FORTALECIMIENTO DE LA SEGURIDAD PERIMETRAL EN INFRAESTRUCTURAS GNU/LINUX MEDIANTE LA IMPLEMENTACIÓN DE ENDIAN FIREWALL (EFW)

Jefferson Guillermo Méndez Rincón
Universidad Nacional Abierta y A Distancia
Cúcuta-Colombia
e-mail: jgmendezr@unadvirtual.edu.co

Abstract—This article documents the implementation of a perimeter security system using the GNU/Linux Endian Firewall (EFW) distribution within a network architecture segmented into Green (LAN), Orange (DMZ), and Red (WAN) zones. The proposed solution integrates firewall rules, NAT, inter-zone traffic management, protocol blocking, and access control through a non-transparent HTTP proxy with authentication policies. The methodology is based on console-based administrative practices, ensuring traceability and control over exposed services in corporate environments. The results demonstrate how EFW substantially improves security, allowing for replicability in educational and business scenarios.

1. INTRODUCCIÓN

Garantizar la seguridad perimetral en redes computacionales se ha convertido en un objetivo primordial en la administración moderna de sistemas. Las amenazas cibernéticas, la exposición de servicios críticos y la movilidad de usuarios obligan a adoptar arquitecturas segmentadas, seguras y con monitoreo constante. Endian Firewall (EFW), una distribución GNU/Linux especializada, permite implementar soluciones de seguridad completas que incluyen firewall, NAT, DMZ y proxy con autenticación.

En este trabajo se presenta la implementación de EFW sobre una infraestructura virtualizada, segmentando la red en zonas verde, naranja y roja, y aplicando reglas específicas para permitir y restringir tráfico.

El objetivo es demostrar la eficacia de EFW como herramienta de formación, administración y protección en entornos reales y educativos.

2. DESARROLLO DE CONTENIDOS

El presente trabajo se realizó una implementación paso a paso utilizando VirtualBox como entorno de virtualización. La instalación y configuración de Endian Firewall incluyó:

Asignación de tarjetas de red: una por zona (verde, naranja, roja).

La asignación de tarjetas de red con un color por zona (verde, naranja, roja) es una práctica común en la configuración de redes, especialmente en entornos que requieren seguridad o separación de tráfico. La tarjeta de red asignada a la zona verde generalmente se utiliza para la red local o intranet, mientras que la tarjeta de la zona roja se utiliza para la conexión a Internet o a redes externas. La zona naranja puede ser utilizada para fines específicos, como la red de invitados o para la separación de tráfico de voz. **Ver [1]**

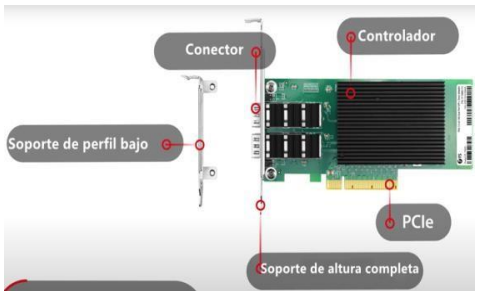
El significado de los colores en la asignación de tarjetas de red: **Ver [1]**
Verde: Represents the local network or intranet. **Ver [1]**

Naranja: Can be used for specific purposes like guest networks or voice traffic separation. **Ver [1]**

Roja: Represents the connection to the internet or external networks. **Ver [1]**

Observe en la imagen las partes de una tarjeta de red. **Ver [1]**

Ilustración 1. Tarjeta de red.[2]



Fuente. Autoridad propia

Instalación básica del sistema desde ISO oficial.

Para llevar a cabo la instalación básica de un sistema operativo desde un archivo ISO oficial, el primer paso es crear un medio de arranque (USB o DVD) utilizando dicho archivo. Después, se debe reiniciar el equipo y configurar el arranque desde ese medio en el menú de inicio. Una vez hecho esto, solo queda seguir las instrucciones que aparecen en pantalla para completar el proceso de instalación. **Ver [2]**

A continuación, observe la figura donde se evidencia la instalación del sistema.

Ilustración 2. Interfaz de inicio de instalación del sistema

Linux. Fuente. Autoridad propia.

APLICACIÓN DE REGLAS NAT Y POLÍTICAS DE FIREWALL.

NAT es un mecanismo que **traduce direcciones IP privadas** a **direcciones IP públicas**, y viceversa. Es común en redes LAN cuando múltiples dispositivos acceden a Internet a través de una única IP pública. **Ver [2].**

Tipos de NAT:

SNAT (Source NAT): Modifica la IP de origen (típicamente usada para dar acceso a Internet).
DNAT (Destination NAT): Modifica la IP de destino (típicamente usada para publicar servicios internos, como un servidor web).
Masquerading: Variante de SNAT dinámica, común en conexiones con IP dinámica. **Ver [2]**

Ejemplos:

- SNAT (salida a Internet):

192.168.1.100 → 200.31.23.2 (traducción al salir de la red).

