Implementación de Seguridad Perimetral Gnu/Linux con Endian Firewall: Instalación, NAT, Servicios DMZ y Proxy HTTP

Wilmer Alfonso Andrade Eguis
waandradee@unadvirtual.edu.co
Rony Mena Curvelo
rjmenac@unadvirtual.edu.co
Rafael Augusto Mendoza Nieves
ramendozan@unadvirtual.edu.co
Ariela José Molina Hernández
ajmolinah@ unadvirtual.edu.co

RESUMEN: *Este documento detalla la implementación de un firewall Endian en Oracle VM VirtualBox, configurando tarjetas de red para segmentar la zona verde (LAN), zona roja (WAN) y la zona naranja (DMZ). Se aplicaron reglas NAT para garantizar la comunicación desde la LAN y DMZ hacia Internet. Asimismo, se habilitaron servicios HTTP y FTP en la DMZ, mientras que el protocolo ICMP fue denegado para fortalecer la seguridad perimetral. Finalmente, se desplegó un proxy HTTP no transparente con autenticación de usuarios y políticas de filtrado mediante listas negras para restringir el acceso a sitios específicos. Los resultados demuestran un control eficiente del tráfico y una defensa robusta contra accesos no autorizados, validando la eficacia de la arquitectura propuesta en la protección de servicios y la gestión de navegación interna.*

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

ABSTRACT: *This document presents the implementation and configuration of the Endian Firewall in a virtualized environment using Oracle VM VirtualBox, focusing on the segmentation of the network into three security zones: green (LAN), orange (DMZ), and red (WAN). It details the installation process, NAT rule configurations for enabling secure internet access from LAN and DMZ, and the deployment of HTTP and FTP services within the DMZ. Furthermore, ICMP protocol was blocked to strengthen perimeter security. A non-transparent HTTP proxy with user authentication and blacklist filtering policies was established to control internal web navigation rigorously. Experimental results confirm that the proposed architecture effectively controls traffic flow, restricts unauthorized access, and provides a scalable and robust perimeter defense solution for GNU/Linux networks.*

Keywords*:* Perimeter Security, Endian Firewall, NAT, DMZ, HTTP Proxy, Authentication

1. INTRODUCCIÓN

En la era digital actual, la protección de las redes y la información constituye un imperativo crítico para organizaciones de todos los tamaños y sectores. El creciente número y sofisticación de amenazas informáticas, incluyendo ataques de denegación de servicio, intrusiones no autorizadas, y propagación de malware, exigen soluciones robustas que brinden seguridad en múltiples niveles. La seguridad perimetral se configura como la primera línea de defensa para salvaguardar los recursos internos desde accesos externos, segregando las redes en zonas según su nivel de confianza y funcionalidad.

Los firewalls representan dispositivos o soluciones de software fundamentales para controlar y filtrar el tráfico entrante y saliente, basándose en reglas configuradas que definen qué comunicaciones son permitidas o bloqueadas. En particular, las soluciones basadas en GNU/Linux, como Endian Firewall, combinan flexibilidad, eficiencia y bajo costo, siendo ampliamente adoptadas en entornos académicos, empresariales y de pequeña o mediana escala, donde la relación costo-beneficio es crucial.

El uso de máquinas virtuales a través de plataformas como Oracle VM VirtualBox permite crear entornos controlados y replicables para el desarrollo, prueba y despliegue de infraestructuras segmentadas que fortalecen la seguridad perimetral. La segmentación en zonas —típicamente definidas como roja (WAN, zona no confiable), verde (LAN, zona confiable) y naranja (DMZ, zona desmilitarizada)— permite aplicar políticas específicas, minimizando la superficie de ataque y facilitando un control granular del flujo de tráfico.

Este artículo documenta de manera sistemática la implementación de Endian Firewall, destacando aspectos técnicos como la configuración de interfaces de red virtual, aplicación de NAT para traducción y mascaramiento de direcciones, habilitación de servicios específicos en la DMZ, y la implementación de un proxy HTTP no transparente con autenticación y filtrado basado en listas negras. La finalidad es evidenciar la viabilidad y eficacia de este enfoque para crear una arquitectura de seguridad perimetral robusta y escalable para redes basadas en GNU/Linux.

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

Para desarrollar el entorno de seguridad, se implementó una máquina virtual en Oracle VM VirtualBox destinada a ejecutar la distribución GNU/Linux Endian Firewall. En la configuración inicial se incorporaron varios adaptadores de red para representar una infraestructura perimetral dividida por segmentos.

La estructura de red quedó organizada en tres áreas principales:

Zona Verde (LAN): utilizada para la comunicación de la red interna y los equipos locales.

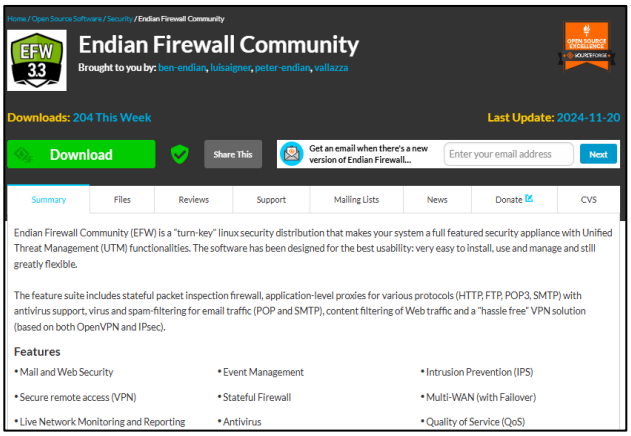
Zona Naranja (DMZ): orientada al alojamiento de servidores con acceso controlado desde el exterior.

Zona Roja (WAN): asignada a la conexión con redes externas o acceso a Internet.

La configuración de las diferentes interfaces permitió separar adecuadamente el flujo de datos entre cada zona, facilitando posteriormente la implementación de políticas de seguridad, filtrado y control del tráfico de red.

Se ingresa a la página de Endian Community para poder descargar la imagen ISO, como se ve en la Fig. 1

Figura 1.
Página de Endian Community

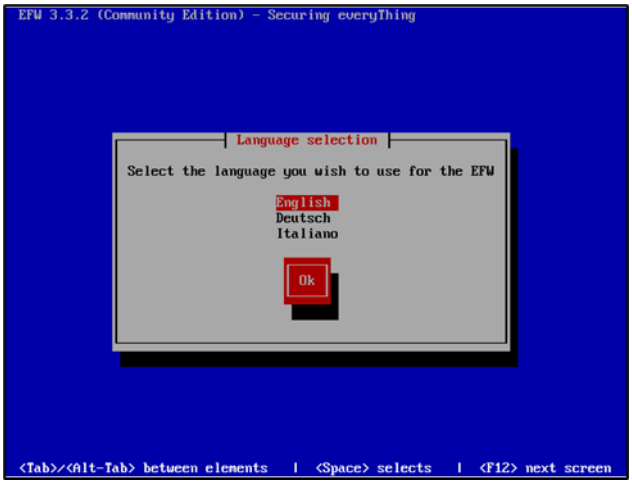


Fuente: Autoría Propia.

