IMPLEMENTACIÓN DE SEGURIDAD DE RED UTILIZANDO ENDIAN FIREWALL: SEGMENTACIÓN, NAT Y CONTROL DE ACCESO HTTP

Deivy Duvan Cartagena Lopez
e-mail: ddcartagena@unadvirtual.edu.co

José Alejandro Vélez Paniagua
e-mail: javelezp@unadvirtual.edu.co

María Fernanda Montoya Méndez
e-mail: mfmontoyam@unadvirtual.edu.co

Loren *Daniela Sandoval Morales*
e-mail: ldsandovalm@unadvirtual.edu.co

RESUMEN: *El presente documento aborda la implementación de medidas de seguridad en entornos GNU/Linux, específicamente mediante la configuración de GNU/Linux Endian Firewall. Se desarrollan cinco temáticas principales: la configuración de la instancia Endian en VirtualBox con sus zonas de red (LAN, WAN y DMZ), la administración del sistema operativo GNU/Linux según el tema 101 del Linux Professional Institute (LPI), la configuración de NAT para comunicación entre zonas, la habilitación de servicios en la zona DMZ, y la implementación de un Proxy HTTP no transparente con políticas de autenticación. A través de ejercicios prácticos se demuestra la configuración de interfaces de red, la gestión de hardware y arranque del sistema, y el control de acceso web mediante listas negras. Los resultados evidencian una infraestructura de seguridad perimetral funcional que permite proteger recursos internos mientras se mantiene la disponibilidad de servicios críticos.*

PALABRAS CLAVE: DMZ, Endian Firewall, GNU/Linux, NAT, Proxy HTTP, Seguridad perimetral.

1 INTRODUCCIÓN

La implementación de un firewall perimetral es un componente esencial dentro de la infraestructura de redes de cualquier organización. En este ejercicio práctico, se aborda la instalación y configuración de GNU/Linux Endian Firewall dentro de una máquina virtual en VirtualBox, enfatizando la correcta asignación y funcionamiento de sus interfaces de red.

A través de este proceso, se comprende la estructura y funciones de las zonas VERDE (LAN), ROJA (WAN) y NARANJA (DMZ), así como su importancia en la segmentación, seguridad y control del tráfico dentro de una red. Esta actividad permite desarrollar competencias técnicas clave para la administración de sistemas basados en Linux y la gestión de entornos virtualizados.

En el desarrollo de esta etapa se especifica el protocolo que se requiere para la traducción de direcciones de red (NAT), en un escenario de red desglosado, donde su núcleo es un Firewall. Este se conforma de tres áreas lógicas diferentes donde cada una contiene un nivel de seguridad distinto: las redes internas verde y naranja, más la red externa (WAN/Roja).

La implementación de un proxy HTTP no transparente con políticas de autenticación representa una solución fundamental en la arquitectura de seguridad perimetral de cualquier organización moderna. En el contexto actual, donde las amenazas cibernéticas evolucionan constantemente y el control del acceso a Internet se vuelve crítico para mantener la productividad y seguridad empresarial, la configuración adecuada de un servidor proxy con capacidades de filtrado y autenticación se convierte en una herramienta esencial.

Mejorar la seguridad del perímetro y gestionar bien los sistemas GNU/Linux son condiciones muy relevantes para la protección de la información y los servicios vinculados a la infraestructura de red de las organizaciones empresariales. Al planificar, construir y gestionar una arquitectura con una topología de red LAN, una DMZ y un firewall perimetral se espera conseguir la disponibilidad, la integridad y la confidencialidad sobre los recursos críticos.

2 OBJETIVOS

2.1 OBJETIVO GENERAL

Establecer y proteger un entorno de red basado en GNU/Linux, creando una zona DMZ que esté protegida mediante Endian Firewall, asegurando el correcto funcionamiento de los servicios principales y aplicando políticas de seguridad que consigan tener una mejor protección del sistema operativo y de los recursos de la red.

2.2 OBJETIVOS ESPECÍFICOS

• Configurar las tarjetas de red de la máquina virtual en VirtualBox para establecer correctamente las zonas

GREEN (LAN), RED (WAN) y ORANGE (DMZ) requeridas por Endian Firewall.

• Realizar la instalación completa del sistema GNU/Linux Endian, asegurando la correcta asignación de direcciones IP y parámetros de red para cada una de las zonas.

• Definir y practicar los conceptos básicos del tema 101 del material Linux Essentials de LPI, introduciendo los ejercicios guiados y exploratorios que permitan conocer el funcionamiento de la administración del sistema operativo GNU/Linux.

• Configurar la regla de NAT (Network Address Translation) demostrando el establecimiento de la comunicación desde la LAN hacia la WAN y desde la DMZ hacia Internet.

• Implementar un sistema de filtrado web mediante la creación de perfiles y listas negras que bloqueen el acceso a sitios web específicos desde la red LAN.

• Establecer un mecanismo de autenticación de usuarios creando usuarios y grupos en el sistema proxy, vinculándolos con políticas de acceso específicas.

• Aplicar normas para la seguridad perimetral en Endian Firewall permitiendo servicios HTTP y FTP del servidor web y denegando el protocolo ICMP.

3 MARCO TEÓRICO

3.1 GNU/LINUX ENDIAN FIREWALL

Endian Firewall es una distribución Linux especializada en seguridad perimetral que integra múltiples servicios de seguridad: Firewall Stateful (control de tráfico mediante iptables), Proxy HTTP/HTTPS (basado en Squid), VPN (soporte para OpenVPN e IPSec), IDS/IPS (sistema de detección y prevención de intrusiones), Antivirus (escaneo de contenido web) y Gestión Web (interfaz de administración centralizada).

3.2 ARQUITECTURA DE RED CON DMZ

La implementación del firewall se realiza en un entorno con tres zonas de seguridad:

• Zona Verde (GREEN): Red LAN interna protegida

• Zona Roja (RED): Conexión a Internet (WAN)

• Zona Naranja (ORANGE): DMZ para servidores expuestos

Esta segmentación permite aplicar políticas diferenciadas según el nivel de confianza de cada zona.

3.3 NAT (NETWORK ADDRESS TRANSLATION)

NAT es un protocolo que permite la traducción de direcciones de red. Las direcciones privadas no son enrutables en conexión directa a la red pública, explicando que solo los dispositivos internos pueden conectar con la WAN implementando la configuración de NAT. El tipo Masquerading permite que las redes privadas compartan una única dirección IP asignada a la interfaz WAN.

3.4 PROXY HTTP: CONCEPTOS FUNDAMENTALES

Un servidor proxy HTTP actúa como intermediario entre los clientes de una red local y los servidores web en Internet. Cuando un cliente realiza una solicitud HTTP, esta es interceptada por el proxy, que a su vez realiza la solicitud al servidor web destino en nombre del cliente.

3.4.1 Proxy No Transparente vs Transparente

• Proxy Transparente: Los clientes no requieren configuración especial. El tráfico HTTP es interceptado automáticamente mediante reglas de firewall.

• Proxy No Transparente: Requiere configuración explícita en cada cliente, especificando la dirección IP y puerto del servidor proxy.

3.5 SISTEMA DE AUTENTICACIÓN EN PROXIES

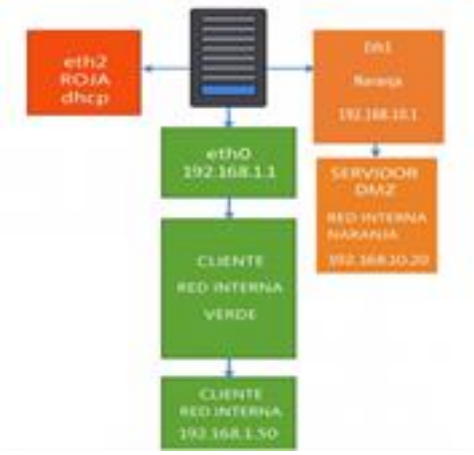
La autenticación en servidores proxy permite identificar individualmente a cada usuario que accede a Internet. Los métodos más comunes incluyen: Autenticación Básica HTTP, Autenticación NTLM, Autenticación LDAP y Autenticación Local.

4 DESARROLLO

4.1 TEMÁTICA 1: CONFIGURACIÓN DE GNU/LINUX ENDIAN EN VIRTUALBOX

Se procede con la implementación de GNU/Linux Endian con las zonas verde, roja y naranja, según la siguiente topología de red:

Ilustración 1. Topología de red implementada

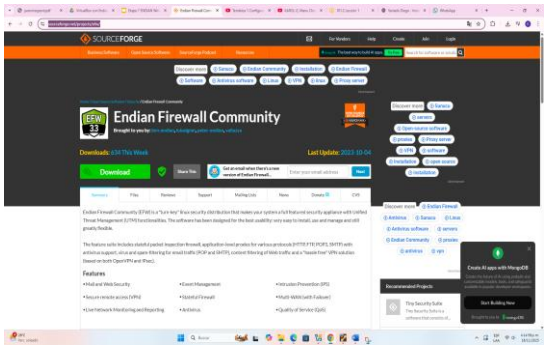


Fuente: autoría Propia

4.1.1 Instalación de ENDIAN

Se procede con la descarga de Endian Firewall desde el enlace oficial: https://sourceforge.net/projects/efw/

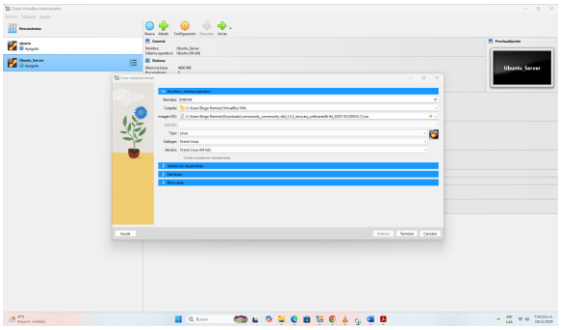
Ilustración 2. Descarga de Endian Firewall



Fuente: autoría Propia

Se configura la identificación y el sistema operativo base de la máquina virtual donde se instalará Endian Firewall, seleccionando la imagen ISO correspondiente y definiendo el tipo de sistema como Linux.

