Implementación y Fortalecimiento de la Seguridad Perimetral en Entornos GNU/Linux: Una Aproximación Práctica con Endian Firewall para Redes LAN, WAN y DMZ

Yeison Fredy Chala
e-mail: yfchala@unadvirtual.edu.co

RESUMEN: *Este artículo ofrece una guía práctica y detallada sobre cómo implementar reglas de seguridad perimetral utilizando Endian Firewall en entornos GNU/Linux, con el objetivo de mejorar el control del tráfico entre las distintas zonas de red. A lo largo del documento, se explican los pasos necesarios para configurar políticas de acceso entre las zonas VERDE (LAN interna), NARANJA (DMZ) y ROJA (WAN), asegurando un manejo adecuado de los servicios expuestos y del tráfico que circula entre ellas.*

La propuesta se enfoca en definir reglas específicas que permiten o bloquean conexiones HTTP y FTP según las necesidades del laboratorio, demostrando cómo estas políticas afectan directamente la seguridad y el aislamiento de cada segmento de red. Para validar que las configuraciones se aplican correctamente, se llevan a cabo pruebas funcionales de conectividad, siguiendo criterios claros que permiten verificar el flujo permitido, el tráfico denegado y el comportamiento esperado de cada zona.

Así, el artículo no solo detalla la configuración técnica, sino que también ofrece un entorno controlado de experimentación que facilita la comprensión del funcionamiento del firewall, sus políticas perimetrales y su impacto en la protección del sistema. Esta metodología brinda una visión integral para estudiantes o administradores de redes que desean profundizar sus conocimientos en seguridad perimetral dentro de infraestructuras basadas en software libre.

PALABRAS CLAVE: Software libre, Reglas de firewall, Políticas de acceso, Zona verde (LAN), Zona naranja (DMZ), Zona roja (WAN) HTTP, FTP.

1 INTRODUCCIÓN

La seguridad perimetral es uno de los pilares fundamentales en la protección de las infraestructuras de red modernas. A medida que las organizaciones incorporan servicios críticos y sistemas de comunicación, se vuelve esencial establecer mecanismos que permitan controlar, limitar y supervisar el tráfico que circula entre los diferentes segmentos de la red. En este sentido, los firewalls basados en GNU/Linux, como Endian Firewall, se presentan como una opción robusta, flexible y de código abierto para gestionar las políticas de acceso.

Endian Firewall organiza la red en zonas de seguridad, lo que permite que cada segmento implemente reglas específicas para la transferencia de datos. En particular, las zonas VERDE (LAN), NARANJA (DMZ) y ROJA (WAN) actúan como barreras lógicas que segmentan el tráfico según el nivel de confianza asignado. Este enfoque facilita la aplicación de medidas de seguridad diferenciadas, asegurando la integridad y disponibilidad de los servicios.

Este artículo ofrece una guía detallada para crear y validar reglas que permitan o bloqueen el tráfico HTTP y FTP entre estas zonas. Para ello, se establece un entorno de laboratorio controlado que permite observar, registrar y analizar el comportamiento del firewall en condiciones reales de operación. Así, el estudio se convierte en una herramienta práctica para entender cómo funciona el control del tráfico entre zonas, sirviendo como un recurso útil tanto para estudiantes como para administradores de sistemas.

2 OBJETIVOS

2.1 OBJETIVO GENERAL

Implementar y validar reglas de acceso perimetral en Endian Firewall para controlar el tráfico entre las zonas VERDE, NARANJA y ROJA, garantizando la correcta comunicación mediante los protocolos HTTP y FTP, así como la verificación funcional del comportamiento del tráfico inter-zona en un entorno de laboratorio

2.2 OBJETIVOS ESPECÍFICOS

- Configura las reglas de acceso necesarias para permitir la comunicación entre la zona VERDE (LAN) y la zona NARANJA (DMZ) utilizando los protocolos HTTP y FTP, asegurando que sus puertos correspondientes funcionen correctamente
- Establecer reglas de conectividad entre la zona ROJA (Internet/WAN) y la zona DMZ, ajustando permisos de entrada y salida según los requerimientos del escenario.
- Comprobar la correcta creación, aplicación y registro de las reglas de tráfico inter-zona mediante herramientas de monitoreo, tablas de filtrado y verificaciones internas del firewall.
- Realizar pruebas funcionales desde un navegador web para validar el acceso HTTP y FTP.
- documentar los resultados de cada prueba, analizando cómo se comporta el firewall ante las directivas configuradas y asegurándonos de que las reglas

cumplan con los objetivos de seguridad que hemos establecido.

