IMPLEMENTANDO GNU/LINUX ENDIAN: SEGMENTACIÓN DE REDES Y POLÍTICAS DE SEGURIDAD

Beatriz Andrea Garzón Garzón
e-mail: bagarzong@unadvirtual.edu.co
Briyid Dayana Coy Coy
e-mail: bdcoyc@unadvirtual.edu.co
Julián Andrés Ariza Pérez
e-mail: jaarizape@unadvirtual.edu.co
Manuel Humberto Ortega Méndez
e-mail: mhortegame@unadvirtual.edu.co

RESUMEN: *Este artículo presenta la implementación de una instancia GNU//Linux Endian en un entorno virtualizado mediante VirtualBox, con el objetivo de analizar la administración de redes segmentadas y la aplicación de medidas de seguridad. Se establecieron tres zonas de red: verde (LAN), roja (WAN) y naranja (DMZ) estableciendo reglas de traducción de direcciones (NAT) y políticas de acceso. Asimismo, se habilitaron servicios como HTTP y FTP en la DMZ y se restringieron protocolos como ICMP para reforzar la seguridad. Los resultados incluyen pruebas de conectividad, acceso web y bloqueo de tráfico, las cuales validan la correcta aplicación de las reglas de seguridad y el comportamiento esperado de la red. Estos hallazgos destacan la utilidad de los entornos virtuales como herramienta pedagógica para la comprensión práctica de la administración y protección de infraestructuras de red, así como del fortalecimiento de los aspectos teóricos aprendidos.*

PALABRAS CLAVE: DMZ, Endian, NAT, Seguridad de redes.

1. INTRODUCCIÓN

La administración de redes segmentadas y la implementación de medidas de seguridad constituyen pilares fundamentales en el diseño de infraestructuras informáticas modernas. En la era actual donde las amenazas digitales evolucionan constantemente, resulta indispensable comprender cómo se estructuran y protegen las redes mediante la separación de zonas y la aplicación de políticas de control de tráfico. En este trabajo se presenta la configuración de una instancia GNU/Linux Endian, con el propósito de analizar de manera aplicada la gestión de redes segmentadas y la implementación de reglas de seguridad. La actividad incluyó la instalación del sistema y la definición de tres zonas de red: la zona verde, correspondiente a la LAN interna; la zona roja, encargada del acceso a Internet; y la zona naranja, destinada a los servidores ubicados en la DMZ (Zona desmilitarizada).

Posteriormente, se implementaron reglas de traducción de direcciones (NAT) y de reenvío de puertos, garantizando la comunicación entre las distintas zonas y validando el comportamiento esperado de los servicios. Asimismo, se configuraron servicios en la DMZ, habilitando protocolos como HTTP y FTP y restringiendo otros como ICMP, con el fin de reforzar la seguridad y evitar respuestas innecesarias a solicitudes externas. Finalmente, se establecieron reglas de acceso entre las diferentes zonas, lo que permitió definir con precisión qué tIPo de tráfico podía circular entre ellas y desde Internet hacia los servidores expuestos.

Los resultados obtenidos evidencian la correcta aplicación de las reglas de seguridad y el funcionamiento de la red segmentada.

2. INSTALACION Y CONFIGURACIÓN DE ENDIAN

2.1 INSTALACIÓN Y CONFIGURACIÓN

La instalación del firewall Endian se realizó sobre una máquina virtual dedicada, configurada con: Procesador de 3.2 con 6 núcleos, GHz, RAM, 12 gigabytes disco sata de 20 gigabytes. Se utilizó la imagen ISO oficial de Endian Community 3.3.2, la cual fue montada desde el entorno de virtualización VirtualBox.

Figura 1. Instalación y configuración de Endian

Autoría: Manuel Ortega

Durante el proceso de instalación, se seleccionó el modo de instalación estándar, configurando el disco como partición única y estableciendo la zona horaria correspondiente a Colombia. Una vez completada la instalación, se procedió al primer arranque del sistema, accediendo a la interfaz web de administración mediante la dirección IP predeterminada asignada por DHCP.

