ETAPA 7 IMPLEMENTANDO SEGURIDAD EN GNU/LINUX

Jerffen Mendoza Regino - 1105687062
jmendozare@unadvirtual.edu.co
Yeferson Rodríguez Moyano – 1106951664
yrodriguezmoy@unadvirtual.edu.co

ABSTRACT: *This work developed a perimeter security infrastructure using a DMZ to protect internal and external services. Endian Firewall Community was implemented in VirtualBox, configuring LAN, DMZ and WAN networks with organized IP addressing. GNU/Linux systems were integrated and NAT rules were validated, preparing the environment for future security and service-control configurations.*

RESUMEN: *En este trabajo se desarrolló una infraestructura de seguridad perimetral utilizando una zona DMZ para resguardar servicios internos y externos. Se implementó Endian Firewall Community en VirtualBox, configurando redes LAN, DMZ y WAN con direccionamiento IP organizado. Además, se integraron equipos GNU/Linux y se verificó el correcto funcionamiento de las reglas NAT, preparando el entorno para futuras configuraciones de seguridad y control de servicios.*

PALABRAS CLAVE: Endian Firewall, NAT, GNU/Linux, DMZ, LAN.

1 INTRODUCCIÓN

La protección perimetral es fundamental para resguardar redes empresariales y académicas, permitiendo separar servicios internos y externos mediante distintos niveles de seguridad. Una técnica común es el uso de una DMZ, donde se ubican servidores accesibles desde otras redes sin exponer la LAN. En este proyecto se implementó una arquitectura con Endian Firewall Community en VirtualBox, configurando las zonas GREEN, ORANGE y RED junto con equipos GNU/Linux. También se aplicaron reglas NAT y de tráfico para controlar el acceso a Internet y la comunicación entre segmentos, comprobando su funcionamiento mediante pruebas de conectividad y servicios.

2 TEMÁTICAS

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

Para comenzar la implementación de la seguridad perimetral, se descargó Endian Firewall Community y posteriormente se creó una máquina virtual en VirtualBox. Durante la configuración se definieron parámetros básicos como el nombre de la máquina, el tipo de sistema operativo

Linux y la versión adecuada, preparando el entorno necesario para instalar y ejecutar el firewall.

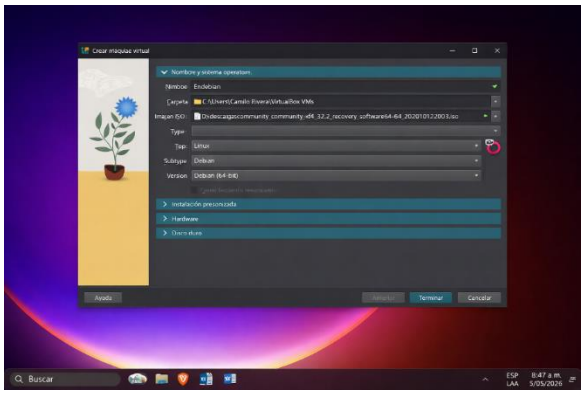

Fig. 1 asignación de nombre y sistema operativo en VirtualBox. Fuente: Autoría Propia

Posteriormente, en la sección de hardware de VirtualBox, se configuraron los recursos destinados a la máquina virtual. Se asignaron 3072 MB de memoria RAM y un procesador del equipo anfitrión, asegurando un funcionamiento estable del sistema. Esta etapa resulta importante porque define la capacidad operativa que tendrá el firewall virtual antes de continuar con la creación y configuración del almacenamiento del entorno.

