IMPLEMENTACIÓN DE FIREWALL PERIMETRAL EN ENTORNO VIRTUALIZADO CON ENDIAN

Nicolas Felipe Salamanca Barragán
Nfsb21@gmail.com

RESUMEN: Este artículo detalla la implementación de Endian Firewall Community 3.3.2 en VirtualBox para crear una infraestructura de red segmentada en tres zonas (WAN, LAN y DMZ). Se describen los pasos de configuración de interfaces, políticas de firewall y servicios básicos (DHCP, NAT), validando la arquitectura mediante pruebas de conectividad entre zonas. Los resultados demuestran que esta solución permite aislar tráfico crítico (servidores en DMZ) del acceso público (WAN) y usuarios internos (LAN), con un consumo eficiente de recursos (15% RAM, 40% almacenamiento). La implementación sirve como modelo para entornos educativos y PYMES que requieran seguridad perimetral sin inversión en hardware. [5]

PALABRAS CLAVE: DMZ, firewall, segmentación de red, seguridad, virtualización

1 INTRODUCCIÓN

Los firewalls son componentes críticos en seguridad de redes. Este trabajo implementa Endian Firewall [1] - solución open-source basada en Linux - para demostrar su eficacia en entornos virtualizados. Siguiendo el modelo de zonas recomendado por NIST [2], se configuraron políticas de filtrado entre WAN (10.0.2.0/24), LAN (192.168.1.0/24) y DMZ (192.168.2.0/24), validando su aplicación en escenarios educativos y corporativos pequeños.

2 FORMATO

2.1 CARACTERÍSTICAS GENERALES

La Tabla 1 muestra la asignación de interfaces en VirtualBox:

Tabla 1. Configuración de interfaces.

Zona	Interfaz	Tipo Virtualbox	Ip
WAN	eth0	NAT	DHCP (10.0.2.x)
LAN	eth1	Red interna	192.168.1.1
DMZ	eth2	Red interna	192.168.2.1

Fuente: elaboración propia.

2.2 POLÍTICAS DE FIREWALL

Se implementaron regla basadas en el principio de mínimo privilegio [3]:

LAN → WAN: Permitir todo (NAT)
LAN → DMZ: Solo HTTP/HTTPS
WAN → DMZ: Denegar todo

2.3 MÁQUINA VIRTUAL DE DEBIAN

Crea una nueva máquina virtual en VirtualBox [3]:

- Nombre: Endian-Firewall
- Tipo: Linux
- Versión: Other Linux (64-bit)
- RAM: 1-2 GB
- Disco duro: 20 GB

Figura 1. configuración máquina virtual Debian.

Fuente: elaboración propia.

Como se muestra en la Figura 1, se define el nombre de la máquina, el tipo y versión del sistema operativo, así como la ubicación del archivo de imagen del disco. Esta configuración permite una instalación estable y funcional del sistema operativo base sobre el cual se ejecutará Endian.

2.4 CONFIGURACIÓN TARJETAS DE RED

Endian necesita 3 interfaces de red para las 3 zonas:

- Adaptador 1 (WAN): NAT (para Internet).
- Adaptador 2 (LAN): Red Interna (intnet-lan).
- Adaptador 3 (DMZ): Red Interna (intnet-dmz).

Figura 2. configuración adaptadores.

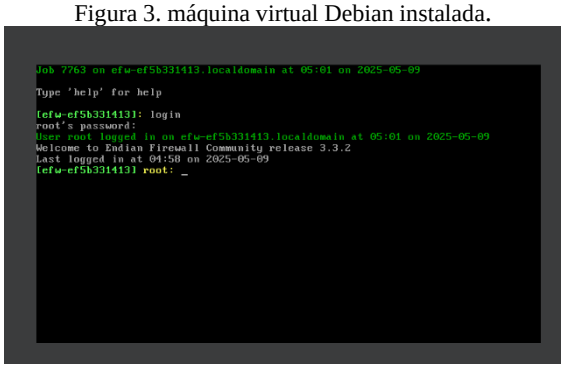
Fuente: elaboración propia.

