ENDIAN FIREWALL COMMUNITY COMO MOTOR DE ARQUITECTURAS DE SEGURIDAD PERIMETRAL MULTI-ZONA.

Ramses Almanza Avila
e-mail: ralmanzaa@unadvirtual.edu.co

RESUMEN: *Este documento presenta la implementación y configuración de una solución integral de seguridad perimetral basada en el Firewall que nos provee la comunidad de Endian, formalmente llamada la Endian Firewall Community (EFW) para el establecimiento de una arquitectura de red dividida en tres zonas: LAN (zona verde), WAN (zona roja) y DMZ (zona naranja). La investigación aborda la configuración de servicios críticos de red incluyendo NAT (Network Address Translation), reglas de firewall multi-zona, servicios web y FTP en zona desmilitarizada, y la implementación de un servidor proxy HTTP con políticas de autenticación y filtrado de contenido. Los resultados demuestran la efectividad del software de firewall de Endian como solución empresarial para la segmentación y control de tráfico de red, proporcionando un nivel robusto de seguridad perimetral con capacidades avanzadas de monitoreo y control de acceso.*

PALABRAS CLAVE: Endian Firewall, Segmentación de red, Seguridad perimetral, NAT.

1 INTRODUCCIÓN

La seguridad informática (principalmente la de las redes de telecomunicaciones), han tenido que evolucionar y reinventarse significativamente en las últimas décadas, requiriendo soluciones cada vez más avanzadas, complejas o, por llamarlo de una manera distinta, vanguardistas para proteger los activos digitales organizacionales. La implementación de arquitecturas de seguridad perimetral basadas en zonas representa una metodología fundamental para el control granular del tráfico de red y la protección contra amenazas externas [1].

Endian Firewall Community (EFW) surge como una solución de la comunidad del “free software”, como una alternativa de código abierto que combina las funcionalidades de firewall, proxy, VPN y sistemas de detección de intrusiones en una única plataforma. Esta distribución GNU/Linux especializada proporciona una interfaz web intuitiva para la gestión de políticas de seguridad complejas, facilitando la implementación de arquitecturas multi-zona en entornos empresariales [2].

En el presente artículo, se documenta la implementación de una arquitectura de seguridad perimetral completa haciendo uso de Endian Firewall, abarcando desde la configuración básica de interfaces de red hasta la implementación de políticas avanzadas de filtrado de contenido y autenticación de usuarios.

2 MARCO TEÓRICO

2.1 ARQUITECTURAS DE SEGURIDAD PERIMETRAL

Para este tipo de arquitecturas, nos basamos en el concepto de "castillo y foso", donde se establece una barrera defensiva entre la red interna confiable y las redes externas no confiables [3]. Sin embargo, las arquitecturas modernas han evolucionado hacia modelos de segmentación por zonas que permiten un control más granular del tráfico.

2.2 MODELO DE TRES ZONAS

Se constituye la base de la arquitectura propuesta de la siguiente manera:

- Zona Verde (LAN): Red interna donde residen las estaciones de trabajo y recursos críticos de la organización.
- Zona Roja (WAN): Interfaz hacia redes externas, típicamente Internet.
- Zona Naranja (DMZ): Zona desmilitarizada (públicas) que aloja servicios públicos como servidores web y de correo.

2.3 NETWORK ADDRESS TRANSLATION (NAT)

Permite que múltiples dispositivos en una red privada compartan una dirección IP pública, proporcionando además una capa adicional de seguridad al ocultar la topología interna de la red [4].

2.4 PROXY HTTP Y FILTRADO DE CONTENIDO

Los Proxy sirven como intermediarios entre clientes internos e Internet, permitiendo la implementación de políticas de acceso granulares y el filtrado de contenido basado en categorías, dominios específicos o patrones de URL [5].