Figura 2. Seleccionando el modo de instalación

Autoría: Manuel Ortega

Figura 3. Esperamos el proceso de instalación

Autoría: Manuel ortega

La configuración inicial incluyó la definición de las zonas de red (GREEN, RED), asignando a cada una la interfaz de red virtual previamente creada.

Figura 4. Finalizamos la instalación y damos ok

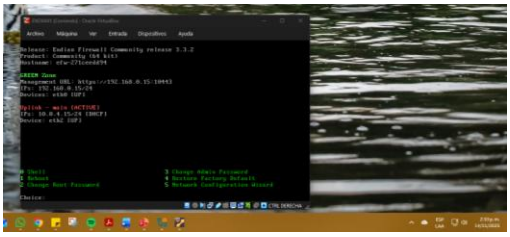
Autoría: Manuel ortega

La zona GREEN fue configurada con la subred [192.168.0.15/24], mientras que la zona RED se conectó al gateway de salida hacia Internet. Se habilitó el servicio DHCP para la zona GREEN, definiendo un rango de direcciones dinámicas y reservando IP estáticas para dispositivos críticos.

Figura 5. Endian instalado correctamente.

Autoría: Manuel Ortega

Figura 6. Ejecutando Endian donde se evidencia la red GREED y la red RED



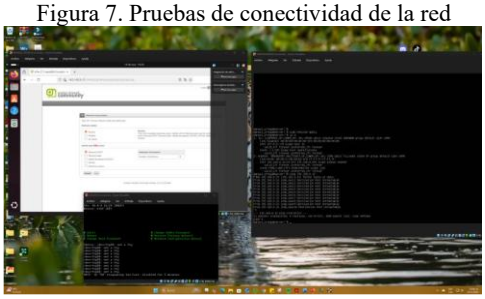
Autoría: Manuel Ortega

Finalmente, se realizaron pruebas de conectividad, navegación y aislamiento entre zonas, validando el correcto funcionamiento de la arquitectura segmentada. Toda la configuración fue documentada y respaldada para futuras restauraciones o auditorías.

3. TEMATICA 1: CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX (TARJETAS DE RED) E INSTALACIÓN EFECTIVA DEL MISMO.

Producto esperado: Implementación de GNU/Linux Endian con las zonas verde, roja y naranja, así: Zona verde: Red interna (LAN), Zona roja: Acceso a internet (WAN) y Zona naranja: Servidores (DMZ).

Figura 7. Pruebas de conectividad de la red



Autoría: Manuel Ortega

Para la implementación del firewall GNU/Linux Endian, se configuró una instancia virtual utilizando VirtualBox como entorno de virtualización. La máquina virtual fue creada con recursos: 6 núcleos de CPU, 12 GB de memoria RAM y 20 GB de almacenamiento en disco dinámico.

Se asignaron tres adaptadores de red virtuales, cada uno vinculado a una zona de seguridad específica del esquema Endian: GREEN (red interna), RED (salida a Internet), ORANGE (zona DMZ). Los adaptadores fueron configurados en modo “Red interna” según la función de cada zona, permitiendo la segmentación lógica y física del tráfico.

La imagen ISO de Endian Community 3.3.2 fue montada en la unidad óptica virtual, iniciando el proceso de instalación desde el arranque. Se seleccionó el modo de instalación estándar, definiendo el disco como partición única y estableciendo la zona horaria correspondiente a Colombia. Tras la instalación, se accedió a la interfaz web del desktop mediante

la IP asignada a la zona GREEN, desde donde se completó la configuración inicial.

