IMPLEMENTACIÓN DE SEGURIDAD PERIMETRAL EN GNU/LINUX USANDO ENDIAN FIREWALL

Jose Rodolfo Florez Ortiz
jrflorezo@unadvirtual.edu.co
Elkin Eduardo Rojas Lizcano
eerojasl@unadvirtual.edu.co
Manuel Rene Carvajal Mogollón
mrcarvajalm@unadvirtual.edu.co

RESUMEN: *Este documento describe la implementación de mecanismos de seguridad perimetral en redes GNU/Linux utilizando Endian Firewall como solución virtualizada. La propuesta se centra en la segmentación de la red en zonas LAN (VERDE), DMZ (NARANJA) y WAN (ROJA), y la configuración de reglas NAT para permitir una comunicación controlada hacia redes externas. Los resultados validan el correcto funcionamiento de los servicios HTTP y FTP en la DMZ, así como el bloqueo de tráfico ICMP para fortalecer la seguridad. La implementación demuestra cómo una arquitectura segmentada y correctamente gestionada puede mejorar significativamente la postura de seguridad en entornos empresariales.*

PALABRAS CLAVE: Endian Firewall, GNU/Linux, NAT, Seguridad Perimetral.

1 INTRODUCCIÓN

En el panorama actual, la protección de recursos digitales se ha convertido en una prioridad para las organizaciones. La segmentación de redes y la implementación de firewalls son prácticas esenciales para evitar accesos no autorizados. Este artículo presenta una solución práctica basada en Endian Firewall, destacando el diseño de zonas seguras y la gestión de reglas de traducción de direcciones (NAT) para garantizar la conectividad controlada hacia Internet.

2 METODOLOGÍA

2.1 DISEÑO DE LA TOPOLOGÍA DE RED

La creación de la red se llevó a cabo utilizando tres máquinas virtuales: Endian, Ubuntu Server y Ubuntu Desktop. La configuración de los adaptadores de red en cada una de las máquinas virtuales se estableció de la siguiente manera:

- Endian:

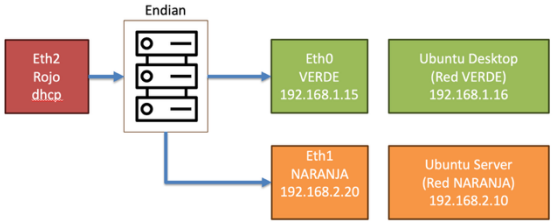
Tabla 1. Adaptadores máquina virtual Endian

Interfaz	Adaptador 1	Adaptador 2	Adaptador 3
Nombre	VERDE	NARANJA	NAT
Conectado a	Red interna	Red interna	Internet

- Ubuntu Desktop.
- Ubuntu Server.

La instalación de las máquinas virtuales se realizó sin inconvenientes, siguiendo cuidadosamente los pasos necesarios para garantizar una configuración óptima. Se prestó especial atención a la configuración de red de cada máquina. En el Ubuntu Server, se asignó una dirección IP fija 192.168.2.10 y como puerta de enlace 192.168.2.20, configurada en la máquina virtual Endian como acceso a la zona naranja. Por su parte, al Ubuntu Desktop se le asignó la IP fija 192.168.1.16 para asegurar la correcta conexión dentro de la zona verde.

Figura 1. Diagrama de red



Fuente: Autoría Propia

2.2 INSTALACIÓN Y CONFIGURACIÓN DE ENDIAN FIREWALL

Las actividades adicionales realizadas durante la instalación y configuración fueron:

- Verificación de la correspondencia entre los adaptadores de red en la máquina virtual Endian.
- Comparación de las direcciones MAC mostradas por la interfaz de Endian con los parámetros de VirtualBox para asegurar una asignación correcta.
- Configuración de las zonas VERDE y NARANJA usando las direcciones IP designadas como puerta de enlace para cada zona.

Durante las pruebas de conectividad, se verificó el acceso al panel de administración de Endian desde la máquina cliente Ubuntu Desktop en la zona verde, utilizando el puerto 10443. Esta configuración permitió una gestión eficiente y segura de la red. Se realizaron múltiples pruebas para validar la estabilidad y el rendimiento de la red, asegurando la correcta

comunicación entre las zonas VERDE y NARANJA a través de los adaptadores correspondientes.

