Implementación de seguridad perimetral en GNU/Linux mediante Endian Firewall, segmentación DMZ, NAT y proxy HTTP autenticado

Manuel Alexis Mosquera Amézquita
email: mamosqueraam@unadvirtual.edu.co
Universidad Nacional Abierta y a Distancia - UNAD

RESUMEN: Este artículo presenta la implementación de un laboratorio académico de seguridad perimetral en GNU/Linux mediante Endian Firewall Community. El escenario se diseñó para segmentar una infraestructura virtualizada en tres zonas de red: LAN o zona verde, WAN o zona roja y DMZ o zona naranja. Sobre esta arquitectura se configuraron reglas de salida, reglas de acceso entre zonas, traducción de direcciones, servicios HTTP y FTP en un servidor Ubuntu Server ubicado en la DMZ, bloqueo del protocolo ICMP y un proxy HTTP no transparente con autenticación de usuario y lista negra de sitios web. La validación se realizó mediante pruebas de conectividad desde consola, acceso a servicios por navegador o terminal, revisión del estado de servicios con systemctl y verificación de políticas aplicadas en Endian. Los resultados evidencian que la segmentación por zonas permite controlar el tráfico entre clientes, servidores y salida a Internet, mientras que el proxy autenticado permite aplicar restricciones de navegación sin bloquear completamente el acceso a la red. La práctica fortalece competencias de administración GNU/Linux, virtualización, redes, firewall perimetral y documentación técnica replicable.

Index Terms—Endian Firewall, GNU/Linux, DMZ, NAT, HTTP proxy, perimeter security, VirtualBox.

I. INTRODUCCIÓN

La seguridad perimetral es un componente fundamental en la administración de infraestructuras de red, debido a que permite controlar el tráfico entre redes internas, servicios publicados y conexiones externas. Cuando los servidores se exponen sin una segmentación adecuada, aumenta el riesgo de accesos no autorizados, fallas de disponibilidad y afectaciones sobre la integridad de las aplicaciones y bases de datos. Por esta razón, el uso de firewalls, reglas de acceso, NAT y zonas desmilitarizadas constituye una práctica esencial en escenarios GNU/Linux y en procesos de administración de sistemas abiertos [1].

La guía de la Etapa 7 plantea la necesidad de proteger servidores de una intranet y una extranet mediante la delimitación de una zona DMZ. En respuesta a este contexto, se implementó Endian Firewall como plataforma de seguridad perimetral, conectando una red interna de clientes, una salida simulada hacia Internet y una zona de servidores. El objetivo del laboratorio fue comprobar, mediante evidencias técnicas, que el tráfico entre las zonas puede ser permitido o denegado de manera controlada según los servicios requeridos.

El desarrollo se orientó a la configuración de las temáticas solicitadas: instalación y preparación de Endian Firewall con zonas verde, roja y naranja; configuración NAT; publicación de servicios HTTP y FTP desde la DMZ; reglas de acceso entre zonas; y aplicación de un proxy HTTP no transparente con autenticación y lista negra. El artículo resume el procedimiento técnico y presenta los resultados obtenidos con enfoque de capacitación, de forma que el laboratorio pueda ser comprendido y replicado en otros escenarios académicos.

II. REFERENTES TÉCNICOS

Los conceptos de administración GNU/Linux, servicios, virtualización y seguridad perimetral utilizados en el laboratorio se apoyan en materiales técnicos de LPI, documentación oficial de Ubuntu Server, Debian, Oracle VirtualBox y Endian Firewall [1], [2], [3], [4], [5].

A. Seguridad perimetral, firewall y zonas de red

Un firewall perimetral actúa como punto de control entre diferentes segmentos de red. En este laboratorio, Endian Firewall se utilizó para separar la zona verde, correspondiente a la LAN o red interna de confianza; la zona roja, correspondiente a la WAN o salida hacia Internet; y la zona naranja, correspondiente a la DMZ donde se alojan los servidores publicados. Esta separación reduce la exposición de los servicios y permite aplicar reglas específicas para cada flujo de comunicación.