3 METODOLOGÍA

3.1 ARQUITECTURAS DE SEGURIDAD PERIMETRAL

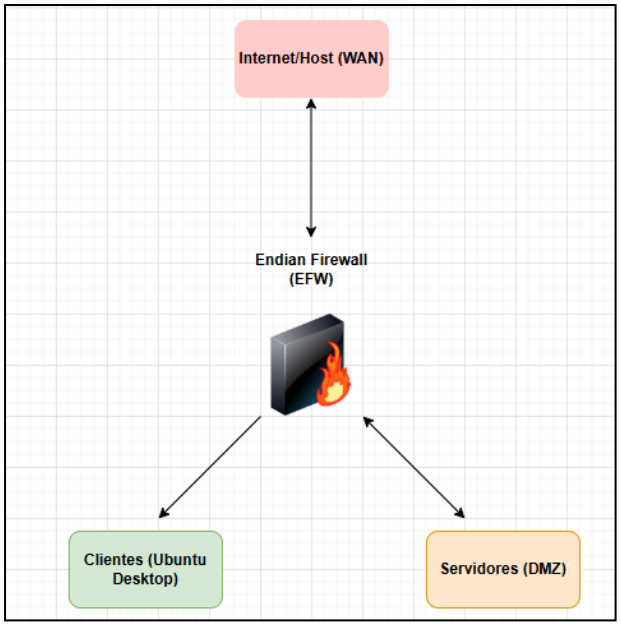
Se realiza en un entorno virtualizado utilizando VirtualBox 7.0, con las siguientes especificaciones:

- Servidor Endian Firewall: 2GB RAM, 20GB almacenamiento, 3 interfaces de red.
- Servidor DMZ (Ubuntu Server): 1GB RAM, 15GB almacenamiento.
- Estación de trabajo LAN: 1GB RAM, 10GB almacenamiento.

3.2 ARQUITECTURA DE RED IMPLEMENTADA

Se hace uso de una topología de red estructurada de la siguiente manera:

Fig. 1. Arquitectura de red implementada



Fuente: Autoría Propia (Gráfico hecho en draw.io).

Direccionamiento IP asignado:

- Zona Roja (WAN): 192.168.1.0/24
- Zona Verde (LAN): 10.0.1.0/24
- Zona Naranja (DMZ): 172.16.1.0/24’

3.3 FASES DE IMPLEMENTACIÓN

Se estructuró en cinco fases correspondientes a las temáticas principales:

1. Instalación y configuración inicial de Endian Firewall.
2. Configuración de servicios NAT.
3. Habilitación de servicios en zona DMZ.
4. Configuración de reglas de tráfico inter-zona.
5. Implementación de proxy HTTP con autenticación.

4 DESARROLLO E IMPLEMENTACIÓN

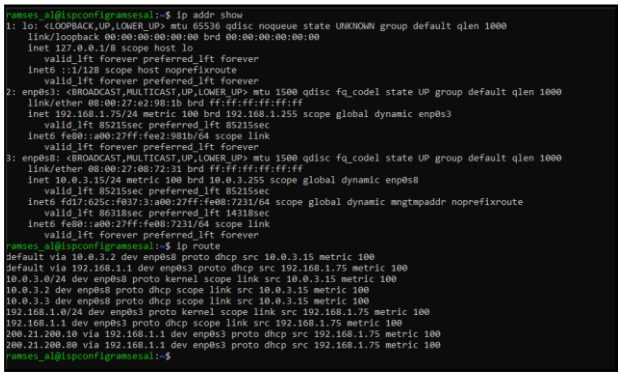
4.1 INSTALACIÓN Y CONFIGURACIÓN.

Se realiza la instalación de Endian Firewall Community desde la imagen ISO oficial, configurando tres interfaces de red correspondientes a las zonas definidas:

- eth0 (Zona Roja): Conectada a red NAT de VirtualBox para simulación de WAN
- eth1 (Zona Verde): Red interna para LAN
- eth2 (Zona Naranja): Red interna dedicada para DMZ

Durante el proceso de instalación se configuraron los parámetros básicos de red y se estableció la interfaz web de administración accesible desde la zona verde en la dirección 10.0.1.1:10443.