Asimismo, se verificó la estabilidad de la conexión a Internet desde la zona ROJA, confirmando que todas las máquinas virtuales podían acceder a los recursos externos necesarios para su funcionamiento. Finalmente, se documentaron todos los pasos y configuraciones realizados para facilitar futuros ajustes y mantenimientos.

2.3 CONFIGURACIÓN Y PRUEBAS DE NAT

La configuración de Network Address Translation (NAT) tuvo como objetivo permitir que los dispositivos de las zonas internas (LAN y DMZ) accedieran a redes externas (simuladas a través de la zona ROJA).

2.3.1 CONFIGURACIÓN Y PRUEBAS DE NAT

Desde el panel web de administración de Endian Firewall, en la sección Firewall > Outgoing Traffic, se creó una regla que permite la comunicación NAT desde la zona VERDE hacia la zona ROJA, definida de la siguiente manera:

- Origen: VERDE
- Servicio/Puerto: CUALQUIERA
- Destino: ROJO
- Acción: PERMITIR
- NAT: Activado (Masquerade)

Después de aplicar la regla, se realizó una prueba de conectividad desde la máquina cliente en la zona VERDE (Ubuntu Desktop), utilizando comandos como ping y traceroute hacia 8.8.8.8 (servidor DNS público). La prueba fue exitosa, confirmando la correcta traducción NAT.

2.3.2 HABILITACIÓN DE NAT DESDE LA ZONA NARANJA HACIA LA ZONA ROJA

De manera similar, se añadió una segunda regla que permite la comunicación NAT desde la DMZ (zona NARANJA) hacia la zona ROJA, con la siguiente configuración:

- Origen: NARANJA
- Servicio/Puerto: CUALQUIERA
- Destino: ROJO
- Acción: PERMITIR
- NAT: Activado (Masquerade)

Se validó la conectividad mediante una prueba ping desde el Ubuntu Server ubicado en la zona NARANJA hacia 8.8.8.8, la cual también fue exitosa.

2.4 CONFIGURACIÓN DE SERVICIOS EN LA DMZ Y CONTROL DE TRÁFICO

Se configuraron reglas adicionales para permitir los servicios HTTP y FTP desde la DMZ (zona NARANJA) hacia las redes interna (VERDE) y externa (ROJA), mientras se restringía el tráfico ICMP para evitar solicitudes ping.

2.4.1 PERMITIR SERVICIOS HTTP Y FTP

Desde Firewall > Port Forwarding, se crearon las siguientes reglas:

Regla 1 - HTTP (Puerto 80)

- Origen: VERDE o ROJO
- Destino: NARANJA
- Servicio/Puerto: HTTP (80)
- Acción: PERMITIR

Regla 2 - FTP (Puerto 21)

- Origen: VERDE o ROJO
- Destino: NARANJA
- Servicio/Puerto: FTP (21)
- Acción: PERMITIR

Se verificó el acceso a estos servicios desde un navegador y un cliente FTP, confirmando el correcto funcionamiento.

2.4.2 BLOQUEO DE TRÁFICO ICMP

Desde Firewall > Outgoing Traffic, se creó una regla para bloquear el tráfico ICMP desde la zona NARANJA hacia cualquier destino, definida como:

- Origen: NARANJA
- Servicio/Puerto: ICMP (todos los tipos, incluyendo Echo Request - Tipo 8)
- Destino: CUALQUIERA
- Acción: DENEGAR

Las pruebas de conectividad confirmaron que el tráfico ICMP estaba efectivamente bloqueado.

2.4.3 CONFIGURACIÓN DE BLOQUEO DE ICMP

1. **Acceder a la Interfaz Web de Endian Firewall:** Inicia sesión en la interfaz web de administración de Endian Firewall utilizando tu navegador.

2. **Navegar a la Sección de Configuración de Tráfico Saliente:** Dirígete a Firewall > Tráfico Saliente (Outgoing Traffic) en la interfaz web. Esta sección permite configurar reglas que controlan el tráfico que sale desde la red interna (zonas VERDE o NARANJA).

