IMPLEMENTACIÓN DE GNU/LINUX ENDIAN EN VIRTUALBOX PARA LA CONFIGURACIÓN DE ZONAS GREEN, RED Y ORANGE Y LA IMPLEMENTACIÓN DE NAT

Michaell Stiven Sánchez Sánchez
e-mail: mssanchezsan@unadvirtual.edu.co

ABSTRACT: *This article presents the implementation of a virtualized network environment using GNU/Linux Endian Firewall on VirtualBox. The environment was structured into three network zones: GREEN (LAN), ORANGE (DMZ) and RED (WAN). NAT rules were configured to allow secure communication between internal networks and the Internet. In addition, connectivity tests were performed to validate outbound communication from the LAN and DMZ to external networks. The implementation demonstrates the usefulness of Endian Firewall as a perimeter security solution in virtualized academic environments.*

KEYWORDS: Endian, Firewall, NAT, VirtualBox, GNU/Linux, DMZ.

RESUMEN: *El presente artículo describe la implementación de un entorno virtualizado utilizando GNU/Linux Endian Firewall sobre VirtualBox. La infraestructura fue segmentada en tres zonas de red: GREEN (LAN), ORANGE (DMZ) y RED (WAN). Posteriormente, se configuraron reglas NAT para permitir la comunicación segura entre las redes internas e Internet. Finalmente, se realizaron pruebas de conectividad para validar el acceso desde la red LAN y la DMZ hacia redes externas. Los resultados obtenidos demuestran la utilidad de Endian Firewall como solución de seguridad perimetral en entornos académicos virtualizados.*

PALABRAS CLAVE: Endian, Firewall, NAT, VirtualBox, GNU/Linux, DMZ.

1 INTRODUCCIÓN

La seguridad perimetral representa uno de los componentes más importantes dentro de las infraestructuras de red modernas. Las organizaciones requieren mecanismos que permitan controlar el tráfico, proteger recursos internos y segmentar adecuadamente las comunicaciones entre diferentes zonas de red [1].

En este contexto, GNU/Linux Endian Firewall constituye una solución basada en software libre que facilita la administración de redes y la implementación de políticas de seguridad. Endian permite crear zonas segmentadas como LAN, DMZ y WAN, además de administrar reglas de filtrado y traducción de direcciones de red NAT [2].

El objetivo de esta práctica fue implementar un entorno virtualizado utilizando VirtualBox y Endian Firewall, configurando las zonas GREEN, RED y ORANGE, además de establecer reglas NAT que permitieran comunicación segura desde las redes internas hacia Internet.

2 IMPLEMENTACIÓN DEL ENTORNO VIRTUAL

2.1 CREACIÓN DE LA MÁQUINA VIRTUAL

Para el desarrollo de la práctica se utilizó Oracle VM VirtualBox. Se creó una máquina virtual destinada al firewall Endian con las siguientes características:

Tabla 1. Configuración de la máquina virtual.

Parámetro	**Configuración**
Nombre	EndianFirewall
Tipo	Linux
Versión	Other Linux 64-bit
Memoria RAM	2048 MB
Procesadores	2 CPU
Disco duro	20 GB

Fuente: Autoría propia

2.2 CONFIGURACIÓN DE LOS ADAPTADORES DE RED

La arquitectura de red fue segmentada en tres zonas:

- GREEN: red interna LAN.
- RED: conexión a Internet.
- ORANGE: red DMZ para servidores.

Los adaptadores de VirtualBox fueron configurados de la siguiente manera:

Tabla 2. Configuración de adaptadores

Adaptador	Función	Tipo de conexión
Adaptador 1	RED (WAN)	NAT
Adaptador 2	GREEN (LAN)	Red interna
Adaptador 3	ORANGE (DMZ)	Red interna

Fuente: Autoría propia

La red interna del adaptador GREEN fue nombrada como "Zona- Verde", mientras que la red interna del adaptador ORANGE fue configurada con el nombre "Zona-Naranja".