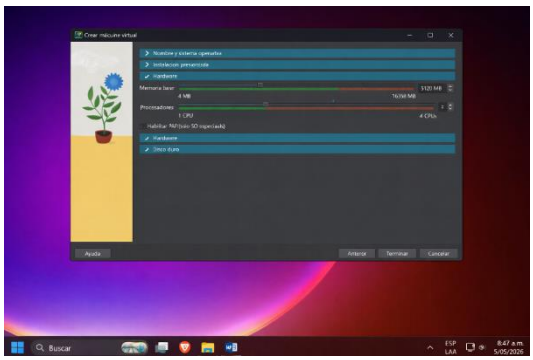

Fig. 2 Se agrega la memoria RAM en VirtualBox.
Fuente: Autoría Propia

Después, en el apartado de almacenamiento de VirtualBox, se vinculó la imagen ISO descargada al controlador IDE como unidad óptica secundaria. Con esta configuración, la máquina virtual puede iniciar directamente desde el archivo de instalación del sistema operativo. Este procedimiento es indispensable para comenzar correctamente el proceso de instalación y despliegue del firewall sobre el disco duro virtual creado previamente.

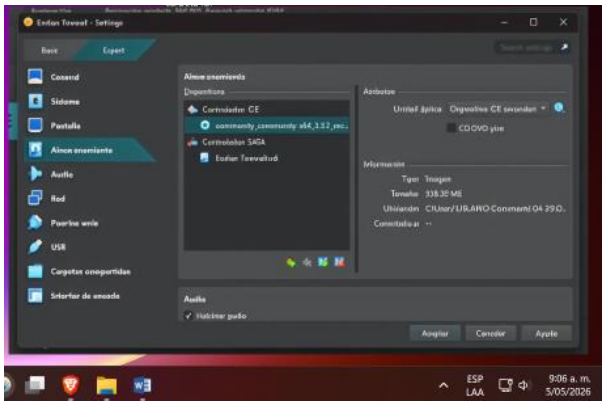

Fig. 3 Instalación de la OS ENDIAN. Ejemplo para todas las figuras. Fuente: Autoría Propia

Zona de Red	Descripción	Dirección IP / Máscara de Subred	Tipo de Conexión
GREEN (LAN)	Red de Área Local	192.168.0.15/24	Fija/Estática
ORANGE (DMZ)	Zona Desmilitarizada	192.168.20.1/24	Fija/Estática
RED (WAN)	Red de Área Extensa	Definida por DHCP	Dinámica

Tabla 1. Fuente: Autoría Propia

Durante la instalación se configuraron los datos de red correspondientes a la interfaz GREEN, destinada a la red interna. Se asignó la dirección IP estática 192.168.0.15 junto con la máscara 255.255.255.0, permitiendo identificar correctamente el segmento local. Esta etapa es importante porque establece la base de comunicación y segmentación que utilizará el firewall dentro de la infraestructura de red.

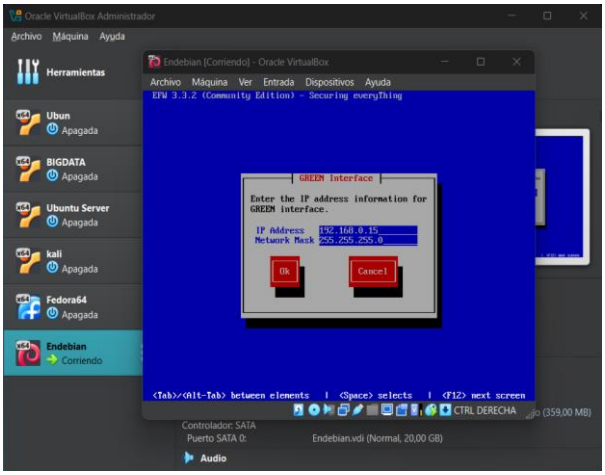

Fig. 4 Direccionamiento IP estático para la máquina virtual.
Fuente: Autoría Propia

La ventana indica que la instalación se completó correctamente y muestra la configuración activa de la zona GREEN con la dirección IP 192.168.0.15. También se presenta la dirección de acceso a la administración web del firewall. Desde este panel es posible ingresar a la terminal, modificar credenciales o ejecutar nuevamente las opciones de configuración de red del sistema.