3. **Crear una Regla para Bloquear ICMP:** En la sección de tráfico saliente, crea una nueva regla para bloquear paquetes ICMP. Esta configuración impedirá que los dispositivos en la DMZ o en la LAN envíen solicitudes de ping a otros dispositivos dentro o fuera de la red.

   Los parámetros para la regla son los siguientes:

- Origen: NARANJA (o VERDE si también deseas bloquear ICMP para la LAN)
- Servicio/Puerto: ICMP (todos los tipos, incluyendo el tipo 8, que corresponde a solicitudes de eco o "ping")
- Destino: CUALQUIERA (esto incluye tanto destinos internos como externos)
- Acción: DENEGAR

4. **Aplicar y Validar la Regla:** Después de configurar la regla, guarda y aplica los cambios.

   Luego, realiza una prueba ejecutando el comando ping desde cualquier dispositivo ubicado en las zonas NARANJA o VERDE hacia una dirección IP interna o externa.

   Si todo funciona correctamente, no recibirás respuestas a las solicitudes de ping, lo que confirmará que el tráfico ICMP ha sido bloqueado exitosamente.

5. **Verificar la Regla en el Tráfico Saliente:** Puedes verificar que la regla se ha aplicado correctamente revisando la lista de reglas en la sección Tráfico Saliente. Allí debería aparecer la regla que creaste para bloquear ICMP.

3 RESULTADOS

3.1 CONFIGURACIÓN DE ENDIAN Y ZONAS DE RED

La configuración de red en Endian Firewall incluyó la asignación de la dirección IP 192.168.1.15 para la zona VERDE. Se prestó especial atención a la correcta asignación de las direcciones IP y a la correspondencia de los adaptadores de red, garantizando así una conexión estable y segura.

Además, se verificó la estabilidad de la conexión a Internet desde la zona ROJA, asegurando que todas las máquinas virtuales pudieran acceder a los recursos externos necesarios para su funcionamiento. Se realizaron ajustes y optimizaciones adicionales en la configuración de red para mejorar tanto el rendimiento como la seguridad.

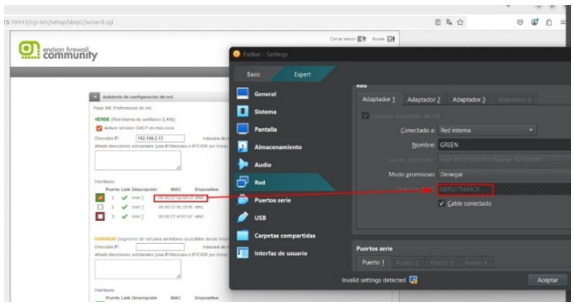
Una vez finalizada la instalación, fue posible acceder al panel de administración de Endian a través de un navegador web desde el cliente Ubuntu Desktop ubicado en la zona VERDE, utilizando el puerto 10443. Este acceso permitió una gestión eficiente de la red, facilitando la supervisión y administración de recursos, así como la configuración de las diferentes zonas.

Antes de proceder con la configuración de las zonas, se verificó que los adaptadores de red correspondieran correctamente a los asignados en la máquina virtual de Endian, comparando las direcciones MAC mostradas por la interfaz de Endian con los parámetros de VirtualBox. Esta verificación fue crucial para evitar conflictos de red y garantizar una comunicación correcta entre las máquinas virtuales.

Posteriormente, se configuraron las zonas VERDE y NARANJA utilizando las direcciones IP asignadas como puerta de enlace para cada una. La zona VERDE se configuró para la conexión interna segura, mientras que la zona NARANJA se destinó a una red de acceso controlado.

Es importante destacar que esta configuración permitió una segregación efectiva de la red, mejorando tanto la seguridad como el rendimiento.