Fig. 2. Configuración de interfaces de red en Endian



Fuente: Autoría Propia.

4.2 CONFIGURACIÓN DE LA NAT.

Para el correcto desarrollo de esta parte, fue necesario desarrollar la configuración de la NAT que iba a ser usada por la red LAN para establecer comunicación con el servidor

WAN y una distinta para los servidores DMZ con el mismo fin. Además de ello, se realiza reenvío de puertos (más comúnmente conocido por su significado en inglés "port forwarding") para permitir el acceso a diversos servicios en la red. Mas detalles a continuación:

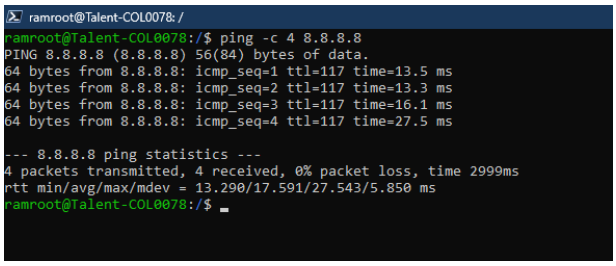
NAT para Zona Verde hacia WAN: Se configura una regla NAT básica que permite a todas las estaciones de la LAN (10.0.1.0/24) acceder a Internet a través de la interfaz WAN. Esta configuración se realizó mediante la interfaz web en la sección "Network → NAT".

NAT para Zona DMZ hacia WAN: Definimos una regla específica para permitir que los servidores en la DMZ (172.16.1.0/24) puedan establecer conexiones salientes hacia Internet, necesario para actualizaciones y sincronización de servicios.

Configuración de Port Forwarding: Implementación de reglas de reenvío de puertos para permitir el acceso desde Internet hacia servicios específicos en la DMZ:

- Puerto 80 (HTTP) → 172.16.1.10:80
- Puerto 21 (FTP) → 172.16.1.10:21

Fig. 3. Verificación de conectividad LAN hacia WAN (máquina cliente)



Fuente: Autoría Propia.

4.3 CREACIÓN DE SERVICIOS EN LA ZONA DMZ.

En este punto, realizamos la habilitación de Servicios HTTP y FTP, en donde apache2 actúa como servidor web y vsftpd como servidor FTP.

Luego de esto, se configuran las reglas del firewall directamente en endian para permitir el tráfico de los protocolos HTTP y FTP a través de los puertos seleccionados para este fin (80 para HTTP y 21 para FTP), esto, desde el Endian hacia el servidor DMZ en "Firewall → Outgoing traffic".

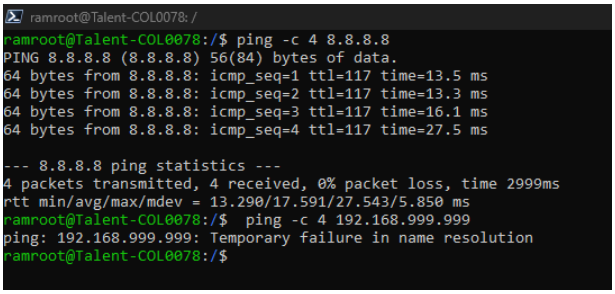
Por último, para mejorar la seguridad y reducir la superficie de ataque, se configuraron reglas para denegar el protocolo ICMP (ping):

Regla 1: Denegar ICMP Echo Request (Tipo 8)

Regla 2: Denegar ICMP Echo Reply (Tipo 0)

La verificación se realizó mediante pruebas de conectividad desde diferentes zonas:

Fig. 4. Bloqueo de protocolo ICMP configurado (prueba de envío de paquetes).



Fuente: Autoría Propia.