3 MARCO TEÓRICO

3.1 SEGURIDAD PERIMETRAL EN ENTORNOS GNU/LINUX

La seguridad perimetral se refiere a un conjunto de mecanismos diseñados para controlar y proteger el flujo de información entre redes internas y externas. En entornos que utilizan GNU/Linux, este control se suele llevar a cabo a través de firewalls que implementan políticas de filtrado, segmentación de red y control de acceso.

La arquitectura perimetral generalmente se organiza en diferentes zonas lógicas, como, por ejemplo:

- LAN o zona interna (VERDE): red de confianza que concentra los equipos de usuarios.
- DMZ o zona desmilitarizada (NARANJA): espacio de servicios expuestos a Internet con un nivel de riesgo intermedio.
- WAN o zona externa (ROJA): red no confiable, normalmente asociada a Internet.

El principio básico es permitir solo el tráfico que realmente se necesita entre diferentes zonas, utilizando un enfoque de seguridad por capas y estableciendo reglas específicas para cada protocolo, como HTTP, FTP, DNS, y otros.

3.2 FIREWALL EN GNU/LINUX

Los firewalls en Linux se fundamentan, por lo general, en iptables o su evolución, nftables. Estos sistemas permiten un control detallado del tráfico a través de la inspección de paquetes, el filtrado por estado (stateful inspection), la traducción de direcciones de red (NAT) y reglas que se basan en puertos, direcciones IP y protocolos.

Estos sistemas hacen posible la implementación de políticas como:

- Permitir o denegar según el origen o destino.
- Validación de los estados de conexión (NUEVO, ESTABLECIDO, RELACIONADO).
- Redirección o publicación de servicios en la DMZ.

3.3 ENDIAN FIREWALL

Endian el uso de firewalls en Linux dentro de redes segmentadas es clave para asegurar que los servicios internos estén siempre disponibles, proteger la infraestructura que está expuesta y reducir los riesgos de intrusión desde el exterior.

Las funciones principales incluyen:

A. Firewall Stateful

Basado en iptables, Endian Firewall ofrece un filtrado dinámico que examina los estados de conexión, lo que permite identificar el tráfico legítimo y bloquear las solicitudes no autorizadas. Este enfoque es clave para gestionar protocolos como HTTP (puerto 80) y FTP (puerto 21) en situaciones inter-zona.

B. Segmentación por Zonas

Endian organiza la red en zonas de seguridad que ya están definidas:

- Verde (LAN interna) – una red confiable, en este caso 192.168.0.0/24.
- Naranja (DMZ) – una zona semiconfiable destinada a servidores públicos (192.168.10.0/24).
- Rojo (WAN) – una zona insegura que está expuesta a Internet.

Cada zona tiene sus propias reglas, lo que permite implementar un modelo de defensa en capas.

C. Proxy y Control Web

Incluye un proxy HTTP/HTTPS basado en Squid que se encarga de filtrar contenido, hacer caching y controlar el acceso a la web. Sin embargo, en este estudio, nos enfocamos únicamente en el control del tráfico entre zonas.

D. VPN y Servicios Seguros

Endian ofrece soporte para OpenVPN, IPSec y túneles cifrados, lo que permite accesos remotos seguros y segmentados a la LAN o DMZ.

E. IDS/IPS

El sistema combina tecnologías de detección y prevención de intrusiones que pueden alertar o bloquear el tráfico malicioso.