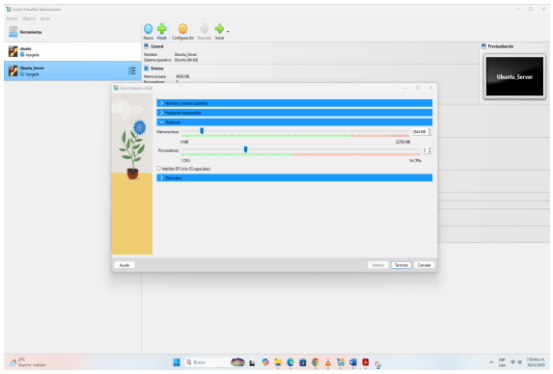
Ilustración 3. Configuración de la máquina virtual para Endian



Fuente: autoría Propia

Se configura la cantidad de recursos de procesamiento (RAM, CPU y video) que la máquina virtual de Endian usará.

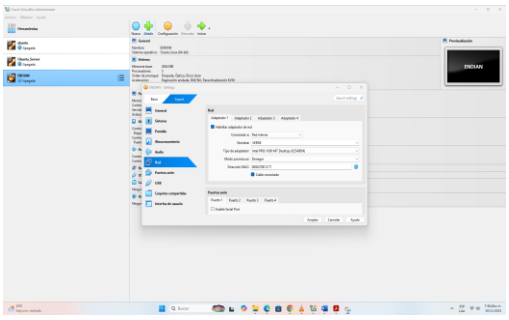
Ilustración 4. Asignación de recursos de hardware



Fuente: autoría Propia

El Adaptador 1 se configura como red interna, asignándole el nombre correspondiente a la interfaz VERDE. Esto establece la red LAN interna de Endian Firewall.

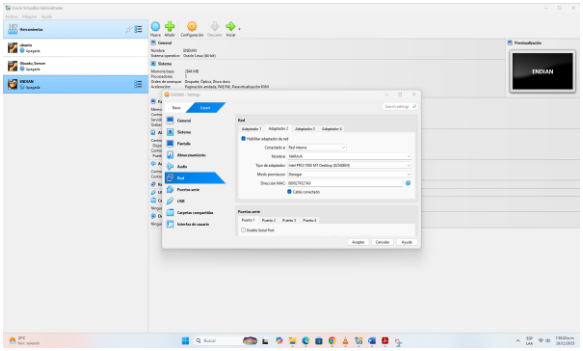
Ilustración 5. Configuración del Adaptador 1 - Zona GREEN



Fuente: autoría Propia

El Adaptador 2 se configura como red interna, asignándole el nombre correspondiente a la interfaz Naranja (DMZ).

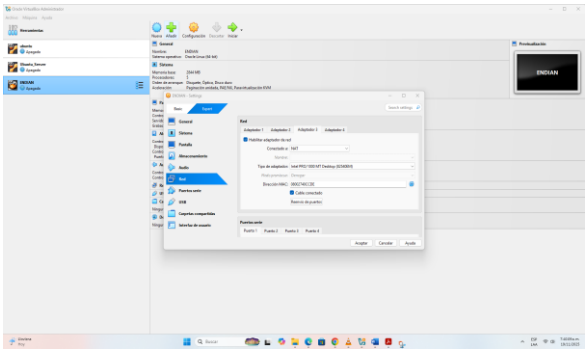
Ilustración 6. Configuración del Adaptador 2 - Zona ORANGE



Fuente: autoría Propia

Se configura el Adaptador 3 en modo NAT, permitiendo que Endian pueda tener conexión a Internet mediante la red del equipo anfitrión.

Ilustración 7. Configuración del Adaptador 3 - Zona RED (NAT)

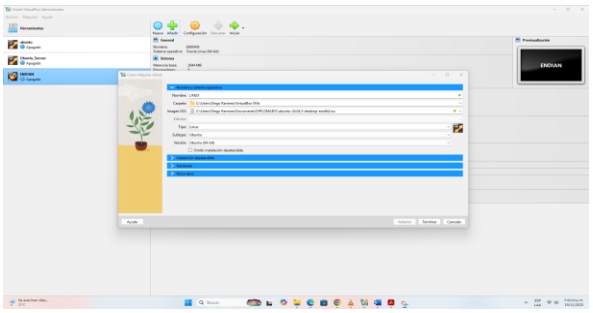


Fuente: autoría Propia

4.1.2 Instalación del Linux Cliente

Se procede con la instalación de Ubuntu cliente, configurando la identificación y el sistema operativo base de la máquina virtual.

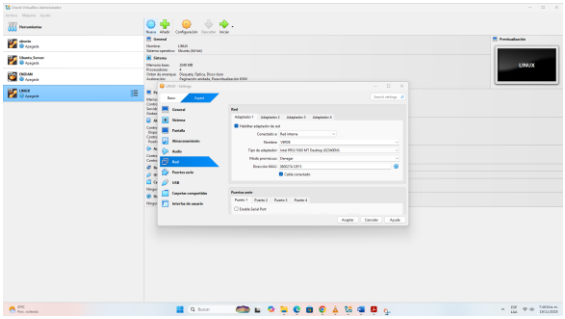
Ilustración 8. Configuración de la máquina virtual Ubuntu Cliente



Fuente: autoría Propia

Se configura el Adaptador 1 de la máquina virtual LINUX para que funcione dentro de una red interna VirtualBox, permitiendo comunicación con el firewall ENDIAN.

Ilustración 9. Configuración de red del cliente Ubuntu

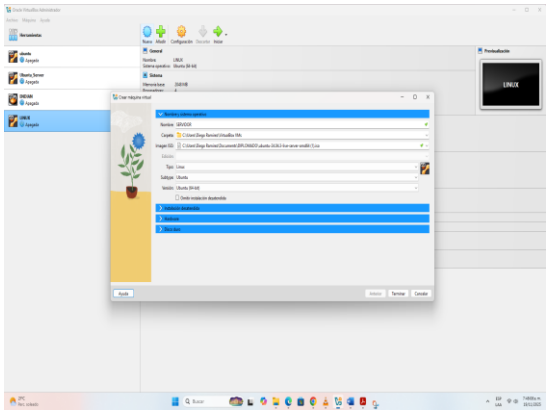


Fuente: autoría Propia

4.1.3 Instalación del Servidor DMZ

Se procede con la instalación del servidor que se ubicará en la zona DMZ (ORANGE).

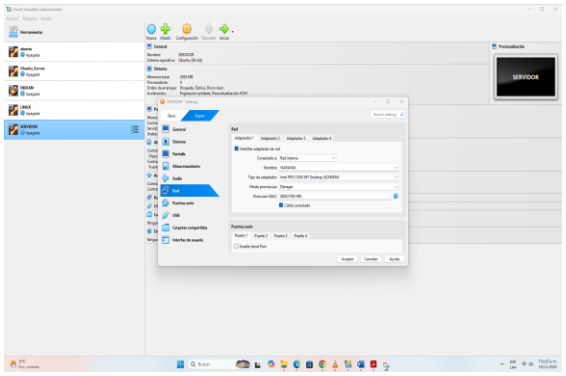
Ilustración 10. Configuración del servidor DMZ



Fuente: autoría Propia

Se asigna la configuración del Adaptador 1 del servidor a la red interna NARANJA, que funcionará como la DMZ.

Ilustración 11. Configuración de red del servidor DMZ

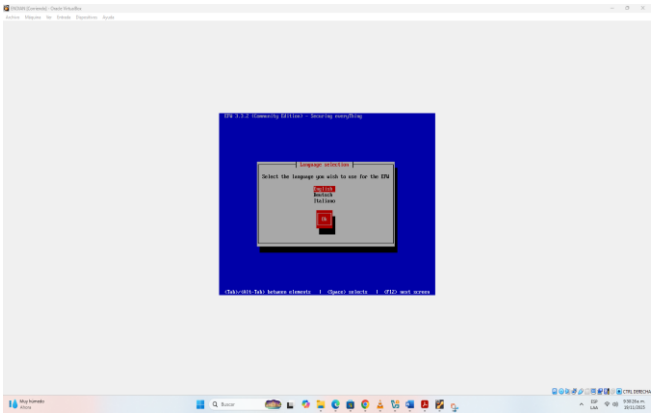


Fuente: autoría Propia

4.1.4 Proceso de Instalación de Endian

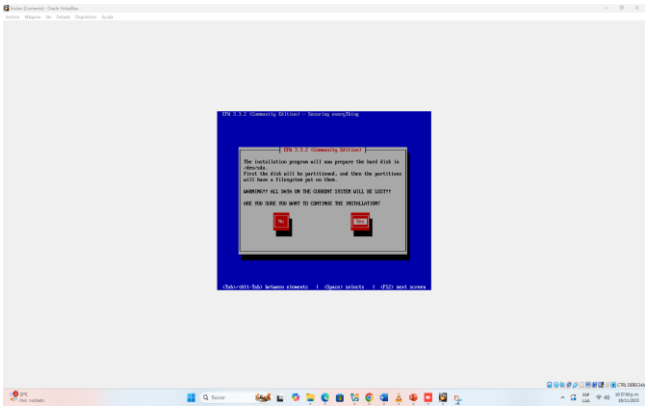
El instalador de Endian muestra el menú de selección de idioma para iniciar el proceso de instalación del firewall.

Ilustración 12. Selección de idioma en instalador Endian



Fuente: autoría Propia

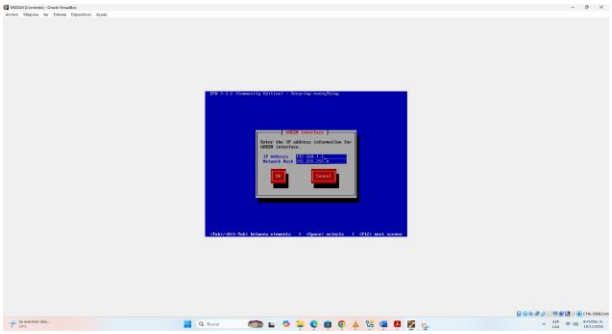
Ilustración 13. Confirmación para borrar disco e instalar



Fuente: autoría Propia

Se define la IP del firewall en la red interna (GREEN). Se asigna la dirección 192.168.1.1 con máscara /24.