B. NAT, servicios y proxy HTTP

NAT permite traducir direcciones privadas para habilitar la comunicación hacia redes externas. En la práctica se validó la salida desde LAN hacia WAN y desde DMZ hacia WAN. Los servicios HTTP y FTP se implementaron en Ubuntu Server para comprobar la publicación controlada de servicios en la DMZ. Adicionalmente, el proxy HTTP no transparente permitió exigir configuración explícita en el navegador del cliente, autenticar usuarios y aplicar una lista negra de sitios web.

III. METODOLOGÍA Y ARQUITECTURA DEL LABORATORIO

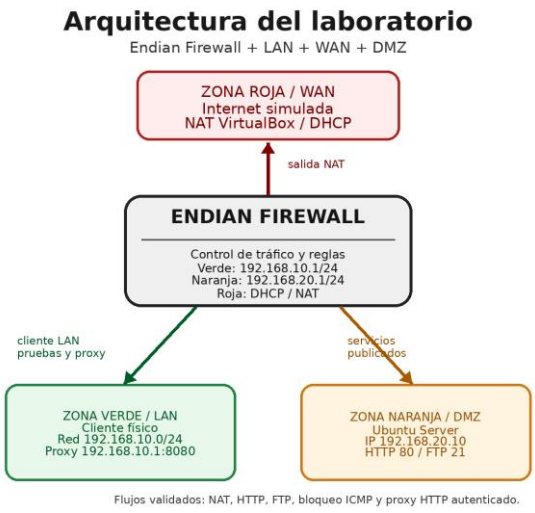
La práctica se desarrolló en un entorno virtualizado con Oracle VM VirtualBox, utilizado como plataforma para construir las máquinas virtuales y simular las zonas de red del

laboratorio [4]. Se utilizaron dos máquinas virtuales: una instancia de Endian Firewall Community como firewall perimetral y un servidor Ubuntu Server LTS ubicado en la zona DMZ. El equipo físico actuó como cliente de la LAN para acceder al panel web de Endian, ejecutar pruebas desde navegador, usar terminal de Windows y validar conectividad hacia los servicios publicados.

La máquina virtual de Endian se configuró con tres adaptadores: el adaptador 1 como NAT para representar la zona roja o WAN, el adaptador 2 como adaptador solo-anfitrión para la zona verde o LAN, y el adaptador 3 como red interna denominada dmz-net para conectar el servidor Ubuntu Server en la DMZ.

Desde el punto de vista de la arquitectura, Endian Firewall no se utilizó únicamente como un router virtual, sino como el punto central de decisión entre las tres zonas. La zona verde concentró el acceso del cliente LAN y el proxy HTTP; la zona naranja aisló el servidor Ubuntu Server que publicó HTTP y FTP; y la zona roja representó la salida externa mediante NAT de VirtualBox. Esta separación permitió comprobar que cada flujo de tráfico debía pasar por reglas explícitas antes de ser permitido o denegado.

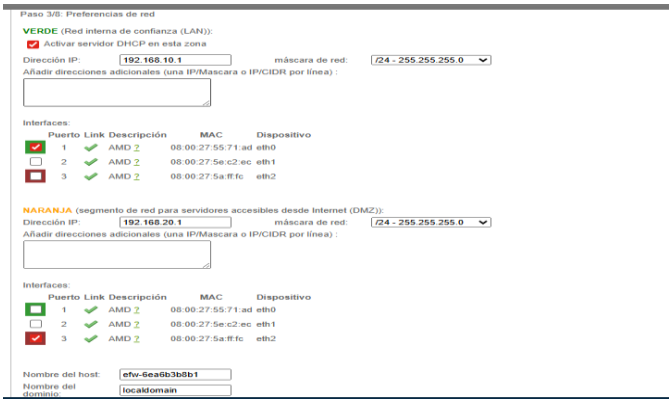
Fig. 1. Arquitectura lógica del laboratorio implementado con Endian Firewall.



