IMPLEMENTACIÓN DE SEGURIDAD PERIMETRAL EN GNU/LINUX MEDIANTE ENDIAN FIREWALL Y CONFIGURACIÓN DE DMZ

Edilson Orlando Alvarado Mendez
e-mail: eoalvaradom@unadvirtual.edu.co
Fernando Antonio Galvez Moreno
e-mail: fagalvezm@unadvirtual.edu.co

RESUMEN: *El presente trabajo describe la implementación de un esquema de seguridad perimetral en sistemas GNU/Linux mediante el uso de Endian Firewall en un entorno virtualizado. Se configuraron las zonas de red LAN, WAN y DMZ, estableciendo políticas de control de acceso, reglas de firewall y traducción de direcciones de red (NAT) para gestionar el tráfico entre segmentos. Asimismo, se habilitaron servicios como HTTP y FTP en la zona DMZ, y se aplicaron restricciones de seguridad como el bloqueo de ICMP. Las pruebas realizadas permitieron verificar la conectividad controlada entre las diferentes zonas y el correcto funcionamiento de las políticas implementadas. Los resultados evidencian la importancia de segmentar la red y aplicar mecanismos de filtrado para garantizar la integridad, disponibilidad y confidencialidad de los servicios en entornos GNU/Linux.*

PALABRAS CLAVE: DMZ, Endian Firewall, GNU/Linux, Seguridad perimetral

1 INTRODUCCIÓN

En la actualidad, la seguridad en redes informáticas representa un elemento crítico para la protección de la información y la continuidad de los servicios en entornos organizacionales [9]. La implementación de mecanismos de seguridad perimetral permite controlar el tráfico entre redes internas y externas, reduciendo riesgos asociados a accesos no autorizados y posibles amenazas [10].

En este contexto, los sistemas GNU/Linux proporcionan herramientas eficientes para la administración de redes y la aplicación de políticas de seguridad [6]. El uso de soluciones como Endian Firewall permite segmentar la red en diferentes zonas, tales como LAN (zona verde), WAN (zona roja) y DMZ (zona naranja), facilitando el control del tráfico y la protección de los servicios expuestos [5].

El presente trabajo aborda la estructuración de un entorno de red seguro en un escenario virtualizado, mediante la configuración de reglas de acceso, servicios de red y mecanismos como NAT y filtrado de paquetes. A través de esta práctica, se valida la comunicación controlada entre las diferentes zonas de red, así como la importancia de aplicar políticas de seguridad para garantizar la integridad, disponibilidad y confidencialidad de los sistemas en GNU/Linux.

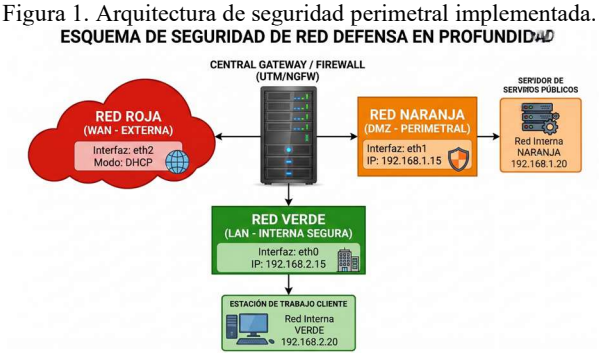
2 DESARROLLO

2.1 TEMÁTICA 1: CONFIGURACIÓN DE ENDIAN Y ZONAS DE RED

Para el desarrollo de la práctica se implementó una arquitectura de seguridad perimetral en un entorno virtualizado utilizando GNU/Linux Endian Firewall sobre Oracle VirtualBox [4]. La infraestructura fue diseñada bajo un modelo de segmentación de red compuesto por las zonas GREEN (LAN), RED (WAN) y ORANGE (DMZ), permitiendo controlar el tráfico entre redes internas y externas mediante políticas de filtrado y administración centralizada.

La implementación tuvo como objetivo garantizar una comunicación segura entre los diferentes segmentos de red, permitiendo la publicación controlada de servicios en la DMZ y protegiendo la red interna frente a accesos no autorizados. En la Fig. 1 se esquematiza el mapa de interconexión física y lógica proyectado para el laboratorio.

Figura 1. Arquitectura de seguridad perimetral implementada.

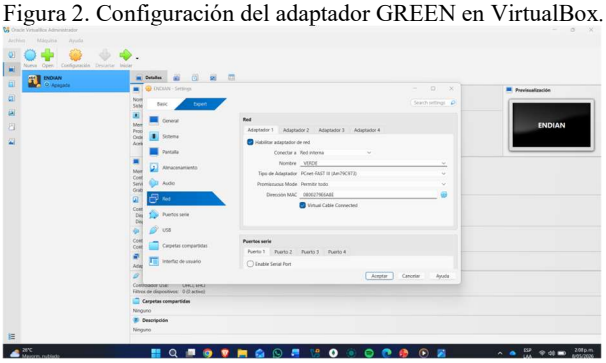


Fuente: Autoría Propia

2.1.1 CONFIGURACIÓN DE REDES VIRTUALES EN VIRTUALBOX

Inicialmente, se configuraron las redes virtuales necesarias para representar las diferentes zonas de seguridad dentro del entorno de virtualización [4]. Para la zona GREEN se creó una red Host-Only con el segmento 192.168.2.0/24, la cual servirá de canal exclusivo para los clientes internos de confianza. La asignación del adaptador lógico correspondiente en el hipervisor se detalla en la Fig. 2.

