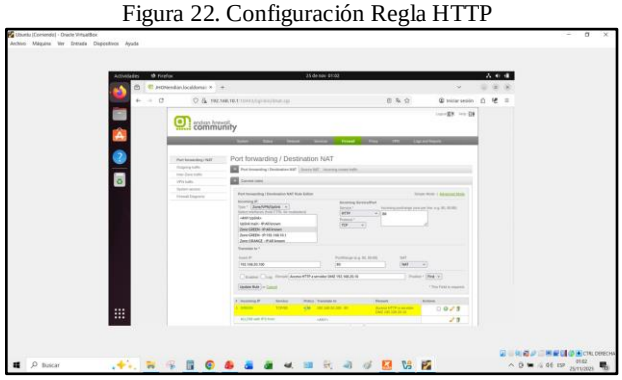


Fuente: Autoría Propia

En el Ubuntu Server se comprueba la ip del Servidor en la zona naranja.

Configuración Regla 1

Figura 22. Configuración Regla HTTP

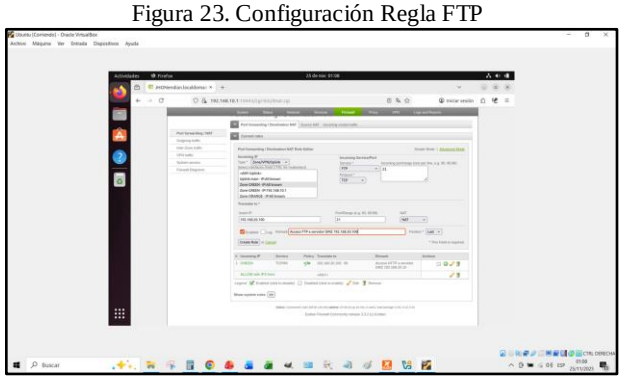


Fuente: Autoría Propia

Se realiza la respectiva configuración de la regla HTTP puerto 80 (destino NAT)

Configuración Regla 2

Figura 23. Configuración Regla FTP

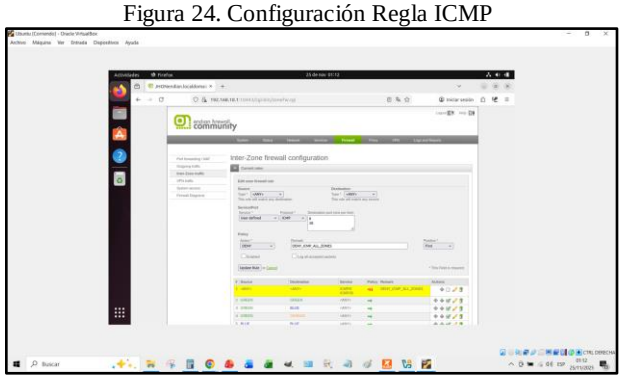


Fuente: Autoría Propia

Se realiza la respectiva configuración de la regla FTP puerto 21 (destino NAT)

Configuración Regla 3

Figura 24. Configuración Regla ICMP

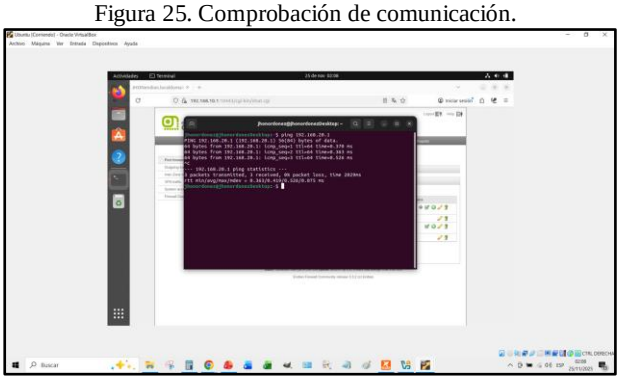


Fuente: Autoría Propia

Se realiza la configuración de la regla para denegar ICMP (ping).