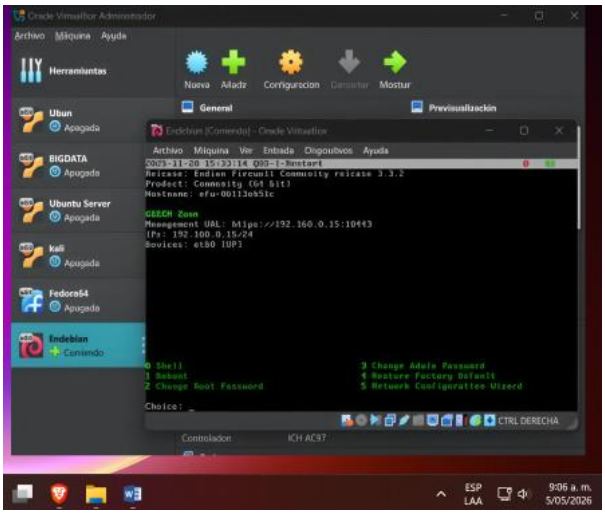

Fig. 5 Consola de gestión inicial del firewall instalado. Fuente: Autoría Propia

Posteriormente, se revisó el resumen general de la configuración para comprobar los parámetros establecidos en el firewall. Se verificó que la interfaz RED obtuviera conexión mediante DHCP, además de validar los DNS configurados y las direcciones IP asignadas a las zonas GREEN y ORANGE. Finalmente, se aplicaron los cambios para dejar activa la arquitectura de red implementada.

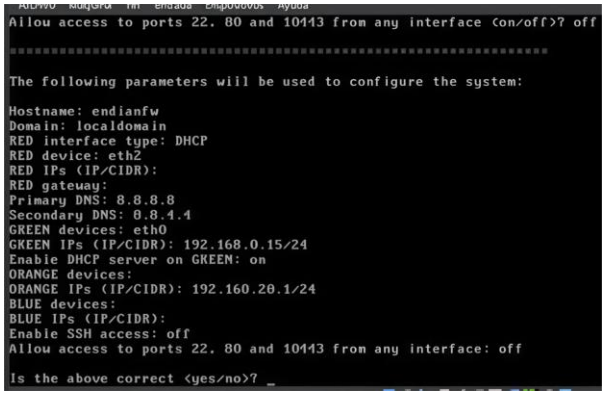

Fig. 6 Validación y resumen de las IPs de red. Fuente: Autoría Propia

Después de aplicar la configuración, se realizó una verificación desde la consola del sistema para comprobar el estado de las interfaces de red. Durante la revisión se confirmó que las interfaces br0 y br1 estaban activas y funcionando correctamente. Asimismo, se validó la asignación adecuada de las direcciones IP correspondientes a las zonas GREEN y ORANGE, asegurando que la topología de red implementada quedó operativa y configurada de manera exitosa.

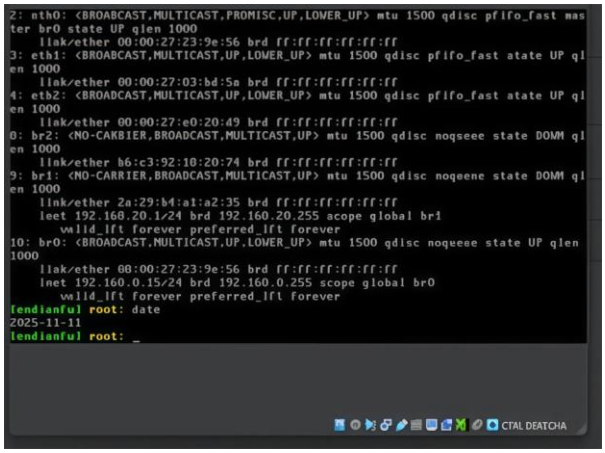

Fig. 7 Evidencia de configuración
. Fuente: Autoría Propia

3 TEMÁTICA 2: CONFIGURACIÓN NAT

El propósito de esta etapa consiste en comprobar el funcionamiento de la configuración NAT dentro de Endian. Para ello, se habilita la comunicación de las redes LAN y DMZ hacia la WAN, garantizando el acceso controlado a redes externas. Al mismo tiempo, se conserva la separación y protección entre los distintos segmentos de la infraestructura implementada.