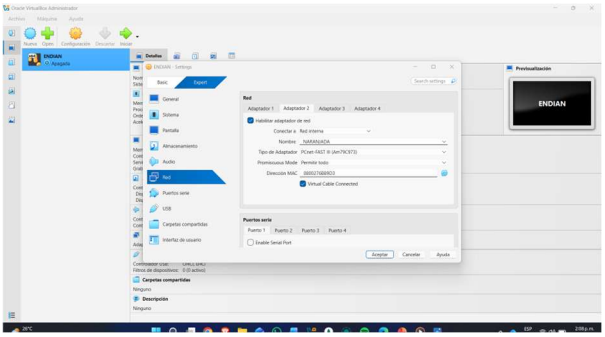
Figura 2. Configuración del adaptador GREEN en VirtualBox.



Fuente: Autoría Propia

Para la zona ORANGE dedicada exclusivamente a los servidores de acceso público se parametrizó un segundo adaptador de red independiente asociado al segmento de red privado 192.168.1.0/24, cuyo estado de aislamiento se ilustra en la Fig. 3.

Figura 3. Configuración del adaptador ORANGE en VirtualBox.



Fuente: Autoría Propia

En ambas configuraciones se deshabilitó el servicio DHCP integrado de VirtualBox con el fin de evitar conflictos de direccionamiento, permitiendo que Endian Firewall administrara completamente las direcciones IP and el tráfico de red. Asimismo, la zona RED fue configurada mediante un adaptador NAT para simular la conectividad WAN y el acceso externo a Internet, ajuste que se evidencia en la Fig. 4.

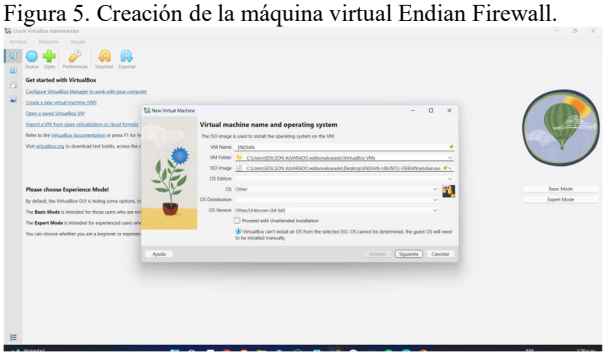
Figura 4. Configuración del adaptador RED mediante NAT.

Fuente: Autoría Propia

2.1.2 CREACIÓN E INSTALACIÓN DE GNU/LINUX ENDIAN FIREWALL

Posteriormente, se creó la máquina virtual correspondiente a GNU/Linux Endian Firewall dentro de VirtualBox [4]. Para ello, se asignaron 2 GB de memoria RAM y un disco duro virtual dinámico de 20 GB, integrando los tres adaptadores de red previamente creados. La declaración inicial del nodo en la plataforma se muestra en la Fig. 5.

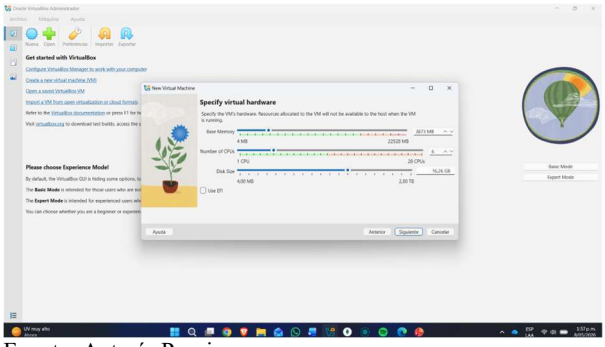
Figura 5. Creación de la máquina virtual Endian Firewall.



Fuente: Autoría Propia

Durante el aprovisionamiento de hardware en la plataforma de virtualización, se asoció cada tarjeta de red virtual con su respectivo segmento lógico, garantizando que el appliance UTM identifique de forma única los canales de comunicación, tal como se documenta en la Fig. 6.

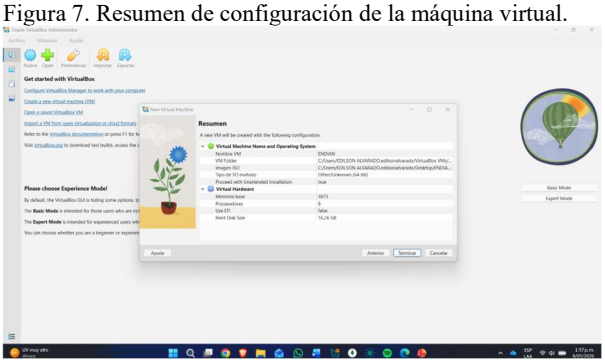
Figura 6. Asignación de recursos de hardware para Endian Firewall.