4.4 CREACIÓN DE SERVICIOS EN LA ZONA DMZ.

Aquí trabajamos en las configuraciones necesarias para que los servicios de la zona DMZ estuvieran disponibles para su uso dentro de la red, la cual se realizó de la siguiente manera:

Comunicación Zona Verde → Zona Naranja: Incluye reglas específicas para permitir el acceso desde la LAN hacia servicios en la DMZ:

Regla HTTP: Permitir 10.0.1.0/24 → 172.16.1.0/24:80

Regla FTP: Permitir 10.0.1.0/24 → 172.16.1.0/24:21

Comunicación Internet → Zona DMZ: Se establecieron reglas para permitir el acceso público hacia servicios en la DMZ:

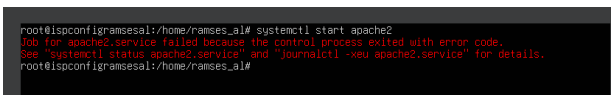
Regla HTTP público: Permitir ANY → 172.16.1.10:80

Regla FTP público: Permitir ANY → 172.16.1.10:21

Pruebas de conectividad realizadas:

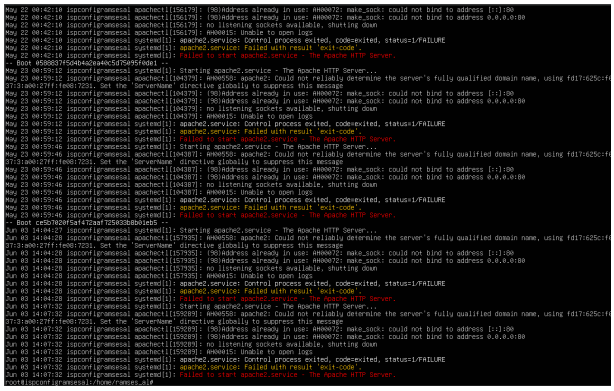
1. HTTP desde LAN hacia DMZ:
2. HTTP desde LAN hacia WAN:
3. FTP desde LAN hacia WAN:
4. HTTP desde WAN hacia DMZ: Verificado mediante acceso externo simulado, confirmando la correcta configuración del port forwarding.

Fig. 5. Ejemplo de conflicto de configuración al montar el servicio Apache2 en la máquina DMZ.



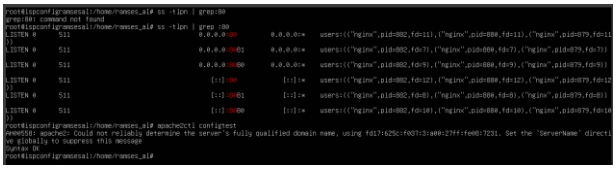
Fuente: Autoría Propia.

Fig. 6. Logs de errores de Apache2.



Fuente: Autoría Propia.

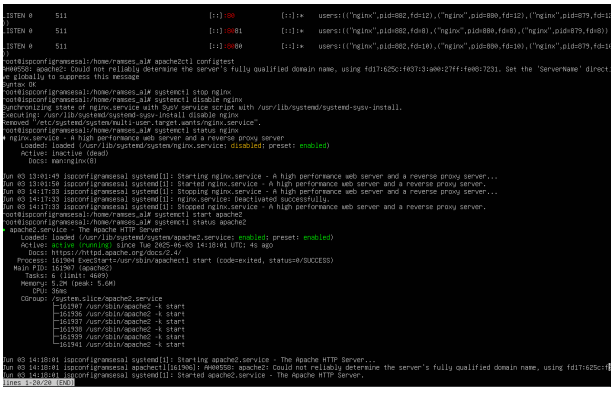
Fig. 7. Demostración de la razón del error (puerto 80 ocupado por NGINX).



Fuente: Autoría Propia.

Se resuelve el problema desactivando NGINX y luego evidenciamos que los servicios de http y ftp se ejecutan correctamente

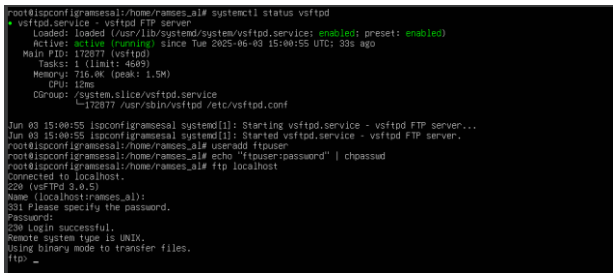
Fig. 8. Servicio HTTP habilitado en DMZ.