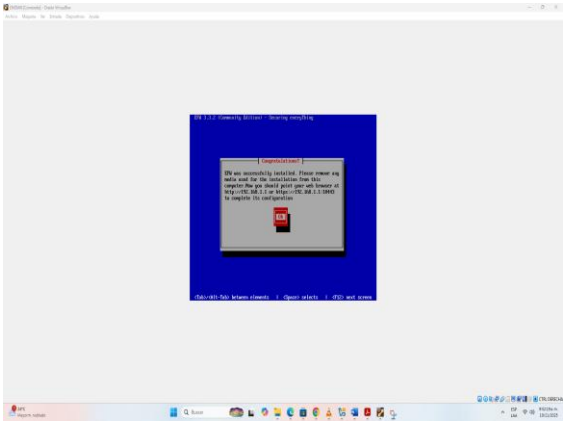
Ilustración 14. Configuración de IP para zona GREEN



Fuente: autoría Propia

El instalador informa que es posible acceder a la configuración inicial desde un navegador web usando: http://192.168.1.1 o https://192.168.1.1:10443

Ilustración 15. Finalización de instalación de Endian

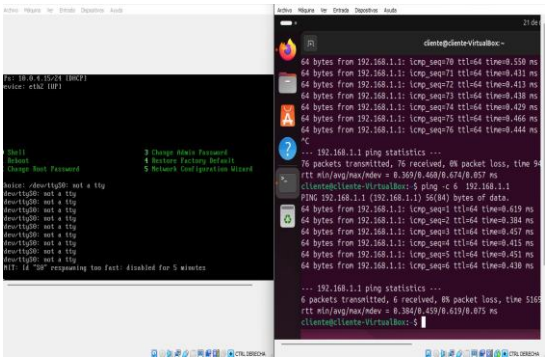


Fuente: autoría Propia

4.1.5 Verificación de Conectividad

Se verifica la comunicación entre Endian y el cliente. Desde la máquina Ubuntu se realizan pruebas exitosas de conectividad hacia la dirección IP GREEN del firewall (192.168.1.1).

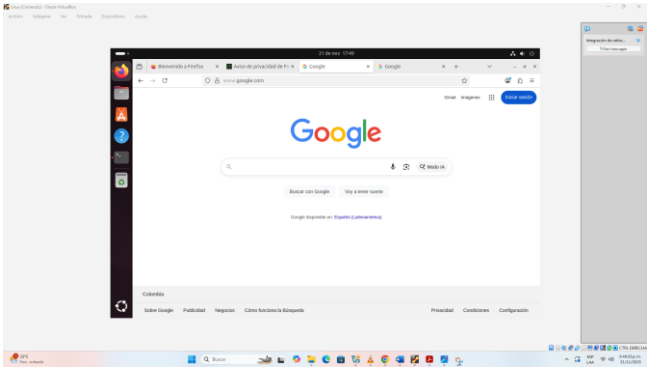
Ilustración 16. Prueba de conectividad desde cliente Ubuntu



Fuente: autoría Propia

Se confirma que el cliente Ubuntu se comunica correctamente con la red GREEN (192.168.1.1), tiene acceso a la red RED/DMZ (192.168.10.1) y puede llegar al servidor en la DMZ (192.168.10.20).

Ilustración 17. Verificación de acceso a Internet

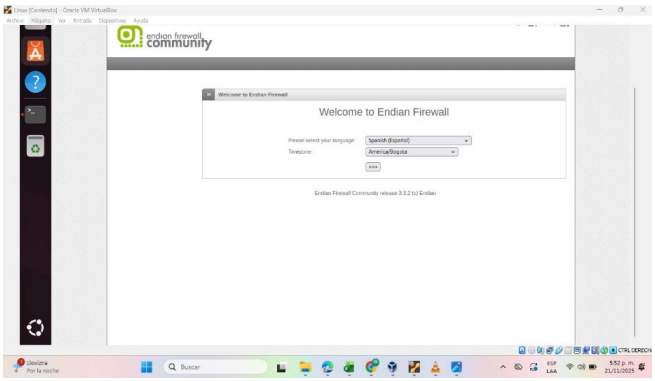


Fuente: autoría Propia

4.1.6 Configuración Web de Endian

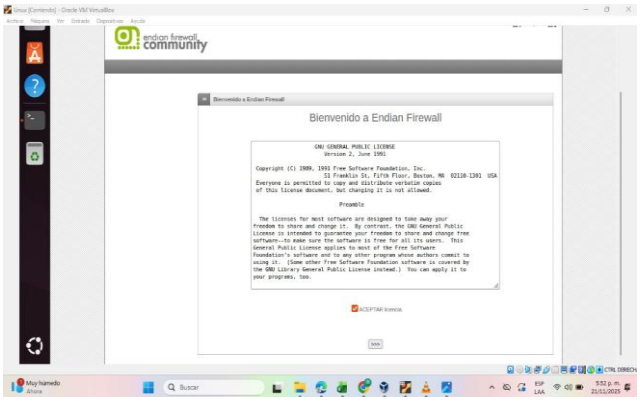
Desde el equipo cliente se accede a la interfaz de administración mediante https://192.168.1.1:10443

Ilustración 18. Interfaz web inicial de Endian



Fuente: autoría Propia

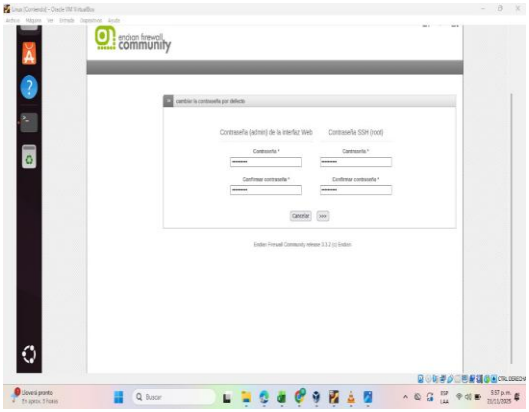
Ilustración 19. Aceptación de términos de uso



Fuente: autoría Propia

Se deben cambiar las contraseñas por defecto tanto del usuario admin (interfaz web) como del usuario root (acceso SSH).

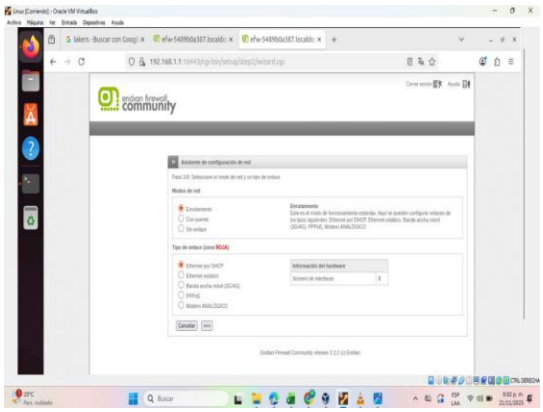
Ilustración 20. Configuración de contraseñas



Fuente: autoría Propia

Se configura el modo de red Enrutamiento y el tipo de enlace Ethernet por DHCP para la zona ROJA (WAN).

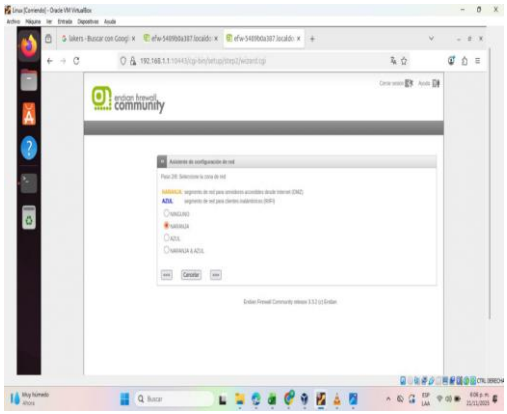
Ilustración 21. Configuración de red - Modo enrutamiento



Fuente: autoría Propia

Se habilita la zona NARANJA para la DMZ y se configuran los parámetros de la zona ROJA.

Ilustración 22. Activación de zona NARANJA (DMZ)



Fuente: autoría Propia

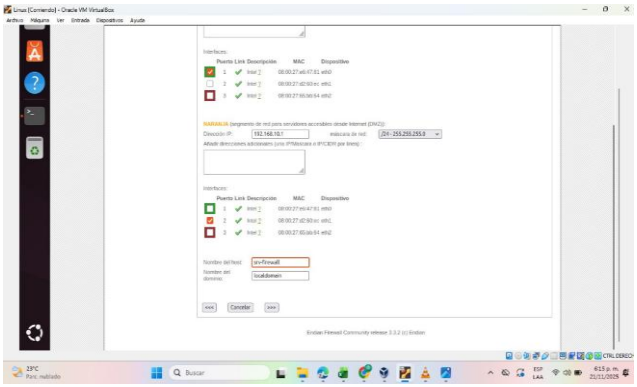
Se configuran los parámetros de la zona VERDE (LAN): IP interna del firewall (192.168.1.1), servidor DHCP activado.

Ilustración 23. Configuración de zona GREEN

Fuente: autoría Propia

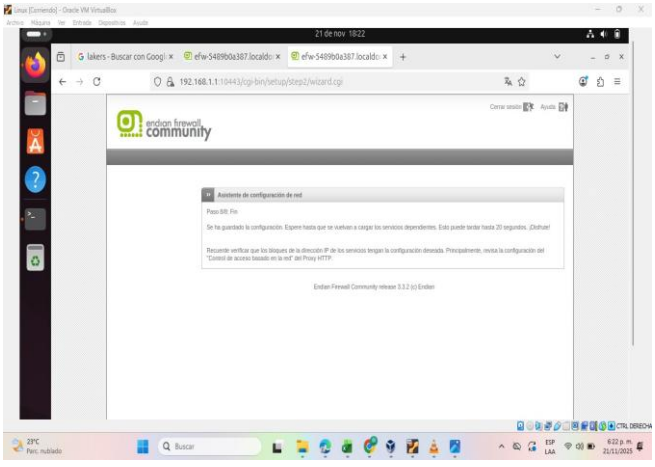
Se configuran los parámetros de la zona NARANJA (DMZ). Se asigna la IP 192.168.10.1 con máscara /24.