En esta ilustración se observa la interfaz principal del portal oficial, donde se encuentran las opciones de descarga disponibles para la versión Community. Desde allí el usuario puede seleccionar la versión más reciente del sistema, verificar los requisitos de instalación y proceder con la descarga segura del archivo ISO.

La instalación de Endian Firewall 3.3.2 Community Edition se presenta una ventana inicial de selección de idioma donde el instalador solicita elegir entre English, Deutsch o italiano; una vez seleccionado, la elección se confirma presionando el botón rojo Ok, ver la Fig.2.

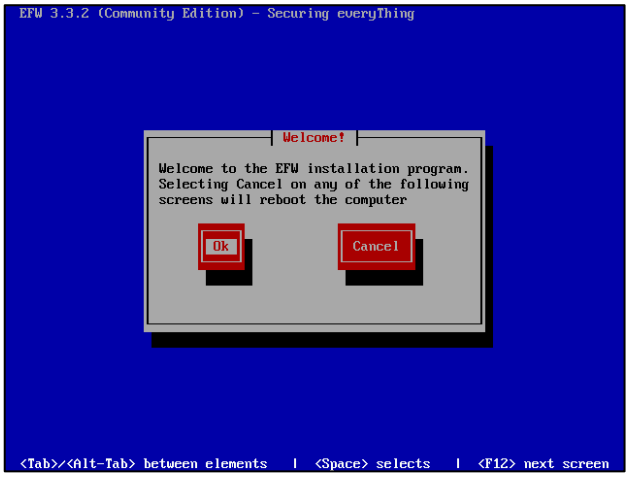
Figura 2.
Instalación de Endian



Fuente: Autoría Propia.

En esta imagen, el instalador de Endian Firewall 3.3.2 Community Edition muestra una pantalla titulada Welcome!, donde se da la bienvenida al programa de instalación e indica que, si se selecciona Cancel en cualquiera de las pantallas siguientes, el equipo se reiniciará; en esta etapa, el usuario debe confirmar con el botón Ok para continuar, ver Fig. 3.

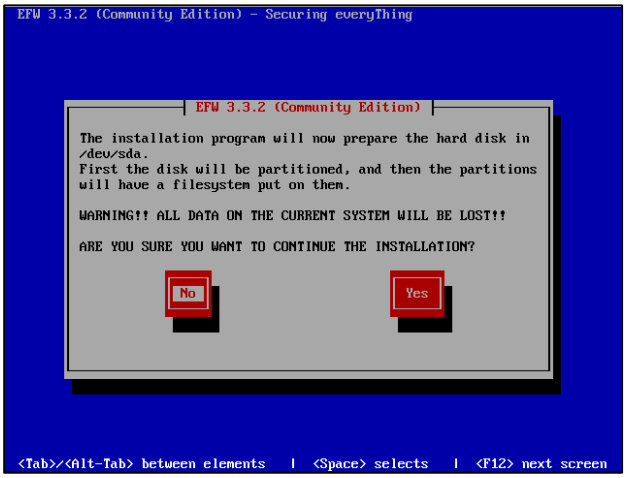
Figura 3.
Instalación de Endian



Fuente: Autoría Propia.

En la imagen se observa la etapa de preparación del disco durante la instalación de Endian Firewall 3.3.2 Community Edition, donde el asistente advierte que el disco /dev/sda será particionado y formateado, lo que implica la pérdida total de los datos existentes; en este punto, el usuario debe confirmar la acción seleccionando Yes para continuar con la instalación, ver Fig. 4.

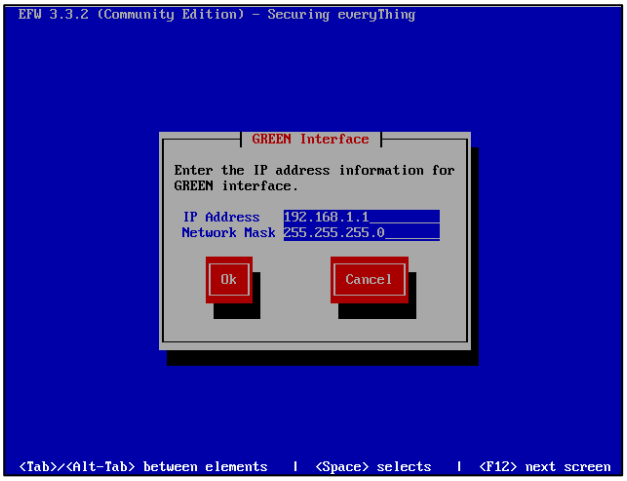
Figura 4.
Instalación de Endian



Fuente: Autoría Propia.

En esta etapa de la instalación se muestra la ventana de configuración de la interfaz GREEN como lo evidencia la Fig. 5, donde se solicita ingresar la dirección IP (por defecto 192.168.1.1) y la máscara de red (255.255.255.0); una vez definidos estos parámetros, se confirma con el botón Ok.

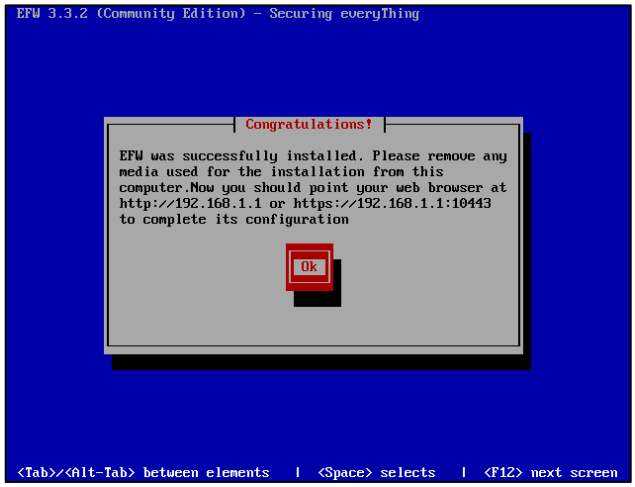
Figura 5.
Instalación de Endian



Fuente: Autoría Propia.