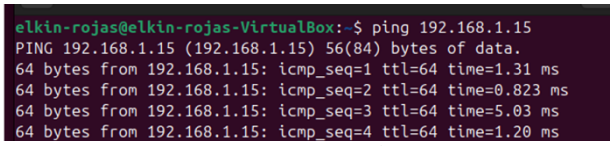
Figura 2. Validación de direcciones MAC de adaptadores



Fuente: Autoría Propia

Una vez aplicadas todas las configuraciones, se realizaron pruebas de conexión desde cada máquina en sus respectivas zonas. Se ejecutaron múltiples pruebas de conectividad para garantizar la estabilidad y el rendimiento de la red, verificando la comunicación correcta entre las zonas VERDE y NARANJA a través de los adaptadores de red correspondientes.

Figura 3. Pruebas con conexiones de red



Fuente: Autoría Propia

Finalmente, todos los pasos y configuraciones fueron documentados, asegurando que cualquier ajuste o actualización futura pueda realizarse de manera ordenada y eficiente.

3.2 RESULTADOS DE LA CONFIGURACIÓN DE NAT

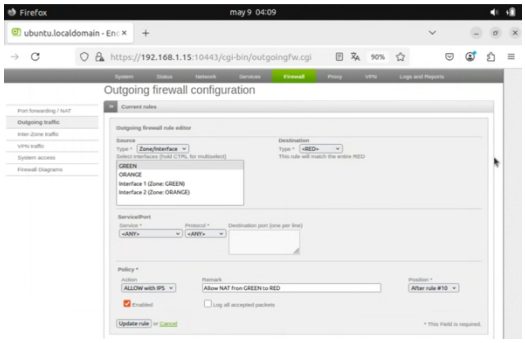
En esta sección, se describen los resultados obtenidos al configurar las reglas de Traducción de Direcciones de Red (NAT) en el Endian Firewall, con el propósito de habilitar la comunicación desde la red interna (zona VERDE) hacia la Internet simulada (zona ROJA), y desde la DMZ (zona NARANJA) hacia Internet.

1. **Creación de la Regla NAT para Tráfico Saliente.**

   Luego de acceder al panel de administración web de **Endian Firewall**, se creó una nueva **regla NAT** en la sección **Firewall > Tráfico Saliente (Outgoing Traffic)**.

   Esta regla permite que **todo el tráfico** proveniente de la **zona VERDE (LAN)** se dirija a la **zona ROJA (WAN)**, habilitando el **acceso a Internet** para los dispositivos de la red interna.

Figura 4. Regla de Tráfico Saliente NAT aplicada en Endian Firewall para la zona VERDE.



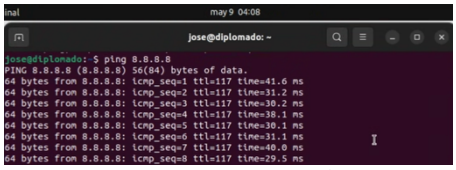
Fuente: Autoría Propia

2. **Validación de la Regla NAT para Tráfico Saliente**

   Para validar la regla NAT, se realizó una prueba de conectividad ejecutando un ping desde la máquina Ubuntu Desktop ubicada en la zona VERDE, hacia la dirección 8.8.8.8, que corresponde a un servidor DNS público de Google en Internet.

   La respuesta obtenida en la prueba confirmó que la conectividad fue exitosa a través del firewall, validando así el correcto funcionamiento de la regla configurada.

Figura 5. Prueba exitosa de ping desde la zona VERDE hacia la zona ROJA (8.8.8.8).



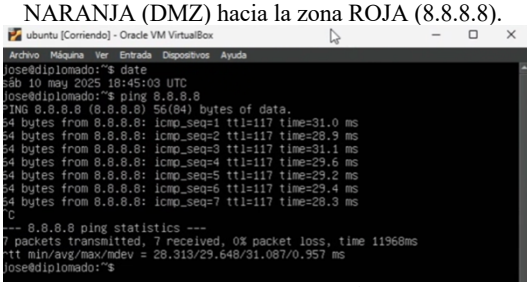
Fuente: Autoría Propia

3. **Validación de la Regla NAT: DMZ hacia la Zona WAN**

   De manera similar, se aplicó una segunda regla NAT para permitir el tráfico desde la zona NARANJA (DMZ) hacia la zona ROJA (WAN).