Fuente: Autoría Propia

Antes de inicializar el volcado del sistema operativo, se revisó el cuadro consolidado de propiedades físicas de la máquina virtual dentro del hipervisor, garantizando la persistencia y compatibilidad de los recursos asignados, aspecto descrito en la Fig. 7.

Figura 7. Resumen de configuración de la máquina virtual.



Fuente: Autoría Propia

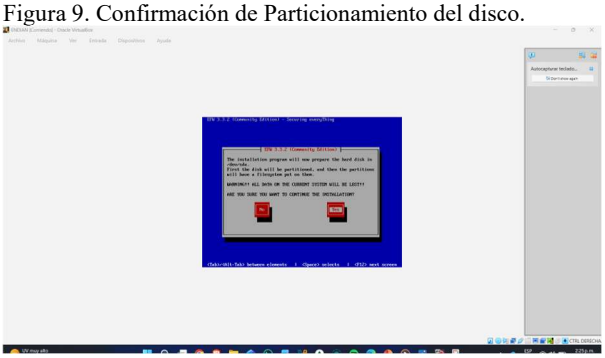
Durante el proceso de instalación se montó la imagen ISO oficial de Endian Firewall [5]. El asistente gráfico guio el arranque inicial del núcleo Linux, permitiendo establecer las configuraciones básicas de idioma y teclado para la posterior gestión de comandos, fase expuesta en la Fig. 8.

Figura 8. Proceso de instalación de Endian Firewall.

Fuente: Autoría Propia

Posteriormente, el instalador procedió con la creación de la tabla de particiones dentro del almacenamiento virtualizado, formateando los volúmenes lógicos bajo sistemas de archivos adecuados para la retención del sistema y las bitácoras de eventos, paso validado en la Fig. 9.

Figura 9. Confirmación de Particionamiento del disco.



Fuente: Autoría Propia

Una vez finalizada la copia de los paquetes bases y definidas las credenciales de acceso administrativo para el usuario de sistema, el instalador notificó la culminación del despliegue y solicitó el reinicio del nodo para inicializar las funciones perimetrales, tal como se aprecia en la Fig. 10.

Figura 10. Finalización de instalación de Endian Firewall.

Fuente: Autoría Propia

2.1.3 CONFIGURACIÓN DE INTERFACES DE RED Y DIRECCIONAMIENTO IP

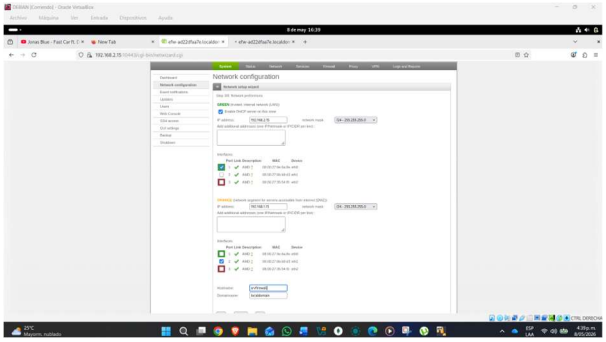
Una vez instalado el sistema, se procedió a configurar las interfaces de red correspondientes a cada zona de seguridad a través del menú de consola nativo [5]. La interfaz GREEN fue destinada a la red LAN interna, asignando la dirección IP 192.168.2.15/24. La asignación conjunta de los segmentos GREEN y ORANGE se visualizan en la Fig. 11.

Figura 11. Configuración de interfaces GREEN y ORANGE.

Fuente: Autoría Propia

De igual forma, se parametrizó la interfaz ORANGE asignada al segmento físico de la zona desmilitarizada (DMZ) estableciendo la dirección estática 192.168.1.15/24, bloque de ruteo perimetral que se describe en el asistente de consola de la Fig. 12.

Figura 12. Configuración de direccionamiento para la zona ORANGE.

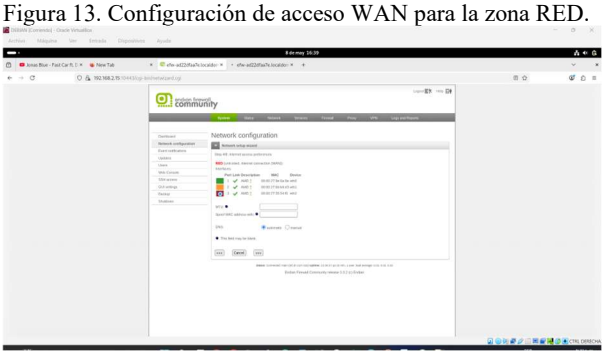


Fuente: Autoría Propia

Por último, la interfaz RED obtuvo conectividad automáticamente mediante el protocolo DHCP proporcionado por el adaptador NAT de VirtualBox para simular la salida del

cortafuegos hacia enlaces externos, ajuste completado como se visualiza en la Fig. 13.

Figura 13. Configuración de acceso WAN para la zona RED.