F. Interfaz de Gestión Web

Todo el sistema se gestiona a través de una interfaz gráfica, lo que facilita la creación rápida de reglas sin tener que modificar iptables manualmente. Las imágenes del laboratorio muestran cómo se crean las reglas Green → Orange, Green → Red y Red → Orange utilizando esta GUI

3.4 REGLAS DE ACCESO INTER-ZONA

La gestión de tráfico entre zonas es el elemento central del firewall perimetral. Cada regla establece:

Zona origen y destino

- Protocolo (TCP/UDP)

- Puerto de servicio
- Acción (permitir o denegar)

En este estudio se validan flujos como:

- HTTP desde LAN → DMZ
- HTTP desde LAN → WAN
- HTTP desde DMZ → WAN
- HTTP desde WAN → DMZ
- FTP desde LAN → WAN
- FTP desde WAN → DMZ

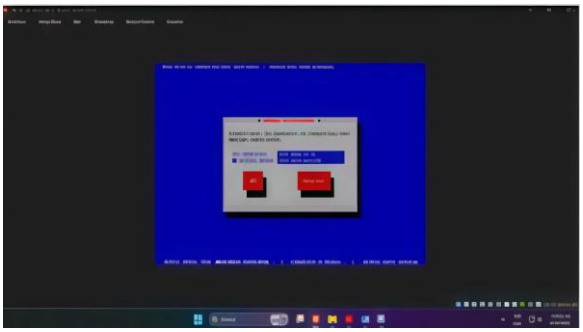
4 DESARROLLO

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

El control del tráfico entre zonas es uno de los pilares clave para garantizar la seguridad perimetral. En arquitecturas que utilizan firewalls por zonas, como Endian Firewall, cada segmento (LAN, DMZ y WAN) funciona con diferentes niveles de confianza. Esto requiere establecer reglas claras que permitan o bloqueen el flujo de datos entre estas zonas:

La interfaz GREEN (red local) tiene que ser configurada con la máscara de subred y su dirección IP estática. Esta dirección funcionará como el vínculo interno. Para que Endian tenga la capacidad de enrutar eficazmente el tráfico a la DMZ (Naranja) y al exterior (RED), es fundamental que la Zona GREEN esté configurada correctamente.

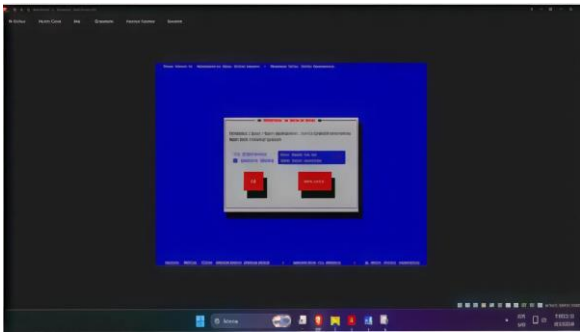
Ilustración 1: configuración de Endian



Fuente: autoría Propia

Cuando el EFW (posiblemente Endian Firewall) se ha instalado de manera adecuada, se elimina el instalador. Para comenzar con la configuración, se entra a la interfaz web (WebGUI) mediante un aparato distinto que esté conectado a la misma red. Para acceder a la dirección IP que se ha dado (por ejemplo, http://192.168.3.15), se emplea un navegador web.

Ilustración 1: Instalación EFW Completada Acceso Web

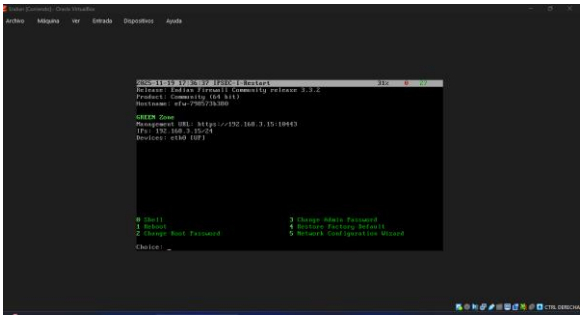


Fuente: autoría Propia

La consola de Endian Firewall ahora muestra el menú principal (CLI), lo que señala que el sistema está activo. La URL para la interfaz de administración web (WebGUI) es: https://192.168.3.15:10443. Además, el menú brinda alternativas fundamentales como reiniciar, apagar, modificar contraseñas o poner en marcha el asistente para la configuración de red.

.

