IMPLEMENTACIÓN DE FIREWALL PERIMETRAL EN ENDIAN PARA GESTIÓN SEGURA DE ZONAS GREEN Y ORANGE

Camilo Andres Quijano Godoy
caquijanogo@unadvirtual.edu.co

RESUMEN: *El artículo detalla la implementación de un entorno de firewall perimetral utilizando Endian Firewall Community , con el propósito de segmentar la red en zonas de seguridad (GREEN y ORANGE) y establecer reglas de acceso controladas entre ellas. Se configuraron rutas, servicios, reglas Inter-Zone y políticas de NAT para validar la adecuada publicación y consumo de servicios, particularmente un servidor web ubicado en la DMZ. El estudio demuestra la efectividad del modelo de defensa en profundidad y los beneficios de la inspección y control del tráfico entre zonas, minimizando la superficie de ataque del servidor expuesto bajo la política de "mínimo privilegio".*

PALABRAS CLAVE: Endian, Firewall, NAT, Redes

1 INTRODUCCIÓN

La seguridad perimetral continúa siendo un pilar fundamental en la protección de infraestructuras tecnológicas. En escenarios corporativos, los firewalls permiten segmentar la red en zonas con distintos niveles de confianza y controlar el flujo de tráfico entre ellas, reduciendo riesgos de intrusiones y accesos no autorizados [1], [5].

El presente trabajo documenta la implementación técnica correspondiente a la Etapa 7 del diplomado, desplegando un laboratorio funcional basado en Endian Firewall. El objetivo central es segmentar la red en zonas GREEN (LAN) y ORANGE (DMZ), desplegar un servidor web seguro en la DMZ y establecer reglas que permitan el acceso controlado desde la red interna hacia la zona desmilitarizada, aplicando políticas de "mínimo privilegio"[2].

Asimismo, se desarrollan pruebas de validación técnica que garantizan el funcionamiento de las reglas configuradas, asegurando la disponibilidad, integridad y confidencialidad de los servicios expuestos.

2 OBJETIVOS

2.1 OBJETIVO GENERAL

Implementar un firewall perimetral utilizando Endian Firewall Community, aplicando segmentación por zonas y configurando reglas de acceso entre GREEN y ORANGE para validar la correcta operación de un entorno seguro.

2.2 OBJETIVOS ESPECÍFICOS

- Configurar las interfaces de red del firewall y asignarlas a sus zonas correspondientes (GREEN, ORANGE, RED).
- Implementar un servidor web (Apache) en la zona DMZ (ORANGE) sobre un sistema Linux.
- Establecer reglas de acceso Inter-Zone permitiendo únicamente el tráfico HTTP autorizado.
- Configurar reglas de Port Forwarding (NAT) para la publicación del servicio web hacia redes externas.
- Validar la conectividad y las políticas de seguridad mediante herramientas de diagnóstico (ping, curl, logs).

3 METODOLOGÍA

Para el desarrollo de la actividad se empleó un entorno de virtualización, implementando una arquitectura de red compuesta por tres nodos principales. La metodología se dividió en fases secuenciales: diseño de topología, configuración de interfaces, despliegue de servicios y aplicación de políticas de seguridad [4], [6].

Entorno del Laboratorio

El laboratorio consta de los siguientes componentes:

- Endian Firewall 3.3.2: Actúa como puerta de enlace y gestor de seguridad perimetral.
- Kali Linux (Zona GREEN): Simula un cliente interno con IP 192.168.2.20.
- Ubuntu Server (Zona ORANGE): Servidor alojado en la DMZ con IP 192.168.1.20.

Figura 1: Topología de red implementada en VirtualBox

```
Choice: 5
Enter Root Password:
Network Configuration Wizard
----------------------------
Hostname: efw-da2243efc7
Domain: localdomain
RED interface type: DHCP
RED device: eth2
RED IPs (IP/CIDR):
RED gateway:
Primary DNS:
Secondary DNS:
GREEN devices: eth0
GREEN IPs (IP/CIDR): 192.168.2.15/24
Enable DHCP server on GREEN: on
ORANGE devices: eth1
ORANGE IPs (IP/CIDR): 192.168.1.15/24
BLUE devices:
BLUE IPs (IP/CIDR):
Enable SSH access: on
Allow access to ports 22, 80 and 10443 from any interface: on

Hostname? efw-da2243efc7_
```

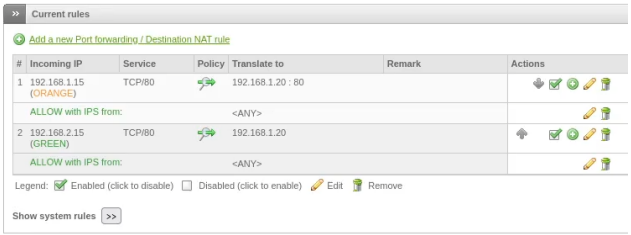
Fuente: Elaboración propia

3.1 Configuración de Interfaces y Zonas

Se configuraron tres interfaces físicas en el firewall Endian para garantizar la separación del tráfico [1], [5]:

- eth0 (GREEN): 192.168.2.15/24 – Red de confianza (LAN).
- eth1 (ORANGE): 192.168.1.15/24 – Zona Desmilitarizada (DMZ).
- eth2 (RED): Asignación dinámica (DHCP) – Conexión hacia Internet (WAN).