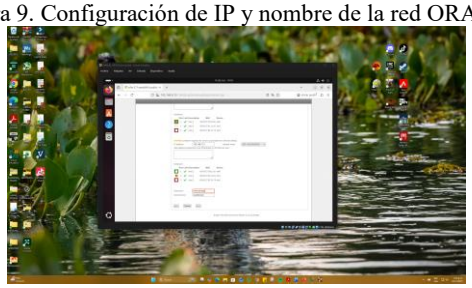
Una vez completada la instalación base de Endian, se accedió a la interfaz web del desktop mediante la dirección IP asignada a la zona GREEN. Al iniciar sesión por primera vez, el sistema solicita la modificación de credenciales predeterminadas, permitiendo el cambio de usuario y contraseña según las políticas de seguridad del entorno.

El asistente de configuración guía al administrador a través de los pasos iniciales. En la primera pantalla se visualizan las zonas RED y GREEN, previamente configuradas durante la instalación, junto con sus respectivas direcciones IP y máscaras de subred. A continuación, se habilitó la zona ORANGE, asignándole una dirección IP previamente definida para dicha segmentación. El sistema permite además establecer un nombre identificador para el servidor.

Figura 8. Selección de la red ORANGE

Autoría: Manuel Ortega

Figura 9. Configuración de IP y nombre de la red ORANGE

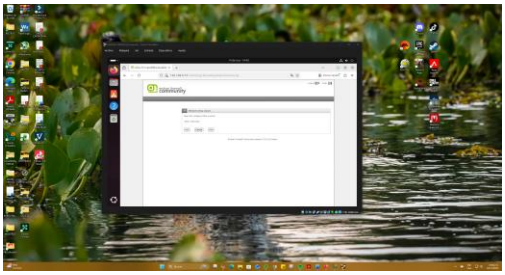


Autoría: Manuel Ortega

Figura 10. Visualizamos las redes con sus respectivas IP y damos clic en siguiente

Autoría: Manuel Ortega

Figura 11. Podemos dejar esta configuración tal cual como esta y damos clic en siguiente

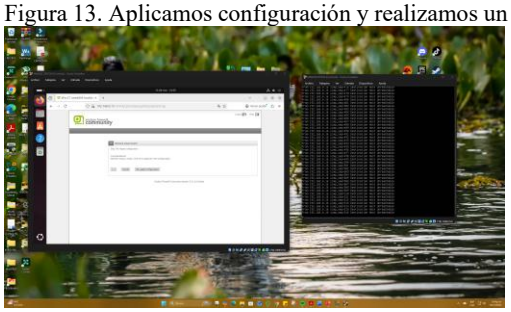


Autoría: Manuel Ortega

Figura 12. Podemos dejar esta configuración tal cual como esta y damos clic en siguiente

Autoría: Manuel Ortega

Figura 13. Aplicamos configuración y realizamos un ping



Autoría: Manuel Ortega

Al avanzar en el asistente, se muestran las tres zonas configuradas (RED, GREEN y ORANGE), confirmando su estado activo. En esta etapa no se requiere ingresar información adicional, por lo que se procede directamente con la finalización del proceso. Una vez completada la configuración, se validó la conectividad mediante pruebas de ping exitosas hacia el servidor, confirmando la operatividad de la arquitectura segmentada.

4. TEMATICA 2: CONFIGURACIÓN NAT EN ENDIAN

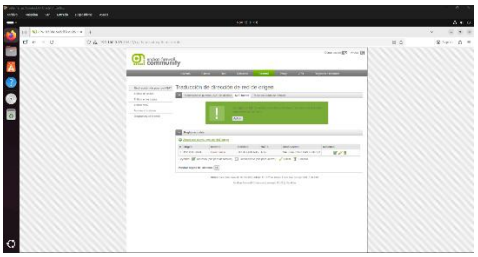
Para permitir que los equipos ubicados en las redes internas puedan acceder a Internet a través del firewall, se configuraron reglas de traducción de direcciones de red (NAT) sobre la instancia GNU/Linux Endian previamente instalada. La finalidad de estas reglas es que las subredes privadas asociadas a las zonas verde (LAN) y naranja (DMZ) utilicen la dirección IP de la interfaz roja (WAN) como dirección de salida, manteniendo oculto el direccionamiento interno y centralizando el control del tráfico externo.