Ilustración 24. Configuración de zona ORANGE (DMZ)



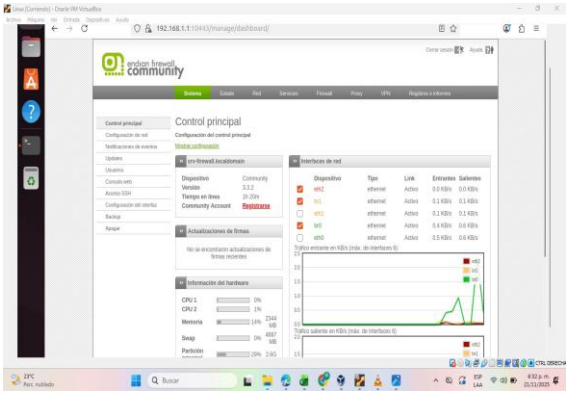
Fuente: autoría Propia

Ilustración 25. Finalización del asistente de configuración



Fuente: autoría Propia

Ilustración 26. Panel principal de Endian Firewall

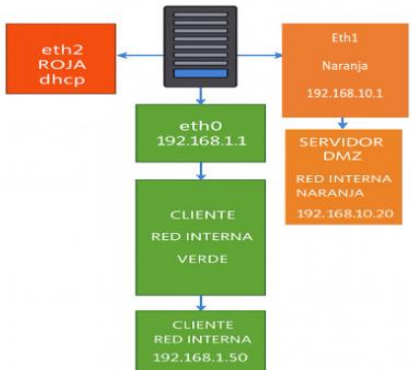


Fuente: autoría Propia

4.2 TEMÁTICA 2: CONFIGURACIÓN NAT

La configuración de NAT (Network Address Translation / Traducción de Direcciones de Red) permite el establecimiento de la comunicación desde la LAN hacia la WAN y desde la zona DMZ hacia Internet.

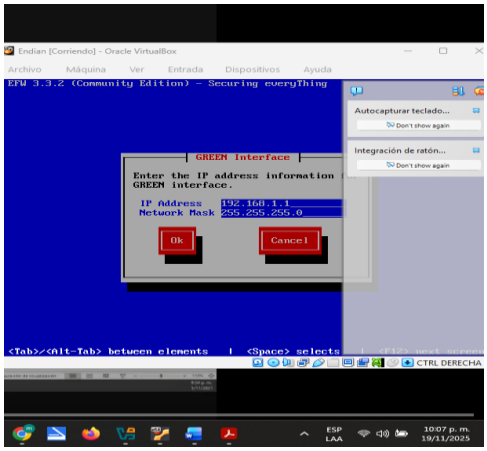
Ilustración 27. Zonas seleccionadas para la configuración



Fuente: autoría Propia

Se realiza la configuración de las zonas mediante red y se procede con la instalación de Endian.

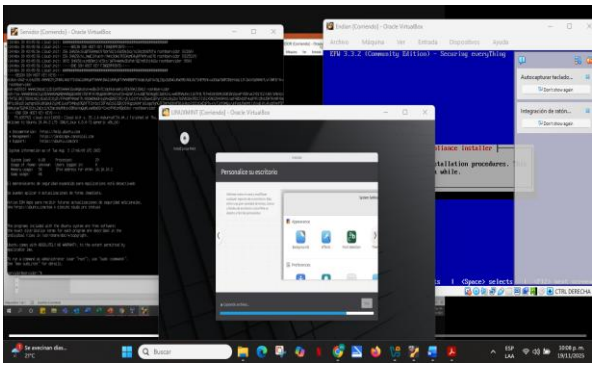
Ilustración 28. Configuración de zonas en Endian



Fuente: autoría Propia

Se realiza la instalación de Linux Mint como cliente, Ubuntu Server como servidor y Endian con la configuración de la zona verde y zona naranja.

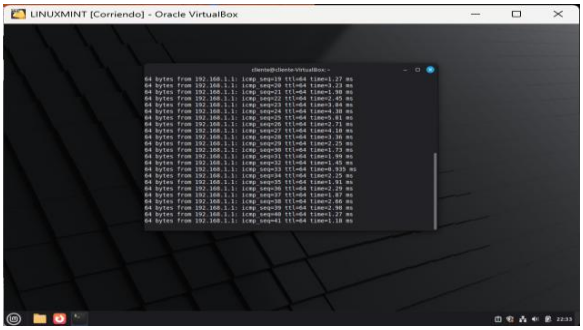
Ilustración 29. Instalación de cliente y servidor



Fuente: autoría Propia

Se observa que la IP dada por Endian fue reconocida por medio de Linux Mint.

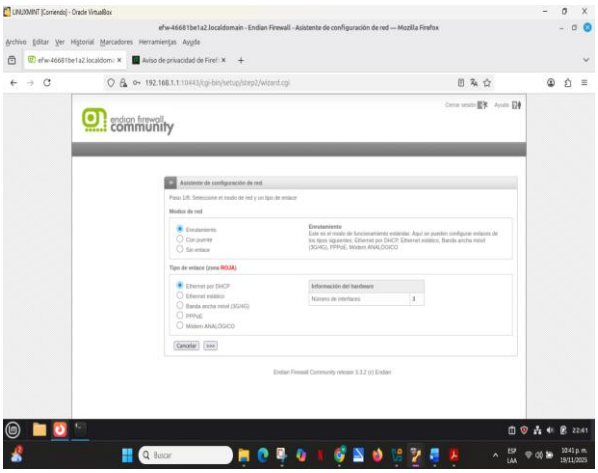
Ilustración 30. Reconocimiento de IP en Linux Mint



Fuente: autoría Propia

Se verifica que la instalación fue exitosa. Se confirman las 3 tarjetas de red en Endian.

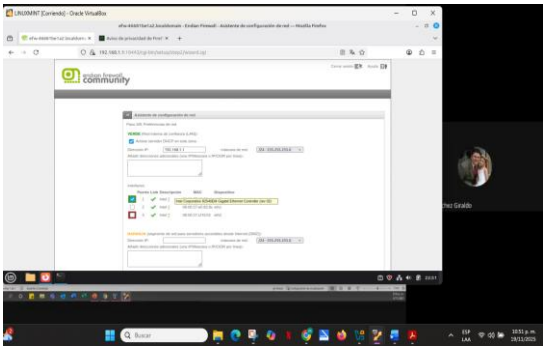
Ilustración 31. Verificación de tarjetas de red



Fuente: autoría Propia

Se verifica la configuración de la red verde 192.168.1.1, la red naranja y la red roja.

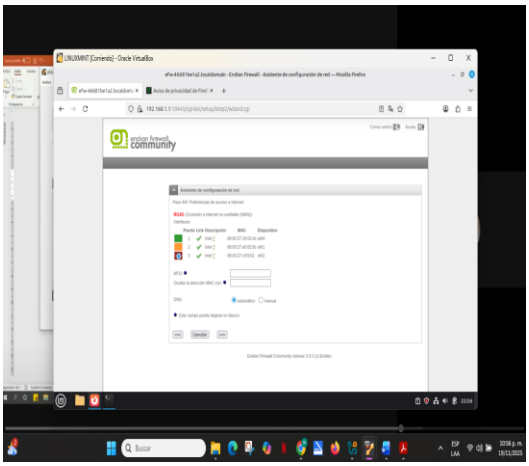
Ilustración 32. Estado de las tres zonas de red



Fuente: autoría Propia

Se realiza la configuración de la red naranja 192.168.10.1

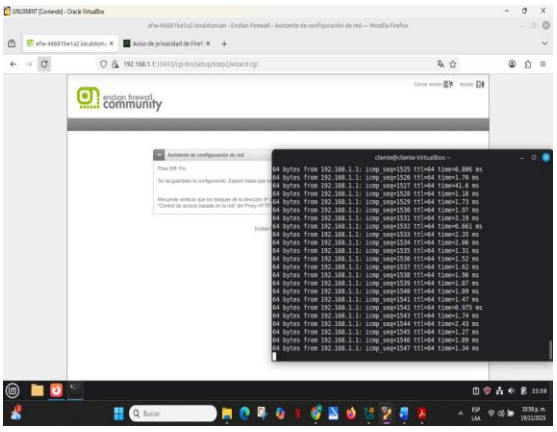
Ilustración 33. Configuración de red naranja



Fuente: autoría Propia

Se verifica que con la configuración asignada el servidor empezó a reconocer el cambio.

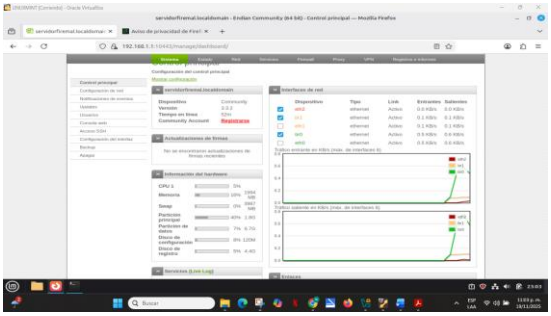
Ilustración 34. Reconocimiento de cambios en servidor



Fuente: autoría Propia

Se observan las tres redes configuradas correctamente.

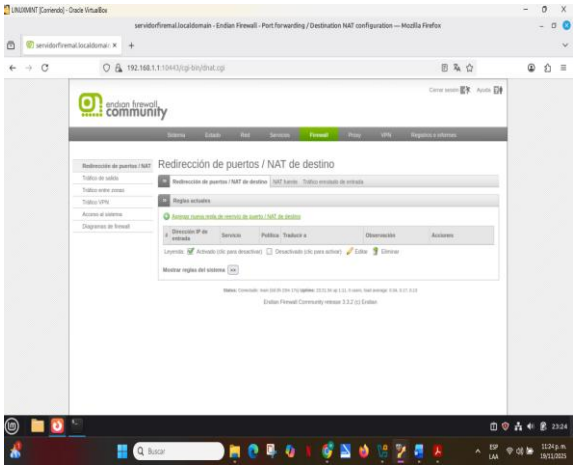
Ilustración 35. Vista de las tres redes configuradas



Fuente: autoría Propia

Ya realizados los pasos de configuración, se continúa con la temática. En el menú Firewall se encuentran diferentes opciones.