Figura 2: Reglas Actuales desde Endian.



Fuente: Autoría Propia

4 DESARROLLO DE LA ACTIVIDAD

4.1 Implementación del Servidor Web

En el nodo de la zona ORANGE (Ubuntu Server), se instaló y configuró el servicio Apache HTTP Server. Se verificó el estado del servicio escuchando en el puerto 80 TCP mediante comandos de inspección de sockets.

$ ss -tulpn | grep :80

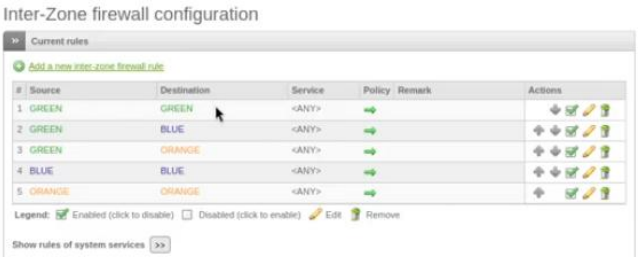
La correcta ejecución del servicio es prerrequisito para validar las reglas de reenvío y acceso desde otras zonas.

4.2 Configuración de Reglas Inter-Zone

Por defecto, Endian bloquea el tráfico entre zonas para maximizar la seguridad. Se creó una regla de firewall específica para permitir el consumo del servicio web desde la red interna [2], [10]:

- Origen: Zona GREEN.
- Destino: Zona ORANGE.
- Servicio: HTTP (TCP/80).
- Acción: ALLOW (Permitir).

Figura 3: Configuración del Firewall en Endian.



Fuente: Autoría Propia

Esta configuración asegura que los usuarios internos puedan acceder a la aplicación web, mientras que cualquier otro tipo de tráfico (SSH, FTP no autorizado) permanece bloqueado.

Tabla 1: Configuración de Regla Inter-Zone en Endian]

Zona	Función	Interfaz (ejemplo)	Rango
GREEN	LAN	eth0	192.168.10.0/24
ORANGE	DMZ	eth1	192.168.20.0/24
RED	WAN	eth2	DHCP o IP Pública

Fuente: Autoría Propia

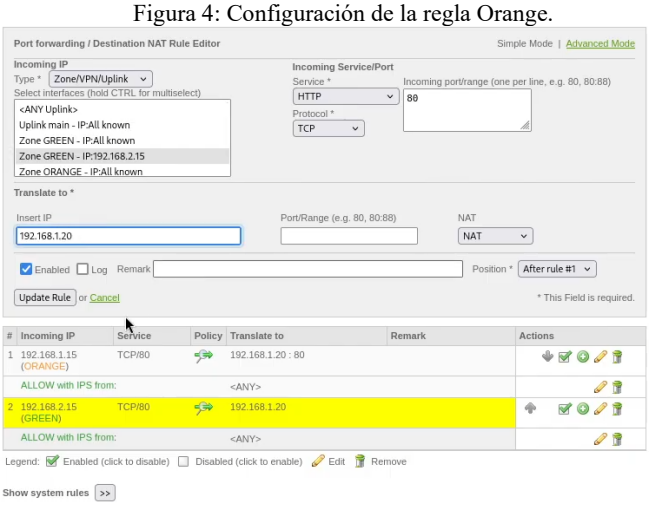
4.3 Configuración de NAT y Port Forwarding

Para permitir el acceso al servidor web desde redes externas o para mapear correctamente las peticiones, se habilitó una regla de Destination NAT (DNAT):

- IP Entrante: Cualquiera (Uplink).
- Puerto Servicio: 80.
- IP Destino (Translate to): 192.168.1.20 (Servidor Web).

Esto garantiza que las solicitudes que llegan a la interfaz pública del firewall sean redirigidas transparente y seguramente hacia el servidor aislado en la DMZ.

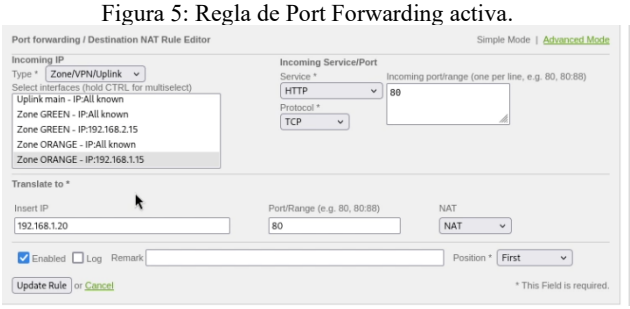
Figura 4: Configuración de la regla Orange.



