# Implementación de Reglas Inter-Zona en Endian Firewall para Control de Tráfico

Simón Isaac Flórez Urango
Simon08isaac@gmail.com

*Abstract— This document presents the implementation and verification of inter-zone rules in Endian Firewall to control HTTP and FTP traffic between the Green (LAN), Orange (DMZ), and Red (WAN) network zones. The configuration process included the installation of virtual machines, network segmentation, creation of security policies, and validation through functional tests. The results demonstrate that the rules applied allowed secure and selective communication between zones, ensuring service availability while maintaining perimeter protection. This work highlights the importance of proper firewall configuration and the role of traffic management in GNU/Linux-based infrastructures.*

Palabras clave— DMZ, Endian Firewall, inter-zona rules, network security.

## I. INTRODUCCIÓN

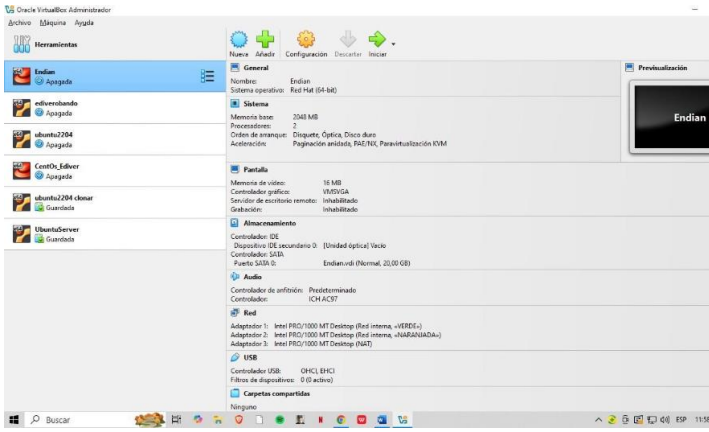
El desarrollo de esta actividad se enfocó en la implementación y verificación de reglas de acceso dentro de Endian Firewall, con el fin de fortalecer la seguridad perimetral entre las zonas Verde (LAN), Naranja (DMZ) y Roja (WAN). A través de la configuración de políticas Inter-Zona y la validación del tráfico HTTP y FTP, se buscó garantizar un control adecuado de la comunicación entre los distintos segmentos de la red. Este proceso permitió comprender el funcionamiento del firewall, su impacto en la gestión del tráfico y la importancia de una correcta segmentación para mitigar riesgos y asegurar los servicios esenciales dentro de un entorno GNU/Linux.

## II. DESARROLLO DEL CONTENIDO

El desarrollo de esta actividad se centra en la implementación y verificación de reglas de acceso dentro de la distribución GNU/Linux Endian, con el propósito de fortalecer la seguridad perimetral de una infraestructura de red compuesta por las zonas Verde (LAN), Naranja (DMZ) y Roja (WAN).

### 2.1 INSTALACION Y CONFIGURACION DE LAS MAQUINAS VIRTUALES

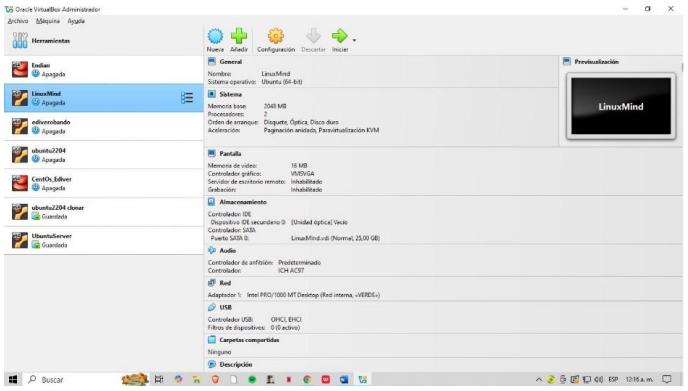
***Fig. 1. Configuración de tarjetas de red en Endian Firewall.***



Fuente: elaboración propia

En la Fig. 1, la figura muestra cómo debe ir configurada las tarjetas de red para que se pueda implementar una buena comunicación entre las diferentes máquinas y las diferentes zonas.