Comprobación

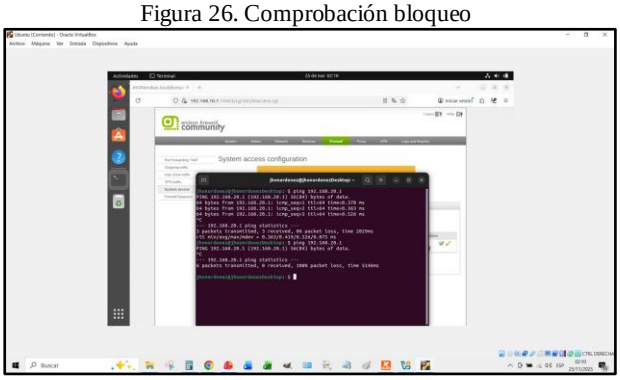
Figura 25. Comprobación de comunicación.



Fuente: Autoría Propia

Se realiza ping a la ip 192.168.20.1 de la red naranja, desde 192.168.10.15 de la red verde, comprobando comunicación.

Figura 26. Comprobación bloqueo



Fuente: Autoría Propia

Se realiza ping a la ip 192.168.20.1 de la red naranja, desde 192.168.10.15 de la red verde comprobando el bloque de ping.

La configuración de reglas de acceso en el firewall Endian tiene como objetivo controlar la comunicación entre las distintas zonas de red (LAN, WAN y DMZ), estableciendo políticas que permitan o restrinjan el tráfico de forma segura. Esto se realiza para proteger la red interna frente a accesos no autorizados desde Internet.

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

Producto esperado: Establecer y verificar las reglas de acceso entre las distintas zonas de la red implementadas (LAN, WAN y DMZ) a través del firewall Endian. Se configurarán políticas específicas que permitan o restrinjan el tráfico mediante los protocolos HTTP (puerto 80) y FTP (puerto 21), con el fin de garantizar una comunicación controlada y segura entre las estaciones de trabajo, los servidores y el acceso a Internet.

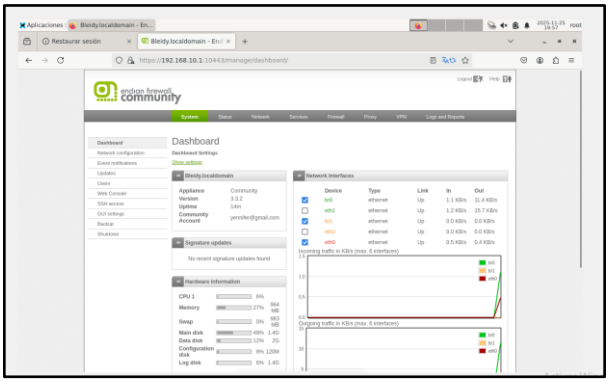
Se definen y verifican las reglas de acceso entre las zonas LAN, WAN y DMZ del entorno configurado con Endian Firewall. Estas políticas regulan qué tráfico puede permitirse o bloquearse, especialmente para los servicios HTTP, HTTPS, FTP e ICMP, con el fin de mantener una comunicación segura y controlada entre estaciones de trabajo, servidores y la conexión a Internet. También se establecen reglas específicas para habilitar o restringir el intercambio de datos entre la zona interna (Verde), la zona de servidores (Naranja) y el acceso externo, garantizando que solo los protocolos autorizados puedan circular entre los distintos segmentos de la red.

Para habilitar la comunicación entre la red Internet y la zona DMZ —destinada a alojar servidores expuestos de manera controlada, como servicios web o FTP— es necesario definir reglas que permitan o bloqueen el tráfico entrante hacia la DMZ según los servicios requeridos, entre ellos HTTP/HTTPS, FTP e ICMP.

Una vez completada la configuración, se procede a verificar que todas las reglas establecidas entre las diferentes zonas funcionen correctamente. Esto incluye confirmar que el tráfico no autorizado permanezca bloqueado por defecto y que únicamente se admitan las conexiones que hayan sido habilitadas de forma explícita.