   Para validar esta configuración, se realizó una prueba de ping desde el servidor Ubuntu ubicado en la DMZ (zona NARANJA) hacia la dirección 8.8.8.8, confirmando así la capacidad de comunicación saliente de la DMZ hacia Internet.

Figura 6. Prueba exitosa de ping desde la zona NARANJA (DMZ) hacia la zona ROJA (8.8.8.8).



Fuente: Autoría Propia

4. **Resumen de la Efectividad de la Configuración de NAT**

   La **evidencia recopilada** demuestra que las **reglas NAT** configuradas en el **Endian Firewall** permiten correctamente:

   - El tráfico saliente desde la zona VERDE hacia la zona ROJA.
   - El tráfico saliente desde la zona NARANJA (DMZ) hacia la zona ROJA.

   Esto asegura que **tanto la red interna como los servidores ubicados en la DMZ** tengan acceso controlado a Internet, **manteniendo al mismo tiempo la segmentación de la red**, lo que contribuye a una mayor seguridad y control de las comunicaciones externas.

3.3 RESULTADOS DE LA CONFIGURACIÓN DE SERVICIOS EN LA DMZ

1. **Configuración de los Servicios HTTP y FTP en la DMZ (Zona NARANJA)**

   Las reglas del firewall fueron configuradas para permitir el acceso a los servicios HTTP (puerto 80) y FTP (puerto 21) ofrecidos por el servidor web ubicado en la DMZ (zona NARANJA).
   Estas reglas fueron definidas para permitir el tráfico hacia el servidor de la DMZ desde ambas zonas:

   - La zona interna (VERDE)
   - La zona externa (ROJA)

   Esta configuración garantiza que los servicios sean accesibles tanto desde la red interna como desde el exterior, de acuerdo con las políticas de seguridad establecidas.

Figura 7. Configuración del acceso a los servicios HTTP y FTP en el puerto 80.

Fuente: Autoría Propia

Figura 8. Configuración del acceso a los servicios HTTP y FTP en el puerto 21.

Fuente: Autoría Propia

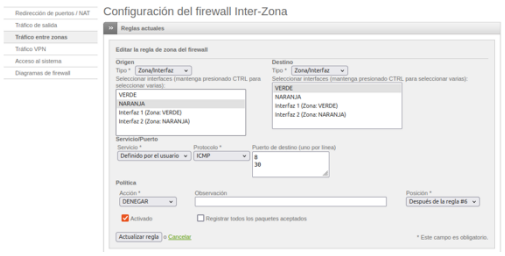
2. Configuración del Bloqueo de ICMP

Se implementaron reglas específicas en el firewall para bloquear el protocolo ICMP, específicamente los puertos 8 y 30.

Esta medida impide que los dispositivos ubicados en la DMZ (zona NARANJA) respondan a solicitudes de ping (ICMP).

De este modo, los dispositivos en la DMZ no quedan expuestos a herramientas de diagnóstico de red como el ping, lo que incrementa la seguridad al evitar intentos de reconocimiento o escaneo de la red por parte de actores externos.

Figura 9. Configuración del bloqueo del protocolo ICMP en los puertos 8 y 30.



Fuente: Autoría Propia

3. Resumen de las Configuraciones Implementadas
Las reglas configuradas en el firewall fueron las siguientes:

- **Permitir HTTP (puerto 80) y FTP (puerto 21):** Se definieron reglas en el firewall para permitir el acceso a estos servicios desde las zonas VERDE (LAN) y ROJA (WAN) hacia la zona NARANJA (DMZ), garantizando la disponibilidad de servicios web y de transferencia de archivos.
- **Bloqueo de ICMP:** Se implementaron reglas para bloquear las solicitudes de ping (ICMP), evitando la exposición de la red interna a posibles ataques de reconocimiento o escaneo.

Todas estas configuraciones fueron aplicadas exitosamente y verificadas visualmente mediante la interfaz del panel de control del firewall, donde se muestran todas las reglas activas.

Figura 10. Panel de control del firewall con todas las configuraciones aplicadas.

