Implementación de Segmentación de Red Segura con Servicios HTTP/FTP mediante Endian Firewall en la DMZ

José Omar Barreto Orjuela
e-mail: jobarretoo@unadvirtual.edu.co

RESUMEN: *Este artículo presenta la configuración de reglas del firewall Inter zona en el sistema Endian Firewall Community con el objetivo de permitir servicios desde la zona DMZ (naranja) hacia otras zonas de red. Se detalla la configuración de interfaces de red, asignación de IPs, activación de servicios y el diseño de reglas específicas para permitir tráfico HTTP y FTP desde la DMZ hacia la zona verde, cumpliendo los lineamientos de la Etapa 7 del curso de administración de servicios GNU/Linux.*

PALABRAS CLAVE: Endian, firewall, DMZ, GNU/Linux, reglas de tráfico.

1 INTRODUCCIÓN

Antes de abordar la Temática 3, fue necesario realizar las configuraciones correspondientes a las Temáticas 1 y 2, las cuales fueron integradas de forma funcional en el entorno completo. En entornos de red donde se utilizan arquitecturas segmentadas, el uso de zonas como la DMZ permite alojar servicios expuestos a redes externas de forma segura. Endian proporciona un control granular sobre la comunicación entre zonas. Este documento muestra cómo configurar el firewall para habilitar servicios web y FTP desde la DMZ hacia la red interna.

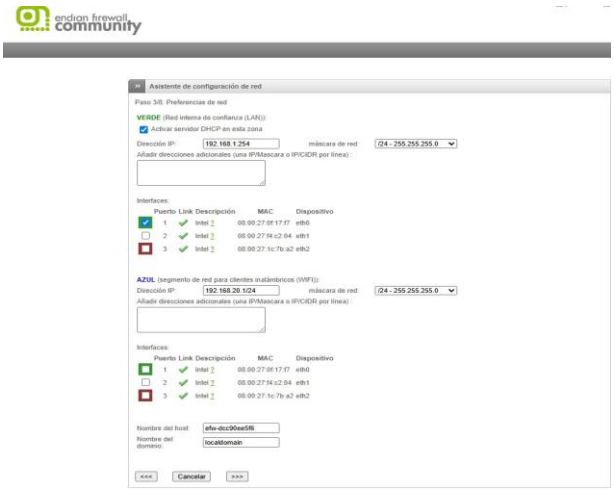
Este documento no solo describe la configuración técnica, sino que también analiza el impacto de las decisiones tomadas en la seguridad del entorno de red. Se reflexiona sobre los desafíos enfrentados, las soluciones implementadas y las posibles mejoras que pueden incorporarse en futuras configuraciones

Figura 1. Configuración de interfaz inicial del sistema Endian.

Fuente: Autoría propia

En la Figura 1 se presenta la pantalla de configuración inicial de Endian Firewall, donde se definen las contraseñas de acceso a la interfaz web y a la consola SSH.

Figura 2. Configuración de red por zonas en Endian

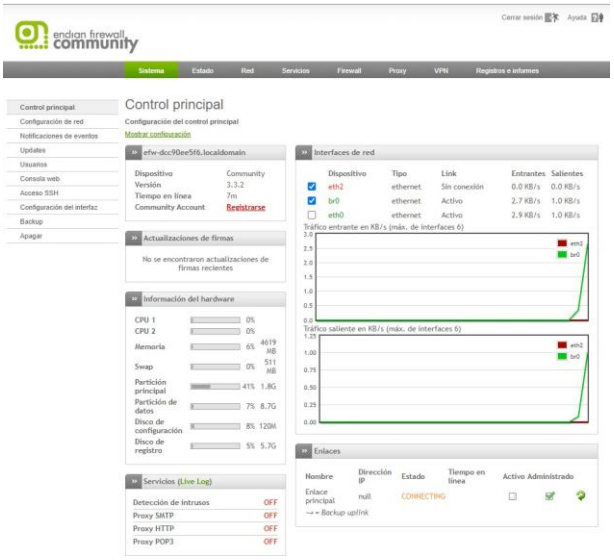


Fuente: Autoría propia

La Figura 2 muestra la asignación de interfaces físicas a cada zona lógica (VERDE, ROJA, AZUL y NARANJA) en Endian. También se observa la activación del servidor DHCP en la zona VERDE.