Por último, el asistente de instalación de Endian muestra un mensaje de finalización que felicita al usuario por haber completado la instalación con éxito; se indica retirar el medio de instalación y acceder a la dirección web predeterminada (http://192.168.1.1:10443) para continuar con la configuración vía el navegador, confirmando la acción con el botón rojo Ok. Este paso finaliza el asistente de instalación en consola e inicia la administración gráfica del firewall, donde se definen reglas, servicios y políticas de seguridad. Ver Fig. 6.

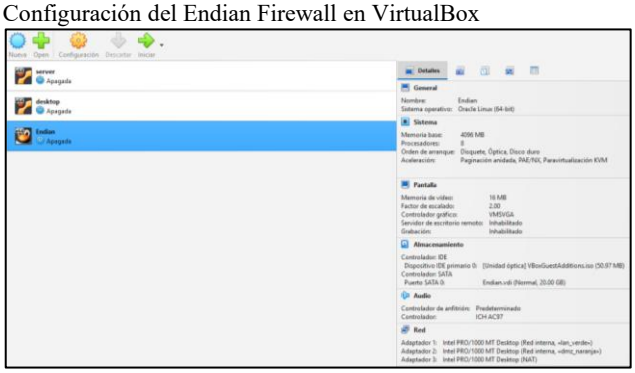
Figura 6.
Instalación de Endian



Fuente: Autoría Propia.

Ahora se observa la gestión de máquinas virtuales en VirtualBox, donde aparecen listadas tres instancias: servidor, desktop y endian, todas en estado apagado; la máquina endian está seleccionada y en el panel derecho se muestran sus detalles de configuración, incluyendo secciones como General, Pantalla y parámetros de memoria y aceleración. Este paso corresponde al entorno de virtualización desde el cual se administra y ejecuta la instalación de Endian Firewall, ver Fig. 7.

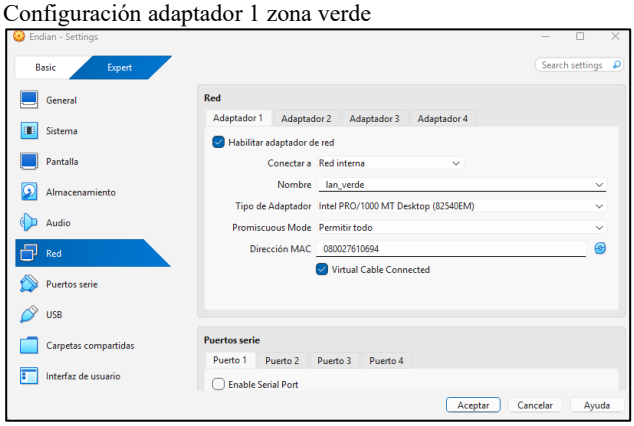
Figura 7.
Configuración del Endian Firewall en VirtualBox



Fuente: Autoría Propia.

La configuración del adaptador 1 para la zona verde (GREEN) se realiza asignando el primer adaptador de red de la máquina virtual en modo Red Interna, estableciendo la dirección IP 192.168.1.1 y la máscara 255.255.255.0 como lo evidencia la Fig. 8, de manera que el firewall actúe como puerta de enlace para los clientes internos; una vez definidos estos parámetros, se confirma con Ok, quedando habilitada la zona verde como la red segura principal desde la cual se administran las políticas de seguridad.

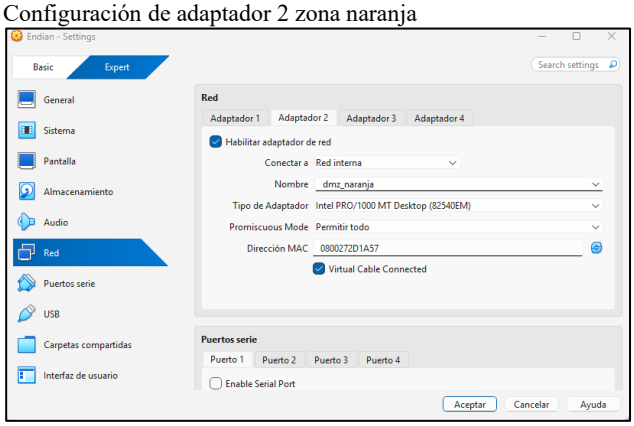
Figura 8.
Configuración adaptador 1 zona verde



Fuente: Autoría Propia.

La configuración del adaptador 2 para la zona naranja (ORANGE) se realiza habilitando el segundo adaptador de red de la máquina virtual y conectándolo en modo Red Interna, asignándole un nombre de red como naranja o intnet como muestra la Fig. 9; de esta manera, el firewall identifica esta interfaz como la DMZ (Demilitarized Zone) destinada a servidores públicos, separada de la LAN segura y del acceso directo a Internet, lo que permite controlar y filtrar el tráfico hacia servicios expuestos sin comprometer la red interna.

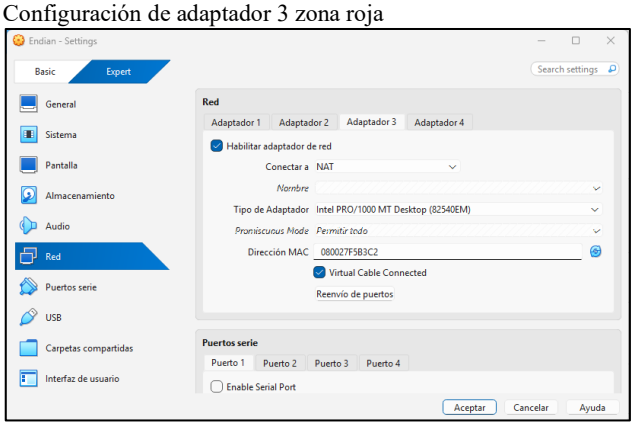
Figura 9.
Configuración de adaptador 2 zona naranja



Fuente: Autoría Propia.