3.1 CONFIGURACIÓN DE LA RED LAN (GREEN)

La estación de trabajo Ubuntu Desktop fue configurada con una IP estática perteneciente a la zona GREEN:

- IP: 192.168.0.20
- Máscara: 255.255.255.0
- Gateway: 192.168.0.15 (interfaz GREEN de Endian)
- DNS: 8.8.8.8

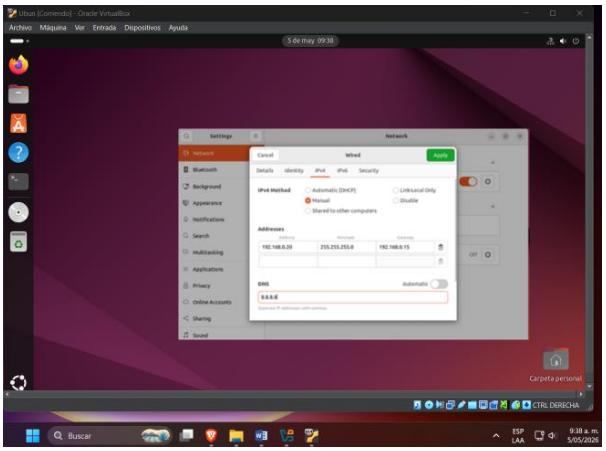

Fig. 8 Configuración de red Desktop. Fuente: Autoría Propia

Verificamos la conectividad al firewall ejecutando el comando ping 192.168.0.15

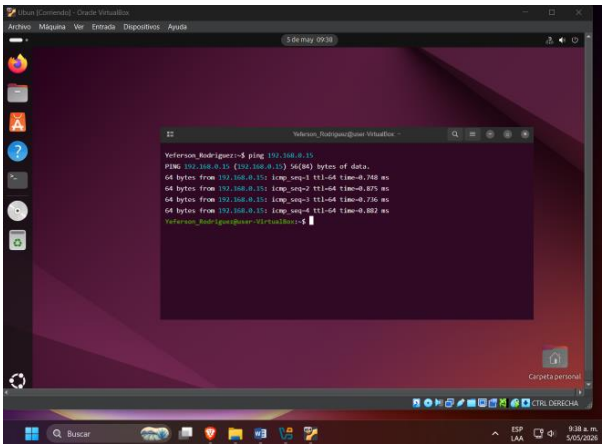

Fig. 9 Verificación de conectividad hacia el firewall. Fuente: Autoría Propia

3.2 Configuración de la red DMZ (ORANGE)

El servidor Ubuntu Server asignado como DMZ se configuró con:

- IP: 192.168.20.10
- Máscara: 255.255.255.0
- Gateway: 192.168.20.1 (interfaz ORANGE de Endian)
- DNS: 8.8.8.8

Como lo podemos evidenciar en la figura 10

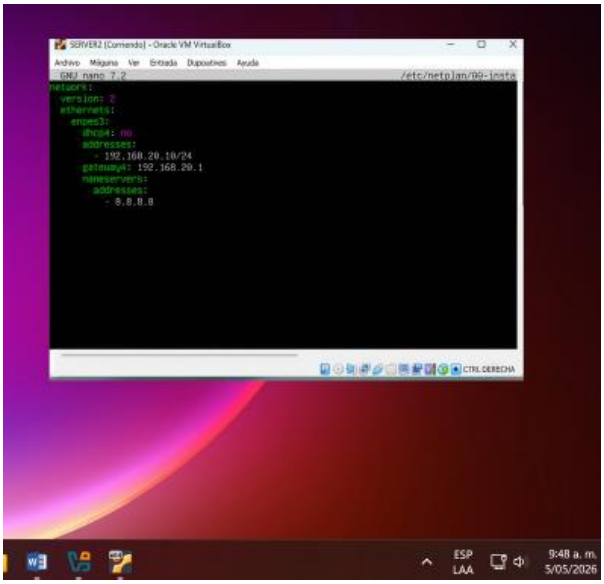

Fig. 10 Configuración de red server. Fuente: Autoría Propia

3.3 VERIFICACIÓN DE NAT (SNAT / MASQUERADE)

Endian genera automáticamente una regla de NAT para todas las zonas internas, esta regla se verificó desde el apartado Firewall → Port forwarding / NAT → Show system rules