Ilustración 36. Menú Firewall de Endian

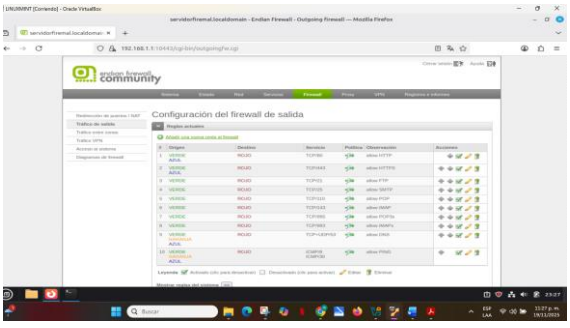


Fuente: autoría Propia

4.2.1 Configuración NAT desde LAN hacia WAN

Entre las opciones se encuentra tráfico de salida donde se verifica que Endian realizó la configuración para que la zona verde salga a la zona roja en algunos servicios de navegación.

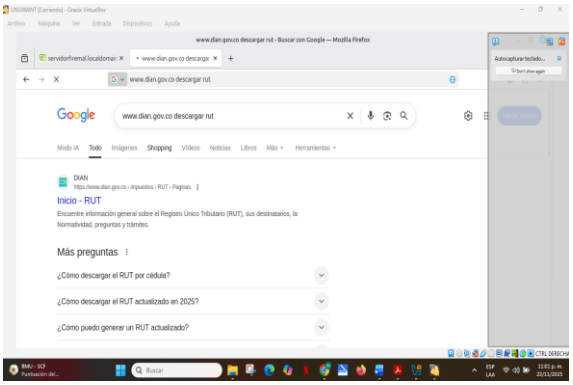
Ilustración 37. Configuración de tráfico de salida



Fuente: autoría Propia

Se visualiza la conexión a Internet www desde la zona LAN.

Ilustración 38. Verificación de conexión a Internet

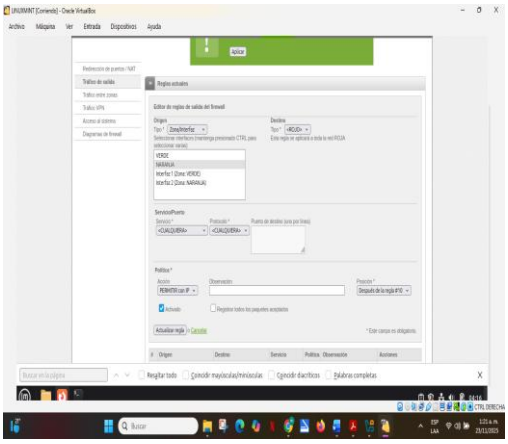


Fuente: autoría Propia

4.2.2 Configuración NAT desde DMZ hacia Internet

Se configura la regla de NAT que crea el protocolo de enmascaramiento (Masquerading), el cual advierte que se debe cambiar la dirección IP antes de enviarla a Internet.

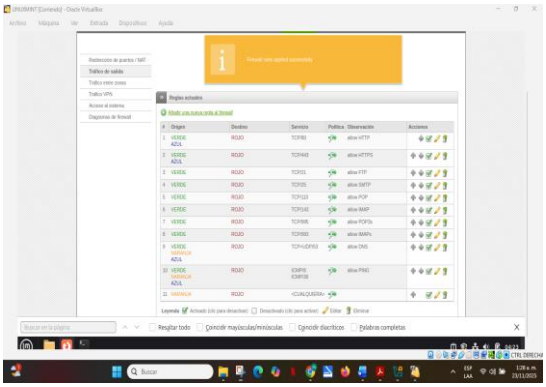
Ilustración 39. Configuración de regla NAT Masquerading



Fuente: autoría Propia

La regla de NAT se encuentra en el ítem número 11.

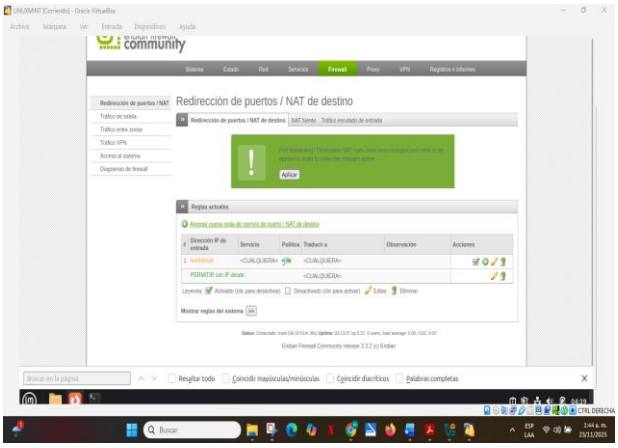
Ilustración 40. Ubicación de regla NAT



Fuente: autoría Propia

En la primera opción aparece el reenvío de puertos NAT.

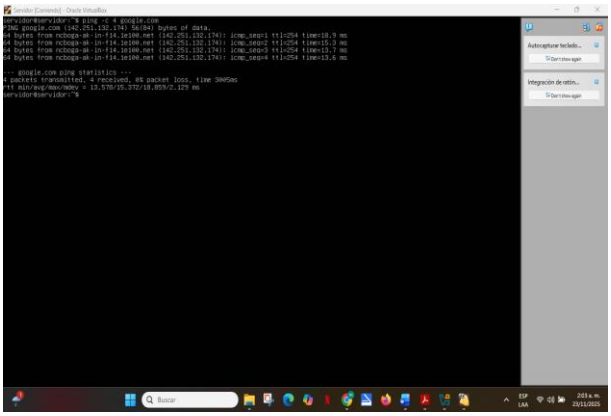
Ilustración 41. Reenvío de puertos NAT



Fuente: autoría Propia

Se demuestra que desde el servidor es posible conectarse desde la zona desmilitarizada (DMZ).

Ilustración 42. Conexión desde DMZ

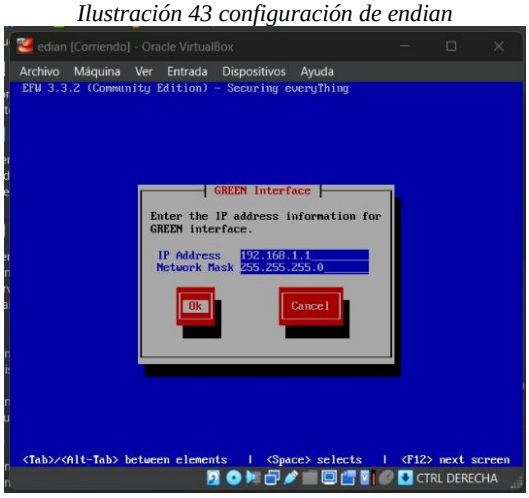


Fuente: autoría Propia

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

En este punto, realicé la configuración estática de la 'GREEN Interface'. Para asegurar la identificación del dispositivo dentro de la red, asigné la dirección IP 192.168.1.1. Paralelamente, establecí la Máscara de Red en 255.255.255.0. Esta acción delimita el segmento de red y es un requisito fundamental antes de proceder a la validación final de los parámetros.

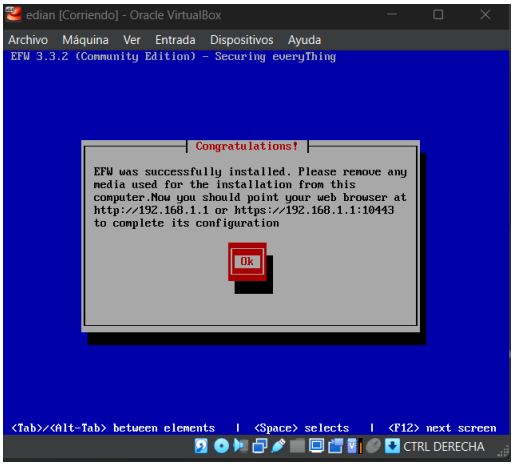
Ilustración 43 configuración de endian



Fuente: autoría Propia

En este punto, recibí la confirmación de que EFW ha sido instalado con éxito. Como acción inmediata, procedí a retirar cualquier medio de instalación del equipo. La pantalla me indica que, para completar la configuración, debo acceder al dispositivo a través de mi navegador web usando la Dirección IP que configuré previamente (192.168.1.1), ya sea por HTTP o HTTPS. Esta es la fase final antes de la puesta en marcha.

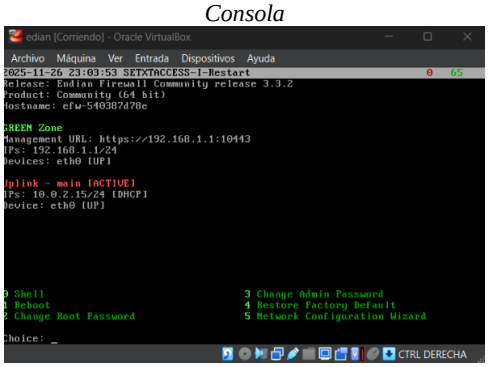
Ilustración 44 Instalación EFW Completada Acceso Web



Fuente: autoría Propia

En este punto, valido el estado operacional de Endian Firewall. La consola confirma la activación de la GREEN Zone con la IP estática 192.168.1.1 y la conexión Uplink funcional por DHCP. Esta verificación es crucial, ya que la IP de la zona GREEN confirma que ahora puedo acceder a la configuración inicial desde un navegador web. El acceso debe realizarse a través de la URL de gestión (https://192.168.1.1:10443) para finalizar la puesta en marcha.