La configuración del adaptador 3 para la zona roja (RED) se realiza habilitando el tercer adaptador de red de la máquina virtual y conectándolo en modo Red Interna, asignándole un nombre de red como red o intnet como lo muestra la Fig. 10; esta interfaz representa la conexión hacia Internet, por lo que el firewall la identifica como la zona no confiable desde donde se filtra y controla todo el tráfico externo, garantizando que los equipos de la LAN (GREEN) y los servidores en la DMZ (ORANGE) estén protegidos frente a accesos directos

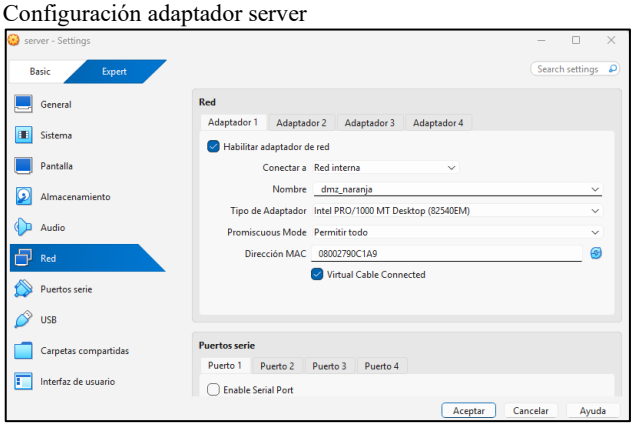
Figura 10.
Configuración de adaptador 3 zona roja



Fuente: Autoría Propia.

La configuración del adaptador del servidor se realiza habilitando el primer adaptador de red y conectándolo en modo Adaptador puente, de manera que la máquina virtual se vincule directamente con la tarjeta de red física del equipo anfitrión (por ejemplo, Realtek PCIe GbE Family Controller); esto permite que el servidor tenga acceso real a la red externa y funcione como punto de enlace hacia Internet, mientras el firewall gestiona el tráfico entrante y saliente. Con esta configuración, la interfaz del servidor se integra en la infraestructura física, diferenciándose de las zonas internas como la GREEN y la ORANGE, y asegurando que la RED cumpla su rol como zona no confiable. Ver la Fig. 11.

Figura 11.
Configuración adaptador server



Fuente: Autoría Propia.

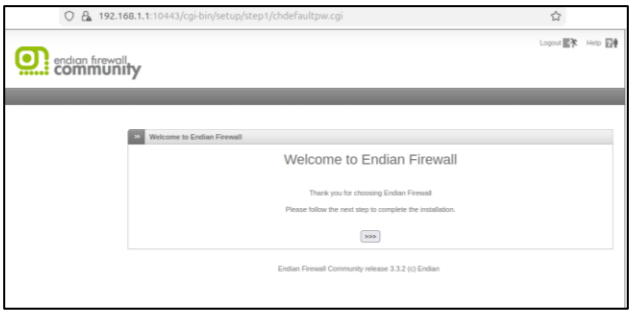
Se incluye al desktop en la zona verde, en esta etapa se observa cómo el equipo de escritorio es asignado dentro de la zona interna segura, denominada zona verde. Esta configuración garantiza que el desktop tenga acceso protegido a los recursos de la red local, diferenciándose del tráfico externo y de la DMZ. De esta manera, se refuerza la seguridad y se asegura que los dispositivos internos operen bajo políticas de control confiables y eficientes. Ver la Fig. 12.

Figura 12.
Configuración de adaptador desktop

Fuente: Autoría Propia.

Se muestra el acceso vía navegador al firewall, donde al ingresar a la dirección 192.168.1.110:443 aparece una advertencia de seguridad en Firefox debido a que el certificado es autofirmado (self-signed). El navegador indica que la conexión no es confiable y muestra el error MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT; en este punto, se puede optar por regresar o bien desplegar las opciones avanzadas y seleccionar Accept the Risk and Continue, lo que permite entrar al panel web de administración del firewall. Ver la Fig. 13.

Figura 13.
Pantalla inicial



Fuente: Autoría Propia.

El acceso al panel web de Endian Firewall se realiza ingresando a la dirección local 192.168.1.1, donde aparece la pantalla de bienvenida con el acuerdo de licencia como se muestra en la Fig. 14. En esta etapa, el sistema solicita la aceptación de las condiciones mediante el botón ACEPTAR, lo que permite continuar con el asistente de configuración. Una vez aceptado, se habilita la administración gráfica del firewall, desde donde se definen las zonas de red la GREEN para la LAN interna, la ORANGE para la DMZ y la RED para la conexión a Internet asegurando la separación y protección de cada segmento de la infraestructura.

Figura 14.
Ingreso al firewall

Fuente: Autoría Propia.

El acceso al panel web de Endian Firewall se realiza ingresando a la dirección 192.168.1.110:10443, donde el sistema presenta la opción de importar un backup. En esta etapa, el administrador debe decidir si restaurar una copia de seguridad previa seleccionando Sí o continuar con una instalación limpia seleccionando No. Una vez tomada la decisión, se confirma con los botones Cancelar o Subir, lo que permite al firewall cargar la configuración guardada o avanzar con parámetros nuevos. Este procedimiento asegura que el sistema pueda recuperar configuraciones anteriores de las zonas GREEN, ORANGE y RED, manteniendo la coherencia de la infraestructura de seguridad. Ver la Fig. 15.

Figura 15.
Panel web de Endian Firewall

Fuente: Autoría Propia.

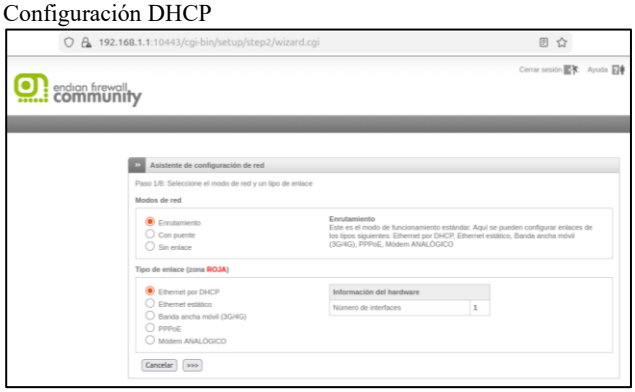
El acceso al panel de configuración de Endian Firewall se realiza ingresando a la dirección local 192.168.1.1, donde el sistema solicita cambiar las contraseñas por defecto. En esta etapa, el administrador debe definir una nueva contraseña para la interfaz web (admin) y otra para el acceso por SSH (root), asegurando que el firewall no permanezca con credenciales predeterminadas. Una vez establecidas y confirmadas las contraseñas mediante el botón Cambiar contraseña, el sistema queda protegido frente a accesos no autorizados y se habilita la administración segura de las zonas GREEN, ORANGE y RED. Ver la Fig. 16.

Figura 16.
Configuración de Endian

Fuente: Autoría Propia.