***Fig. 2. Configuración de adaptador de red en Linux Mint (zona Verde).***

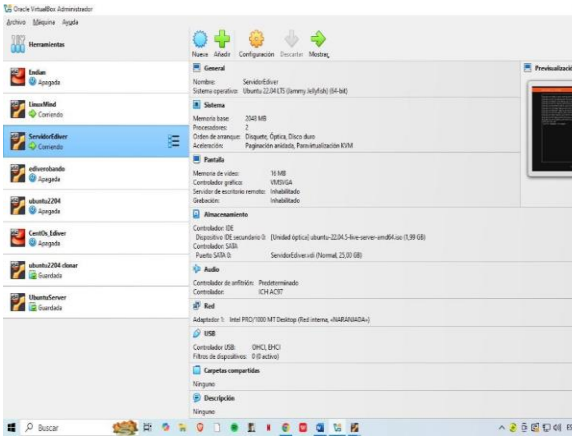


Fuente: elaboración propia

La figura muestra la configuración de Linux Mint en el entorno de VirtualBox esta máquina corresponde al cliente que vamos a utilizar para nuestra actividad, por eso lleva un solo adaptador red, red interna verde.

***Fig. 3. Configuración de la máquina Ubuntu Server en VirtualBox (zona Naranja).***

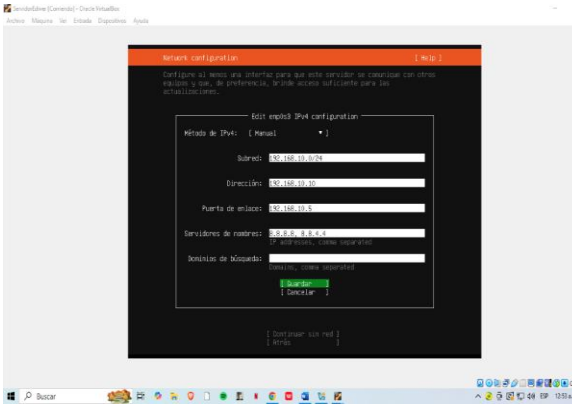
.



Fuente: elaboración propia

En la figura se observa la configuración de Ubuntu Server en el entorno de VirtualBox. Esta máquina es la que gestionará toda la parte del servidor. Estará incluido en la zona DMZ, por lo que su red interna es naranja.

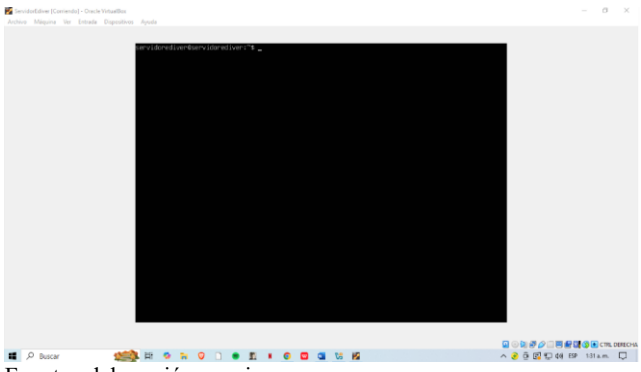
***Fig. 4. Asignación de dirección IP estática en Ubuntu Server.***



Fuente: elaboración propia

La configuración de la IP es de vital importancia, ya que esta va a ser la dirección a la cual nos comunicaremos desde las diferentes zonas.

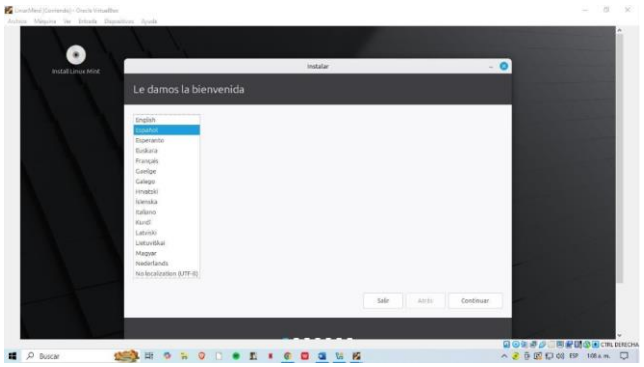
***Fig. 5. Instalación finalizada de Ubuntu Server en la DMZ.***



Fuente: elaboración propia

Podemos observar que el servidor quedó completamente instalado y funcional.