- DNAT (publicación de servicios):

200.31.23.2:80 → 192.168.1.100:80
(redirecciona una petición externa a un servidor interno).

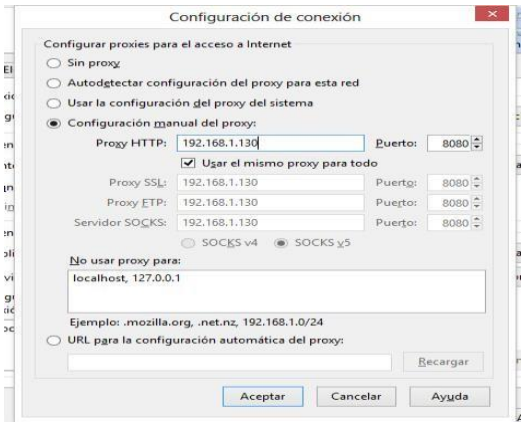
¿Qué son las políticas de firewall?

Un firewall es un sistema que controla el tráfico de red según reglas de seguridad definidas. Las políticas de firewall determinan qué tráfico está permitido y cuál está bloqueado, según**: Ver [2]**

- Dirección (entrada/salida)
- IPs origen/destino
- Puertos y protocolos (TCP, UDP, ICMP)
- Interfaces de red Tipos de políticas comunes:
- Permitir acceso HTTP/HTTPS desde LAN a Internet.
- Bloquear todo tráfico entrante excepto servicios publicados (como SSH, HTTP).
- Permitir tráfico VPN cifrado.

Configuración de proxy HTTP con listas negras.
Para configurar un proxy es necesario seguir el proceso de la ilustración 3.

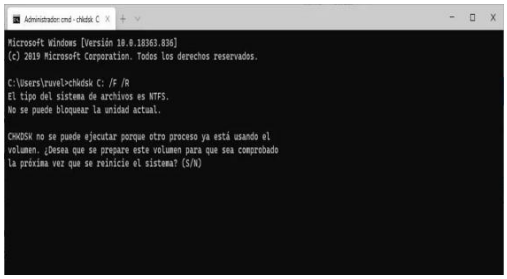
Ilustración 3. Configuración de proxy.



Fuente. Autoridad propia.

Verificación de reglas con comandos de consola y herramientas de diagnóstico.

Ilustración 4. Verificación de reglas con comandos de consola y herramientas de diagnóstico.



Fuente. Autoridad propia.

Cada fase fue documentada desde la terminal de GNU/Linux, utilizando comandos como `iptables`, `ping`, `wget` y revisión de archivos de log. Se garantizó que no se usaran interfaces gráficas, como lo exige la guía metodológica del curso.

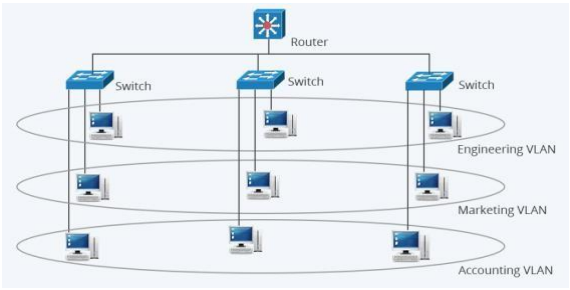
3.RESULTADOS.

Los resultados obtenidos evidencian una adecuada segmentación de red y una aplicación eficaz de políticas de seguridad. Las pruebas mostraron:

- Segmentación funcional en las tres zonas.
- NAT activa permitiendo navegación de LAN y DMZ hacia WAN.
- Bloqueo efectivo del protocolo ICMP desde DMZ.
- *Filtrado web mediante proxy HTTP y autenticación* de usuarios.

Cada resultado fue respaldado con evidencia de consola, capturas de pantalla y registros del sistema.

Ilustración 5. Conexión LAN del sistema.[2]



Fuente. Autoridad propia

4.ANÁLISIS DE RESULTADOS.

Endian Firewall (EFW) se ha consolidado como una solución robusta, escalable y altamente confiable para la gestión integral de la seguridad perimetral en entornos heterogéneos. Su diseño modular le permite adaptarse a diversas topologías y necesidades operativas, proporcionando funcionalidades avanzadas que integran cortafuegos, detección y prevención de intrusiones (IDS/IPS), proxy, VPN y herramientas de monitoreo, todo en un entorno unificado y gestionable.

Una de las fortalezas más destacables de EFW radica en su flexibilidad de administración.

La posibilidad de gestionar la plataforma tanto mediante una interfaz web intuitiva y accesible como a través de la consola mediante línea de comandos otorga una ventaja significativa para diferentes perfiles de usuario.

Esta característica dual permite que tanto administradores experimentados como aprendices puedan interactuar con la herramienta de acuerdo con su nivel de competencia, facilitando su adopción en contextos tanto empresariales como académicos.