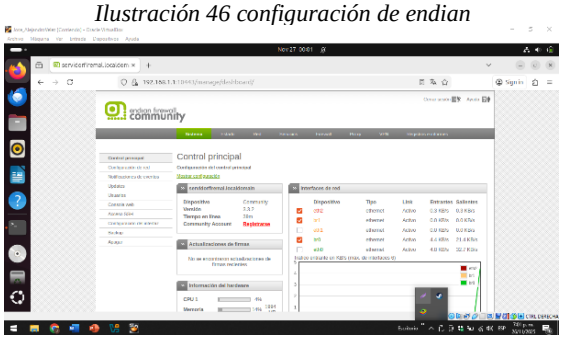
Ilustración 45 Menú Principal Endian Firewall Consola



Fuente: autoría Propia

En este punto, accedí al Asistente de Configuración del Endian Firewall utilizando la URL segura https://192.168.1.1:10443, tal como me indicó el instalador. Estoy en el Paso 3 configurando la Zona VERDE (red interna). Verifico que el firewall active el servidor DHCP para asignar IPs automáticamente y confirmo la IP estática principal (192.168.1.1). Esta interfaz es la puerta de enlace hacia mi red de confianza.

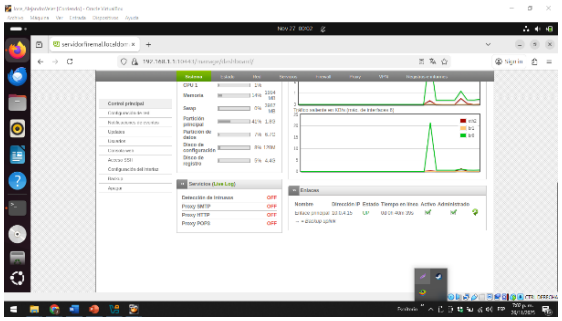
Ilustración 46 configuración de endian



Fuente: autoría Propia

Con el objetivo de permitir servicios de la Zona DMZ hacia la red, procedí a configurar el acceso a Internet (WAN). Seleccioné el puerto RED (eth2) como mi interfaz externa. Esta configuración de enlace a Internet es crucial, pues es el prerrequisito para luego habilitar y exponer de forma segura los servicios de la Zona NARANJA (DMZ) hacia el exterior. Adicionalmente, definí las preferencias de DNS.

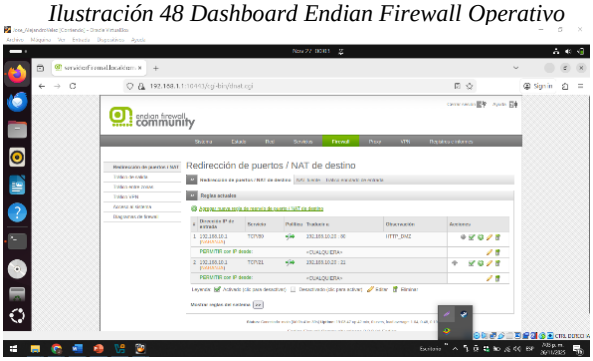
Ilustración 47 Configuración Interfaces Endian Firewall Zonas



Fuente: autoría Propia

Habiendo completado la configuración de red, procedí a la autenticación en la interfaz web de Endian Firewall. Al acceder a la URL segura (https://192.168.1.1:10443), el sistema me solicitó el Nombre de usuario y la Contraseña. Este requisito de seguridad es fundamental para proteger el acceso a los ajustes finales del firewall y continuar con el asistente que permitirá los servicios de la DMZ

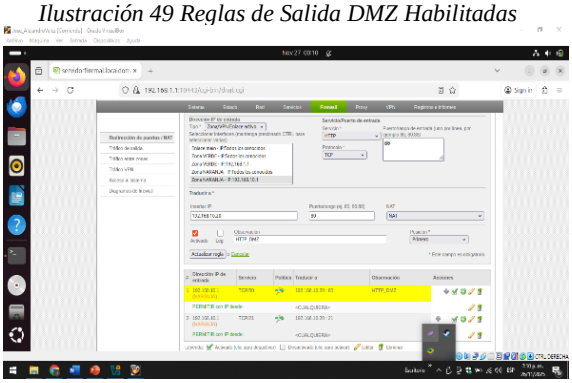
Ilustración 48 Dashboard Endian Firewall Operativo



Fuente: autoría Propia

Tras la autenticación exitosa, accedí al 'Control Principal' (Dashboard) del firewall. En este punto, verifico el estado del sistema y la actividad de las interfaces de red. Lo más importante para la TEMÁTICA 3 es que las tres zonas críticas están Activas: RED (WAN), ORANGE (DMZ) y GREEN (LAN). Esto confirma que el firewall está totalmente operativo y listo para definir las políticas de servicio de la DMZ.

Ilustración 49 Reglas de Salida DMZ Habilitadas



Fuente: autoría Propia

En este punto, procedí a configurar las reglas del 'Firewall de salida'. Para cumplir con la TEMÁTICA 3, que es permitir servicios de la DMZ, creé y validé reglas específicas. Habilité explícitamente el tráfico desde la Zona NARANJA (DMZ) hacia la Zona ROJA (Internet/WAN), permitiendo servicios esenciales como HTTP (puerto 80) y FTP (puerto 21). Esto asegura que los servidores de la DMZ puedan acceder a la red externa.

Ilustración 50 Restricción de Tráfico para DMZ

Fuente: autoría Propia

En este punto, concluí la optimización de la seguridad del Firewall Inter-zona para proteger mi DMZ. Implementé una regla estricta para el tráfico de la Zona VERDE a NARANJA, aplicando una política de 'Negar' a protocolos específicos como ICMP. El resultado positivo de esta configuración es que reforcé la seguridad de la DMZ, asegurando que los clientes internos no puedan comunicarse libremente con los servidores, limitando así las posibles amenazas.

4.4 TEMÁTICA 5: IMPLEMENTACIÓN DE PROXY HTTP NO TRANSPARENTE

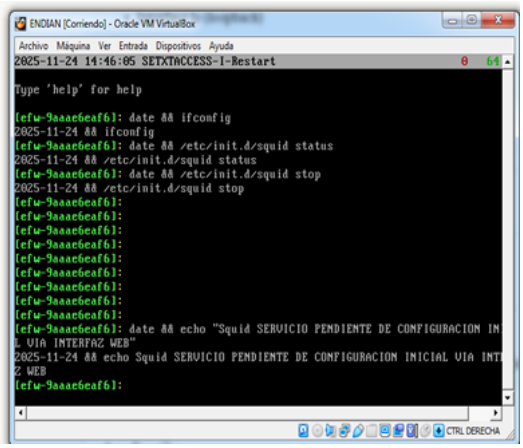
Se implementa un Proxy HTTP no transparente con políticas de autenticación en GNU/Linux Endian Firewall.

4.5.1 Verificación del Entorno Inicial

Antes de proceder con la implementación del proxy HTTP, es necesario verificar que el entorno Endian Firewall esté correctamente configurado.

```
root@endian:~# date && ifconfig
```

Ilustración 51 *Verificación de interfaces de red*

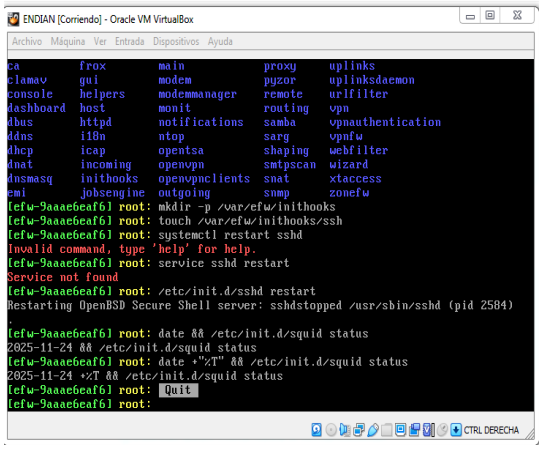


Fuente: autoría Propia

Se verifica el estado actual del servicio Squid (proxy):

```
root@endian:~# date && /etc/init.d/squid
status
```

Ilustración 52 Estado del servicio Squid

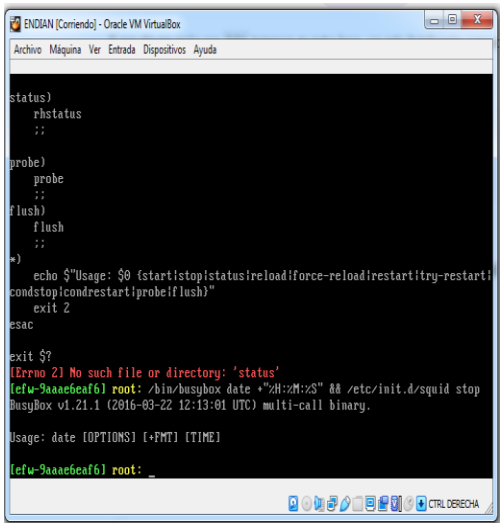


Fuente: autoría Propia

Para realizar cambios en la configuración, se detiene el servicio:

```
root@endian:~# date && /etc/init.d/squid stop
```

Ilustración 53 Parada del servicio Squid

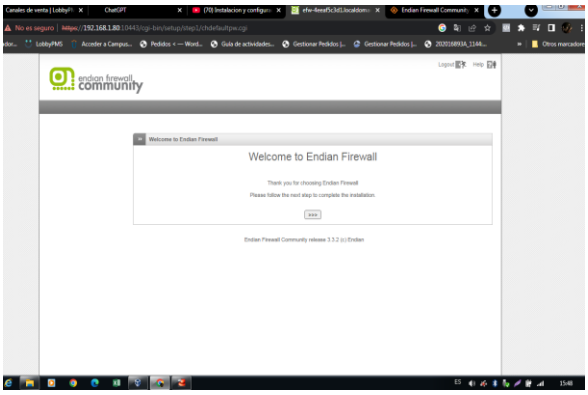


Fuente: autoría Propia

4.5.2 Implementación del Proxy HTTP

Se accede a la interfaz web de Endian Firewall desde una estación de trabajo en la zona verde: https://192.168.1.80:10443