Fuente: Autoría Propia.

Ahora se habilita el servicio de FTP en el servidor DMZ y se configura un usuario con una clave (con el fin de no complicar más la solución, se ponen las mismas del usuario principal):

Fig. 9. Servicio FTP habilitado en DMZ.



Fuente: Autoría Propia.

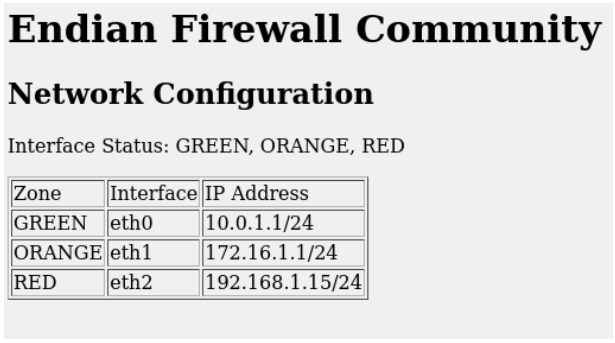
4.5 CONFIGURACIÓN DEL PROXY HTTP

Primero, implementamos un servidor proxy HTTP no transparente con las siguientes características:

- Puerto de escucha: 8080
- Autenticación requerida: Sí
- Registro de actividad: Completo

Luego, se le crean perfiles y se definen las listas negras para prevenir el acceso a ciertos sitios web mientras se esté conectado al proxy.

Fig. 9. Configuración de Endian.



Fuente: Autoría Propia.

Para la “blacklist” establecimos un perfil de filtrado denominado "RestrictedAccess" con las siguientes restricciones:

Sitios con acceso restringido:

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

Configuración de autenticación: Se creó el usuario "ramtest" asociado al grupo "employees" con las siguientes políticas:

- Horario de acceso: 24/7
- Ancho de banda: Sin límite
- Filtrado de contenido: Activo
- Lista negra: RestrictedAccess (uso del perfil que creamos en el paso anterior)

Configuración del cliente: Los navegadores web en la zona verde se configuraron para utilizar el proxy:

- Servidor proxy: 10.0.1.1
- Puerto: 8080
- Autenticación: ramtest/ramroot123

Pruebas de funcionalidad: Se realizan diversas pruebas para confirmar el correcto funcionamiento del sistema de filtrado:

Acceso a sitio permitido (www.google.com):

Resultado: Acceso exitoso tras autenticación

Log: "ALLOWED - User: ramtest - URL: www.google.com"

Acceso a sitio bloqueado (www.youtube.com):

Resultado: Página de bloqueo mostrada

Log: "BLOCKED - User: ramtest - URL: www.youtube.com - Reason: Blacklist"

Fig. 10. Permisos y reglas en Endian.

Endian Firewall - NAT Configuration

Port Forwarding Rules

Source Zone	Destination	Port	Protocol	Action
RED	172.16.1.10	80	HTTP	ALLOW
RED	172.16.1.10	21	FTP	ALLOW
GREEN	ORANGE	80,21	HTTP/FTP	ALLOW
ANY	ANY	ICMP	ICMP	DENY

Status: All rules active

Fuente: Autoría Propia.

Intento de bypass:

Resultado: Todos los intentos fallidos

Log: Registros de intentos de evasión detectados

5 RESULTADOS Y ANÁLISIS

5.1 MÉTRICAS DE RENDIMIENTO

La implementación demostró excelente rendimiento en todas las configuraciones:

- Latencia promedio LAN-WAN: 2.3ms adicionales por proxy
- Throughput HTTP: 95% del ancho de banda disponible
- Tiempo de respuesta del firewall: < 1ms para reglas básicas
- Eficiencia de filtrado: 100% de sitios bloqueados detectados

Fig. 11. Acceso denegado a uno de los sitios de la backlist.