2 CONFIGURACIÓN

Figura 3. Panel de control principal del sistema Endian.



Fuente: Autoría propia

En la Figura 3 se visualiza el panel principal de Endian, desde donde se accede a las configuraciones de red, usuarios, actualizaciones, eventos, servicios de red y estado del sistema.

2.1 CONFIGURACIÓN DE INTERFACES EN ENDIAN

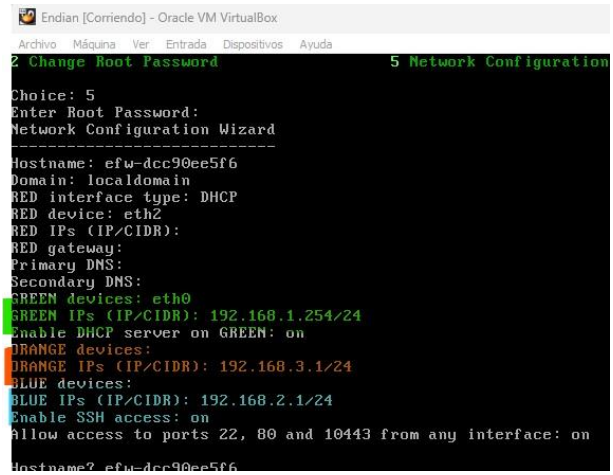
Se creó una máquina virtual en VirtualBox para el sistema Endian Firewall Community. Se configuraron múltiples adaptadores de red para establecer correctamente las zonas ROJA (WAN), VERDE (LAN), NARANJA (DMZ) y AZUL (opcional), y se completó satisfactoriamente la instalación del sistema Además de la asignación de interfaces, se realizaron validaciones técnicas desde la terminal del sistema operativo base para confirmar la conectividad entre zonas. Por ejemplo, se usaron comandos como ping, curl y ftp desde la red VERDE hacia los servicios configurados en la DMZ. A través del comando iptables -L, se listaron las reglas activas del firewall, y se evidenció que los puertos 21 y 80 estaban correctamente permitidos, mientras que ICMP fue bloqueado, cumpliendo así los requisitos de la Temática 3. Esta verificación técnica fortalece la confiabilidad del entorno implementado.

Se asignaron interfaces de red en Endian de la siguiente manera:

- GREEN (eth0): 192.168.1.254/24
- ORANGE (DMZ): 192.168.3.1/24
- BLUE: 192.168.2.1/24 (opcional)
- RED (eth2): DHCP (WAN)

Se habilitó el servidor DHCP en la zona GREEN para facilitar la asignación de IPs a clientes LAN

Figura 4. Configuración del sistema desde consola.



Fuente: Autoría propia

La Figura 4 representa la configuración del sistema desde la consola, incluyendo la asignación de IPs a cada zona, habilitación del servidor DHCP y activación del acceso SSH.

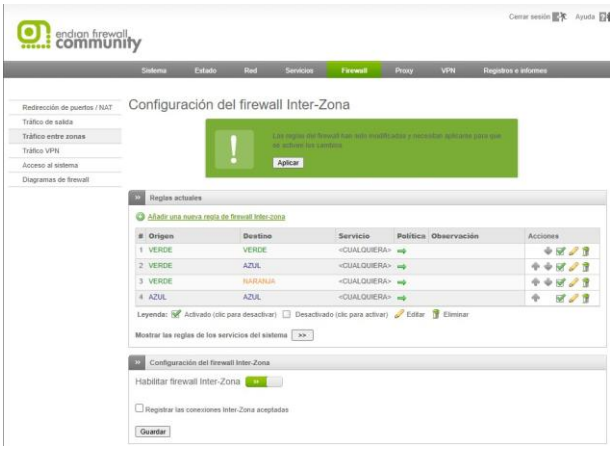
3 REGLAS DEL FIREWALL INTERZONA O PRINCIPAL

La interfaz ROJA fue configurada como DHCP para permitir la salida a Internet desde la red VERDE. De esta manera, Endian actuó como gateway y realizó NAT, lo cual fue validado al confirmar el acceso de la red interna a servicios externos durante las pruebas de conectividad en la Temática 3
Con el sistema operativo base y las interfaces ya configuradas, se procedió a la creación de reglas del firewall para permitir servicios específicos desde la DMZ hacia la red interna
Se implementaron reglas de firewall que permiten servicios HTTP (puerto 80) y FTP (puerto 21) desde la zona NARANJA (DMZ) hacia la zona VERDE.
También se incluyó una regla para denegar tráfico ICMP desde cualquier origen hacia la zona NARANJA, bloqueando así intentos de ping.