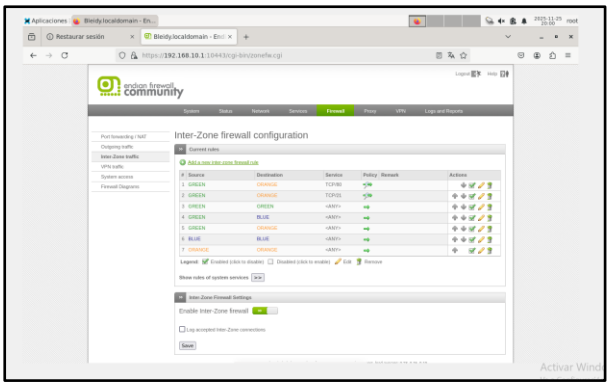
Y se realizan pruebas desde un navegador web para validar el cumplimiento de las directivas de acceso. Estas verificaciones permiten confirmar que las reglas aplicadas operan de acuerdo con los criterios definidos y que la comunicación entre zonas responde a lo esperado.

Figura 27. Dentro de la interfaz web de Endian, se llevan a cabo las configuraciones correspondientes a las reglas de comunicación entre las distintas redes.



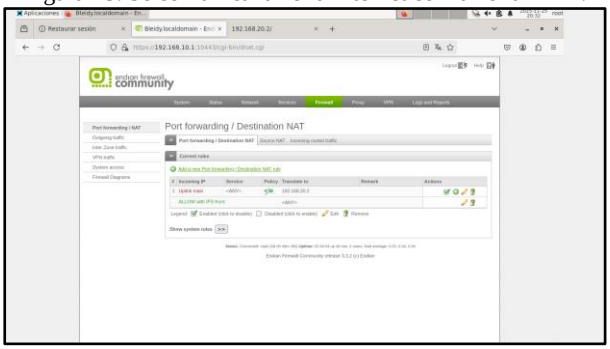
Fuente: Autoría Propia

Figura 28. Se comunica la zona Verde con la zona Naranja con el protocolo HTTP y FTP con sus respectivos puertos.



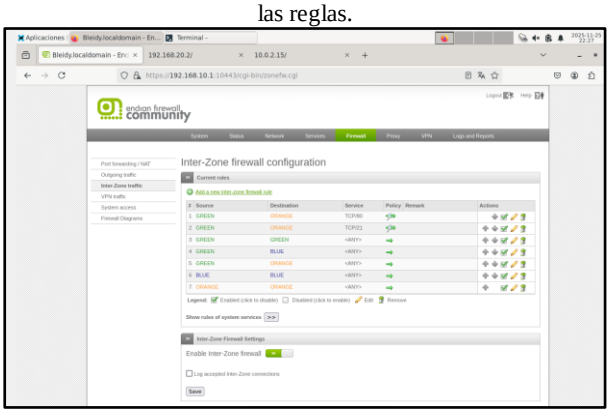
Fuente: Autoría Propia

Figura 29. Se comunica la zona Internet con la zona DMZ.



Fuente: Autoría Propia

Figura 30. Se verificar en el tráfico Inter - Zona, la creación de las reglas.



Fuente: Autoría Propia

Figura 31. Se prueba el ingreso del servicio HTTP desde la LAN hacia la zona DMZ.

Fuente: Autoría Propia

Figura 32. Se prueba el ingreso del servicio HTTP desde la LAN hacia la WAN.

Fuente: Autoría Propia

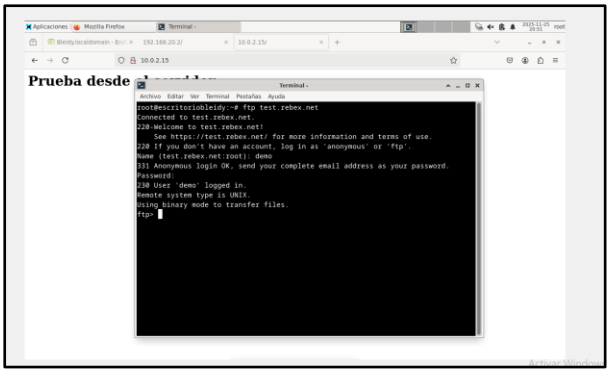
Figura 33. Se prueba el ingreso del servicio HTTP desde la zona DMZ hacia la WAN. Se usa la ip publica de Endian por lo cual redirecciona al ip del servidor.