Durante la configuración de Endian Firewall, el administrador accede al asistente de red desde la dirección 192.168.1.1, donde se muestran las distintas zonas disponibles: RED, VERDE, AZUL, NARANJA y la opción de deshabilitar, ver la Fig. 17. En este caso, se selecciona la zona roja (RED) para que funcione bajo DHCP, lo que permite que el firewall obtenga automáticamente la dirección IP y parámetros de conexión desde el proveedor de servicios de Internet. Esta decisión asegura que la interfaz externa quede correctamente enlazada con la red pública, mientras las zonas internas —la GREEN para la LAN segura y la ORANGE para la DMZ— permanecen protegidas y aisladas del tráfico no confiable.

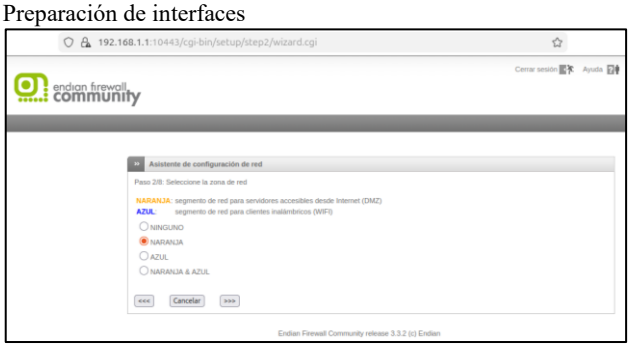
Figura 17.
Configuración DHCP



Fuente: Autoría Propia.

En el paso mostrado, se presentan las opciones NARANJA (segmento para servicios accesibles desde Internet, DMZ),VERDE (segmento de red local, LAN) y ROJA (conexión a ADSL). Al elegir la opción correspondiente, el sistema prepara la interfaz para asignar parámetros de red y continuar con la configuración. Este proceso asegura que cada zona cumpla su función: la GREEN como red segura interna, la ORANGE como área de servidores públicos y la RED como enlace hacia Internet. Ver la Fig. 18.

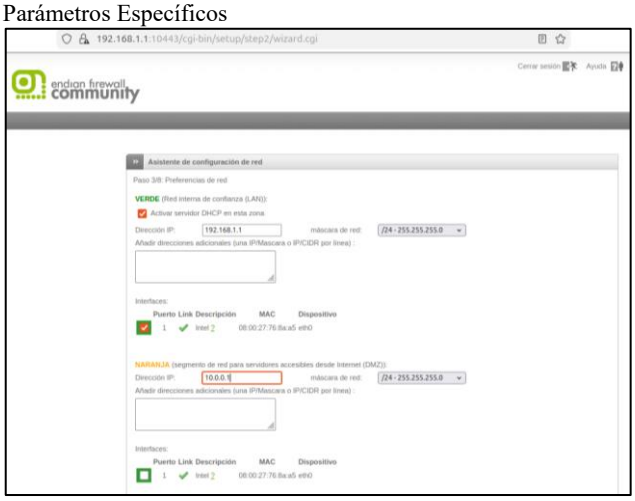
Figura 18.
Preparación de interfaces



Fuente: Autoría Propia.

En esta etapa, se asignan parámetros específicos a las zonas configuradas: la GREEN como red interna segura (LAN), la ORANGE destinada a la DMZ para servicios públicos, la BLUE para clientes inalámbricos y la RED como enlace hacia Internet. Esta definición de direcciones asegura que cada segmento de la red tenga su propia identidad y control, permitiendo al firewall aplicar reglas de seguridad diferenciadas y garantizar la separación entre entornos confiables y no confiables. Observar la Fig. 19.

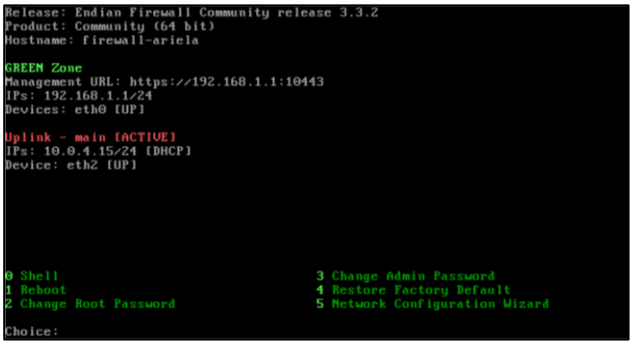
Figura 19.
Parámetros Específicos



Fuente: Autoría Propia.

En la interfaz de administración de Endian Firewall, el sistema muestra el estado de las zonas configuradas y los parámetros activos. En la pantalla se observa que la zona verde (GREEN) está definida con la dirección 192.168.1.1/24, mientras que la zona roja (RED) aparece activa en la interfaz eth0, obteniendo su dirección IP mediante DHCP (10.0.4.152). Esta visualización permite al administrador verificar que la conectividad interna y externa está correctamente establecida, garantizando que la LAN segura (GREEN) y el enlace hacia Internet (RED) funcionen de manera coordinada. Además, desde este menú se ofrecen opciones como acceso a la shell, reinicio del sistema, cambio de contraseñas y el asistente de configuración de red, lo que facilita la gestión integral del firewall. Ver la Fig. 20.

Figura 20.
Interfaz de Endian



Fuente: Autoría Propia.

3. Temática 2: Configuración NAT

3.1 Concepto y Relevancia

Network Address Translation (NAT) permite que múltiples hosts de redes privadas compartan una única dirección IP pública para el acceso a Internet. En Endian Firewall, NAT se gestiona desde el módulo Firewall > Reenvío de puertos / NAT, posibilitando dos escenarios: la comunicación saliente de la LAN hacia la WAN y la exposición selectiva de servicios de la DMZ hacia el exterior [2].

3.2 NAT LAN → WAN

Endian implementa automáticamente el NAT para la LAN, permitiendo la salida hacia Internet sin necesidad de configurar reglas manuales. Se verificó la conectividad desde el Desktop Ubuntu con fecha y hora, como lo evidencia la Fig. 21.

Figura 21.
Conectividad LAN y WAN con NAT activo.

Fuente: Autoría propia.

En lo anterior se observa la ejecución de una prueba de conectividad (ping) hacia la dirección externa 8.8.8.8 confirmando la salida hacia la WAN mediante NAT automático configurado en Endian Firewall.

3.3 NAT DMZ → WAN

Se crea la regla de traducción de direcciones que permite la salida de tráfico desde la red DMZ (10.0.0.0/24) hacia la WAN (RED), ver Fig. 22.