Fuente: Elaboración propia

La figura anterior resume el modelo usado para la capacitación: primero se define el direccionamiento, después se validan las interfaces de Endian y finalmente se prueban los servicios desde el cliente LAN hacia la DMZ y hacia la salida externa. Esta lectura evita confundir las zonas de red con protocolos y facilita que nuevos estudiantes repliquen el laboratorio de manera ordenada.

Fig. 2. Configuración de interfaces y zonas del laboratorio.



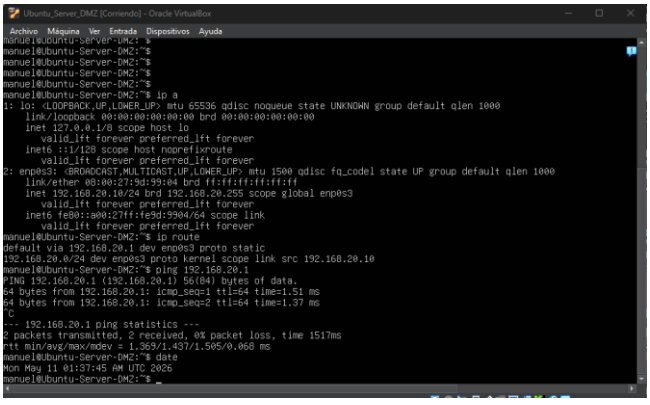
Fuente: Elaboración propia

El direccionamiento empleado en el laboratorio se mantuvo así: zona verde/LAN con red 192.168.10.0/24 y puerta de enlace Endian 192.168.10.1; zona roja/WAN con salida simulada mediante NAT de VirtualBox y asignación por DHCP; zona naranja/DMZ con red 192.168.20.0/24 y puerta de enlace Endian 192.168.20.1; y servidor Ubuntu con IP 192.168.20.10 para los servicios HTTP y FTP.

La preparación del servidor DMZ se validó con los comandos ip a, ip route y ping hacia la puerta de enlace 192.168.20.1. La evidencia mostró la dirección 192.168.20.10/24 asignada a la interfaz del servidor y una ruta por defecto hacia 192.168.20.1, lo que confirma la integración del servidor con la zona naranja.

En este diseño, la dirección 192.168.20.10 no representa un equipo cliente, sino el servidor publicado en la DMZ. Por esa razón, las pruebas HTTP y FTP se realizaron hacia esta dirección, mientras que la administración de reglas se efectuó desde Endian y las validaciones de navegación se realizaron desde la LAN.

Fig. 3. Servidor Ubuntu Server conectado a la red DMZ.



Fuente: Elaboración propia

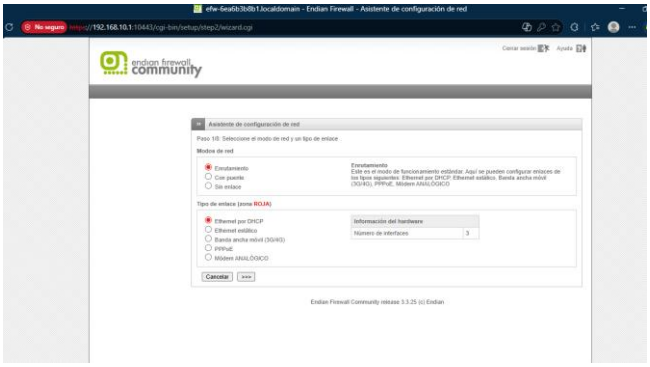
IV. IMPLEMENTACIÓN Y RESULTADOS POR TEMÁTICA

A. Configuración de Endian Firewall en VirtualBox

La primera temática consistió en instalar y configurar Endian Firewall como plataforma principal de seguridad, tomando como referencia la documentación oficial de Endian UTM para la administración de zonas, interfaces y reglas de filtrado [5]. Se descargó la imagen ISO desde el sitio oficial, se creó una máquina virtual dedicada y se configuraron las interfaces necesarias para representar las zonas solicitadas. Durante la instalación se definió la zona verde con la dirección 192.168.10.1/24, lo que permitió acceder posteriormente al panel administrativo desde el cliente LAN.