Fuente: Autoría Propia

La regla NAT implementada es un Destination NAT (DNAT), esencial para redirigir el tráfico entrante de la interfaz RED/Uplink hacia el servidor en la DMZ (192.168.1.20). Esta técnica de Port Forwarding protege la identidad y el acceso directo al servidor, exponiendo solo el puerto 80 del firewall como proxy inverso al mundo exterior [8], [10].

Figura 5: Regla de Port Forwarding activa.



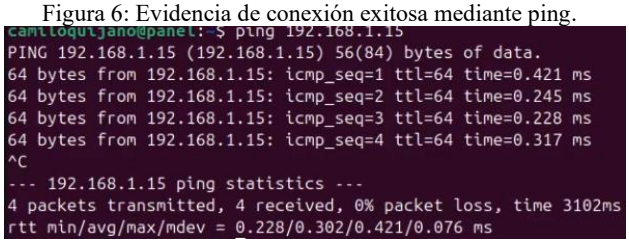
Fuente: Elaboración propia

5 RESULTADOS Y DISCUSIÓN

Las pruebas de conectividad validaron la eficacia de la configuración.

- Validación desde Zona GREEN: El cliente Kali Linux logró conexión exitosa mediante el comando curl http://192.168.1.20, recibiendo la respuesta del servidor Apache. Esto confirma que la regla Inter-Zone está operativa.
- Aislamiento de Tráfico: Intentos de conexión a puertos no autorizados fueron rechazados, cumpliendo con el objetivo de segmentación.
- Conectividad de Red: Las pruebas de ICMP (ping) validaron el enrutamiento correcto entre las interfaces del firewall y los hosts finales.

Figura 6: Evidencia de conexión exitosa mediante ping.



Fuente: Autoría Propia

El uso de zonas diferenciadas (GREEN vs ORANGE) demostró ser una arquitectura robusta, impidiendo que un compromiso hipotético en el servidor web (DMZ) afecte directamente a la red interna (LAN), alineándose con las mejores prácticas de defensa en profundidad [5], [10].

6 CONCLUSIONES

La implementación realizada permitió validar de manera práctica los conceptos de seguridad perimetral. Se logró desplegar un firewall Endian funcional que gestiona el tráfico entre múltiples zonas, garantizando disponibilidad para los servicios autorizados y confidencialidad mediante el bloqueo de tráfico no deseado.

Se concluye que la correcta definición de reglas Inter-Zone y políticas de NAT es crítica para la operación segura de servicios expuestos a internet o a redes internas. El laboratorio cumplió satisfactoriamente con todos los objetivos planteados en la guía de actividades.

7 REFERENCIAS

[1]. W. Stallings, “Seguridad de redes: aplicaciones y estándares,” 6.ª ed., Pearson Educación, 2017.

[2]. Endian, “Documentación oficial de Endian Firewall Community,” Endian S.r.l., 2024. [En línea]. Disponible: https://www.endian.com

[3]. Universidad Nacional Abierta y a Distancia (UNAD), “Guía de laboratorio: Administración de sistemas operativos Open Source,” Escuela de Ciencias Básicas, Tecnología e Ingeniería, 2025.

[4]. Cisco Systems, “Guía de diseño de redes seguras,” Cisco Networking Academy, 2023. [En línea]. Disponible: https://www.cisco.com

[5]. Instituto Nacional de Ciberseguridad (INCIBE), “Guía de seguridad perimetral y firewalls,” INCIBE, España, 2024. [En línea]. Disponible: https://www.incibe.es

[6]. A. Tanenbaum y D. Wetherall, “Redes de computadoras,” 5.ª ed., Pearson Educación, 2022.

[7]. K. Scarfone y P. Hoffman, “Guía para arquitecturas de seguridad en redes,” Instituto Nacional de Estándares y Tecnología (NIST), 2023. [En línea]. Disponible: https://www.nist.gov

[8]. Red Hat, “Implementación de firewalls y zonas de seguridad en Linux,” Red Hat Documentation, 2024. [En línea]. Disponible: https://access.redhat.com

[9]. S. Hernández y J. Martínez, “Seguridad perimetral y segmentación de redes corporativas,” Revista Iberoamericana de Tecnologías de la Información, vol. 18, no. 2, pp. 45–56, 2023.

[10]. OWASP Foundation, “Buenas prácticas para la protección de servicios expuestos en red,” OWASP en Español, 2024. [En línea]. Disponible: https://owasp.org