Fuente: Autoría Propia

Figura 34. Se prueba el ingreso del servicio HTTP desde la WAN hacia la zona DMZ. Mediante el comando curl http://www.Google.com | head –n 1

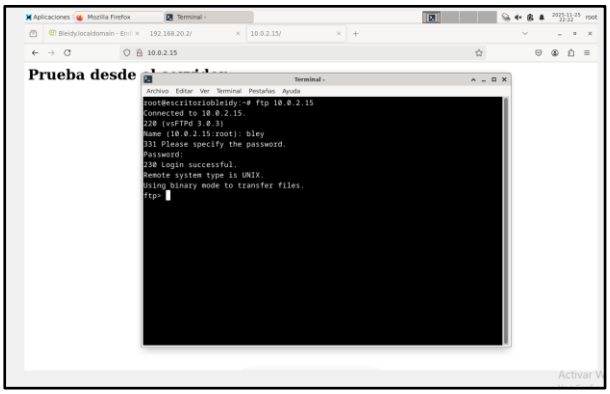
Fuente: Autoría Propia

Figura 35. Se prueba el ingreso del servicio FTP desde la LAN hacia la WAN. Desde la terminal del cliente.



Fuente: Autoría Propia

Figura 36. Se prueba el ingreso del servicio FTP desde la WAN hacia la zona DMZ.



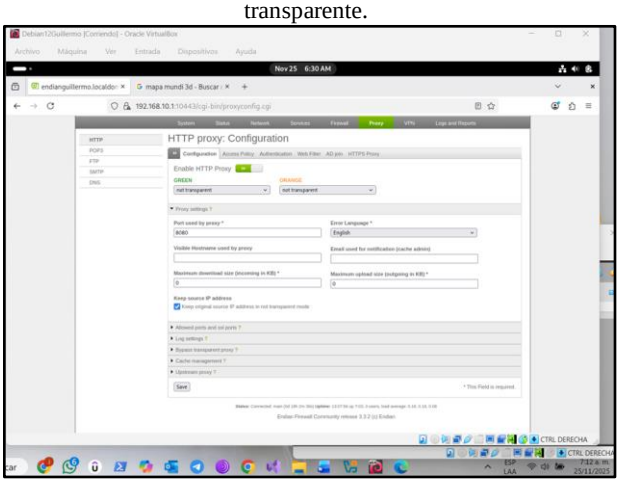
Fuente: Autoría Propia

La configuración de reglas de acceso en Endian Firewall tiene como finalidad gestionar la comunicación entre las zonas LAN, WAN y DMZ mediante políticas que permitan o limiten el tránsito de datos de manera segura. Este proceso protege la red interna frente a conexiones no autorizadas desde el exterior y habilita únicamente los servicios necesarios, como HTTP, HTTPS y FTP. Además, facilita la recreación de entornos similares a los de una infraestructura empresarial, donde ciertos servicios deben ser accesibles públicamente desde la DMZ sin comprometer la seguridad del resto de la red.

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

Activación del Proxy HTTP

Figura 37. Activación del Proxy HTTP en modo no transparente.