En la configuración final se habilitó la zona roja mediante Ethernet por DHCP, compatible con el adaptador NAT de VirtualBox, y se activó la zona naranja con la dirección 192.168.20.1/24. Esta configuración dejó disponible el esquema de segmentación requerido para controlar el tráfico entre LAN, WAN y DMZ.

Fig. 4. Acceso al panel administrativo de Endian Firewall.

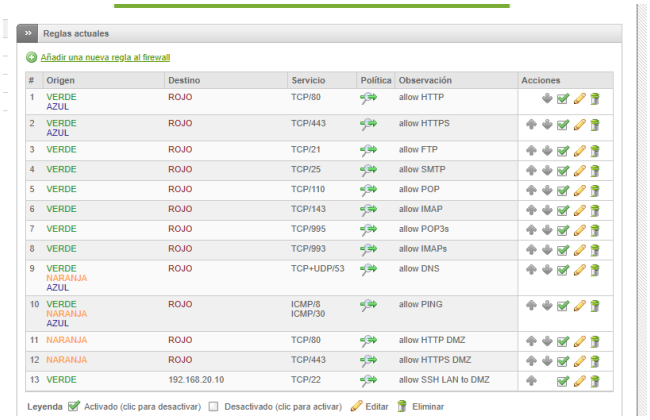


Fuente: Elaboración propia

B. Configuración NAT y salida controlada a Internet

La segunda temática se orientó a permitir comunicación desde la LAN hacia la WAN y desde la DMZ hacia la WAN. En Endian se configuraron reglas de salida para permitir servicios como HTTP, HTTPS, DNS, FTP e ICMP, de acuerdo con el flujo requerido en las pruebas. La evidencia de reglas muestra tráfico permitido desde las zonas verde y naranja hacia la zona roja, así como reglas adicionales para salida HTTP y HTTPS desde la DMZ.

Fig. 5. Reglas de salida configuradas en Endian Firewall.



Fuente: Elaboración propia

La validación se realizó con pruebas desde el cliente LAN y desde el servidor Ubuntu Server. En el cliente LAN se ejecutó ping hacia 8.8.8.8 con respuesta exitosa. Desde Ubuntu Server en la DMZ se ejecutó ping hacia 8.8.8.8 y curl hacia example.com, obteniendo respuesta HTTP. Estos resultados evidencian que las zonas internas lograron salida controlada hacia la red externa simulada.

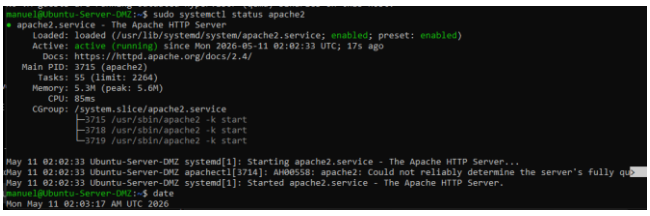
Fig. 6. Validación de salida desde la DMZ hacia la WAN.