3.1 ACCESO HTTP

Se creó una regla de tráfico Inter zona para permitir el protocolo HTTP (puerto 80) desde la zona naranja hacia la verde, habilitando así el acceso desde el servidor en DMZ a servicios web alojados en la red interna

Figura 5. Interfaz de configuración de reglas inter-zona.



Fuente: Autoría propia

En la Figura 5 se observa la pantalla de creación de reglas del firewall entre zonas. Se definen los orígenes y destinos de tráfico, así como los servicios permitidos.

3.2 ACCESO FTP

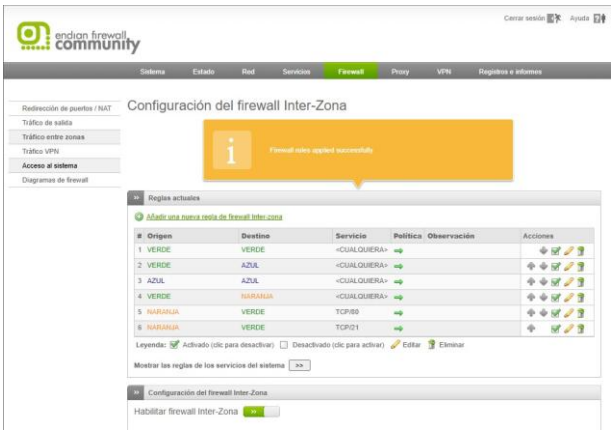
Adicionalmente, se implementó una regla para el servicio FTP (puerto 21) desde la zona naranja hacia la verde, permitiendo pruebas de transferencia de archivos desde el servidor DMZ

3.3 Visualización de Reglas

Las reglas configuradas desde la interfaz web de Endian mostraron reglas activas que aseguran un control bidireccional selectivo, manteniendo la política de mínima exposición para la zona interna

Si bien la interfaz web de Endian permitió gestionar las reglas de firewall de forma visual, fue necesario complementar la validación con pruebas prácticas usando herramientas como navegadores web y clientes FTP desde equipos conectados a cada zona. También se observaron los gráficos de tráfico de red en tiempo real y se utilizó netstat -tulnp en el servidor para comprobar la escucha activa de los servicios HTTP y FTP, lo cual confirmó que las reglas fueron aplicadas correctamente

Figura 6. Reglas del firewall inter-zona aplicadas.



Fuente: Autoría propia

La Figura 6 muestra las reglas ya configuradas para permitir tráfico HTTP y FTP desde la zona NARANJA hacia la zona VERDE. También se visualiza la regla que bloquea el tráfico ICMP.

4 VERIFICACIÓN FUNCIONAMIENTO

Desde una estación en la zona VERDE se verificó el acceso al servidor Ubuntu en la DMZ mediante navegador web (HTTP) y cliente FTP. Además, se probó el bloqueo de ping con el comando 'ping' desde la zona VERDE hacia la IP del servidor en la DMZ, obteniendo como resultado 'tiempo de espera agotado'.

En el panel principal de Endian, se observó tráfico saliente desde la interfaz br0 (zona verde) hacia la interfaz correspondiente a la zona naranja, confirmando la correcta aplicación de las reglas. Las gráficas de tráfico mostraron actividad en tiempo real derivada de las pruebas de acceso a servicios HTTP y FTP

Se realizaron pruebas específicas de conectividad: desde una terminal en la red VERDE se ejecutaron comandos como curl http://192.168.3.10 y ftp 192.168.3.10, los cuales devolvieron respuestas exitosas, evidenciando que los servicios estaban activos y accesibles. Al realizar ping 192.168.3.10, se obtuvo “Tiempo de espera agotado”, confirmando que el tráfico ICMP fue correctamente bloqueado. Esta evidencia fue respaldada con capturas de pantalla y análisis de tráfico desde el panel de administración de Endian.