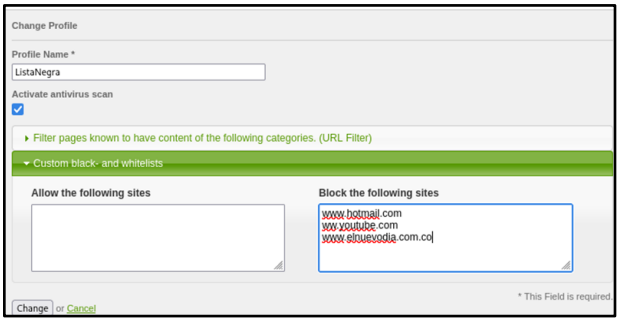


Fuente: Autoría Propia

Se habilitó el Proxy HTTP en Endian seleccionando el modo "not transparent" para que la navegación pase únicamente cuando el navegador esté configurado manualmente. Esto permite controlar el tráfico web desde la zona GREEN y aplicar políticas específicas.

Creación del Perfil de Lista Negra

Figura 38. Configuración del perfil "ListaNegra" en el Web Filter.

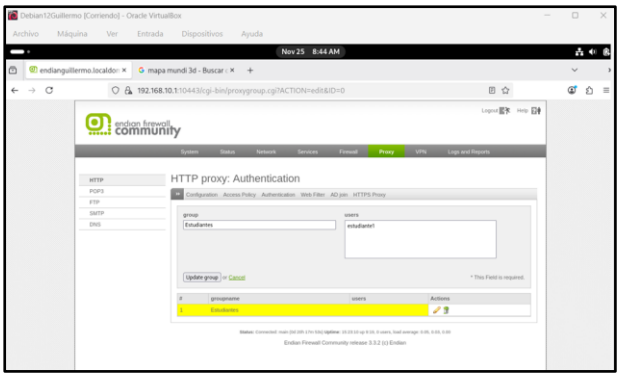


Fuente: Autoría Propia

Se creó un perfil de filtrado llamado "ListaNegra" donde se agregaron los dominios prohibidos (YouTube, Hotmail y El Nuevo Día). Este perfil será usado para bloquear dichos sitios cuando los usuarios naveguen.

Creación de Usuario y Grupo

Figura 39. Creación del grupo Estudiantes y el usuario estudiante1.

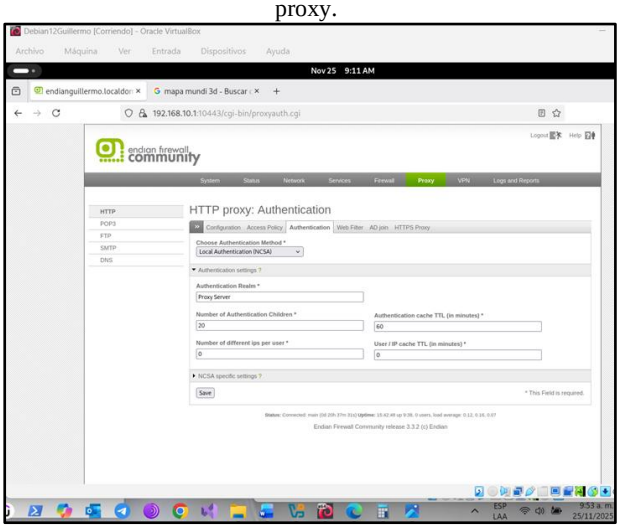


Fuente: Autoría Propia

Se configuró un grupo llamado “Estudiantes” y dentro de él un usuario “estudiante1”, que será el que usará el navegador para autenticarse, esto permite organizar y controlar quién puede navegar y con qué restricciones.

Activación de la Autenticación del Proxy

Figura 40. Activación del modo de autenticación Local en el proxy.

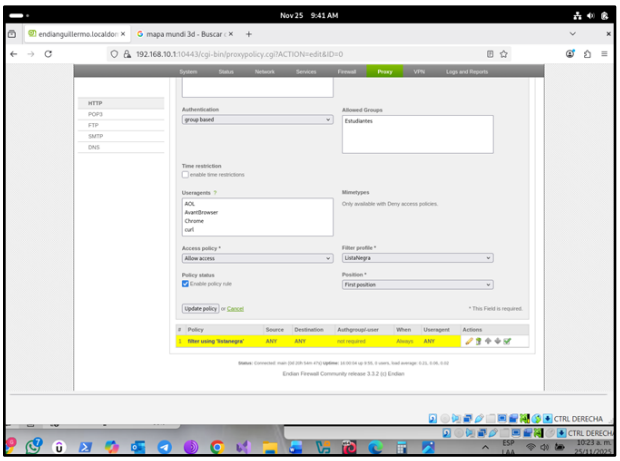


Fuente: Autoría Propia

Se habilitó la autenticación obligatoria del proxy en modo “Local”, exigiendo que los usuarios ingresen con su nombre y contraseña antes de acceder a Internet, esto asegura que solo usuarios autorizados naveguen.