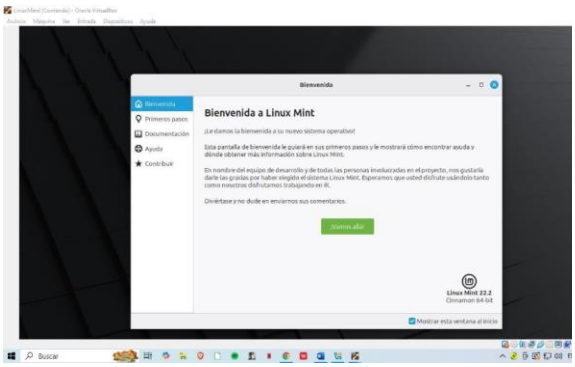
***Fig. 6. Selección del idioma y teclado en Linux Mint.***




Fuente: elaboración propia

Configuramos el idioma de Linux Mint en español, como también el del teclado.

***Fig. 7. Finalización de la instalación de Linux Mint (cliente LAN).***

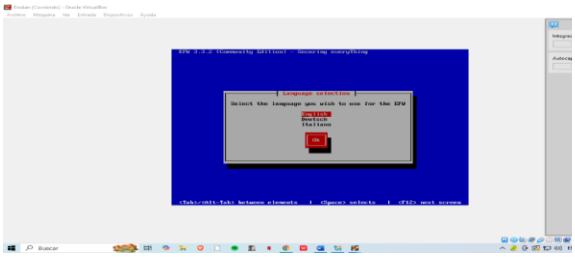



Fuente: elaboración propia

Con esto ya quedaría lista la instalación del cliente que vamos a utilizar para las pruebas

Linux Mint quedará en la zona verde.

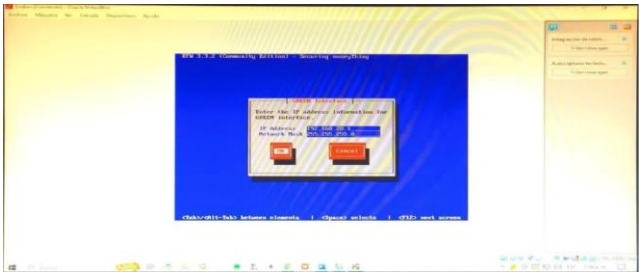
***Fig. 8. Inicio del proceso de instalación de Endian Firewall.***



Fuente: elaboración propia

Para iniciar la instalación de endian primero agregamos el idioma con el cual vamos a trabajar, escogemos inglés porque no aparece la opción del español y es un lenguaje bastante conocido.

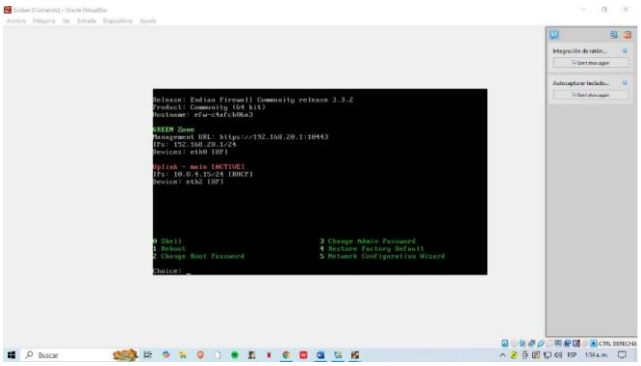
***Fig. 9. Configuración de dirección IP en el sistema Endian Firewall.***



Fuente: elaboración propia

Agregamos la IP de endian, esta IP es de vital importancia porque será Una de las direcciones con las que trabajaremos posteriormente.