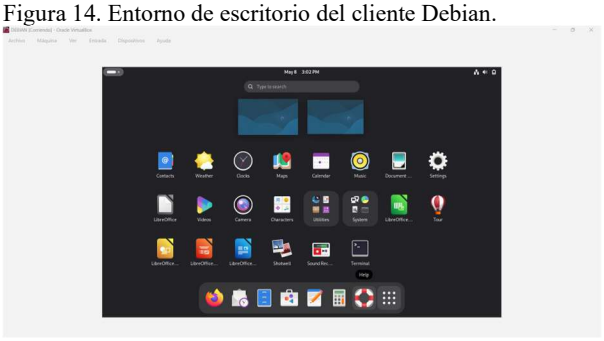


Fuente: Autoría Propia

2.1.4 CONFIGURACIÓN DEL CLIENTE DEBIAN EN LA RED LAN

Como parte del entorno de pruebas, se implementó una máquina virtual Debian destinada a funcionar como cliente dentro de la zona GREEN [3]. El sistema fue configurado con la dirección IP estática 192.168.2.20, la puerta de enlace predeterminada apuntando a Endian (192.168.2.15) y los servidores DNS públicos correspondientes, cargando de forma correcta su entorno de escritorio detallado en la Fig. 14.

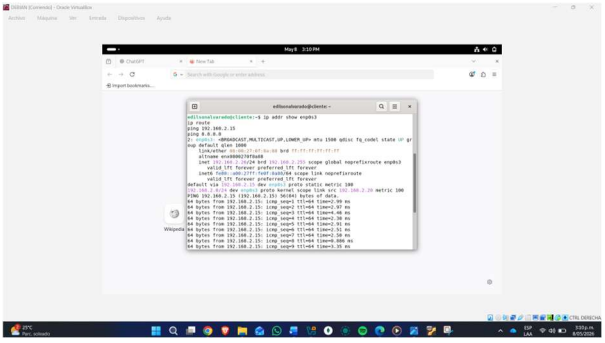
Figura 14. Entorno de escritorio del cliente Debian.



Fuente: Autoría Propia

Posteriomente, se realizaron pruebas de conectividad hacia Endian Firewall utilizando herramientas de diagnóstico de la capa de red como ping e ip addr, permitiendo validar el correcto enlace de datos y la comunicación fluida dentro de la red LAN, traza evidenciada en la Fig. 15.

Figura 15. Verificación de conectividad entre Debian y Endian Firewall.

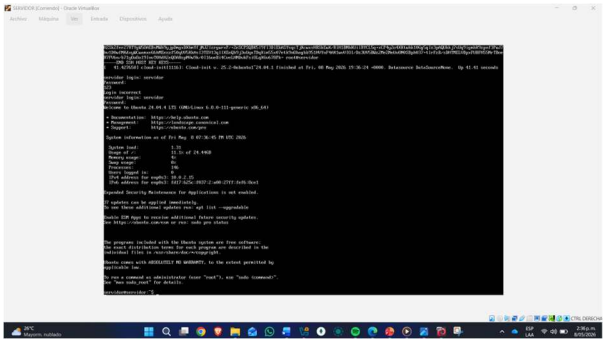


Fuente: Autoría Propia

2.1.5 CONFIGURACIÓN DEL SERVIDOR UBUNTU SERVER EN LA DMZ

Adicionalmente, se implementó un servidor basado en la distribución Ubuntu Server dentro de la zona ORANGE (DMZ) [2]. El host fue parametrizado con la dirección IP estática 192.168.1.20/24 y enlazado a la puerta de enlace perimetral del cortafuegos. El inicio de sesión y la operatividad de la consola de este servidor se exponen en la Fig. 16.

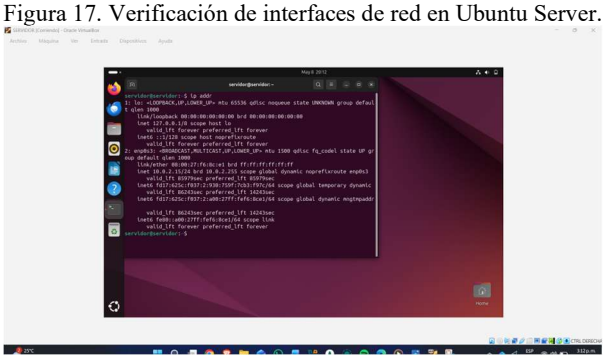
Figura 16. Inicio de sesión y estado operativo de Ubuntu Server.



Fuente: Autoría Propia

Con el propósito de verificar la correcta persistencia del direccionamiento IP y la activación de la interfaz de red asignada al hardware virtual de la DMZ, se corrieron comandos locales de red en el servidor, cuya salida técnica se detalla en la Fig. 17.

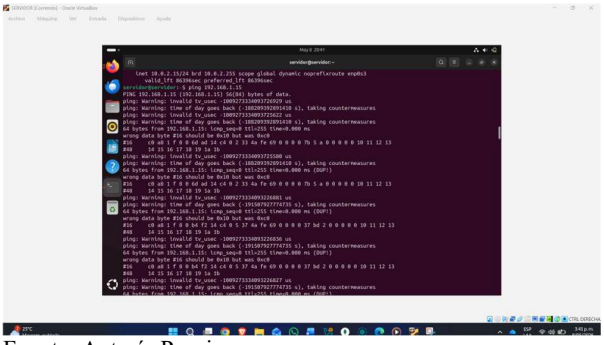
Figura 17. Verificación de interfaces de red en Ubuntu Server.