Fuente: Elaboración propia

C. Servicios HTTP y FTP en la zona DMZ

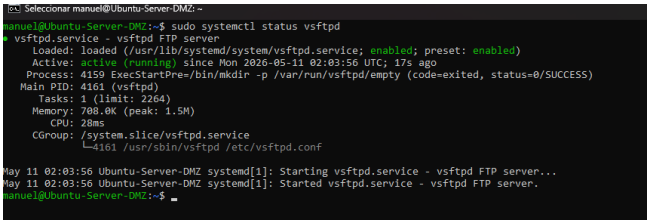
La tercera temática consistió en permitir servicios desde la zona DMZ. Para ello, en Ubuntu Server se instalaron y validaron los servicios Apache HTTP Server y vsftpd. El estado de Apache se verificó con sudo systemctl status apache2, observando el servicio activo y habilitado. De igual forma, el servicio FTP se verificó con sudo systemctl status vsftpd, evidenciando que se encontraba activo y en ejecución.

Fig. 7. Servicio Apache activo en el servidor DMZ.



Fuente: Elaboración propia

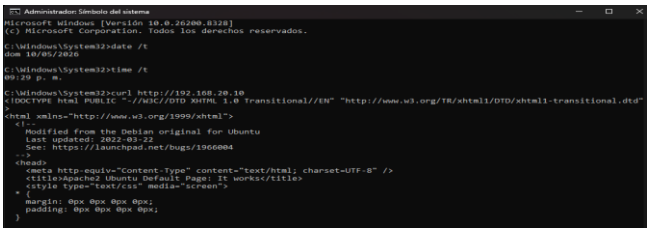
Fig. 8. Servicio FTP activo en el servidor DMZ.



Fuente: Elaboración propia

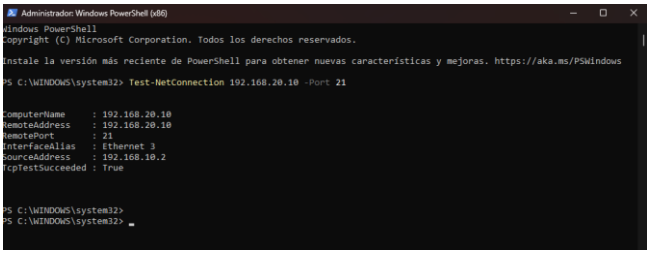
Después de habilitar los servicios, se crearon reglas de firewall para permitir acceso HTTP por el puerto TCP 80 y FTP por el puerto TCP 21 hacia la dirección 192.168.20.10. Las pruebas desde el cliente LAN validaron el acceso al servicio HTTP mediante curl y la conectividad al puerto 21 mediante Test-NetConnection, con resultado TcpTestSucceeded igual a True.

Fig. 9. Validación HTTP desde LAN hacia DMZ.



Fuente: Elaboración propia

Fig. 10. Validación FTP desde LAN hacia DMZ.