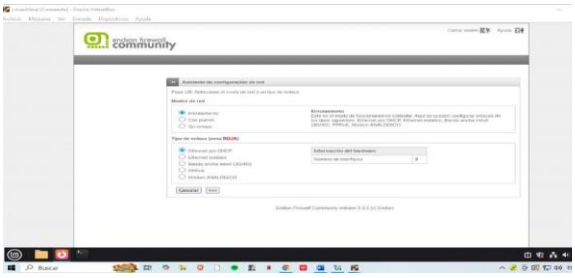
***Fig. 10. Instalación finalizada de Endian con IPs asignadas para zonas Verde y Roja.***



Fuente: elaboración propia

Podemos observar la IP que quedó establecido para la Zona Verde y roja, La verde es para el cliente Linux Mint y la Roja es la conexión a Internet por medio DHCP.

***Fig. 11. Configuración del modo de operación y tarjetas de red en Endian.***



Fuente: elaboración propia

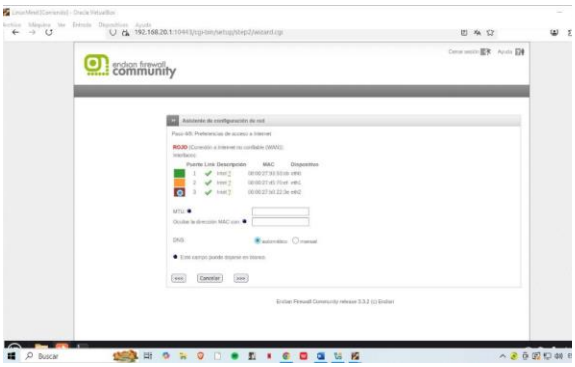
Este paso es fundamental porque indica el sistema endian cómo debe operar dentro de la red y cómo se debe conectar a Internet. Se escogió enrutamiento, por lo que el día actuará como un enrutador. Se valida que esté las 3 tarjetas de red.

***Fig. 12. Asignación de parámetros para la zona Naranja (DMZ).***

Fuente: elaboración propia

La imagen muestra la configuración de la zona naranja, mejor conocida como la zona DMZ (Zona desmilitarizada) Tiene como propósito aislar los servicios Públicos de la red interna de la Zona Verde y al mismo tiempo protegerlos de ataque de la zona roja.

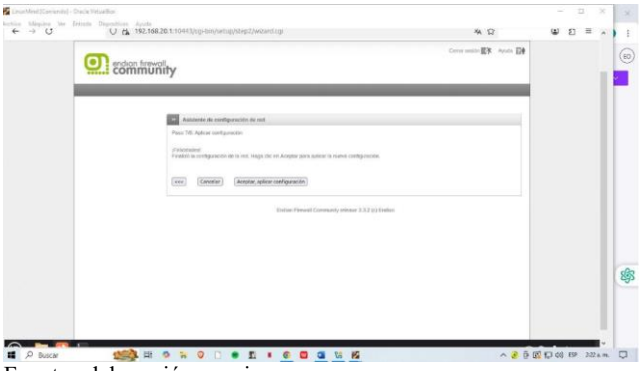
***Fig. 13. Configuración de la zona Roja y ajustes de DNS en Endian.***



Fuente: elaboración propia

Esta parte de la configuración tiene como propósito la configuración de la zona roja, asegurar que el firewall puede comunicarse con Internet y manejar el tráfico externo.

***Fig. 14. Aplicación final de los parámetros de red en Endian Firewall.***



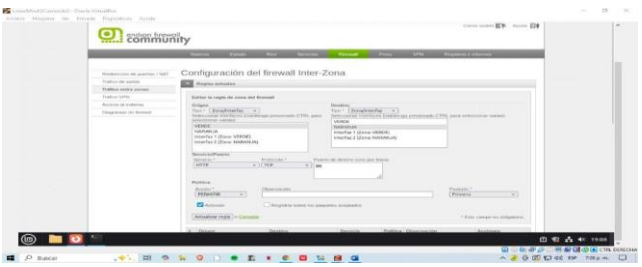
Fuente: elaboración propia

Aplicando la configuración se guardará todos los pasos que ya realizamos, espera unos segundos para que éste se emplee.