El procedimiento se realizó desde la interfaz web de administración de Endian. En primer lugar, se accedió al menú de Traducción de dirección de red de origen (NAT) desde el panel de control del firewall. Sobre este módulo se creó una primera regla de masquerading desde la zona verde (subred 192.168.0.0/24, donde el firewall está configurado con la IP 192.168.0.15) hacia la zona roja. De esta forma, todo el tráfico generado por los equIPos de la LAN y dirigido a Internet es reemplazado dinámicamente por la dirección IP de la interfaz roja del firewall, permitiendo el enrutamiento adecuado sin exponer las direcciones privadas.

Figura 14. Aplicamos configuración y realizamos un ping

Autoría: Andrés Ariza

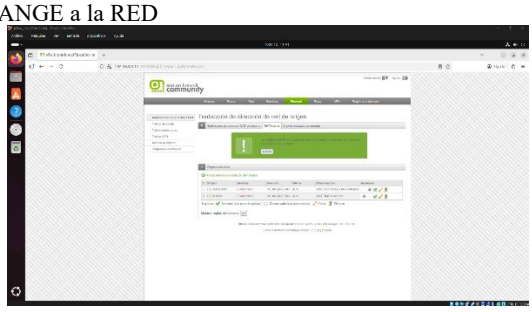
Figura 15. Aplicamos regla NAT desde la LAN GREEN a la RED



Autoría: Andrés Ariza

Posteriormente, se definió una segunda regla de NAT con características equivalentes para la zona naranja, asociada a la DMZ (subred 192.168.1.0/24, con el firewall configurado en 192.168.1.15). Esta regla permite que los servidores ubicados en la DMZ establezcan conexiones salientes hacia Internet utilizando igualmente la dirección pública de la interfaz roja, manteniendo aislado el segmento de servidores y evitando que su direccionamiento interno sea visible desde el exterior. Ambas reglas quedaron registradas en el listado de políticas de NAT de origen de Endian, observándose activas en el panel de administración.

Figura 16. Aplicamos regla NAT desde la DMZ ORANGE a la RED



Autoría: Andrés Ariza

Para validar la correcta operación de la configuración, se realizaron pruebas de conectividad desde un equipo cliente ubicado en la red verde, el cual obtuvo la dirección IPv4 192.168.0.16 a través del servicio DHCP configurado en el firewall. Desde este host se ejecutaron comandos de ping hacia direcciones públicas como 8.8.8.8 y hacia nombres de dominio externos (por ejemplo, google.com), obteniendo respuestas satisfactorias que evidencian la resolución DNS y el acceso a Internet mediante las reglas de NAT. Finalmente, en la interfaz de Endian se revisaron las estadísticas de tráfico y los registros de conexión, donde se observaron las sesiones generadas desde las subredes 192.168.0.0/24 y 192.168.1.0/24 traducidas a la interfaz roja, confirmando así el funcionamiento esperado de la traducción de direcciones en el entorno segmentado.

Figura 17. Pruebas desde la LAN (PC en 192.168.0.0/24

Autoría: Andrés Ariza

5. TEMATICA 3: CONFIGURACIÓN DE SERVICIOS EN LA DMZ

En la temática 3 se configuran los servicios HTTP (Puerto 80) y FTP (Puerto 21) desde el servidor web de Ubuntu Server, y adicionalmente se establece la restricción del protocolo ICMP (puertos 8 y 30) con el fin de impedir la ejecución de comandos de ping en la red, reforzando así las políticas de seguridad aplicadas en la DMZ. Antes de iniciar con la definición de reglas de tráfico, se verificó la correcta asignación de la dirección IP al equipo conectado en la zona verde (LAN). Para ello, se utilizó el comando IP a en la terminal del sistema, confirmando que la dirección IPv4 obtenida fue 192.168.0.16, dentro del rango establecido para la red interna.

Figura 18. Se verifica la IP asignada por la red GREEN

Autoría: Briyid Coy

Posteriormente, se accedió a la interfaz web de Endian Firewall para continuar con la configuración inicial. En esta etapa se seleccionaron el idioma y la zona horaria, se aceptaron los términos de licencia y se definieron las credenciales de acceso para los servicios SSH y administración.