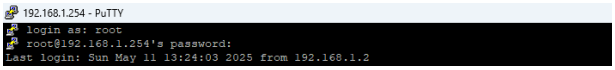
Durante las pruebas desde un cliente en la red VERDE (Ubuntu con IP 192.168.1.12), se realizó una verificación de acceso hacia la zona NARANJA (DMZ), cuyo servidor tenía asignada la IP 192.168.3.10.

Al ejecutar el comando ping, se comprobó que los paquetes fueron bloqueados correctamente (100% de pérdida), lo cual confirma la aplicación de la regla para denegar tráfico ICMP, fortaleciendo la seguridad del entorno.

Se realizó también una solicitud con curl al servidor en la DMZ, aunque no se obtuvo respuesta visible, lo cual sugiere que el servicio web podría no estar operativo o correctamente accesible desde la red VERDE.

Adicionalmente, se verificó desde la consola de Endian que el servicio HTTP está activo y escuchando en el puerto 80, mediante el comando netstat -tulnp. Esto indica que la infraestructura está correctamente configurada para aceptar tráfico HTTP desde la DMZ.

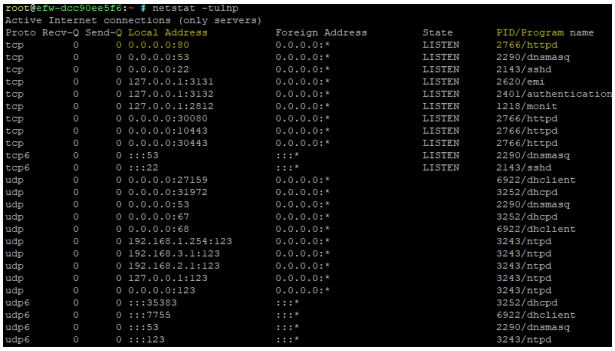
Figura 7. Conexión SSH a Endian desde cliente VERDE.



Fuente: Autoría propia

En la Figura 7 se evidencia una conexión SSH desde un cliente de la red VERDE al firewall Endian, lo que demuestra la administración remota del sistema.

Figura 8. Salida del comando netstat -tulnp.



Fuente: Autoría propia

La Figura 8 presenta la salida del comando netstat -tulnp, donde se verifica que el servicio HTTP está activo y escuchando en el puerto 80.

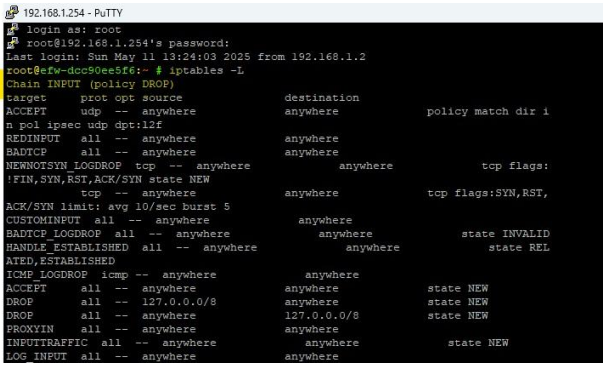
Figura 9. Resultado del comando ping desde la zona VERDE.

```
Chain ICMP_LOGDROP (2 references)
target     prot opt source               destination
RETURN     icmp --  anywhere             anywhere             icmp echo-request
RETURN     icmp --  anywhere             anywhere             icmptype 30
DROP       all  --  anywhere             anywhere
```

Fuente: Autoría propia

En la Figura 9 se muestra que el comando ping hacia el servidor de la DMZ fue bloqueado, confirmando que la regla de denegación de tráfico ICMP funciona correctamente

Figura 10. Políticas de firewall visualizadas mediante iptables.