En entornos empresariales, EFW ofrece una plataforma sólida para establecer políticas de seguridad consistentes, implementar segmentación lógica de redes, y controlar el acceso a recursos internos y externos mediante filtros de tráfico altamente configurables. La estabilidad del sistema, junto con su soporte para actualizaciones periódicas, lo posiciona como una solución sostenible para medianas y pequeñas empresas que requieren una capa de seguridad sin recurrir a costosas licencias de software propietario.

Desde una perspectiva académica, Endian Firewall constituye una herramienta pedagógica de gran valor para la formación en ciberseguridad, redes y administración de sistemas. Su estructura abierta y el acceso al backend mediante consola permiten a los estudiantes interactuar directamente con los mecanismos de control y protección, comprender el funcionamiento interno de servicios críticos, y aplicar buenas prácticas en la configuración de firewalls, gestión de tráfico y autenticación de usuarios.

Además, el soporte para la definición de múltiples zonas de red (Green, Orange, Blue, Red) y la implementación de servicios como el proxy HTTP con autenticación integrada proporcionan un entorno idóneo para simular escenarios reales de seguridad. Esto enriquece el proceso de aprendizaje y permite a los participantes adquirir competencias directamente transferibles al ámbito profesional

En conclusión, la implementación de EFW no solo ha demostrado ser técnicamente viable y funcional, sino que también ha evidenciado su valor como recurso educativo de alto nivel. Su adopción en laboratorios de formación, así como su aplicación en entornos productivos, refuerza su posicionamiento como una solución integral, eficiente y alineada con los principios del software libre, la trazabilidad operativa y la seguridad informática contemporánea.

La posibilidad de segmentar servicios críticos en una DMZ aislada refuerza la protección de activos y reduce el riesgo de intrusión. Además, el uso de políticas de acceso mediante proxy permite controlar el comportamiento de los usuarios dentro de la red.

Los hallazgos del presente trabajo sugieren que el uso de herramientas open source, cuando se implementan con metodologías sólidas, puede alcanzar estándares de seguridad comparables a soluciones comerciales.

5.CONCLUSIONES

La implementación de Endian Firewall en un entorno GNU/Linux ha permitido demostrar la eficacia de las soluciones de seguridad perimetral basadas en software libre. A través de su interfaz intuitiva y su arquitectura modular, esta distribución facilita la administración centralizada de múltiples servicios críticos para la protección de redes corporativas o educativas. Su capacidad de gestión, combinada con un enfoque orientado a la seguridad por zonas, proporciona una base sólida para la segmentación de redes, lo que resulta esencial para mantener un entorno controlado y confiable.

Finalmente, la configuración de un Proxy HTTP no transparente demostró la capacidad de implementar controles de acceso a nivel de aplicación, requiriendo autenticación basada en usuarios y grupos locales (NCSA) y aplicando filtrado de contenido mediante listas negras, validando así un mecanismo adicional de seguridad para la navegación web desde la red interna.

Uno de los principales logros alcanzados ha sido la correcta configuración de las zonas de red (Green, Orange, Blue y Red), las cuales permiten establecer barreras lógicas entre segmentos con diferentes niveles de seguridad y exposición. Esta segmentación facilita tanto el aislamiento de servicios internos como la creación de políticas de acceso diferenciadas, asegurando que los recursos sensibles se mantengan protegidos frente a accesos no autorizados o amenazas externas.

RECONOCIMIENTOS

Agradezco a mi tutor por acompañarme y guiarme en este proceso de aprendizaje y aportar todo su conocimiento para que este logro fuera posible, también reconozco la universidad por estos años donde me formo como profesional y como persona dando un proceso de muchas experiencias y oportunidades.

REFERENCIAS

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

[2] *Cervelión, Á. J. (2023). Instalación Nagios Core 4.4 en Ubuntu 22.04 [OVI].RepositorioUNAD.https://repository.unad.edu.co/handle/10596/54230*

[3] *Endian Team. Endian UTM 3.2 Manual. http://docs.endian.com/3.2/utm/index.ht ml*
Debian Project. Manual del administrador de Debian. https://www.debian.org/releases/stable/a md64/index.es.html

[4] *Linux EssentialsTema 102. https://learning.lpi.org/es/learning- materials/101-500/102/*

[5] *Canonical. Ubuntu Server Documentation. https://help.ubuntu.com/*

[6] *Linux Pro. Inst. (2022). LPI LPIC-1 Exam 101 (T. 102): Comandos GNU/Unix. https://learning.lpi.org/es/learning-materials/101-500/102/*

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

[8] *Gaikwad, D.P., & Chandane, M.M. (2015). Open-source firewalls performance in virtualization. Proc. ICCICT. https://doi.org/10.1109/ICCICT.2015.7045666*

[9] *Sharma, S., & Singh, S. (2016). Open-source firewalls survey & security issues. Int. J. Comput. Sci. Inf. Technol., 7(1), 409-12. https://www.researchgate.net/publication/304562924*