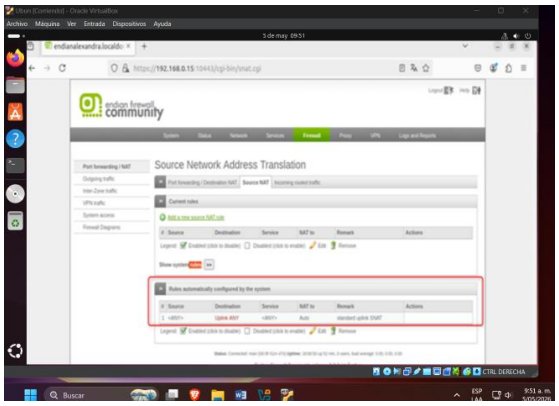

Fig. 12 Regla NAT. Fuente: Autoría Propia

3.4 REGLAS DE SALIDA DESDE LA DMZ HACIA INTERNET

Como seguridad predeterminada, la DMZ no tiene acceso HTTP/HTTPS a la WAN, por lo que se crearon reglas en el apartado Firewall → Outgoing traffic

Reglas creadas:
ORANGE → RED → HTTP (ALLOW)
ORANGE → RED → HTTPS (ALLOW)

Esto habilita la navegación y actualización del servidor DMZ.

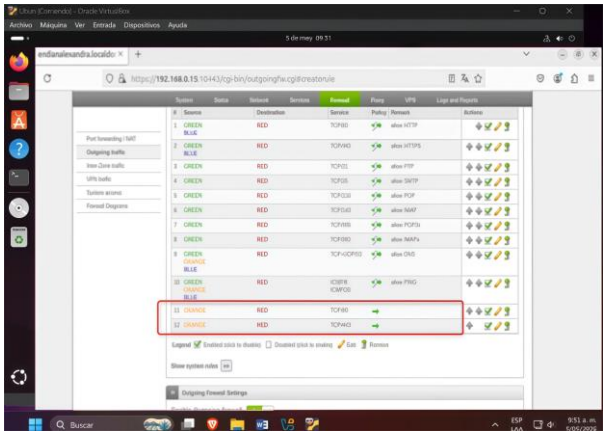

Fig. 13 Reglas de salida. Fuente: Autoría Propia

3.5 PRUEBAS DE CONECTIVIDAD

Verificamos la conexión de NAT desde LAN (Desktop), donde se evidencia a continuación de manera satisfactoria

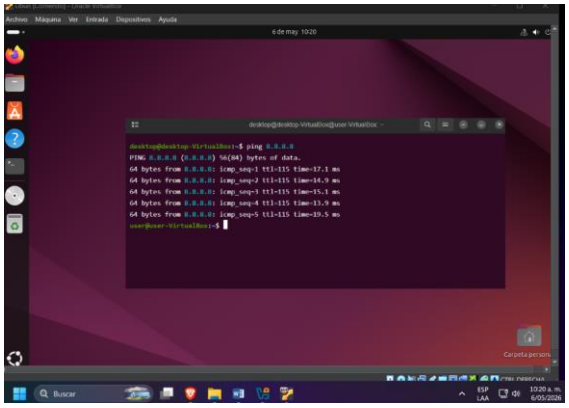

Fig. 14 Conexión por ip. Fuente: Autoría Propia

Se verificó la conexión con ping a www.google.com, confirmando que la LAN resuelve DNS y accede a Internet correctamente, garantizando navegación completa y comunicación efectiva en la red.