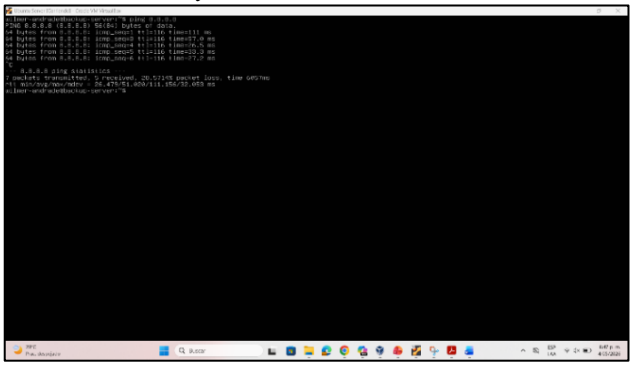
Figura 22.
Regla NAT configurada para la red DMZ

Fuente: Autoría propia.

Lo antes visto muestra el editor de reglas Source NAT en Endian Firewall donde se muestra la configuración detallada de la regla que permite la salida de tráfico desde la red DMZ (10.0.0.0/24) hacia la WAN (RED).

Luego se realizan las pruebas de la conectividad desde la red LAN y desde la DMZ mediante NAT, este paso se puede verificar en la Fig. 23.

Figura 23.
Conectividad DMZ y WAN con NAT activo



Fuente: Autoría propia.

Aquí se observa el servidor ubicado en la red DMZ hacia la dirección externa 8.8.8.8 logrando salir hacia la WAN mediante la regla de Source NAT configurada en Endian Firewall. Autoría propia.

3.4 VERIFICACIÓN DE REGLAS NAT

En el panel de Endian, sección Firewall > Reenvío de puertos / NAT, se confirmó la existencia de las reglas creadas para ambas zonas. Las reglas aparecen listadas con estado activo (ícono verde). Desde consola del firewall Endian se listaron las reglas iptables activas:

```
# date && iptables -t nat -L -n --line-numbers
vie 08 may 2026 09:35:07 COT
Chain POSTROUTING (policy ACCEPT)
1  MASQUERADE  all  192.168.1.0/24  0.0.0.0/0
2  MASQUERADE  all  10.0.0.0/24     0.0.0.0/0
```

4. TEMÁTICA 3: SERVICIOS DE LA ZONA DMZ

4.1 INSTALACIÓN DE SERVICIOS EN EL SERVIDOR DMZ

En el Ubuntu Server 22.04 LTS (IP 10.0.0.3 – Zona Naranja) se instalaron los servicios HTTP y FTP que serán expuestos a través del firewall. Todos los comandos se ejecutaron como superusuario desde consola, ver la Fig. 24.

```
# date && apt update && apt install -y apache2 proftpd
apache2 - instalado correctamente
proftpd - instalado correctamente
```

Se habilitaron y arrancaron ambos servicios:

```
# systemctl enable apache2 proftpd
# systemctl start apache2 proftpd
- apache2.service Active: active (running)
- proftpd.service   Active: active (running)
```

Figura 24.
Estado de servicios HTTP y FTP en servidor DMZ

Fuente: Autoría Propia.

Adicionalmente, se verificó la conectividad HTTP desde la LAN hacia la DMZ, como lo muestra la Fig. 25.

Figura 25.
Respuesta HTTP exitosa desde LAN hacia DMZ.

Fuente: Autoría Propia.

4.2 HABILITACIÓN DEL SERVICIO HTTP (PUERTO 80)

Para permitir el servicio HTTP desde el servidor web en la DMZ, se accedió al panel de administración de Endian Firewall en la sección Firewall > Tráfico de Salida. Se creó una nueva regla con los siguientes parámetros, la cual se puede evidenciar en la Fig. 26.

- Fuente: Zona Naranja (DMZ) – 10.0.0.3
- Destino: Cualquier (ANY)
- Protocolo: TCP
- Puerto destino: 80 (HTTP)
- Política: ACEPTAR

Figura 26.
Creación Regla Acceso Servidor Zona DMZ

Fuente: Autoría Propia.

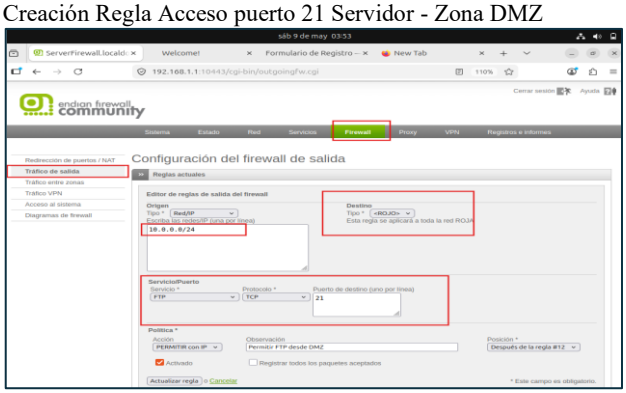
4.3 HABILITACIÓN DEL SERVICIO FTP (PUERTO 21)

De manera análoga, se creó una regla de tráfico de salida para el servicio FTP. Se instaló y configuró proftpd en el servidor Ubuntu de la DMZ. Los parámetros de la regla fueron:

- Fuente: Zona Naranja (DMZ) – 10.0.0.3
- Destino: Cualquier (ANY)
- Protocolo: TCP
- Puerto destino: 21 (FTP)
- Política: ACEPTAR

Esto se puede evidenciar también en la Fig. 27.

Figura 27.
Creación Regla Acceso puerto 21 Servidor - Zona DMZ



Fuente: Autoría Propia.

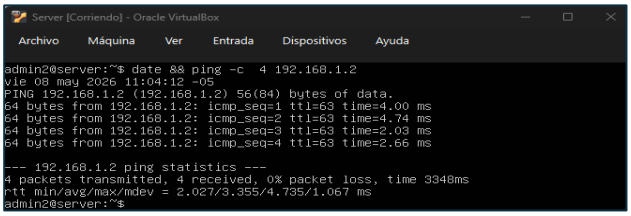
4.4 DENEGACIÓN DEL PROTOCOLO ICMP

Para restringir el protocolo ICMP, se creó una regla de tráfico entre zonas en Endian Firewall con política DENEGAR, configurada con los siguientes parámetros:

- Fuente: Zona Naranja (DMZ)
- Destino: Cualquier (ANY)
- Protocolo: ICMP
- Tipos: 8 (Echo Request) y 30
- Política: DENEGAR

Esta regla fue posicionada antes de cualquier regla permisiva para asegurar su aplicación. La prueba de efectividad se realizó ejecutando ping desde la DMZ hacia la LAN y hacia la WAN, como se observa en las Fig. 28 y 29.