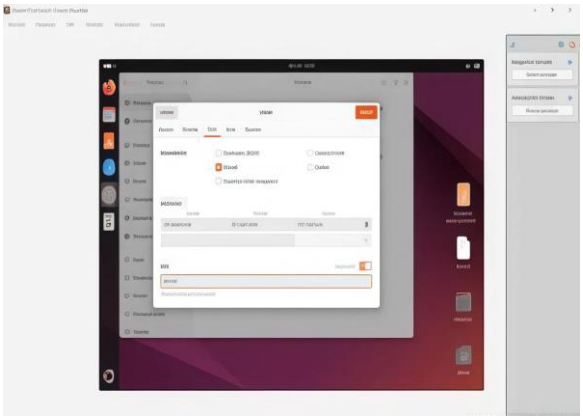
Ilustración 3. Menú Principal Endian Firewall Consola



Fuente: autoría Propia

Se realizó la configuración manual de red en el sistema operativo Ubuntu. Se asignaron a la máquina ciertos parámetros invariables durante este proceso: una dirección IP estática, el servidor DNS 8.8.8.8, la máscara de subred y la puerta de enlace. Estos cambios son esenciales porque aseguran una conexión de red ininterrumpida y estable para el equipo, lo que hace más fácil su comunicación.

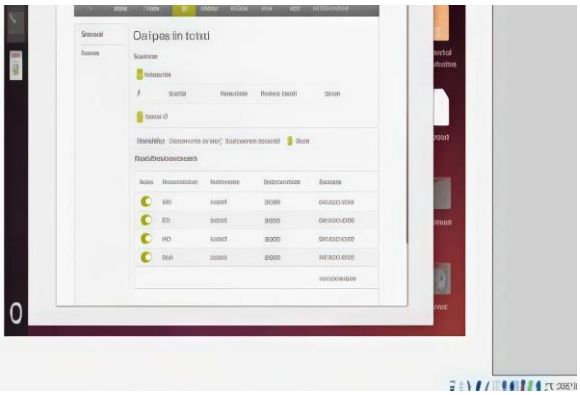
Ilustración 4. Ajuste de Conexión en Ubuntu



Fuente: autoría Propia

Se comienza el procedimiento para configurar el host. En esta fase, el usuario puede ver los perfiles y dispositivos de red que tiene disponibles. En particular, se pueden administrar las interfaces físicas que simbolizan las distintas áreas lógicas del firewall, como son las interfaces ORANGE (DMZ) y GREEN (red interna). Este paso es crucial para asegurar que todos los dispositivos estén conectados de manera adecuada y que cada área cuente con la asignación de seguridad apropiada en el cortafuegos.

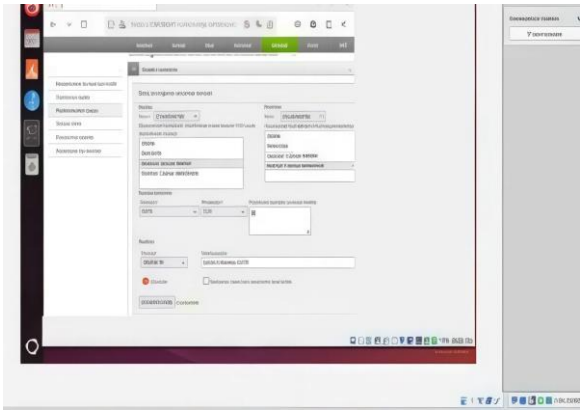
Ilustración 5. Gestión de Perfiles y Dispositivos de Red



Fuente: autoría Propia

El procedimiento consiste en crear una regla de reenvío de puertos en el firewall. Esto exige describir de manera precisa las propiedades del flujo informático que se quiere redirigir. Es necesario determinar la zona de destino y la zona de origen (por ejemplo, la Zona GREEN). Asimismo, es esencial señalar el Protocolo (por ejemplo, TCP) y el puerto de destino específico. El objetivo principal es canalizar el tráfico que proviene del exterior hacia un servidor situado en la red interna.