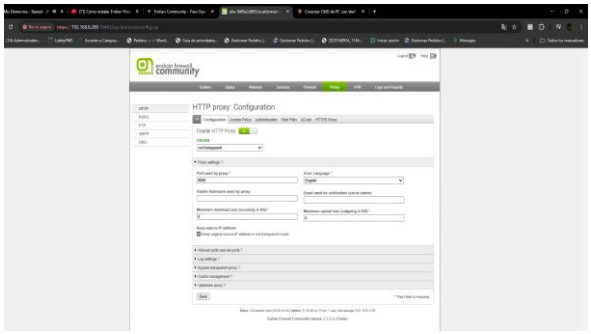
Ilustración 54 Acceso a interfaz web de administración



Fuente: autoría Propia

Se navega a la sección de configuración del proxy: Proxy → HTTP → Configuración

Ilustración 55 Navegación al módulo de Proxy

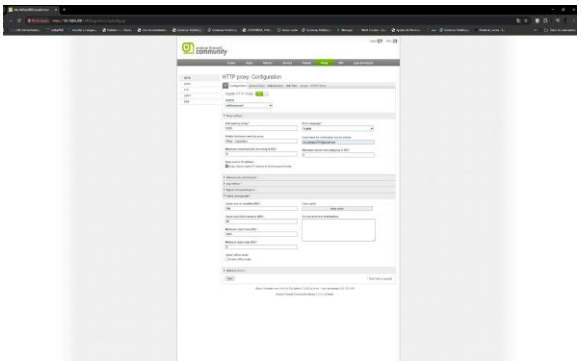


Fuente: autoría Propia

Se configuran los parámetros básicos del proxy en modo no transparente:

- Habilitar Proxy: Activado
- Puerto: 3128 (puerto estándar para proxy)
- Modo Transparente: Desactivado
- Interfaces de escucha: GREEN
- Tamaño de caché: 100 MB

Ilustración. 56 configuración del Proxy en modo no transparente

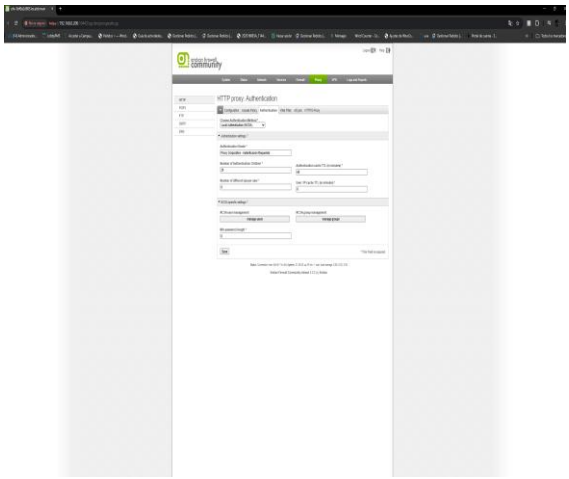


Fuente: autoría Propia

Se activa el sistema de autenticación:

- Autenticación requerida: Activado
- Método de autenticación: Local
- Realm: Proxy Corporativo - Autenticación Requerida

Ilustración 57 Activación del sistema de autenticación



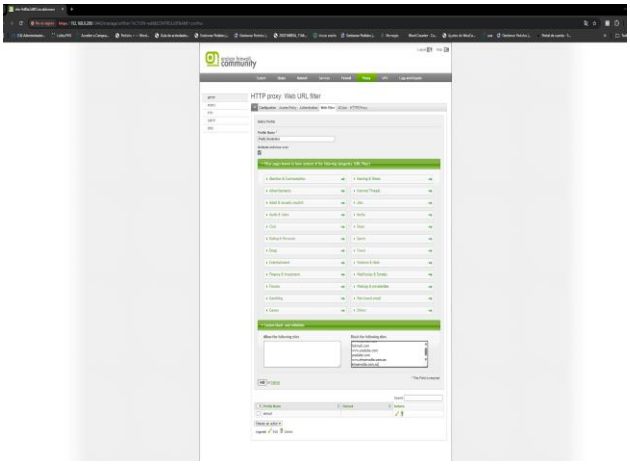
Fuente: autoría Propia

4.5.3 Creación de Perfil y Lista Negra

Se navega a Proxy → HTTP → Perfiles de Acceso y se crea un nuevo perfil:

- Nombre del perfil: Perfil_Restrictivo
- Descripción: Perfil con sitios bloqueados para usuarios estándar
- Acción por defecto: Permitir
- Filtrado de contenido: Activado

Ilustración.58 Creación del perfil de filtrado

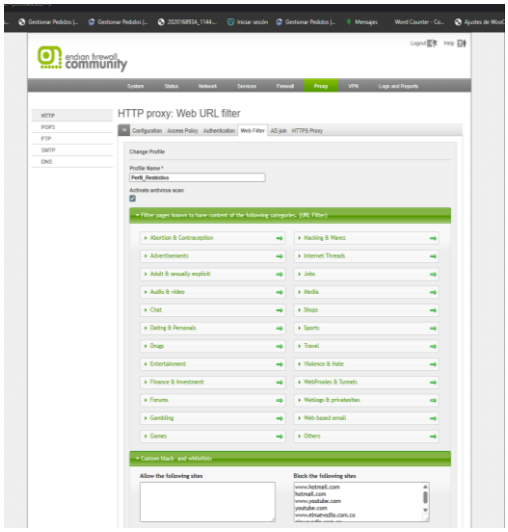


Fuente: autoría Propia

Se configura la Lista Negra con los siguientes dominios:

- www.hotmail.com / hotmail.com
- www.youtube.com / youtube.com
- www.elnuevodia.com.co / elnuevodia.com.co

Ilustración. 59 configuración de Lista Negra



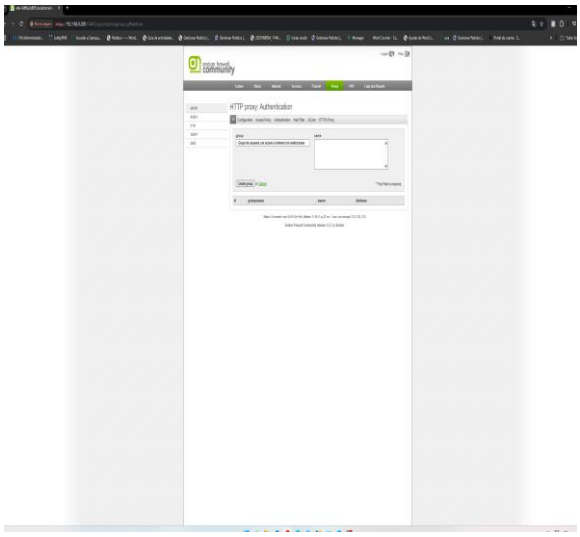
Fuente: autoría Propia

4.5.4 Configuración de Autenticación de Usuario

Se navega a Proxy → HTTP → Autenticación → Grupos y se crea un nuevo grupo:

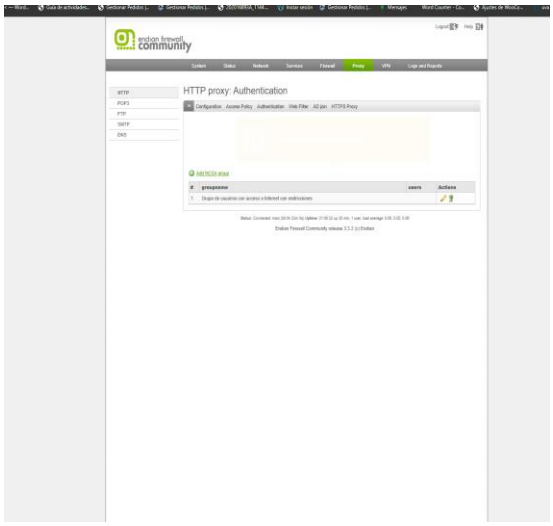
- Nombre del grupo: usuarios_internet
- Descripción: Grupo de usuarios con acceso a Internet con restricciones
- Estado: Habilitado

Ilustración.60 Creación del grupo de usuarios



Fuente: autoría Propia

Ilustración 61 Configuración del grupo

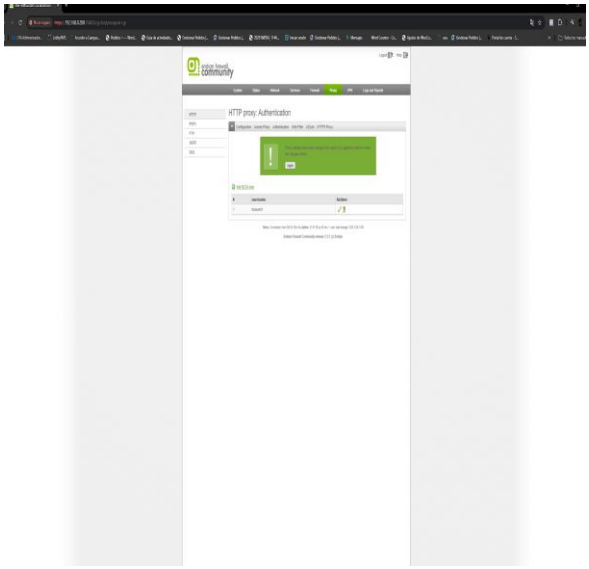


Fuente: autoría Propia

Se crea un usuario de prueba:

- Nombre de usuario: dusuario1
- Nombre completo: Usuario de Prueba 1
- Email: usuario1@empresa.local
- Grupo: usuarios_internet

Ilustración 62 Creación del usuario



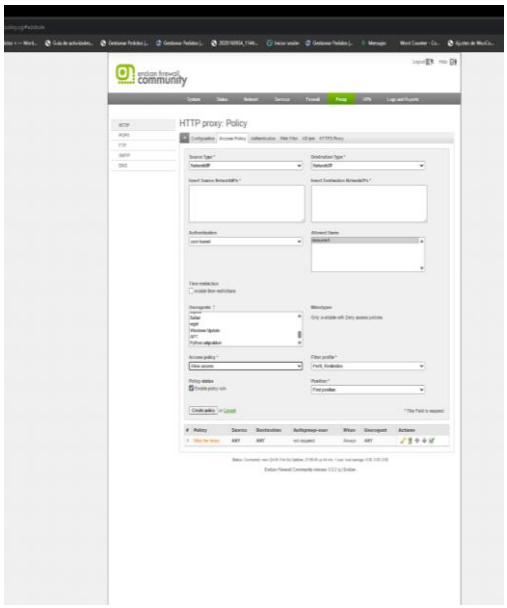
Fuente: autoría Propia

4.5.5 Establecimiento de Políticas de Acceso

Se navega a Proxy → HTTP → Políticas de Acceso y se crea una nueva política:

- Nombre: Politica_Usuarios_Autenticados
- Prioridad: 1 (mayor prioridad)
- Estado: Habilitado

Ilustración 63 Creación de política de acceso

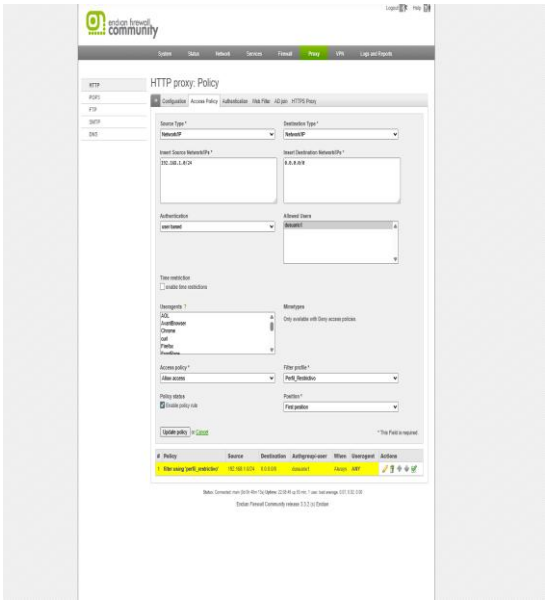


Fuente: autoría Propia

En la configuración de la política se vinculan los elementos:

- Origen: Zona GREEN, Red 192.168.1.0/24
- Autenticación: Requerir, Grupos: usuarios_internet
- Perfil de filtrado: Perfil_Restrictivo
- Horario: Aplicar siempre (24/7)

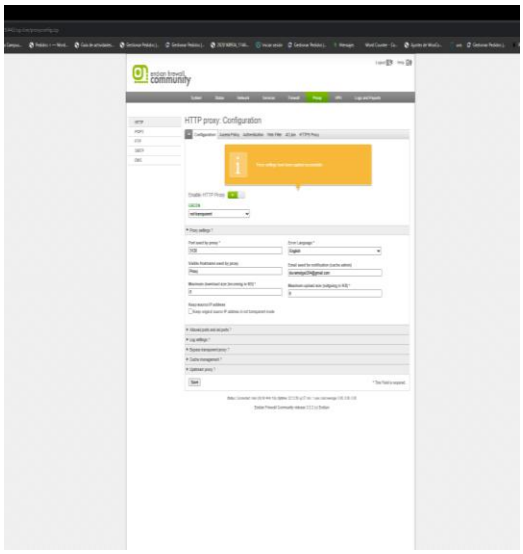
Ilustración 64 Vinculación de elementos en política



Fuente: autoría Propia

Se aplica la configuración:

Ilustración 65 Aplicación de cambios



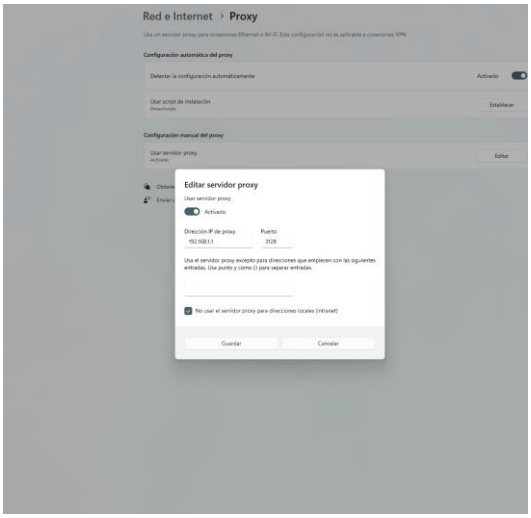
Fuente: autoría Propia

4.5.6 Pruebas de Funcionamiento

Desde una estación de trabajo Ubuntu en la zona GREEN, se configura el navegador Firefox con el proxy manual:

- Proxy HTTP: 192.168.1.1
- Puerto: 3128
- Usar este proxy para todos los protocolos: Activado

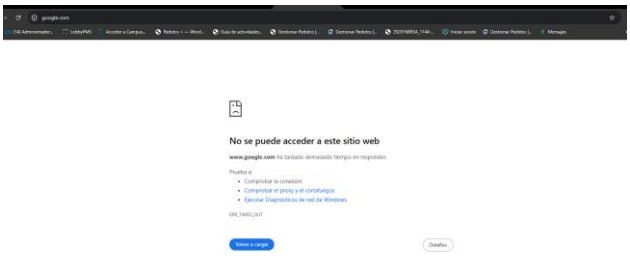
Ilustración 66 Configuración del proxy en el cliente



Fuente: autoría Propia

Al intentar acceder a un sitio web, el navegador solicita credenciales de autenticación:

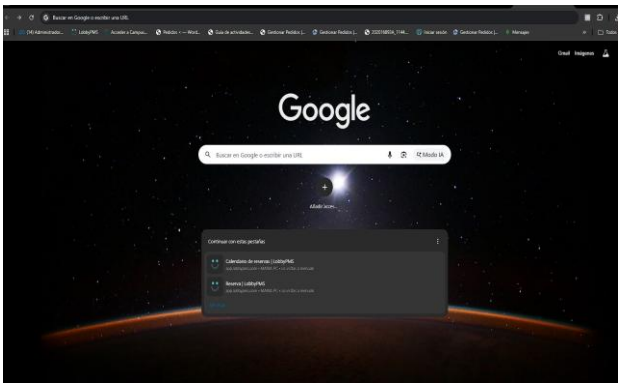
Ilustración 67 Solicitud de autenticación



Fuente: autoría Propia

Tras ingresar las credenciales correctas, se verifica acceso exitoso a sitios permitidos:

Ilustración 68 Acceso exitoso a sitios permitidos



Fuente: autoría Propia

5 CONCLUSIONES

La asignación correcta de las tarjetas de red para cada zona (LAN, WAN y DMZ) evidenció que la virtualización es una herramienta efectiva para simular entornos reales de ciberseguridad sin comprometer infraestructuras físicas.

La implementación efectiva de Endian Firewall demostró que un sistema basado en GNU/Linux puede ofrecer una administración centralizada y robusta del tráfico de red, facilitando el control de servicios y la protección de recursos internos.

La configuración de NAT de tipo Masquerading en la central de Endian Firewall fue exitosa siguiendo las reglas de implementación que dan acceso a las redes privadas LAN-Verde y DMZ-Naranja, las cuales de forma eficiente comparten una única dirección IP asignada a la interfaz WAN-Roja.

La zona DMZ ahora posee conectividad para ejecutar actualizaciones de seguridad, también puede efectuar consultas DNS sumado a múltiples funciones operativas, asegurando su independencia de la Red Verde y permitiendo que el sistema interno interactúe con herramientas externas de la WAN.

La puesta en funcionamiento de una arquitectura DMZ a través de Endian Firewall ayuda a mejorar la seguridad perimetral, puesto que permite la separación de los servicios públicos y del núcleo de la red interna reduciendo la superficie de exposición a ataques desde el exterior.

La práctica en la administración de servicios en GNU/Linux, junto a la revisión del material Linux Essentials confiere al estudiante la posibilidad de iniciar, detener y monitorear servicios críticos para asegurar su disponibilidad y correcto funcionamiento.

La implementación del proxy HTTP no transparente en GNU/Linux Endian Firewall ha demostrado ser una solución robusta y efectiva para el control del acceso web corporativo. La configuración detallada del servicio Squid permitió establecer un sistema de filtrado granular que cumple con los requisitos de seguridad establecidos.

El sistema de autenticación implementado mediante usuarios locales y grupos ha probado ser eficiente para entornos de mediana escala. La vinculación entre usuarios, grupos, perfiles de filtrado y políticas de acceso crea un ecosistema de seguridad coherente.

Las pruebas realizadas confirmaron la efectividad del sistema de filtrado mediante listas negras. Los sitios objetivo fueron bloqueados exitosamente, demostrando que el sistema puede prevenir el acceso a contenido no deseado o potencialmente improductivo.

El ejercicio práctico de instalación y configuración consolidó competencias en administración de redes y seguridad perimetral, reforzando la capacidad de implementar arquitecturas LAN, WAN y DMZ utilizando herramientas de código abierto en escenarios de aprendizaje controlados.

6 REFERENCIAS

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

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

[3] Linux Mint. (2006). Manual de referencia. Linux Mint. https://linuxmint.com/edition.php?id=322

[4] Linux Professional Institute. (2022). Tema 101: Determinar y configurar los ajustes de hardware. LPI. https://learning.lpi.org/es/learning-materials/101-500/101/101.1/

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

[6] SourceForge. (s.f.). Endian Firewall Community. https://sourceforge.net/projects/efw/

[7] Squid Cache. (2023). Squid: Optimising Web Delivery. Squid-cache.org. http://www.squid-cache.org/Doc/

[8] Tanenbaum, A. S., & Wetherall, D. (2011). Redes de computadoras (5ta ed.). Pearson Educación.

[9] Wessels, D. (2004). Squid: The Definitive Guide. O'Reilly Media.

[10] M. Morris, Linux Firewalls: Enhancing Security with nftables and Beyond, 2nd ed., O'Reilly Media, 2020.

[11] R. Russell, Linux Kernel Networking: Implementation and Theory, 2nd ed., Addison-Wesley Professional, 2008.

[12] S. Bhatia, Linux Network Administrator's Guide, 2nd ed., O'Reilly Media, 2005.

[13] GNU Project, “Iptables Tutorial 1.2.2,” [Online]. Available: https://www.netfilter.org/documentation/HOWTO//iptables-HOWTO.html. [Accessed: Nov. 26, 2025].

[14] The Netfilter Project, “Netfilter/Iptables Project,” [Online]. Available: https://netfilter.org/. [Accessed: Nov. 26, 2025]

[15] W. Stallings, Network Security Essentials: Applications and Standards, 6th ed., Pearson, 2017.