Fuente: Autoría Propia.

5.2 ANÁLISIS DE SEGURIDAD

Fortalezas identificadas:

- Segmentación efectiva entre zonas de red
- Control granular de tráfico inter-zona
- Filtrado de contenido funcional y configurable
- Registro completo de actividad de red
- Protección contra ataques de reconnaissance (ICMP deshabilitado)

Consideraciones de mejora:

- Implementación de IDS/IPS integrado
- Configuración de VPN para acceso remoto seguro
- Políticas de backup automatizadas
- Monitoreo proactivo de amenazas

5.3 CUMPLIMIENTO DE OBJETIVOS

Se lograron catalogar como logros con la presente implementación los siguientes objetivos:

- Establecimiento de una arquitectura multi-zona implementada y funcional
- Configuración y verificación de funcionalidad para servicios NAT.
- Servicios DMZ habilitados con restricciones ICMP
- Reglas de tráfico inter-zona funcionales.

- Creación de un servidor Proxy con autenticación y filtrado operativo

6 CONCLUSIONES

1. La instalación del firewall de Endian en VirtualBox resultó sorprendentemente directa, aunque la configuración inicial de las tres interfaces de red requiere atención especial en el mapeo de zonas. La interfaz web de administración facilita demasiado la gestión posterior, eliminando la necesidad de configuraciones complejas por la línea de comandos que caracterizan otros firewalls de Linux.

2. El NAT en Endian demostró ser más flexible de lo esperado, permitiendo reglas granulares tanto para LAN→WAN como DMZ→WAN. La capacidad de port forwarding específico hacia servicios en la DMZ es especialmente valiosa para escenarios reales donde se necesita exponer servicios internos de manera controlada.

3. Habilitar HTTP y FTP fue sencillo, pero el verdadero valor está en la capacidad de bloquear ICMP selectivamente. Esto elimina dificultades a la hora de hacer la configuración inicial y pone sobre la mesa un tema que usualmente se le olvida implementar a los administradores de seguridad de la red, todo esto sin afectar la funcionalidad resulta como un gran ofrecimiento de valor para el usuario.

4. Poder definir exactamente qué protocolos y puertos pueden comunicarse entre LAN y DMZ, mientras se mantiene la separación de Internet, proporciona una segmentación empresarial real.

5. El uso de servidores proxy HTTP en redes empresariales ha sido de vital importancia y lo seguirá siento a raíz de su facilidad de configuración y confiabilidad en cuanto a funcionamiento si sus procesos se realizan correctamente. Además, la autenticación por usuario añade una capa de seguridad que es crucial en entornos corporativos, y la facilidad para gestionar políticas de acceso lo hace viable incluso para equipos de IT pequeños.

7 REFERENCIAS

[1] LPI LPIC-1 Exam 101, "Tema 102: Comandos GNU y Unix," Learning Materials, 2022. [En línea]. Disponible en: https://learning.lpi.org/es/learning-materials/101-500/102/

[2] Canonical, "Guía del Ubuntu desktop 20.04 LTS," Ubuntu Help, 2023. [En línea]. Disponible en: https://help.ubuntu.com/20.04/ubuntu-help/index.html

[3] Debian Project, "El manual del administrador de Debian 12.5.0," Debian Documentation, 2023. [En línea]. Disponible en: https://www.debian.org/releases/stable/amd64/index.es.html

[4] Oracle Corporation, "Manual de usuario VirtualBox," VirtualBox Documentation, 2020. [En línea]. Disponible en: https://www.virtualbox.org/manual/

[5] Endian, "Endian UTM 3.2 Manual referencia," Endian Documentation, 2016. [En línea]. Disponible en: http://docs.endian.com/3.2/utm/index.html

[6] J. LaCroix, "Mastering Ubuntu Server: Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting Ubuntu Server," Packt Publishing, 2020.