**TEMÁTICA 4: REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO.**

Comunicar la zona Verde con la zona Naranja con el protocolo HTTP y FTP con sus respectivos puertos.

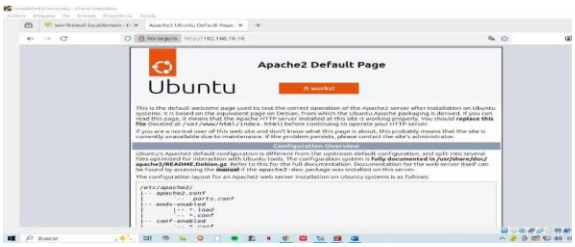
***Fig. 15. Regla de tráfico HTTP configurada entre la zona Verde y la zona Naranja.***



Fuente: elaboración propia

Configurando la Inter -Zona en endian es esencial para establecer las políticas de tráfico y seguridad en la red, en esta interfaz agregamos la regla especifica como la administración del tráfico HTTP. Esta regla permite la comunicación de navegación web dentro de las zonas verde o naranja.

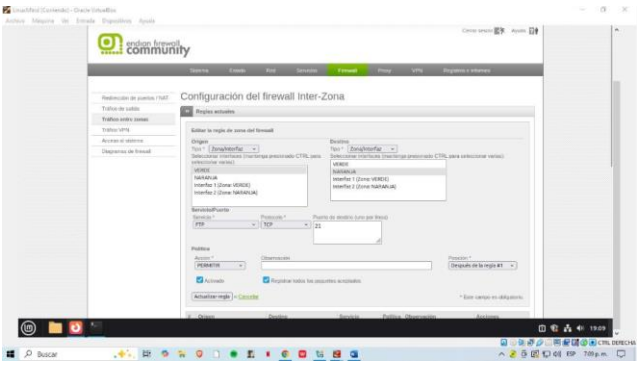
***Fig. 16. Prueba funcional de acceso HTTP desde la zona Verde hacia el servidor en la DMZ.***




Fuente: elaboración propia

Se demuestra una prueba HTTP exitosa: el cliente accede sin problemas a la página por defecto de Apache en el servidor de la zona naranja esto verifica que la regla de Inter-Zona para permitir el tráfico HTTP entre ambas zonas verde y naranja está configurada correctamente.

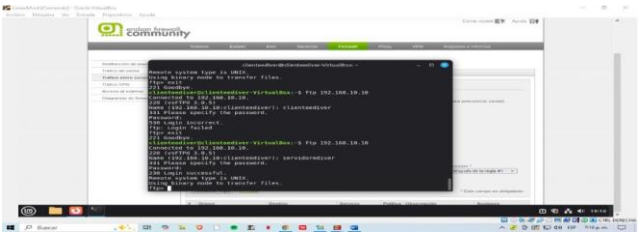
***Fig. 17. Configuración de la regla de tráfico FTP entre zona Verde y zona Naranja.***




Fuente: elaboración propia

Se muestra la creación de una nueva regla enfocada en el servicio FTP. El objetivo es configurar la política permitir, tráfico FTP entre el origen verde y destino naranja lo que asegura que se pueda trasferir archivos usando FTP.

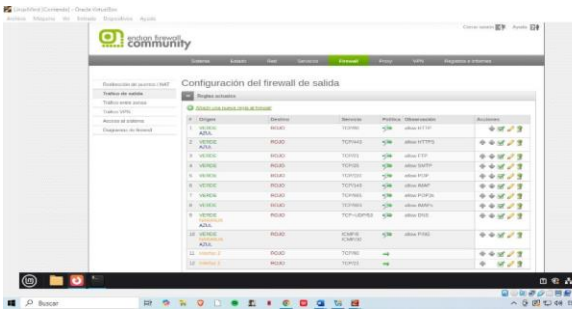
***Fig. 18. Prueba de conectividad FTP entre cliente LAN y servidor DMZ.***



Fuente: elaboración propia

Como prueba, observamos la conexión FTP exitosa entre el cliente zona verde y servidor en la zona naranja esto verifica que la regla FTP del firewall Inter-Zona esta activa y permite la trasferencia de archivos.