3 INSTALACIÓN DE GNU/LINUX ENDIAN

La instalación de Endian se realizó iniciando la máquina virtual desde la imagen ISO previamente montada. Durante el proceso se

seleccionó el idioma inglés y se aceptó el

formateo automático del disco.

Posteriormente, se configuraron las interfaces de red correspondientes a cada zona

Figura 1.
Instalación Endian

Fuente. Autoría propia

3.1 CONFIGURACIÓN DE LA ZONA GREEN

La zona GREEN fue configurada con la dirección IP 192.168.100.1 y máscara de subred 255.255.255.0. Esta dirección funcionó como puerta de enlace para los dispositivos pertenecientes a la LAN.

Figura 2.
Configuración Zona GREEN

Fuente: Autoría propia

3.2 CONFIGURACIÓN DE LA ZONA ORANGE

La zona ORANGE correspondiente a la DMZ fue configurada utilizando la dirección IP 192.168.200.1 y máscara de red 255.255.255.0

Tabla 3. Configuración Zona ORANGE

parámetro	valor
Dirección IP	192.168.200.1
Máscara de red	255.255.255.0

Fuente: Autoría propia

3.3 CONFIGURACIÓN DE LA ZONA RED

La interfaz RED fue configurada utilizando DHCP para permitir el acceso automático a Internet mediante la conexión NAT proporcionada por VirtualBox.

Adicionalmente, se configuraron los servidores DNS públicos de Google:

8.8.8.8
8.8.4.4

4. CONFIGURACIÓN DEL CLIENTE LAN Y SERVIDOR DMZ

4.1 CONFIGURACIÓN DEL CLIENTE UBUNTU DESKTOP

La máquina Ubuntu Desktop fue conectada a la zona GREEN. La configuración IP fue realizada manualmente utilizando los siguientes parámetros:

Tabla 4. Configuración Ubuntu Desktop

parámetro	valor
Dirección IP	192.168.100.2
Máscara de red	255.255.255.0
DNS	8.8.8.8

Fuente: Autoría propia

Después de aplicar la configuración, se verificó el acceso a Internet utilizando el navegador Firefox y comandos ping.

4.2 CONFIGURACIÓN DEL SERVIDOR UBUNTU SERVER EN DMZ

La máquina Ubuntu Server fue conectada a la zona

ORANGE. Posteriormente se configuró una dirección IP estática utilizando Netplan [4].

El archivo de configuración fue editado mediante el siguiente comando:

sudo nano /etc/netplan/00-installer-config.yaml

La configuración implementada fue

la siguiente: network:

version: 2
renderer: networkd
ethernets: enp0s8:

dhcp4: no
addresses:
- 192.168.200.2/24
routes:
- to: default
via: 192.168.200.1
nameservers:
addresses:

- 8.8.8.8
- 8.8.4.4

Finalmente, se aplicaron los

cambios utilizando: sudo

netplan apply

5. CONFIGURACIÓN NAT

Las reglas NAT fueron configuradas desde la interfaz web de Endian Firewall, accesible mediante:

https://192.168.100.1:10443

Desde el módulo Firewall → Source NAT se crearon dos reglas principales:

- Regla NAT para la red GREEN.
- Regla NAT para la red ORANGE.

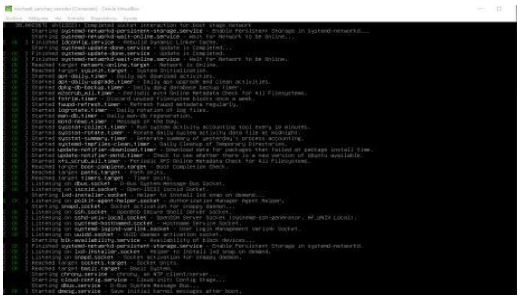
Estas reglas permitieron que ambas redes internas pudieran acceder a Internet utilizando la dirección IP pública asignada a la interfaz RED.