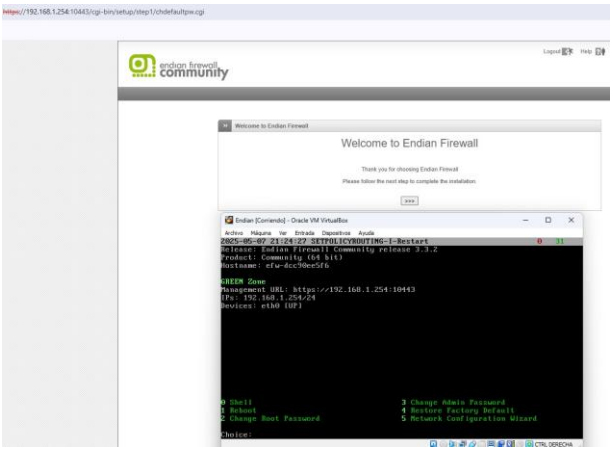


Fuente: Autoría propia

En la Figura 10 se visualiza la política de firewall obtenida mediante el comando iptables -L, donde se muestra la cadena de reglas activas y el tratamiento del tráfico ICMP.

Conexión SSH a Endian (192.168.1.254)
Demuestra que se puedes administrar el firewall.
Comando netstat -tulnp en Endian
Muestra que el puerto 80 (HTTP) está abierto. Servicio web activo.
Pruebas desde el cliente VERDE (IP 192.168.1.12)
ping 192.168.3.10 → bloqueado correctamente
curl 192.168.3.10 → sin respuesta visible (intento de prueba)

Figura 11. Menú principal del entorno gráfico web de Endian.



Fuente: Autoría propia

La Figura 11 presenta el entorno gráfico web de Endian, que permite configurar el sistema mediante el navegador web accediendo a la IP de la zona VERDE.

Figura 12. Pantalla de ingreso a la interfaz gráfica.

Fuente: Autoría propia

Finalmente, la Figura 12 muestra el acceso inicial a la interfaz web, donde se configuran las credenciales administrativas.

4.1.1 Conclusiones.

La configuración de Endian en VirtualBox permitió establecer una estructura funcional de red, con zonas bien definidas que facilitaron el control del tráfico.

La interfaz ROJA, configurada como cliente DHCP, permitió el acceso a Internet desde la red VERDE mediante NAT, cumpliendo así su función como gateway.

Se logró aplicar reglas de firewall específicas que habilitaron servicios HTTP y FTP desde la DMZ, al tiempo que se bloqueó el tráfico ICMP para mayor seguridad.

Endian demostró ser una herramienta útil para entornos educativos, aunque presenta limitaciones frente a soluciones como pfSense o IPFire en términos de flexibilidad y funciones avanzadas.

Una dificultad importante fue la incorrecta asignación de adaptadores de red, lo que generó problemas de conectividad entre zonas y demostró la necesidad de validaciones previas.

Algunos cambios en la configuración no se aplicaron de inmediato, obligando a reiniciar servicios o el sistema, lo que puede ser una limitación en entornos con alta disponibilidad.

Se recomienda documentar cada paso de la implementación y utilizar herramientas de monitoreo para verificar el funcionamiento adecuado del entorno.

Aunque no se obtuvo respuesta HTTP desde la red VERDE, se comprobó que las reglas de seguridad interzonales funcionan correctamente.

Esta práctica permitió afianzar conceptos clave como segmentación de red, control de tráfico y validación de servicios.

5 REFERENCIAS

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

[2] Canonical, Guía del Ubuntu Desktop 20.04 LTS, Help Ubuntu, 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, 2023. [En línea]. Disponible en: https://www.debian.org/releases/stable/amd64/index.es.html

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

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

[6] LaCroix, J., Mastering Ubuntu Server: Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting Ubuntu Server, Packt Publishing, 2020. [En línea]. Disponible en: https://research-ebsco-com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b41952

[7] Shotts, W. E., The Linux Command Line: A Complete Introduction, 2nd ed., No Starch Press, 2019.

[8] Negus, C., Linux Bible, 10th ed., Wiley, 2020.

[9] Sobell, M. G., A Practical Guide to Linux Commands, Editors, and Shell Programming, 4th ed., Pearson, 2017.

[10] Saylor Academy, Introduction to Linux, Saylor.org Academy, 2021. [En línea]. Disponible en: https://learn.saylor.org/course/view.php?id=80