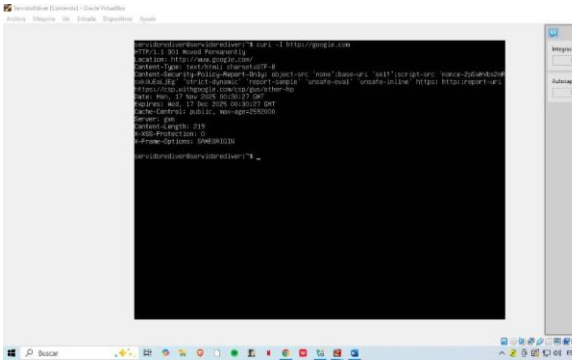
***Fig. 19. Regla de acceso para permitir servicios esenciales desde la DMZ hacia la WAN.***




Fuente: elaboración propia

La función de esta regla es permitir selectivamente servicios esenciales para que los hosts de la red puedan acceder al exterior de forma segura cumpliendo con la política de seguridad.

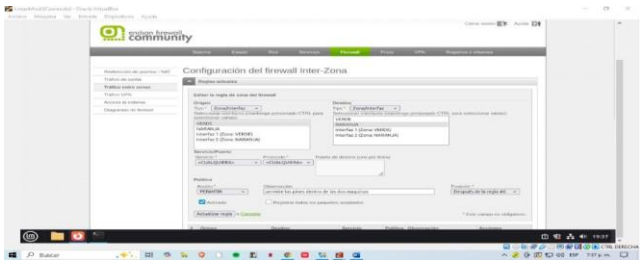
***Fig. 20. Prueba de conectividad a Internet desde la zona Naranja hacia la zona Roja.***



Fuente: elaboración propia

Como prueba, observamos la conexión a internet exitosa desde el servidor en la zona naranja (DMZ) hacia la zona roja. Esto verifica que la regla de salida está configurada correctamente

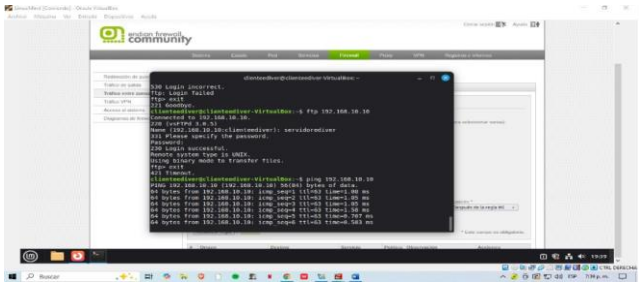
***Fig. 21. Regla general de tráfico inter-zona para pruebas ICMP (ping).***




Fuente: elaboración propia

En la imagen nos muestra la configuración tráfico Inter-Zona permite el tráfico ICMP o ping entre zonas verde y naranja la política es permitir y servicio cualquiera es de gran utilidad para pruebas iniciales.

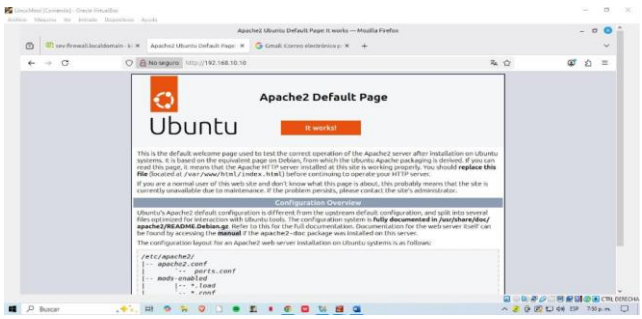
***Fig. 22. Prueba de conectividad mediante ping desde Linux Mint hacia el servidor DMZ.***



Fuente: elaboración propia

Probamos con ping desde Linux min al servidor para demostrar el tráfico que hay entre ambas zonas.