Fuente: Autoría Propia

Para finalizar la fase de enlace del servidor de aplicaciones, se procedió a realizar un test de comunicación básica ICMP desde la DMZ hacia la dirección de control del firewall naranja, obteniendo respuestas satisfactorias, como se muestra en la Fig. 18

Figura 18. Pruebas de conectividad desde la DMZ hacia el firewall.



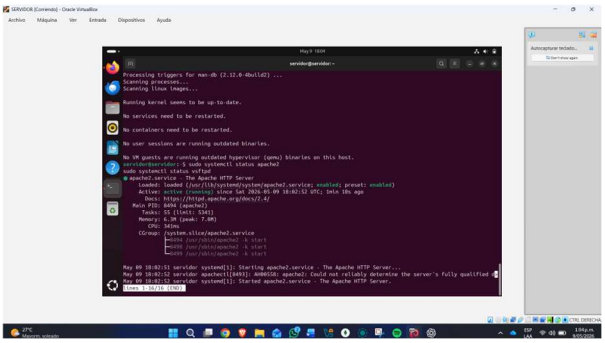
Fuente: Autoría Propia

2.1.6 IMPLEMENTACIÓN DE SERVICIOS HTTP Y FTP

Para la publicación de servicios dentro de la zona DMZ, se actualizaron inicialmente los repositorios del sistema Ubuntu Server y posteriormente se instalaron los servicios de hipertexto Apache2 [7] y de transferencia de archivos VSFTPD [8] mediante el gestor de paquetes APT, corriendo de manera exitosa los comandos de instalación sudo apt update, sudo apt install apache2 -y y sudo apt install vsftpd -y.

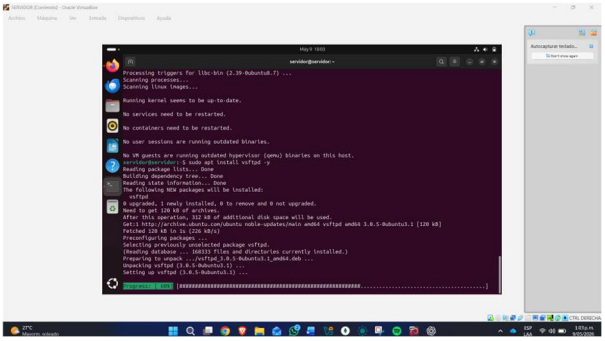
Los daemon de red fueron habilitados y verificados en el sistema mediante la herramienta de control systemctl status, confirmando su correcta ejecución y escucha en los puertos de producción TCP 80 y TCP 21, fases documentadas en las Fig. 19 y Fig. 20.

Figura 19. Verificación del servicio Apache2 en Ubuntu Server.



Fuente: Autoría Propia

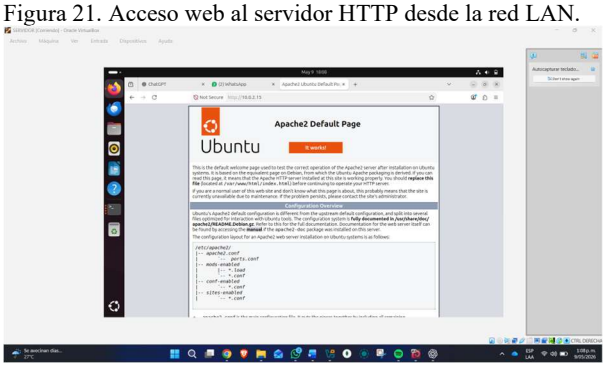
Figura 20. Verificación del servicio VSFTPD en Ubuntu Server.



Fuente: Autoría Propia

Posteriormente, desde el cliente Debian ubicado en la red LAN, se abrió el navegador web apuntando hacia la dirección IP del servidor Ubuntu de la DMZ. La visualización exitosa de la interfaz por defecto de Apache2 demuestra la conectividad inter-zona GREEN-ORANGE y se valida en la Fig. 21.

Figura 21. Acceso web al servidor HTTP desde la red LAN.



Fuente: Autoría Propia

4.1.7 ACCESO AL PANEL ADMINISTRATIVO DE ENDIAN FIREWALL

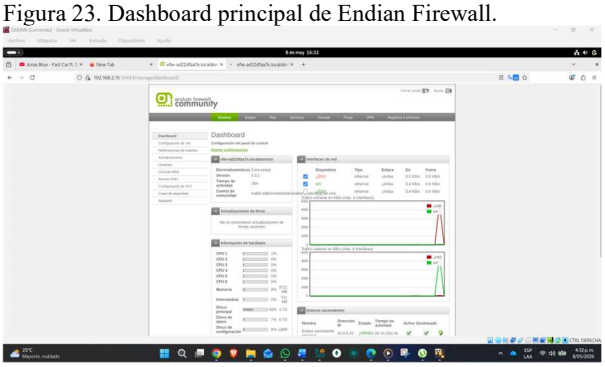
Finalmente, desde el cliente Debian se accedió al panel web administrativo de Endian Firewall mediante la URL segura HTTPS utilizando el puerto de gestión predeterminado (https://192.168.2.15:10443) [5], ingresando las credenciales de seguridad en el panel ilustrado en la Fig. 22.