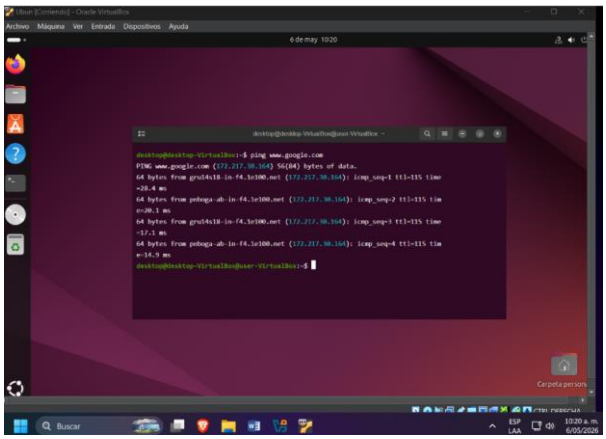

Fig. 15 Conexión por URL. Fuente: Autoría Propia

Probamos la conexión a internet desde el DMZ (SERVER2) ejecutando el comando ping 8.8.8.8 a continuación podemos ver que NAT funciona para DMZ.

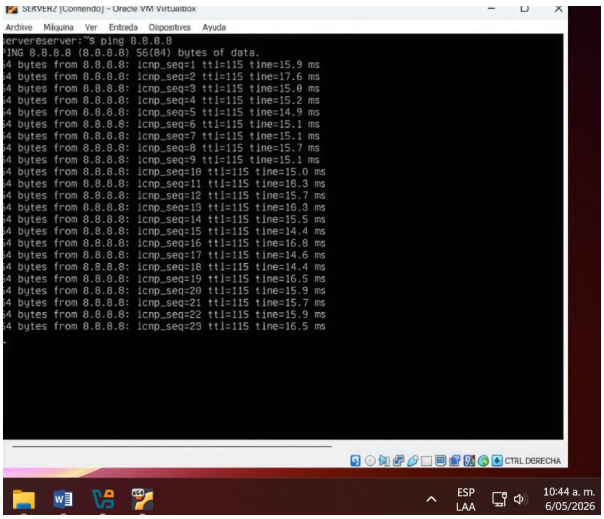

Fig. 16 Conexión por ip. Fuente: Autoría Propia

Se ejecutó ping a www.google.com desde la DMZ, evidenciando que el servidor alcanza el firewall, este permite el tráfico y la conexión hacia Internet funciona correctamente.

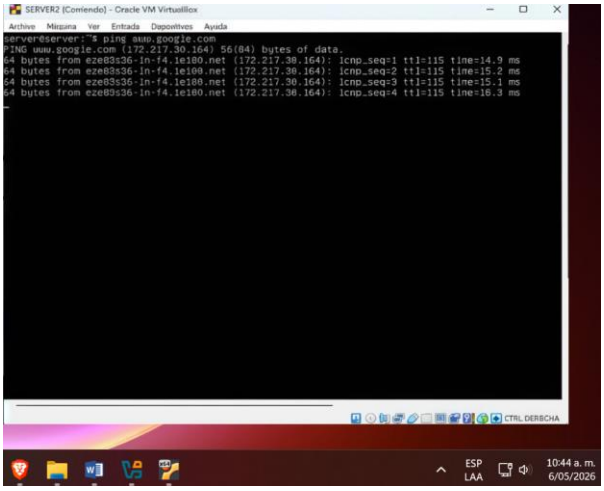

Fig. 17 Conexión por URL. Fuente: Autoría Propia

Se ejecutó el comando sudo systemctl status apache2 para comprobar el estado del servicio, evidenciando que Apache se encuentra activo y funcionando correctamente en el sistema.