***Fig. 23. Ingreso exitoso al servicio HTTP desde la LAN hacia el servidor en la DMZ.***




Fuente: elaboración propia

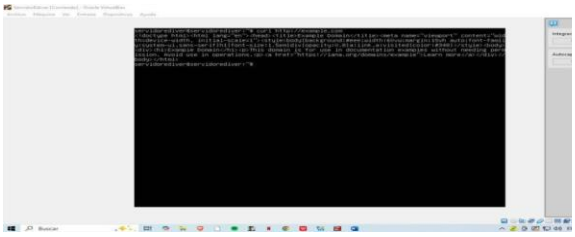
La página predeterminada de apache 2 en Ubuntu se cargo exitosamente en el navegador del cliente LAN (ZONA VERDE). este resultado es l prueba visual que confirma que la regla de firewall Inter-Zona para HTTP esta activa y que el tráfico desde la red interna hacia el servidor DMZ (Zona Naranja) ha sido correctamente permitido por el firewall.

***Fig. 24. Acceso HTTP desde la zona LAN hacia la WAN.***


Fuente: elaboración propia

Como prueba, observamos el acceso HTTP exitoso desde Linux mint al dominio externo zona roja este resultado verifica la regla de firewall de salida para el tráfico HTTP.

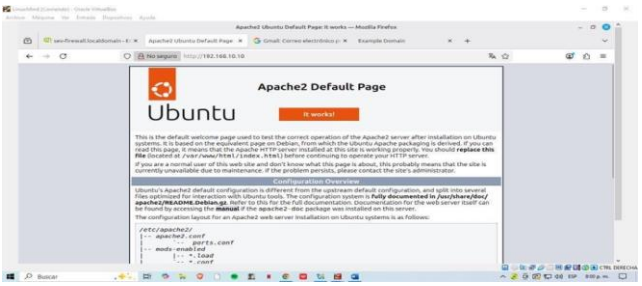
***Fig. 25. Acceso HTTP desde el servidor DMZ hacia la zona WAN.***



Fuente: elaboración propia

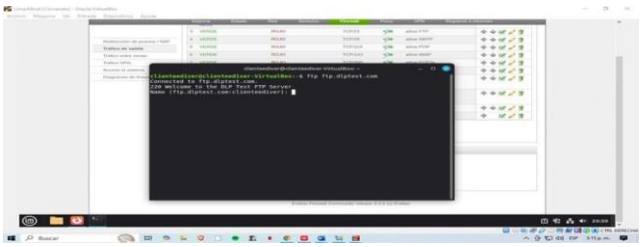
Este es el resultado es la prueba de que el servidor en la DMZ tiene conectividad HTTP saliente hacia la WAN (INTERNET) confirmando que la regla firewall de salida está configurada para permitir el acceso web.

***Fig. 26. Ingreso del servicio HTTP desde la WAN hacia la DMZ.***




Fuente: elaboración propia

***Fig. 27. Conexión FTP desde la LAN hacia la WAN lograda correctamente.***



Fuente: elaboración propia

Esta imagen verifica que la regla de firewall de salida permite el tráfico ftp desde la zona verde hacia la zona roja el mensaje connected to ftp.dlptest.com confirma la comunicación ha cruzado el firewall en endian con éxito.

## 3 *ANÁLISIS COMPLEMENTARIO*

Durante el desarrollo de la práctica se abordaron diversos escenarios relacionados con el funcionamiento del sistema operativo GNU/Linux, el reconocimiento de hardware y la administración del proceso de arranque. Estos ejercicios permitieron reforzar la comprensión de conceptos esenciales aplicados en la infraestructura utilizada para la implementación del firewall Endian.

En primer lugar, se analizó la importancia del orden de arranque dentro del BIOS, observando que un sistema puede no iniciar correctamente si se agregan nuevos dispositivos de almacenamiento sin ajustar las prioridades de boot. Este

comportamiento evidenció la relevancia de la configuración del firmware para garantizar que el cargador de arranque se ejecute desde la unidad correcta.