Figura 22. Acceso al panel administrativo de Endian Firewall.

Fuente: Autoría Propia

El Dashboard principal permitió validar el correcto reconocimiento lógico de las tres interfaces físicas mapeadas (GREEN, RED, ORANGE), así como supervisar el rendimiento de la CPU, la memoria y el comportamiento de las políticas básicas de red, métricas analíticas descritas en la Fig. 23.

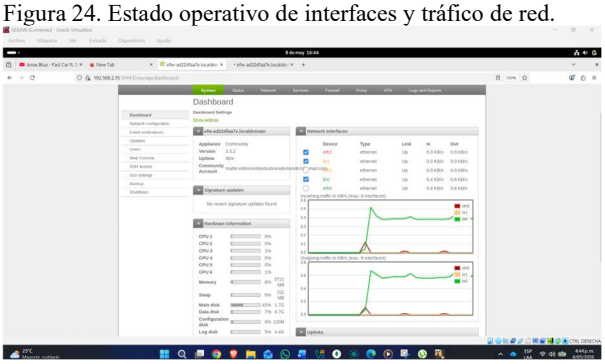
Figura 23. Dashboard principal de Endian Firewall.



Fuente: Autoría Propia

Como cierre de las validaciones de la primera temática, se extrajo el reporte gráfico de ruteo de datos del firewall, confirmando el correcto balance de cargas de entrada y salida a través de las interfaces perimetrales instaladas, aspecto detallado en la Fig. 24.

Figura 24. Estado operativo de interfaces y tráfico de red.

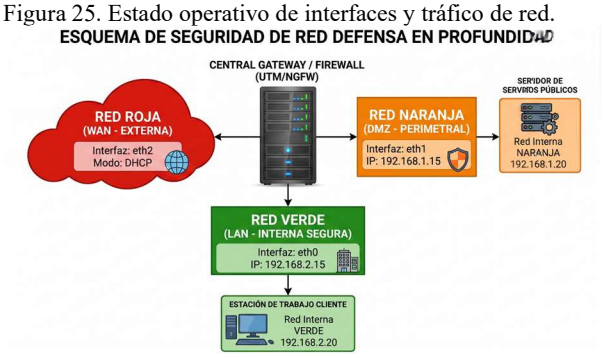


Fuente: Autoría Propia

2.2 TEMÁTICA 2: CONFIGURACIÓN NAT

Para la segunda temática de traducción de direcciones (NAT), se replicó la infraestructura base de la etapa previa, ya que las políticas de enmascaramiento requieren la interconexión estable de los segmentos. Primero, se accedió al módulo de configuración de red para verificar las interfaces. En la Fig. 25 se valida que las tarjetas físicas encuentran operativas bajo las zonas GREEN y ORANGE, y la zona RED asociada al exterior [5].

Figura 25. Estado operativo de interfaces y tráfico de red.



Fuente: Autoría Propia

2.2.1 CONFIGURACIÓN DE REDES VIRTUALES EN VIRTUALBOX

Para asegurar el buen desempeño del entorno virtual antes de enviar tráfico, se revisó el consumo de hardware en Endian [4]. Como se documenta en la Fig. 26, el Dashboard reflejó un estado óptimo en el uso de los recursos [5], mostrando una carga mínima en el procesador y espacio libre en la memoria física y de intercambio (Swap). Esto garantiza que el firewall pueda procesar el enmascaramiento del laboratorio sin problemas.

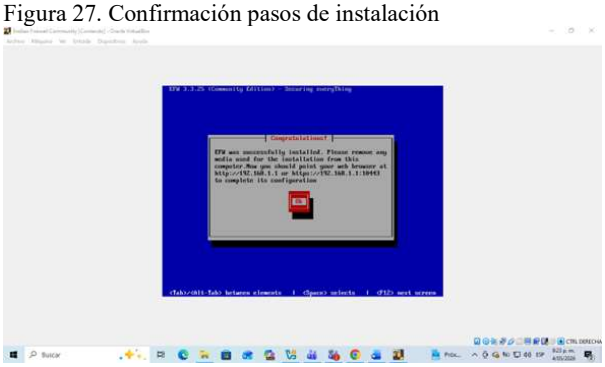
Figura 26. Configuración de redes.

Fuente: Autoría Propia

2.2.2 DESPLIEGUE OPERATIVO DE ENDIAN Y MAPEO DE DIRECCIONES DE HOSTS

Con el sistema estable, se verificó la visibilidad de los nodos de la red [4]. Se ingresó a la sección de direccionamiento estático de nombres y hosts en el panel de Endian [5]. Como se muestra en la Fig. 27, se confirmó el registro y estado activo de las direcciones IP de los servidores y estaciones del laboratorio, asegurando que las futuras directivas NAT tengan una resolución local precisa.