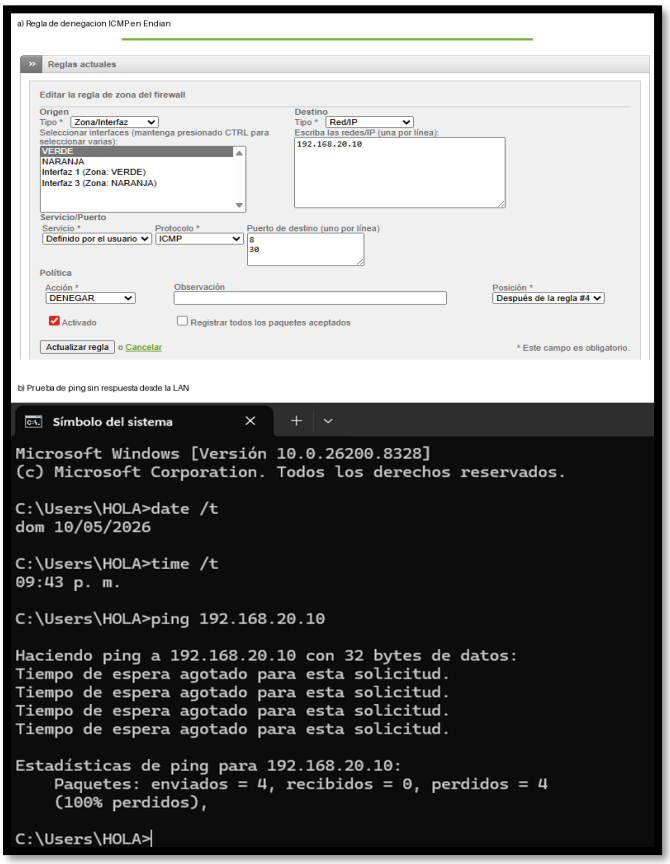


Fuente: Elaboración propia

D. Bloqueo del protocolo ICMP

Como complemento de la publicación de servicios, se implementó una regla para denegar ICMP hacia el servidor DMZ. Aunque ICMP no opera mediante puertos TCP o UDP, en el escenario se documentó el bloqueo del protocolo de acuerdo con la directriz de la actividad. La prueba desde el cliente LAN hacia 192.168.20.10 mostró tiempo de espera agotado y pérdida del 100 % de los paquetes, confirmando que la regla impidió la respuesta al comando ping.

Fig. 11. Bloqueo de ICMP hacia el servidor ubicado en DMZ.



Fuente: Elaboración propia

E. Reglas de acceso entre zonas

La cuarta temática se centró en permitir o denegar tráfico específico entre zonas. Se configuraron reglas para comunicar la zona verde con la zona naranja mediante HTTP y FTP, además de reglas de salida hacia la zona roja. Las evidencias permiten observar reglas inter-zona y pruebas de acceso HTTP desde LAN hacia DMZ, navegación HTTP desde LAN hacia WAN y comunicación HTTP desde DMZ hacia WAN. El control por servicio y destino permite que el firewall no actúe como un puente abierto, sino como un punto de decisión para cada flujo.

Fig. 12. Reglas de acceso entre zonas.

Fuente: Elaboración propia

En síntesis, la implementación validó la configuración de zonas, la salida controlada hacia Internet, la publicación de servicios HTTP y FTP en la DMZ, el bloqueo de ICMP y el control de tráfico inter-zona mediante reglas específicas. Estos resultados confirman que el firewall puede operar como punto central de control para servicios, protocolos y destinos definidos dentro del laboratorio.

F. Proxy HTTP no transparente con autenticación

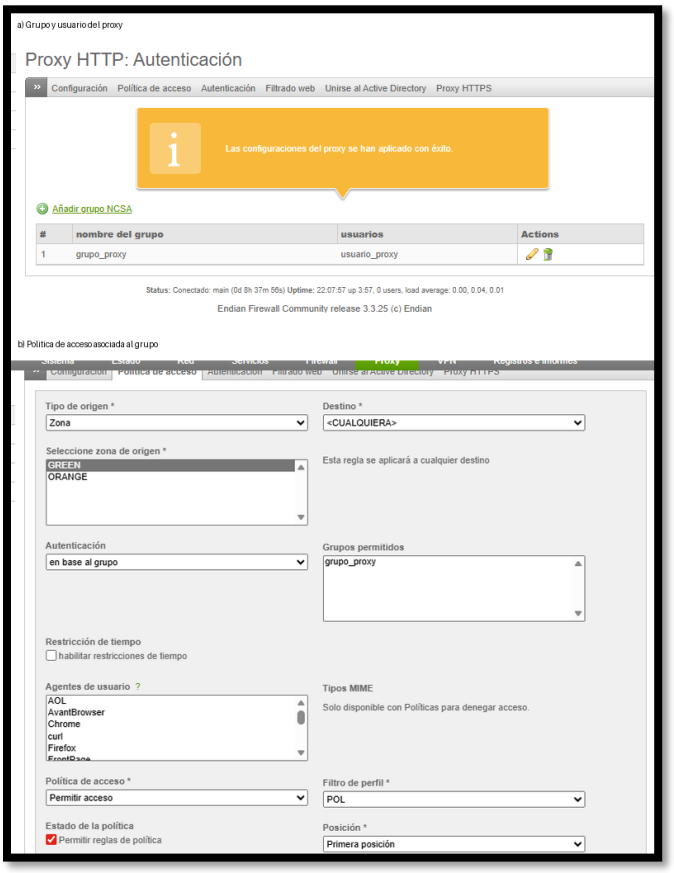
La quinta temática consistió en implementar control de navegación desde la LAN mediante proxy HTTP no transparente. En Endian se habilitó el proxy HTTP en la zona verde, con puerto 8080 y modo no transparente. Esta configuración exige que el navegador del cliente LAN sea configurado manualmente para usar el proxy en la dirección 192.168.10.1:8080.