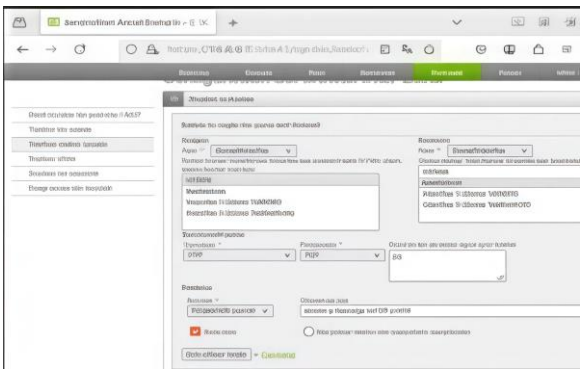
Ilustración 6. Creación de Regla de Reenvío de Tráfico



Fuente: autoría Propia

Una directriz de tráfico en el cortafuegos de Endian está siendo cambiada. La acción consiste en establecer una política de acceso que permita la comunicación. En particular, está configurado para habilitar el empleo del protocolo FTP, que emplea el puerto 21 y el protocolo TCP. Esta norma es válida para los flujos de información que se trasladan desde la zona verde (de confianza e interna) hasta la zona naranja (la DMZ), lo cual permite la interconexión entre las dos áreas de la red

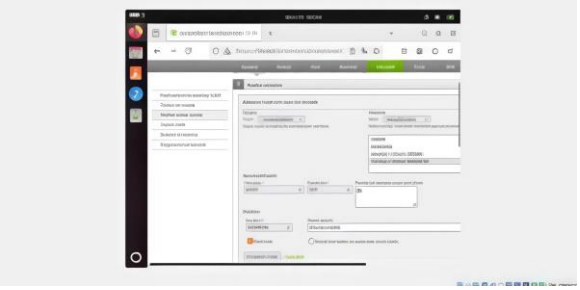
Ilustración 7. Establecimiento de Conectividad entre Zonas



Fuente: autoría Propia

Se procede a la creación de una regla de tráfico específica dentro del firewall denominada "Internet a DMZ". Esta política de seguridad se define para PERMITIR la comunicación utilizando el protocolo TCP a través del puerto 80 (HTTP). El origen de este tráfico es la Zona RED (Internet o WAN) y su destino es la Zona NARANJA (DMZ). El objetivo es facilitar el acceso desde el exterior a un servidor web que se encuentra alojado dentro de la DMZ.

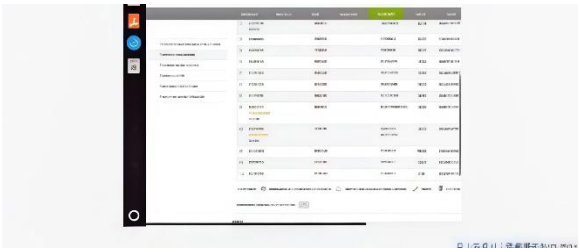
Ilustración 8. Habilitación de Acceso Web Externo a DMZ



Fuente: autoría Propia

Para auditar el sistema, se debe entrar en la sección de "Registros" (Logs) que está incluida en la zona de Seguridad del Firewall. Esta función posibilita examinar y estudiar detenidamente cada uno de los pormenores vinculados al tráfico de salida producido por la red. La herramienta proporciona datos específicos acerca de cómo se comunican las diferentes áreas lógicas del sistema, lo cual es fundamental para tener un control eficaz sobre el flujo de información que circula por la red.

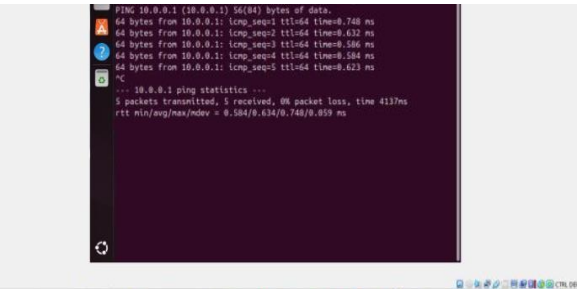
Ilustración 9. Configuración de red del cliente Ubuntu



Fuente: autoría Propia

Se realizó el comando PING a través de la terminal, apuntando en particular a la dirección 10.0.0.1. La finalidad de esta acción fue la de confirmar y diagnosticar que la conexión dentro de la red funciona correctamente. Se logró una comunicación completamente exitosa con el host de destino, según los resultados obtenidos: se mandaron cinco paquetes y llegaron todos, lo cual significa que la pérdida de paquetes (packet loss) fue del 0%. Esto garantiza que la capa de red funcione adecuadamente.