Figura 27. Confirmación pasos de instalación



Fuente: Autoría Propia

2.2.3 CONFIGURACIÓN DEL SERVIDOR DHCP EN LA INTERFAZ DE CONFIANZA

Para automatizar la asignación de direcciones IP a los clientes de la red local y evitar conflictos dentro de VirtualBox, se activó el servidor DHCP de Endian [4], [5]. Como se observa en la Fig. 28, se habilitó este servicio en la zona GREEN, definiendo el rango de IPs dinámicas, la puerta de enlace (192.168.2.15) y los servidores DNS. Así, todo el tráfico interno pasa obligatoriamente por el cortafuegos.

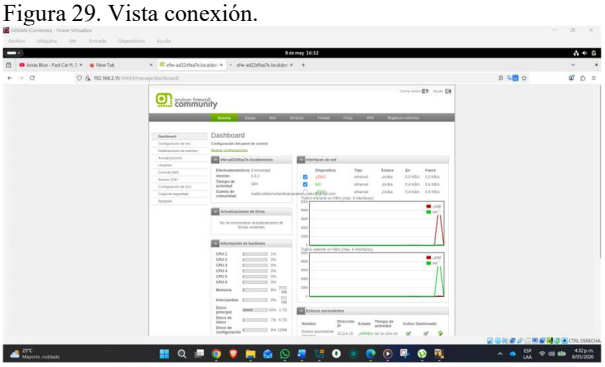
Figura 28. Configuración IP

Fuente: Autoría Propia

2.2.4 CONFIGURACIÓN DE LAPOLÍTICA GLOBAL DEL PROXY WEB EN LA CAPA DE APLICACIÓN

Para mitigar riesgos en la navegación web desde la red interna, se activó el Proxy HTTP integrado en Endian [5]. Este servicio intercepta las peticiones de los usuarios en la Capa de Aplicación [6]. Como se detalla en la Fig. 29, se habilitó en la zona GREEN en modo "Transparente", redirigiendo el tráfico del puerto 80 externo al puerto local 8080 sin necesidad de configurar manualmente los navegadores.

Figura 29. Vista conexión.

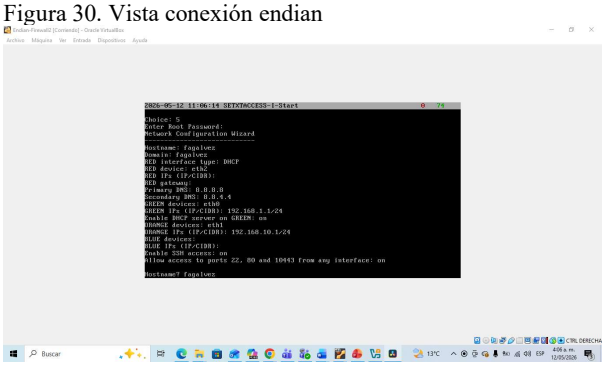


Fuente: Autoría Propia

2.2.5 CONFIGURACIÓN DE PERFILES DE FILTRADO DE URL EN EL PROXY

Para aplicar restricciones de contenido en la red, se definieron las políticas de filtrado basadas en URL [5]. Como se muestra en la Fig. 30, se ingresó al menú "URL Filter" de Endian para activar el bloqueo por categorías temáticas en la zona GREEN [9]. El panel permite además añadir listas negras (Blacklists) y listas blancas (Whitelists) personalizadas para controlar la navegación en el entorno GNU/Linux [6].

Figura 30. Vista conexión endian

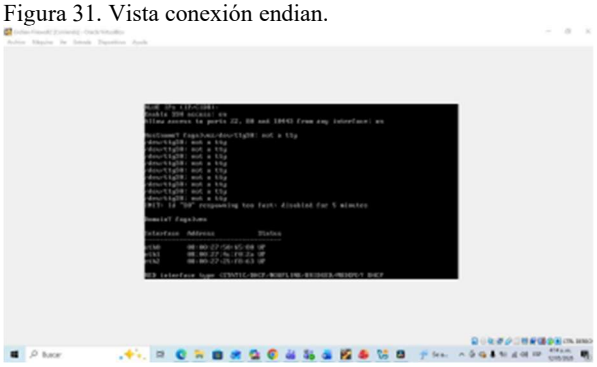


Fuente: Autoría Propia

2.2.6 CONFIGURACIÓN DE POLÍTICAS DNAT Y REENVÍO DE PUERTOS (PORT FORWARDING)

Para cerrar la Temática 2, se configuraron las reglas de traducción de destino (DNAT) para permitir el acceso externo controlado a la zona desmilitarizada (DMZ) [5], [9]. Como se ve en la Fig. 31, en la sección "Port Forwarding" se habilitaron las reglas para interceptar el tráfico de los puertos TCP 80 (HTTP) y TCP 21 (FTP), redirigiéndolos a la IP privada del servidor Ubuntu (192.168.1.20) en la zona ORANGE [5]. Esto publica los servicios de Apache2 y VSFTPD de forma segura [10].

Figura 31. Vista conexión endian.