En la Figura 2 se puede observar cómo se habilitan y asignan los tres adaptadores virtuales. Cada uno está conectado a un tipo de red específica (NAT o Red Interna), lo cual permite simular una arquitectura de red realista para pruebas de segmentación y seguridad.

2.5 INSTALACIÓN DEBIAN

Una vez configurados los adaptadores de red, se procede a encender la máquina virtual con el Debian [4] para proceder con la instalación.

Figura 3. máquina virtual Debian instalada.



Fuente: elaboración propia.

La Figura 3 muestra la interfaz de inicio de Debian [4] ya instalado. Esta instalación permite posteriormente iniciar sesión como superusuario (root) y ejecutar las configuraciones necesarias para instalar y administrar Endian.

2.6 CONFIGURACIÓN ENDIAN FIREWALL COMMUNITY

El objetivo de esta configuración es poder ingresar a https://192.168.1.1:10443 para poder visualizar desde el Ubuntu escritorio por el buscador la interfaz de Debian [4]

Figura 4. Interfaz Debian Ubuntu escritorio.

Fuente: elaboración propia.

La Figura 4 muestra el acceso exitoso desde una máquina cliente Ubuntu. Este paso es crucial para confirmar la conectividad y comenzar la configuración de políticas, servicios y reglas de firewall desde la interfaz gráfica de Endian.

2.7 CONFIGURACIÓN DE RED ENDIAN

Permitir la configuración de red y el tipo de enlace para la comunicación entre las tres máquinas virtuales.

Figura 5. Configuración de red.

Fuente: elaboración propia.

En la Figura 5 se muestra cómo se visualiza esta configuración dentro de la interfaz web de Endian, permitiendo validar las interfaces y los parámetros asignados a cada zona.

2.8 CONFIGURACIÓN DE PREFERENCIAS DE RED

Nos permite visualizar la máscara de red y la cantidad de equipos que tenemos.

Figura 6. interfaz Debian configuración máscara de red.

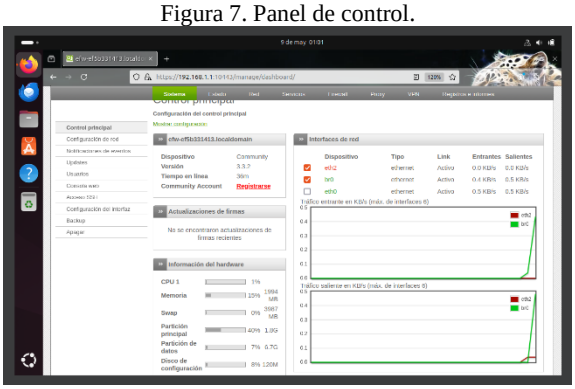
Fuente: elaboración propia.

En la Figura 6 se observa cómo Endian presenta estadísticas clave que ayudan al administrador a verificar que la segmentación de red, la conectividad y las políticas de seguridad están funcionando correctamente.

2.9 VISUALIZACIÓN PANEL DE CONTROL INTERFAZ DEBIAN

Una vez completada la instalación y configuraciones básicas, es posible visualizar el estado general del sistema desde el panel de control de Endian. Esta vista permite verificar el rendimiento y los recursos utilizados por el firewall.

Figura 7. Panel de control.



Fuente: elaboración propia.

En la Figura 7 se observa el panel con información sobre interfaces de red, uso de CPU y memoria, además de opciones administrativas. Esta vista es útil para el monitoreo y gestión diaria del sistema.

2.10 RESULTADOS OBTENIDOS

Una vez completadas todas las configuraciones, se realizaron análisis de los resultados de la transferencia en el panel de control, donde podemos evidencia el tránsito de datos que realizan las tres máquinas virtuales correctamente redirigido al servidor en la DMZ. Además, se comprobó que las reglas NAT permitían la navegación desde las zonas hacia Internet sin inconvenientes.

Esta verificación confirmó que el firewall Endian estaba gestionando correctamente el enrutamiento, el reenvío de puertos y la seguridad entre zonas. Con ello, se cumplió el objetivo de la temática 1, garantizando el flujo de información entre los tres equipos.