Creación de la Política de Acceso

Figura 41. Regla de acceso que enlaza la zona GREEN, el grupo “Estudiantes” y el perfil “ListaNegra”.

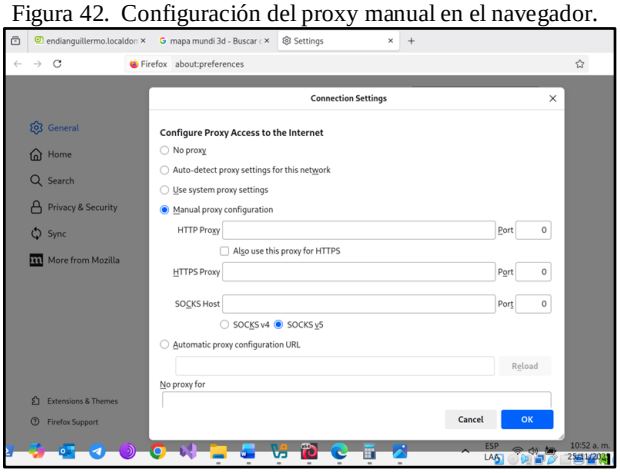


Fuente: Autoría Propia

Se generó una regla de acceso que relaciona la zona GREEN, el grupo “Estudiantes” y el perfil “ListaNegra”, la política permite navegar, pero aplicando el bloqueo de los sitios definidos.

Configuración del Proxy en el Navegador

Figura 42. Configuración del proxy manual en el navegador.



Fuente: Autoría Propia

En el navegador de Debian se activó el uso del proxy manual, colocando la IP de Endian y el puerto 8080. Esto asegura que todo el tráfico pase por el firewall para ser filtrado.

Prueba de Autenticación

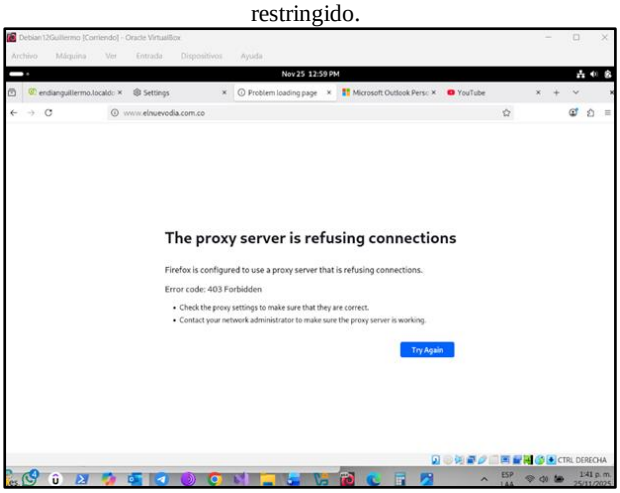
Figura 43. Solicitud de usuario y contraseña al acceder a Internet.

Fuente: Autoría Propia

Al abrir cualquier página, el navegador solicita usuario y contraseña, confirmando que la autenticación del proxy está activa y funcionando correctamente.

Prueba de Bloqueo de Sitios

Figura 44. Mensaje de bloqueo al intentar abrir un sitio restringido.



Fuente: Autoría Propia

Finalmente se intentó entrar a las páginas prohibidas y el proxy las bloqueó, demostrando que la lista negra y la política de acceso están aplicándose correctamente.