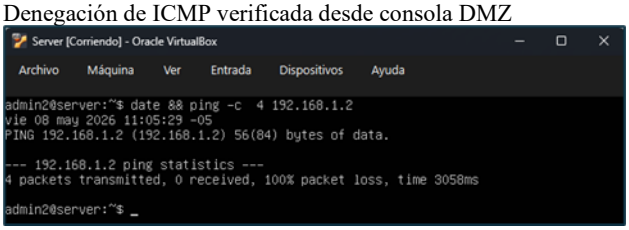
Figura 28.
Prueba de ICMP desde Servidor en DMZ



Fuente: Autoría Propia.

PING 192.168.1.2: 100% packet received.

Figura 29.
Denegación de ICMP verificada desde consola DMZ



Fuente: Autoría Propia.

PING 192.168.1.2: 100% packet loss.

4.5 RESUMEN DE REGLAS CONFIGURADAS

Tabla 1.
Reglas de tráfico de salida configuradas en Endian Firewall

Servicio	Protocolo	Puerto	Política	Estado
Apache2 HTTP	TCP	80	Aceptar	Activo
proftpd FTP	TCP	21	Aceptar	Activo
ICMP T8	ICMP	Tipo 8	Denegar	Activo
ICMP T30	ICMP	Tipo 30	Denegar	Activo

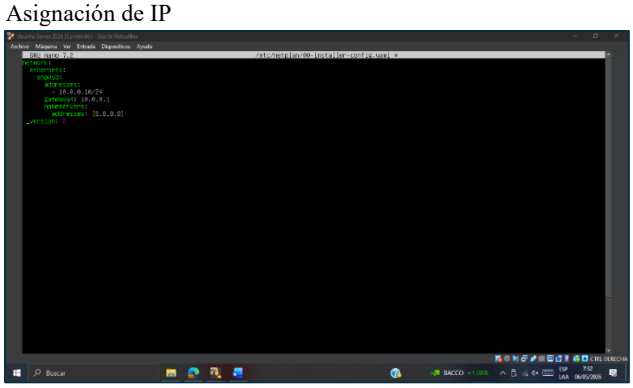
Fuente: Autoría Propia.

5. TEMÁTICA 5: PROXY HTTP NO TRANSPARENTE CON AUTENTICACIÓN

Continuando el proceso de las temáticas lo primero que se hizo fue configurar de forma manual el servidor Ubuntu editando el archivo netplan para quedar con la dirección 10.0.0.10 dentro de la zona naranja, como se observa en la Fig. 30.

Esta configuración fue necesaria ya que la zona naranja se configuró al inicio sin DHCP, por lo tanto, correspondió hacerlo de forma manual

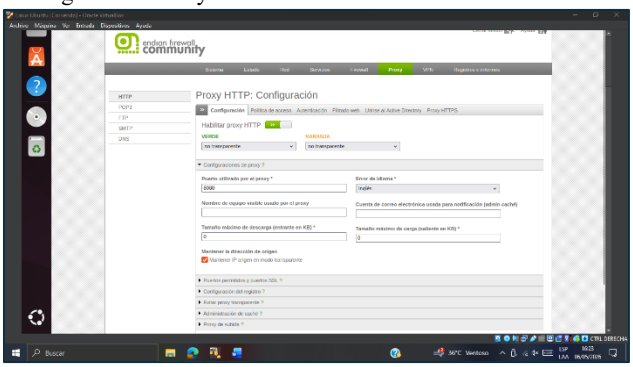
Figura 30.
Asignación de IP



Fuente: Autoría propia.

Una vez establecida la red, se activó el Proxy HTTP desde el panel de Endian en modo no transparente para las zonas verde y naranja usando el puerto 8080 como lo muestra la Fig. 31. Este modo fue elegido deliberadamente porque exige que cada usuario configure manualmente el proxy en su navegador y se autentique antes de poder navegar, dando al administrador control total sobre quién accede y a qué.

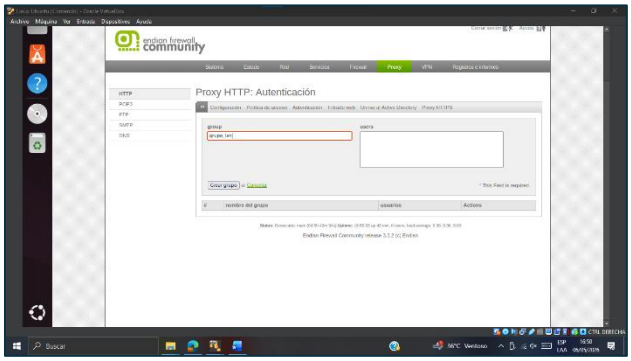
Figura 31.
Configuración Proxy



Fuente: Autoría propia.

Para implementar la autenticación se creó el grupo grupo_lan y el usuario rafael, el cual fue asociado al grupo dentro del sistema Endian como lo muestra la Fig. 32.

Figura 32.
Grupo y usuario



Fuente: Autoría propia.

Con el proxy activo y los usuarios creados, se configuró el filtrado de contenido. Se creó el perfil denominado

perfil_bloqueado con una lista negra que incluye los sitios www.hotmail.com, www.youtube.com y www.elnuevodia.com.co.

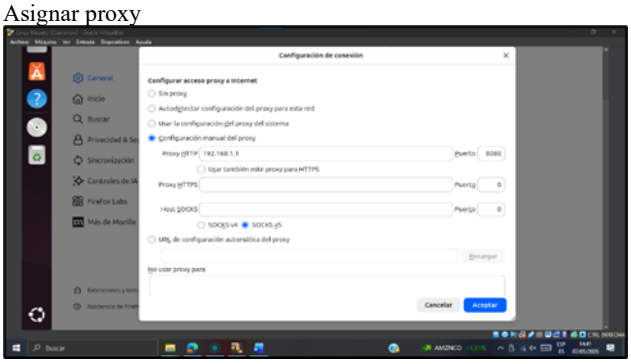
Luego se creó una política de acceso que vincula la zona verde como origen, el grupo grupo_lan como requisito de autenticación y el perfil_bloqueado como filtro, configurada con prioridad sobre las demás reglas de acceso, la Fig. 33 permite observar la configuración aplicada en este punto.

Figura 33.
Configuración de la política

Fuente: Autoría propia.

Finalmente se realizaron las pruebas desde el Desktop configurando el proxy manualmente en Firefox apuntando a 192.168.1.1 en el puerto 8080. La Fig. 34 muestra como se hizo esto en el navegador.