Figura 19. Se inicia interfaz web Endian

Autoría: Briyid Coy

Una vez completado este proceso, se procedió a la configuración de las zonas de red de la siguiente manera:

Zona roja (WAN): configurada en modo enrutamiento mediante DHCP, con DNS automático.

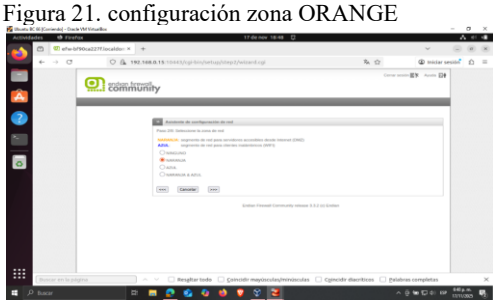
Zona naranja (DMZ): destinada a los servidores, con dirección IP 192.168.1.15, máscara de red 255.255.255.0 y nombre de host.

Zona verde (LAN): previamente configurada como red interna.

Figura 20. configuración zona RED

Autoría: Briyid Coy

Figura 21. configuración zona ORANGE

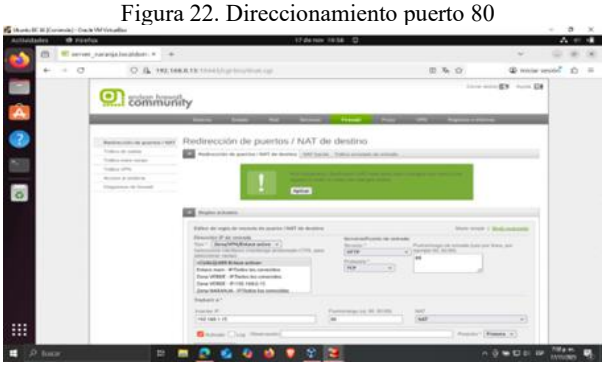


Autoría: Briyid Coy

Con la estructura de red establecida, se accedió al panel de control del firewall para configurar las reglas de tráfico entre zonas. La primera etapa consistió en habilitar los servicios HTTP y FTP en la DMZ:

Servicio HTTP (TCP/80): se creó una regla que permitiera el acceso desde la zona naranja hacia la red externa, asociando la dirección IP del servidor (10.0.2.15) al puerto 80.

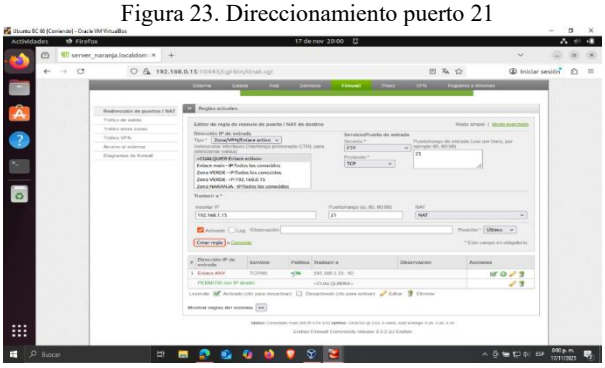
Figura 22. Direccionamiento puerto 80



Autoría: Briyid Coy

Servicio FTP (TCP/21): se definió una regla similar, habilitando el puerto 21 para transferencia de archivos.

Figura 23. Direccionamiento puerto 21

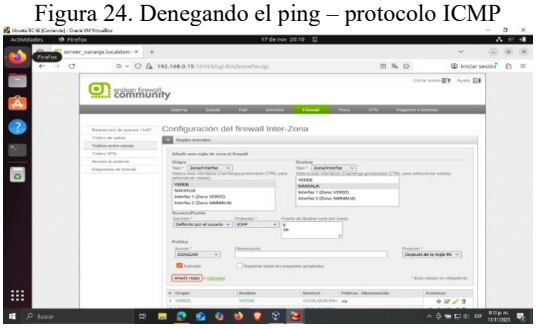


Autoría: Briyid Coy

Adicionalmente, se configuró el redireccionamiento de puertos, asociando las direcciones de entrada con los servicios HTTP y FTP, de manera que las solicitudes externas fueran dirigidas correctamente al servidor ubicado en la DMZ.