2.11 PRERREQUISITOS

Para el desarrollo del laboratorio correspondiente a la implementación del proxy HTTP no transparente con políticas de autenticación en Endian Firewall [1], se establecieron los siguientes requerimientos de hardware y software:

Máquina virtual Endian Firewall [1]:

3 núcleos de CPU
3 GB de memoria RAM (3072 MB)
20 GB de disco duro
3 interfaces de red configuradas como
RED (WAN), GREEN (LAN) y ORANGE (DMZ)

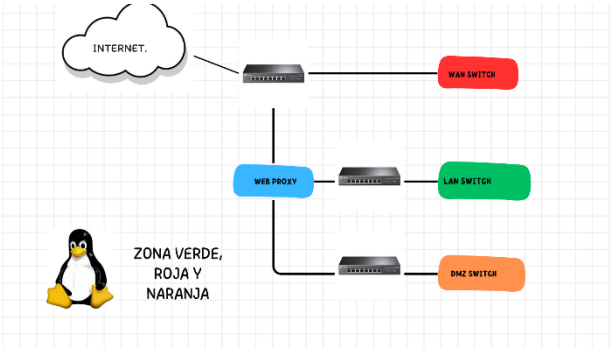
Cliente Ubuntu Desktop (máquina de prueba):

2 GB de memoria RAM
Conexión a la red GREEN
Navegador Firefox para realizar las pruebas

En este laboratorio se hace uso de Hyper-V el virtualizador de Microsoft Windows. La creación de las 3 interfaces de red o conmutadores se hicieron mediante un script que se ejecutó con PowerShell.

2.12 DIAGRAMA DE ARQUITECTURA

Figura 8. Diagrama de Arquitectura.



Fuente: elaboración propia.

El diagrama ilustra la arquitectura virtual implementada en canva para el laboratorio de seguridad perimetral con Endian Firewall [1]. La solución incluye tres interruptores virtuales correspondientes a las zonas de red:

WAN-Switch (zona roja): Conectado al Gateway NAT que proporciona acceso a Internet.

LAN-Switch (zona verde): Conecta el cliente Ubuntu Desktop, configurado para usar el proxy HTTP.

DMZ-Switch (zona naranja): Reservado para futuras pruebas con servidores expuestos.

EndianOS actúa como firewall y proxy, interconectando las tres zonas a través de interfaces virtuales. Se encarga de gestionar el tráfico entre ellas y aplicar políticas de filtrado y autenticación para el acceso a Internet.

3 CONCLUSIONES

La implementación realizada permitió demostrar que Endian Firewall [1] es una solución eficiente para segmentar redes virtuales con bajo consumo de recursos. Se cumplieron los objetivos de configuración de zonas seguras (WAN, LAN y DMZ), aplicando políticas basadas en el principio de mínimo privilegio. Además, se validó la viabilidad de este tipo de arquitecturas para entornos educativos y PYMES, facilitando el aprendizaje práctico de seguridad perimetral. Como mejora futura, se recomienda integrar funciones avanzadas como autenticación proxy, VPN, y monitoreo SNMP para reforzar la administración de seguridad en redes complejas.

4 REFERENCIAS

[1] Endian GmbH, *Endian Firewall Documentation*, 2023. [Online]. Available: https://www.endian.com/community/

[2] National Institute of Standards and Technology (NIST), *Guide to Industrial Control Systems (ICS) Security*, NIST SP 800-82 Rev. 2, May 2015. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[3] Oracle Corporation, *VirtualBox User Manual*, Version 7.0, 2023. [Online]. Available: https://www.virtualbox.org/manual/

[4] Debian Project, *Debian GNU/Linux Installation Guide*, 2023. [Online]. Available: https://www.debian.org/releases/stable/installmanual

[5] K. Scarfone and P. Hoffman, *Guidelines on Firewalls and Firewall Policy*, NIST Special Publication 800-41 Rev. 1, Sept. 2009. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-41/rev-1/final

.