Fig. 13. Configuración del proxy HTTP en Endian Firewall.

Fuente: Elaboración propia

Posteriormente se creó un grupo de autenticación denominado grupo_proxy y un usuario asociado denominado usuario_proxy. También se definió una política de acceso basada en grupo, con el perfil de filtrado correspondiente. Esta configuración permitió aplicar restricciones de navegación únicamente a los usuarios autenticados o asociados a la política.

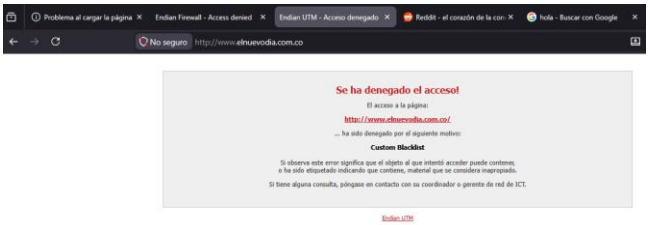
Fig. 14. Autenticación y política de acceso del proxy.



Fuente: Elaboración propia

La lista negra incluyó los sitios www.hotmail.com, www.youtube.com y www.elnuevodia.com.co. Las pruebas desde Firefox mostraron bloqueo para los sitios definidos y navegación permitida hacia otro portal, lo que evidencia que la política no bloqueó toda la navegación, sino únicamente los destinos configurados en el perfil de filtrado.

Fig. 15. Validación de bloqueo de sitio mediante proxy.



Fuente: Elaboración propia

V. DISCUSIÓN TÉCNICA, CAPACITACIÓN Y REPLICABILIDAD

Los resultados obtenidos deben interpretarse como una cadena de dependencias técnicas. La segmentación de Endian fue la base del laboratorio; sobre ella se habilitó la salida controlada mediante NAT; posteriormente se publicaron servicios en la DMZ; después se restringieron protocolos como ICMP; y finalmente se aplicó control de navegación mediante proxy autenticado. Si una fase falla, la siguiente puede mostrar errores que no corresponden a la regla evaluada, sino a una configuración previa incompleta.

Para fines de capacitación, este orden es valioso porque obliga a validar cada capa antes de avanzar. Primero se confirma que las interfaces y las rutas existen; luego se comprueba la salida a Internet; después se verifican los servicios en Ubuntu Server con systemctl; más adelante se prueban puertos específicos desde la LAN; y al final se configuran políticas de usuario en el proxy. Esta secuencia reduce la posibilidad de diagnosticar un bloqueo de proxy cuando en realidad el problema está en el direccionamiento, en NAT o en el servicio publicado.

Como guía mínima de réplica para próximos estudiantes, se recomienda validar seis puntos antes de dar por terminado el laboratorio: que las zonas verde, roja y naranja estén activas; que Ubuntu Server conserve la IP 192.168.20.10 y la puerta de enlace 192.168.20.1; que LAN y DMZ tengan salida controlada hacia la WAN; que Apache y vsftpd estén activos; que el ping hacia el servidor DMZ quede bloqueado cuando aplique la regla ICMP; y que el navegador del cliente LAN use el proxy 192.168.10.1:8080 para comprobar la lista negra configurada.