También se estudiaron mecanismos para identificar dispositivos PCI utilizando herramientas del sistema como lspci, lo cual resulta fundamental para validar que los componentes físicos detectados coinciden con los especificados por el fabricante. Este análisis incluyó la identificación de módulos del kernel asociados mediante parámetros extendidos como lspci -k.

Otros ejercicios permitieron evidenciar la interacción entre módulos del kernel y procesos activos. Por ejemplo, se revisó el caso en el que no es posible descargar un módulo debido a que está siendo utilizado por un proceso en ejecución, lo que refuerza la necesidad de comprender dependencias internas del núcleo antes de modificar su funcionamiento.

Así mismo, se estudiaron condiciones particulares de sistemas legacy, como la necesidad de deshabilitar el bloqueo por ausencia de teclado en firmwares antiguos, o la razón por la cual herramientas como lspci no están disponibles en plataformas ARM —debido a la ausencia del bus PCI en dichas arquitecturas.

Finalmente, se revisaron conceptos asociados al proceso de arranque, tales como la ubicación del MBR, el papel de la partición EFI en sistemas UEFI, el uso de parámetros del kernel (por ejemplo root=/dev/sda3) y la importancia de disponer de una imagen initramfs adecuada para garantizar el acceso al sistema de archivos raíz. También se profundizó en herramientas de diagnóstico como journalctl y dmesg, esenciales para la revisión de logs del sistema y resolución de fallos de arranque.

## IV.CONCLUSIONES

- La implementación de reglas inter-zona en Endian Firewall permitió validar la importancia de una correcta segmentación de red para garantizar la seguridad perimetral en entornos GNU/Linux. La comunicación controlada entre las zonas Verde (LAN), Naranja (DMZ) y Roja (WAN) evidenció cómo las políticas de firewall influyen directamente en la disponibilidad y protección de los servicios expuestos.
- Los resultados obtenidos demostraron que las reglas configuradas para los protocolos HTTP y FTP funcionaron de manera adecuada, asegurando que solo el tráfico autorizado pudiera atravesar las distintas zonas. Asimismo, el análisis de pruebas funcionales y de conectividad reveló que la DMZ cumple su propósito de aislar los servicios críticos y brindar una capa adicional de seguridad frente a accesos desde la red interna o externa.
- Finalmente, el proceso reafirmó la relevancia de herramientas de gestión de tráfico como Endian, destacando el papel fundamental de la administración por consola, la revisión de logs y la verificación de reglas para mantener una infraestructura segura, estable y coherente con los lineamientos establecidos.

## RECONOCIMIENTOS

El autor expresa su agradecimiento a los docentes del curso por su orientación en el desarrollo de la Etapa 7, así como a los compañeros del grupo colaborativo por sus aportes técnicos y participación en la validación de cada una de las temáticas propuestas. Igualmente, se reconoce el apoyo brindado por la comunidad de software libre, cuyos manuales y recursos documentales permitieron profundizar en el funcionamiento de Endian Firewall y en la administración de redes bajo sistemas GNU/Linux.

## REFERENCIAS

[1] Canonical, Ubuntu Desktop 20.04 LTS – Help Guide, 2023. [Online]. Available: https://help.ubuntu.com/20.04/ubuntu-help/index.html

[2] Debian Project, Debian Administrator's Handbook, Debian 12.5.0, 2023. [Online]. Available: https://www.debian.org/releases/stable/amd64/index.es.html

[3] Endian, Endian UTM 3.2 – Manual de referencia, 2016. [Online]. Available: http://docs.endian.com/3.2/utm/index.html

[4] P. F. Hernández and J. Sánchez, Monitoreo y administración de sistemas Linux. UNAD Institutional Repository, 2022. [Online]. Available: https://repository.unad.edu.co/handle/10596/53211

[5] Oracle, VirtualBox – User Manual, 2020. [Online]. Available: https://www.virtualbox.org/manual/

[6] Shorewall Documentation, Firewall Policies and Zones, Shorewall, 2021.