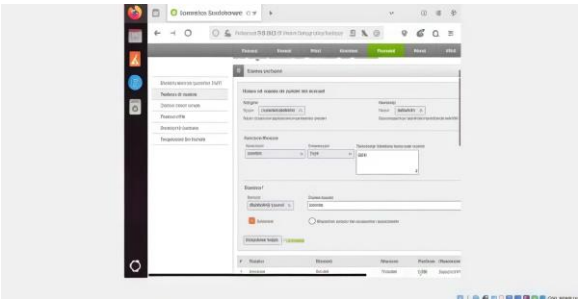
Ilustración 10. Verificación de Conectividad con PING



Fuente: autoría Propia

En el cortafuegos, se lleva a cabo una modificación de la directriz para tráfico saliente (Outbound Traffic). La configuración define una política de PERMISO para utilizar el servicio HTTPS, que se reconoce a través del puerto 443 y el protocolo TCP. Esta regla es válida para la comunicación que proviene de la Zona VERDE (la red interna de confianza) y va hacia la Zona ROJA (Internet). El objetivo es permitir que los usuarios internos tengan la posibilidad de navegar de forma segura y cifrada en páginas web hacia la red exterior.

Ilustración 11. Configuración de red del servidor DMZ



Fuente: autoría Propia

Se implementó la comunicación de ida y vuelta entre la Zona Verde (LAN) y la Zona Naranja (DMZ), lo que permitió el uso local de servicios esenciales como HTTP y FTP. Al mismo tiempo, se estableció el acceso restringido desde la Zona Internet (WAN) a la DMZ, lo que posibilitó que los servicios web se publicaran de manera segura hacia el exterior.

Por último, se llevaron a cabo pruebas exhaustivas y validaciones de cada una de las reglas de reenvío de puertos y directivas de tráfico. La comprobación se llevó a cabo revisando las entradas del firewall y haciendo pruebas exitosas con el navegador web. El sistema ahora funciona con una política de acceso consolidada que asegura el funcionamiento adecuado de HTTP y FTP en todas las combinaciones posibles de zonas. Endian Firewall correctamente configurado para la seguridad y el enrutamiento inter-zona.

5 CONCLUSIONES

La implementación que se llevó a cabo muestra que Endian Firewall es una herramienta muy eficaz para gestionar el tráfico entre diferentes zonas en entornos GNU/Linux. Su estructura zonificada permite separar de manera efectiva los segmentos de red que tienen distintos niveles de confianza, mientras que las reglas que se han configurado aseguran un control preciso sobre el acceso a servicios críticos.

Las pruebas funcionales confirmaron que las políticas se aplican de manera correcta, garantizando así la protección perimetral y permitiendo un análisis detallado del flujo de datos. Este estudio se presenta como una referencia valiosa para enseñar y aplicar conceptos de seguridad de red tanto en entornos académicos como profesionales

Finalmente, el ejercicio demostró que una buena configuración del firewall no solo protege los recursos

de la organización, sino que también asegura la disponibilidad de servicios críticos como HTTP y FTP entre las distintas zonas, logrando un equilibrio entre seguridad y una operación eficiente.

6 REFERENCIAS

[1] Endian Firewall Community, "Documentation Portal," Endian.com. Disponible en: https://www.endian.com/community/. Accedido: 02-dic-2025.

[2] The Linux Foundation, "Linux Documentation Project," The Linux Foundation. Disponible en: https://www.kernel.org/doc/. Accedido: 02-dic-2025.

[3] O. P. Eklund, "Netfilter/Iptables Firewall Architecture," Netfilter.org. Disponible en: https://www.netfilter.org/documentation/. Accedido: 02-dic-2025.

[4] OpenVPN Project, "OpenVPN Documentation," OpenVPN.net. Disponible en: https://openvpn.net/community-resources/. Accedido: 02-dic-2025.

[5] Squid Project, "Squid Proxy Official Documentation," Squid-cache.org. Disponible en: https://wiki.squid-cache.org/Documentation. Accedido: 02-dic-2025.

[6] Cisco Systems, "Firewall Best Practices Guide," Cisco.com. Disponible en: https://www.cisco.com/c/en/us/support/docs/security/firewalls/. Accedido: 02-dic-2025.

[7] SANS Institute, "Firewalls and Network Security Principles," SANS.org. Disponible en: https://www.sans.org/white-papers/. Accedido: 02-dic-2025.