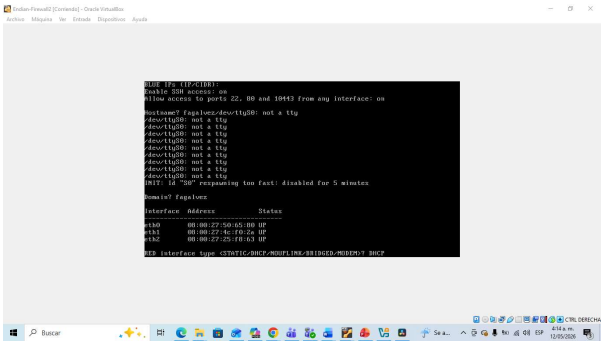


Fuente: Autoría Propia

2.2.7 CONFIGURACIÓN DE POLÍTICAS DE TRÁFICO INTER-ZON

Para complementar el control perimetral, se definieron las reglas de paso entre los segmentos lógicos de la red [5]. Como se documenta en la Fig. 32, se ingresó al panel de "Inter-Zone Traffic" en Endian para gestionar los permisos de comunicación desde la zona GREEN hacia la ORANGE (DMZ) [9]. En esta interfaz se validó el estado de las políticas que restringen el tráfico y abren los canales exclusivamente para los puertos HTTP y FTP autorizados en la práctica de laboratorio [10].

Figura 32. Panel de administración de reglas de tráfico inter-zona en End.

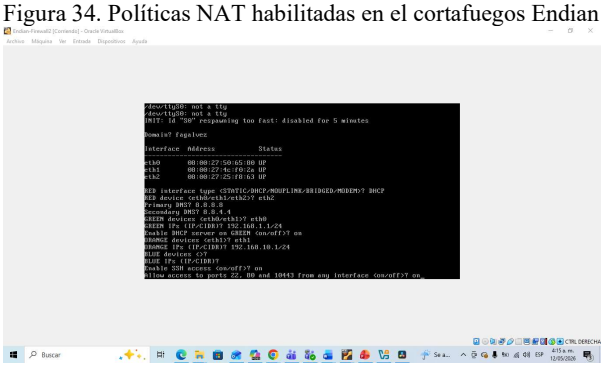


Fuente: Autoría Propia

2.2.9 VERIFICACIÓN DE REGLAS DE REENVÍO ACTIVAS EN EL MÓDULO NAT

En esta sección se detalla la comprobación visual del estado de activación de las reglas de traducción de direcciones creadas [5]. Como se observa en la Fig. 34, la tabla de "Port Forwarding" de Endian refleja la lista de políticas asignadas para el reenvío de puertos. Los indicadores de estado activos confirman que el cortafuegos mantiene las directivas de red habilitadas hacia la DMZ para la gestión del tráfico del laboratorio [10].

Figura 34. Políticas NAT habilitadas en el cortafuegos Endian



Fuente: Autoría Propia

3 CONCLUSIONES

La implementación de Endian Firewall en un entorno GNU/Linux virtualizado permitió establecer un esquema de seguridad perimetral basado en la segmentación estricta de red mediante las zonas GREEN, RED y ORANGE. Esta arquitectura facilitó el aislamiento de los servicios publicados en la zona desmilitarizada (DMZ) y fortaleció la protección de la red interna de confianza frente a vectores de acceso no autorizados, evidenciando la importancia de aplicar mecanismos de control robustos y filtrado de tráfico en infraestructuras de red distribuidas [5], [9].

La configuración de políticas de traducción de direcciones de red (NAT), reglas de firewall inter-zona y el despliegue de servicios HTTP/FTP permitió validar el funcionamiento controlado de las comunicaciones entre los diferentes segmentos de seguridad. Las pruebas de conectividad y mitigación realizadas como la restricción del protocolo ICMP y la auditoría de navegación demostraron que la aplicación de directrices de acceso y filtrado perimetral contribuye directamente a garantizar los pilares de integridad, disponibilidad y confidencialidad de los servicios implementados sobre sistemas GNU/Linux [6], [10].

4 REFERENCIAS BIBLIOGRÁFICAS

[1] LPI, “LPIC-1 Exam 101: Determinar y configurar los ajustes de hardware,” 2022. [En línea]. Disponible: https://learning.lpi.org/es/learning-materials/101-500/101/101.1/

[2] Canonical, “Guía del Ubuntu Desktop 20.04 LTS,” 2023. [En línea]. Disponible: https://help.ubuntu.com/

[3] Debian Project, “Manual del administrador de Debian 12.5.0,” 2023. [En línea]. Disponible: https://www.debian.org/releases/stable/amd64/index.es.html

[4] Oracle, “VirtualBox User Manual,” 2020. [En línea]. Disponible: https://www.virtualbox.org/manual/

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

[6] Red Hat, “Security Guide for Red Hat Enterprise Linux,” 2021. [En línea]. Disponible: https://access.redhat.com/documentation/

[7] Apache Software Foundation, “Apache HTTP Server Documentation,” 2023. [En línea]. Disponible: https://httpd.apache.org/docs/

[8] VSFTPD Project, “Very Secure FTP Daemon Documentation,” 2022. [En línea]. Disponible: https://security.appspot.com/vsftpd.html

[9] Cisco Networking Academy, “Introduction to Cybersecurity,” 2022. [En línea]. Disponible: https://www.netacad.com/

[10] W. Stallings, Network Security Essentials: Applications and Standards, 6th ed. United Kingdom: Pearson Education, 2017.