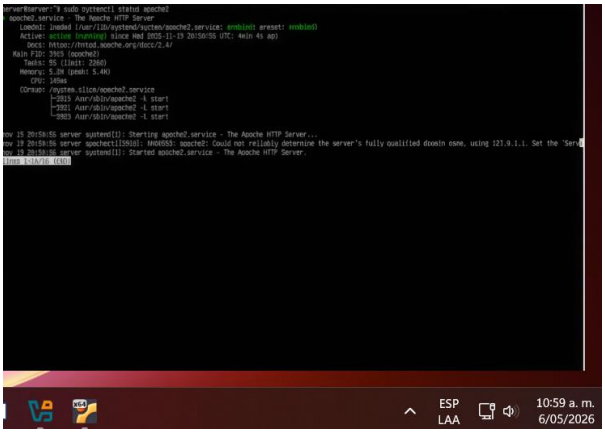

Fig. 18 Conexión con sudo apt. Fuente: Autoría Propia

Con el fin de comprobar la conectividad entre la LAN y la DMZ, se accedió desde el navegador del equipo Desktop a la dirección http://192.168.20.10 . La visualización correcta de la página predeterminada de Apache confirmó que el servidor alojado en la DMZ podía ser alcanzado desde la red interna, demostrando el adecuado funcionamiento de la infraestructura implementada.

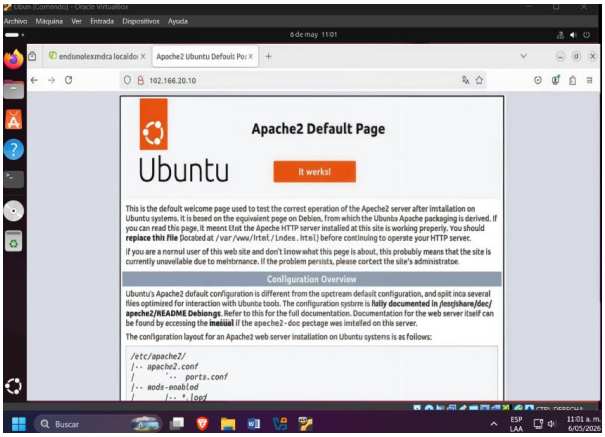

Fig. 20 Ejecución de apache en Desktop. Fuente: Autoría Propia

4 CONCLUSIONES

4.1 TEMÁTICA 1

La implementación de Endian Firewall Community en VirtualBox fue completada satisfactoriamente, logrando establecer una arquitectura de seguridad segmentada y funcional. Se configuraron correctamente las zonas GREEN para la red local, ORANGE para la DMZ y RED para la conexión externa mediante DHCP. Posteriormente, se realizaron pruebas de conectividad y validación de interfaces, comprobando la correcta comunicación entre los distintos segmentos de red. Los resultados obtenidos evidencian que el firewall opera de manera adecuada, dejando preparada la infraestructura para futuras configuraciones de seguridad, control de acceso y administración de servicios.

4.2 TEMÁTICA 2

La práctica permitió validar la correcta operación de las funciones NAT en Endian Firewall Community para las zonas GREEN y ORANGE. Mediante diferentes pruebas se confirmó que ambas redes lograron establecer conexión con la WAN, permitiendo acceso controlado a Internet. Asimismo, se comprobó el funcionamiento del enmascaramiento automático del tráfico saliente, garantizando una comunicación segura. La segmentación entre la LAN y la DMZ permaneció protegida, manteniendo el aislamiento requerido en una arquitectura perimetral. Finalmente, se verificó que el servidor web ubicado en la DMZ era accesible tanto desde la red interna como desde la red externa.

5 REFERENCIAS

[1] G. Obregón-Pulido, B. Castillo-Toledo and A. Loukianov, *"A globally convergent estimator for n frequencies"*, IEEE Trans. On Aut. Control. Vol. 47. No 5. pp 857-863. May 2002.

[2] H. Khalil, *"Nonlinear Systems"*, 2nd. ed., Prentice Hall, NJ, pp. 50-56, 1996.

[3] Francis. B. A. and W. M. Wonham, *"The internal model principle of control theory"*, Automatica. Vol. 12. pp. 457-465. 1976.

[4] E. H. Miller, *"A note on reflector arrays"*, IEEE Trans. Antennas Propagat., Aceptado para su publicación.

[5] *Control Toolbox* (6.0), User´s Guide, The Math Works, 2001, pp. 2-10-2-35.

[6] J. Jones. (2007, Febrero 6). Networks (2nd ed.) [En línea]. Disponible en: http://www.atm.com.