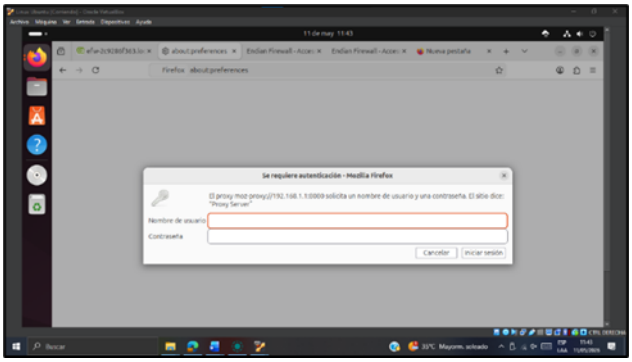
Figura 34.
Asignar proxy



Fuente: Autoría propia.

Al intentar navegar, el sistema solicitó usuario y contraseña, confirmando que la autenticación estaba funcionando, como lo muestra la Fig 35.

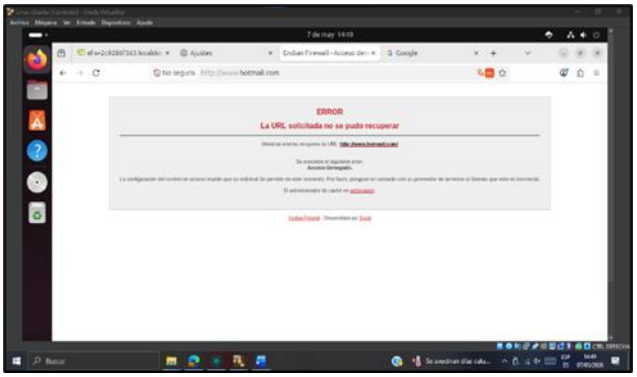
Figura 35.
Autenticación



Fuente: Autoría propia.

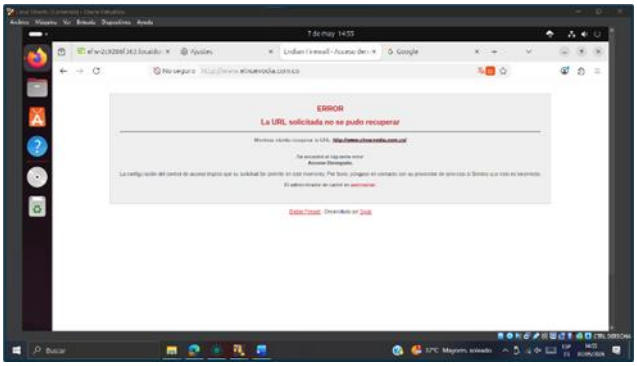
Las pruebas de bloqueo demostraron que hotmail.com y elnuevodia.com.co fueron bloqueados exitosamente mostrando el mensaje de acceso denegado de Endian Firewall. Las Fig. 36 y 37 evidencian lo mencionado.

Figura 36.
Hotmail



Fuente: Autoría propia.

Figura 37.
El nuevo día



Fuente: Autoría propia.

En el caso de YouTube se identificó una limitación técnica del proxy no transparente con sitios HTTPS por lo cual la efectividad del proxy en este sitio web no pudo ser comprobada.

6. CONCLUSIONES

La principal conclusión es que Endian Firewall garantiza la seguridad perimetral al controlar qué zonas pueden comunicarse entre sí. Por ejemplo, la DMZ (servidores) no puede acceder directamente a la LAN (usuarios), mientras que la LAN sí puede comunicarse con la DMZ. Esto evita riesgos de intrusión y protege la integridad de los datos.

La configuración de NAT en Endian Firewall permitió establecer de forma correcta la comunicación desde la red LAN y la zona DMZ hacia la WAN. Las pruebas realizadas confirmaron el funcionamiento adecuado de las reglas de traducción de direcciones, evidenciando el uso del firewall como una solución eficaz para la seguridad perimetral y el control del tráfico en redes GNU/Linux.

La habilitación selectiva de servicios HTTP y FTP en la Zona DMZ, combinada con la denegación de ICMP, demostró cómo una correcta política de tráfico de salida reduce la superficie de ataque. Los resultados obtenidos en consola, con pérdida del 100% de paquetes ICMP, corroboraron la efectividad de las reglas configuradas en Endian Firewall.

La implementación del proxy HTTP no transparente con Squid permitió establecer un control efectivo del acceso a Internet desde la LAN. La integración de autenticación local, listas negras y políticas de acceso por grupo constituye una solución escalable para el control de la navegación en organizaciones que requieran auditoría y trazabilidad del uso de Internet por parte de sus usuarios.

En términos generales, puede destacarse que la implementación de Endian Firewall en un entorno virtualizado con VirtualBox demostró ser una solución técnicamente viable, valiosa y prácticamente aplicable para establecer seguridad perimetral en redes basadas en Linux. A lo largo del desarrollo de las cinco temáticas, cada fase del proceso aportó evidencia concreta sobre la efectividad de esta herramienta de seguridad.

Por último, es importante mencionar también que este proyecto permitió al equipo adquirir competencias técnicas en la administración de firewalls, además permitió comprender de forma práctica cómo las decisiones que se toman en cada paso de la configuración tienen consecuencias que pueden afectar la seguridad, el rendimiento y la usabilidad de la red.

REFERENCIAS

[1] Endian. (2016). Endian UTM 3.2 – Manual de referencia. Endian. http://docs.endian.com/3.2/utmindex.html

[2] LPI. (2022). LPIC-1 Exam 101: Tema 101 – Determinar y configurar los ajustes de hardware. Linux Professional Institute. https://learning.lpi.org/es/learning-materials/101-500/101/101.1/

[3] Canonical. (2023). Guía del Ubuntu Desktop 20.04 LTS. Help Ubuntu. https://help.ubuntu.com/

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

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

[6] Fernández, Y. (2023, November 9). Qué es la NAT, ventajas y desventajas, tipos y cuál se usa en cada caso. Xataka. https://www.xataka.com/basics/que-nat-ventajas-desventajas-tipos-cual-se-usa-cada-caso?utm_source=copilot.com

[7] Álvarez, S. (2025, November 11). Guía definitiva de proxies: qué son, tipos y cómo elegir el adecuado (2026). Octoparse. https://www.octoparse.es/blog/guia-definitiva-de-proxies-que-son-tipos-y-como-elegir-el-adecuado-2025

[8] Campo, J. R. (2025, October 31). Seguridad Perimetral: qué es, cómo funciona y sus tipos clave. TECNOSeguro. https://www.tecnoseguro.com/faqs/que-es-seguridad-perimetral