Resultados de conectividad

- La LAN logró navegar en Internet mediante NAT → comprobado con ping y navegación.
- La DMZ recibió solicitudes externas mediante DNAT.
- Las reglas fueron aplicadas y visibles en la sección "Port Forwarding / NAT".

4 CONCLUSIONES

La implementación de Endian Firewall permitió comprender de manera práctica cómo la segmentación de red mediante zonas Verde (LAN), Naranja (DMZ) y Roja (WAN) fortalece la seguridad perimetral dentro de una infraestructura tecnológica, esta división lógica posibilitó controlar el tráfico según el tipo de usuario o servicio, garantizando que los accesos se mantuvieran organizados, aislados y protegidos frente a amenazas externas.

La configuración de NAT, tanto para la LAN como para la DMZ, demostró la importancia de la traducción de direcciones para permitir la salida hacia Internet manteniendo la seguridad y el anonimato interno de la red, las pruebas realizadas mediante comandos de conectividad y navegación confirmaron el funcionamiento adecuado de las reglas implementadas, validando que el firewall gestionó correctamente el tráfico entrante y saliente.

La habilitación de servicios específicos en la DMZ, junto con la restricción del protocolo ICMP, evidenció el rol fundamental del firewall en la administración granular de los permisos de comunicación. El poder habilitar puertos como HTTP y FTP, al tiempo que se bloquean protocolos que pueden comprometer la red interna, constituye una práctica esencial en la construcción de ambientes seguros.

La configuración del Proxy HTTP no transparente con autenticación añadió un nivel adicional de control sobre la navegación web, al implementar listas negras y políticas de acceso asociadas a usuarios y grupos, se reforzó la filtración del contenido permitido en la LAN, garantizando un uso responsable, regulado y supervisado de Internet dentro de la organización.

En conjunto, el ejercicio permitió visualizar la importancia de las herramientas de software libre como Endian Firewall para el fortalecimiento de la seguridad perimetral, la integración de NAT, reglas de acceso, filtrado de tráfico y políticas avanzadas de control demuestra que es posible construir soluciones robustas, escalables y eficientes, capaces de proteger información crítica y garantizar la disponibilidad de los servicios en entornos empresariales.

5 REFERENCIAS

[1] Cabello, M. C. (2020). Nethserver Tutorial | Instalación, actualización y primeros pasos. de https://www.youtube.com/watch?v=FNGmM-2fa_0&t=1615s

[2] Perfil, V. T. mi. (s/f). Con las Redes y la Nasa. Conlasredes.info. ¿Recuperado el 12 de mayo de 2025, de https://www.conlasredes.info/2021/10/endian-firewall-proteccion de-codigo.html?m=1

[3 Wang, S. S. (2019). Integrated framework for information security investment and cyber insurance. Pacific-Basin Finance Journal, 57(101173), 101173. https://doi.org/10.1016/j.pacfin.2019.101173

[4] (S/f). Edu.ec. Recuperado el 12 de mayo de 2025, de https://dspace.udla.edu.ec/bitstream/33000/10041/1/UDLA-EC TIRT-2018-16.pdf

[5] Endian Community, "Endian Firewall Documentation," [En línea]. Disponible: https://www.endian.com/

[6] 2023. Canonical (2023). Guía del Ubuntu desktop 20.04 LTS. HelpUbuntu. https://help.ubuntu.com/20.04/ubuntu help/index.html

[7] Oracle (2020), Manual de usuario VirtualBox. VirtualBox.https://www.virtualbox.org/manual/

[8] Endian UTM 3.2 Reference Manual — Endian UTM 3.2 Reference Manual. (s. f.). https://docs.endian.com/3.2/utm/index.html

[9] Jay LaCroix. (2020). Mastering Ubuntu Server : Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting

[10] Jonathan Sanchez Giraldo. (2021, 6 noviembre). VirtualBox con Endian 3.3.2, 3 Zonas: Verde, Naranjada y Roja [Vídeo]. YouTube. https://www.youtube.com/watch?v=Dvht5wCPIrI