6 PRUEBAS DE CONECTIVIDAD

Una vez aplicada la configuración NAT, se realizaron pruebas de conectividad desde Ubuntu Desktop y Ubuntu Server.

Figura 3.

Pruebas de conectividad.



Fuente. Autoria propia.

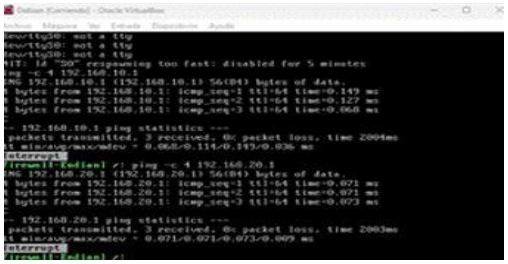
6.1 PRUEBA DESDE LA RED GREEN

Se ejecutó el siguiente comando:

ping 8.8.8.8

Figura 4.

Conexión Red GREEN



Fuente. Autoria propia

La prueba fue exitosa, confirmando la salida hacia Internet desde la red LAN.

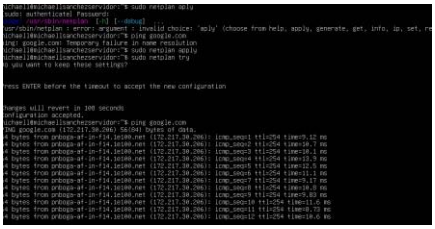
6.2 PRUEBA DESDE LA RED ORANGE

Igualmente, desde el servidor ubicado en la DMZ se ejecutó:
ping 8.8.8.8

La conectividad fue satisfactoria, validando el correcto funcionamiento de las reglas NAT para la zona ORANGE.

Figura 5.

Pruebas Red ORANGE



Fuente. Autoría propia

7. RESULTADOS

La implementación permitió comprobar el funcionamiento correcto de GNU/Linux Endian Firewall dentro de un entorno virtualizado. Se logró segmentar la red en tres zonas independientes y establecer políticas de comunicaciones seguras.

Asimismo, las pruebas realizadas evidenciaron:

- Comunicación exitosa entre LAN e Internet.
- Comunicación exitosa entre DMZ e Internet.
- Funcionamiento adecuado de NAT.
- Administración remota mediante interfaz web.
- Segmentación correcta entre zonas GREEN, RED y ORANGE.

8. CONCLUSIONES

GNU/Linux Endian Firewall demostró ser una solución eficiente para la implementación de seguridad perimetral y segmentación de redes en entornos virtualizados.

La utilización de VirtualBox facilitó la simulación de escenarios empresariales reales, permitiendo validar configuraciones NAT y segmentación de tráfico sin necesidad de infraestructura física.

Las reglas NAT configuradas permitieron el acceso seguro desde las redes internas hacia Internet, ocultando las direcciones privadas y mejorando la seguridad de la infraestructura.

La separación de zonas GREEN, RED y ORANGE permitió establecer un entorno de red organizado y seguro, reduciendo riesgos de acceso no autorizado entre segmentos.

Finalmente, la práctica permitió fortalecer conocimientos relacionados con virtualización, administración de firewalls y configuración de redes GNU/Linux.

9. REFERENCIAS

[1] LPI Linux Essentials, “Seguridad y sistema de permisos de archivos,” 2022. [Online]. Available: https://learning.lpi.org/es/

[2] Endian Community, “Endian Firewall Documentation,” 2024. [Online]. Available: https://www.endian.com

[3] Oracle Corporation, “Oracle VM VirtualBox User Manual,” 2024. [Online]. Available: https://www.virtualbox.org/manual/

[4] Canonical, “Ubuntu Server Documentation,” 2024. [Online]. Available: https://ubuntu.com/server/docs

[5] Hernández, P. F., y Sánchez, J., “Monitoreo y administración de sistemas Linux,” Universidad Nacional Abierta y a Distancia – UNAD, 2022.

[6] Debian Project, “Debian Administrator’s Handbook,” 2024. [Online]. Available: https://www.debian.org/doc/