Como medida de seguridad complementaria, se estableció una regla para denegar el protocolo ICMP (puertos 8 y 30), evitando la respuesta a solicitudes de ping desde la red interna hacia la DMZ. Esta restricción se configuró en el tráfico interzonal, definiendo como origen la zona verde y como destino la zona naranja, con acción de bloqueo. Las pruebas realizadas desde la consola confirmaron la ausencia de respuesta a los comandos de ping, validando la correcta aplicación de la política de seguridad.

Figura 24. Denegando el ping – protocolo ICMP

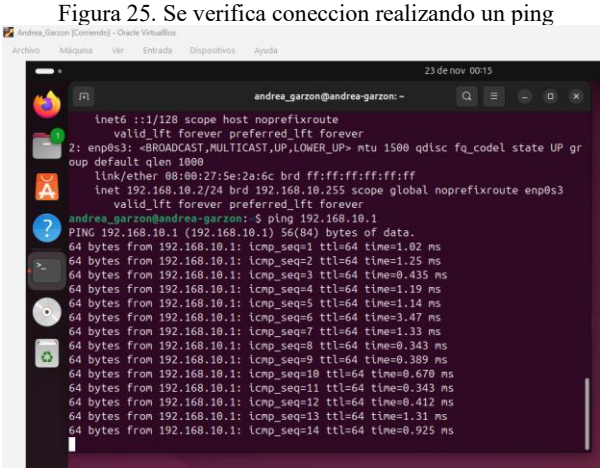


Autoría: Briyid Coy

6. TEMATICA 4: REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO.

Durante el desarrollo de la temática 4: reglas de acceso para permitir o denegar el tráfico, se realizó la implementación de un esquema de red segmentado utilizando el firewall Endian, con zonas GREEN (LAN), ORANGE (DMZ) y RED (WAN), la cual está en Uplink Manager. Inicialmente se configuraron las máquinas virtuales de cada zona, asignando direcciones IP estáticas y verificando la conectividad básica mediante pruebas de ping. Posteriormente se construyeron las reglas de tráfico inter-zona, comenzando por permitir la comunicación desde GREEN hacia ORANGE utilizando los protocolos HTTP y FTP, lo que se verificó exitosamente accediendo al servidor web y estableciendo sesiones FTP externas. Adicionalmente, se habilitó la salida hacia Internet para las máquinas de la DMZ, ajustando las reglas de tráfico saliente y resolviendo problemas relacionados con DNS y enrutamiento hasta obtener navegación completa desde GREEN y ORANGE hacia la WAN.

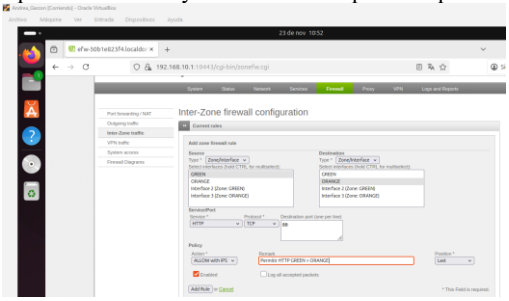
Figura 25. Se verifica coneccion realizando un ping



Autoría: Beatriz Andrea Garzón

Durante la fase de validación se ejecutaron las pruebas definidas en la guía con el fin de comprobar el funcionamiento del firewall y las distintas políticas aplicadas entre las zonas GREEN, ORANGE y RED. Se confirmó exitosamente la comunicación desde la LAN hacia la WAN utilizando servicios como FTP, lo cual evidenció que las reglas de salida y la resolución DNS estaban operando correctamente. Igualmente, se avanzó en la construcción de las reglas necesarias para publicar servicios de la DMZ hacia la WAN, así como en la preparación del servidor web y FTP requerido para dichas pruebas. Aunque aún se encuentran en proceso de ajuste final las pruebas relacionadas con el acceso HTTP y FTP desde la WAN hacia la DMZ, la configuración realizada hasta el momento demuestra el correcto funcionamiento de la segmentación de red, el control del tráfico inter-zona y las políticas de seguridad implementadas en Endian Firewall.