Fuente: Autoría Propia

3.4 CONCLUSIONES

Este artículo presentó la implementación práctica de Network Address Translation (NAT) en un dispositivo Endian Firewall como parte de un ejercicio de seguridad perimetral, enfocándose especialmente en la configuración y gestión de servicios dentro de la DMZ (zona NARANJA). Los resultados confirmaron que:

- Se habilitó correctamente el acceso a Internet desde la LAN (zona VERDE) y la DMZ (zona NARANJA) mediante reglas NAT, permitiendo comunicaciones seguras con recursos externos.
- El sistema gestionó la comunicación controlada sin exponer los servicios internos directamente a Internet, permitiendo solo el tráfico autorizado y restringiendo accesos no deseados.
- Se habilitaron servicios específicos como HTTP (Puerto 80) y FTP (Puerto 21) en el servidor Ubuntu ubicado en la DMZ, mientras que se bloquearon protocolos no deseados como ICMP (Puertos 8 y 30) para prevenir solicitudes de ping, fortaleciendo así la postura de seguridad de la red al reducir la superficie de ataque.
- La segmentación de la red en zonas LAN (VERDE), DMZ (NARANJA) y WAN (ROJA) permitió aplicar

reglas específicas adaptadas a cada necesidad, asegurando que los servicios críticos fueran accesibles de forma controlada mientras las redes internas permanecían protegidas.

Esta implementación demuestra que el uso de NAT, junto con una adecuada segmentación por zonas y una gestión precisa de los servicios, mejora significativamente la seguridad en las redes corporativas. Esta estrategia crea un perímetro seguro mientras mantiene la conectividad necesaria para las operaciones.

Se logró demostrar en este ejercicio que el uso de ambientes virtualizados a través de Virtualbox permite evaluar la seguridad de redes informáticas y el comportamiento de los nodos respecto a diferentes zonas definidas con segmentos de y reglas específicas.

4 REFERENCIAS

[1] Canonical. (2023). Guía del Ubuntu Desktop 20.04 LTS. https://help.ubuntu.com/20.04/ubuntu-help/index.html

[2] Check Point. (2021). Mejores prácticas de seguridad de segmentación de red. https://www.checkpoint.com/es/cyber-hub/network-security/what-is-network-segmentation/network-segmentation-security-best-practices/

[3] Ciberseguridad Hoy. (2024). Mejores prácticas para el uso de firewalls. https://ciberseguridadhoy.es/mejores-practicas-firewalls/

[4] Cisco Systems. (2020). Introduction to firewalls. Cisco Networking Academy. https://www.netacad.com/courses/security/introduction-firewalls

[5] Debian. (2023). Manual del administrador de Debian 12.5.0. https://www.debian.org/releases/stable/amd64/index.es.html

[6] Endian. (2016). Endian UTM 3.2 Manual de referencia. http://docs.endian.com/3.2/utm/index.html

[7] Fortinet. (2025). ¿Qué es la configuración del firewall y por qué es importante?. https://www.fortinet.com/lat/resources/cyberglossary/firewall-configuration

[8] freeCodeCamp. (2020). El manual de comandos de Linux. https://www.freecodecamp.org/espanol/news/comandos-de-linux/

[9] Hostinger. (2025). Los 40 comandos de Linux más populares y utilizados en para 2025. https://www.hostinger.com/es/tutoriales/linux-comando

[10] LPI. (2022). LPIC-1 Exam 101: Tema 102: Comandos GNU y Unix. https://learning.lpi.org/es/learning-materials/101-500/102/

[11] ManageEngine. (2025). Mejores prácticas para firewall. https://www.manageengine.com/es/firewall/firewall-best-practices.html

[12] Oracle. (2020). Manual de usuario VirtualBox. https://www.virtualbox.org/manual/

[13] Rouse, M. (2021). What is network segmentation?. TechTarget. https://www.techtarget.com/searchsecurity/definition/network-segmentation

[14] Sánchez Corbalán, J. (2022). Los 50 mejores comandos Linux del Shell Bash que debes conocer. https://sanchezcorbalan.es/mejores-comandos-linux-bash/

[15] Zscaler. (2025). ¿Qué es la segmentación de red? - Definición y casos prácticos. https://www.zscaler.com/es/resources/security-terms-glossary/what-is-network-segmentation