Figura 26. Comunicar la zona Verde con la zona Naranja con el protocolo HTTP y FTP con sus respectivos puertos.



Autoría: Beatriz Andrea Garzón

Figura 27. Validación de funcionamiento de la regla:

Autoría: Beatriz Andrea Garzón

Figura 28. Con protocolo FTP

Autoría: Beatriz Andrea Garzón

Figura 29. Reglas de inter-zona.

Autoría: Beatriz Andrea Garzón

7. Conclusiones.

La implementación de las zonas **verde, naranja y roja en Endian** constituye un paso fundamental para garantizar una arquitectura de red segura, segmentada y eficiente. La correcta configuración de cada zona permite:

Zona Verde: asegurar la conectividad confiable de la red interna, destinada a usuarios y servicios autorizados.
Zona Naranja: habilitar un espacio controlado para servidores y aplicaciones expuestas, protegiendo la infraestructura princIPal mediante un perímetro intermedio.
Zona Roja: establecer el límite externo frente a Internet, reforzando la seguridad mediante reglas estrictas de acceso y filtrado.

La configuración del firewall GNU/Linux Endian permitió validar la eficacia de la segmentación de red mediante la implementación de la zona DMZ. La arquitectura resultante mostró un comportamiento consistente con los princIPios de aislamiento lógico y control de tráfico esperados en infraestructuras orientadas a la seguridad.

La habilitación de servicios en la DMZ, específicamente HTTP y FTP, junto con la restricción del protocolo ICMP, evidenció el funcionamiento del perímetro seguro y la utilidad de la DMZ como zona intermedia. Las políticas configuradas mostraron un control efectivo del acceso, permitiendo únicamente el tráfico autorizado.

8. REFERENCIAS

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

[2] Cervelión, Á. J. (2023). Instalación de Nagios Core 4.4 en Ubuntu 22.04. [Objeto_virtual_de_información_OVI]. Repositorio Institucional UNAD. Disponible en: https://repository.unad.edu.co/handle/10596/54230

[3] Debian (2023). El manual del administrador de Debian 12.5.0 . Debian. Disponible en: https://www.debian.org/releases/stable/amd64/index.es.html

[4] Endian (2016), Endian UTM 3.2 Manual referencia. Endian: Disponible en: http://docs.endian.com/3.2/utm/index.html

[5] LPI LPIC-1 Exam 101. (2022). Tema 101: Arquitectura del sistema. Disponible en: https://learning.lpi.org/es/learning-materials/101-500/101/

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

[7] OpenAI. (2025). *OpenAI.* Obtenido de OpenAI. ChatGPT (versión 5.1) [Modelo de lenguaje]: https://chat.openai.com

[8] Hernandez, P. F., & Sánchez, J. (2022). Monitoreo y administración de sistemas Linux . [Objeto_virtual_de_información_OVI]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/

[9] Ilinuxgeek. (s.f.). *Cómo verificar y parchear la vulnerabilidad de la CPU de la CPU en Linux*. Ilinuxgeek. https://es.ilinuxgeek.com/article/how-to-check-and-patch-meltdown-cpu-vulnerability-in-linux

[10] Jiménez, J. H. (2016). Shell ScrIPt para Bash . [Objeto_virtual_de_información_OVI]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/9758

[11] Linux Professional Institute Inc. Tema 5: Seguridad y sistema de permisos de archivos. Lección 5.1, Lección 5.2, Lección 5.3, Lección 5.4. (s. f.). https://learning.lpi.org/es/learning-materials/010-160/1/1.1/1.1_01/