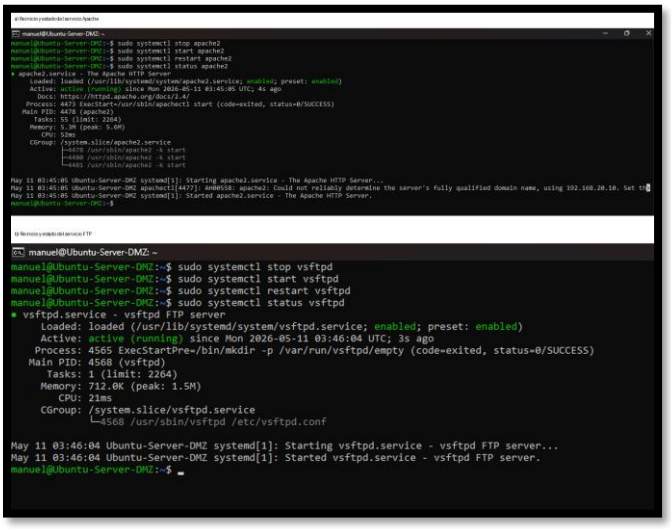
Con esta lectura, el laboratorio no queda únicamente como evidencia de instalación, sino como una ruta de comprobación. Cada fase produce una señal técnica verificable y permite comprender la relación entre teoría de redes, administración de GNU/Linux y seguridad perimetral aplicada.

El laboratorio desarrollado tiene valor formativo porque integra varios conceptos que normalmente se estudian de manera independiente: instalación de una solución de firewall, segmentación por zonas, configuración de interfaces, direccionamiento IP, publicación de servicios, reglas por protocolo, pruebas desde consola y control de navegación mediante proxy. Esta integración permite que el estudiante comprenda la relación entre la teoría de redes y la administración real de servicios GNU/Linux.

Desde una perspectiva de capacitación, la práctica puede replicarse como una secuencia guiada: primero se construye la topología virtual, luego se valida la conectividad base, posteriormente se publican servicios en la DMZ, se restringen protocolos no deseados y finalmente se aplican políticas de navegación. Este orden facilita el diagnóstico de errores, ya que cada fase produce una evidencia verificable antes de continuar con la siguiente configuración.

La revisión de servicios desde consola fortalece el componente administrativo solicitado en la guía. Comandos como date, systemctl status, systemctl stop, systemctl start y systemctl restart permiten demostrar que los servicios se encuentran instalados, activos y administrables desde terminal. Esto favorece la construcción de evidencias técnicas reproducibles y evita depender únicamente de interfaces gráficas.

Fig. 16. Administración de servicios desde consola.



Fuente: Elaboración propia

VI. CONCLUSIONES

La principal recomendación técnica para replicar el escenario es documentar cada cambio junto con su prueba inmediata. En este laboratorio, las capturas más útiles fueron aquellas que mostraron la relación entre configuración y resultado: interfaces activas, rutas del servidor DMZ, reglas de salida, servicios activos, puertos accesibles, bloqueo ICMP y restricción de sitios mediante proxy. Este tipo de evidencia permite verificar que la solución funciona por capas y no solo por configuración visual.

La implementación de Endian Firewall permitió construir una infraestructura de seguridad perimetral segmentada en LAN, WAN y DMZ. Esta separación demostró la utilidad de aislar los servicios publicados de la red interna y controlar el tráfico mediante reglas específicas.

La configuración de reglas de salida y acceso entre zonas permitió validar comunicación controlada desde la LAN y la DMZ hacia la red externa simulada, así como acceso específico a servicios HTTP y FTP alojados en Ubuntu Server. Este comportamiento evidencia la importancia de permitir únicamente los servicios necesarios.

El bloqueo de ICMP confirmó que el firewall puede restringir protocolos de diagnóstico cuando se requiere reducir la exposición de los servidores. La prueba de ping sin respuesta permitió comprobar de forma clara el efecto de la regla aplicada.

El proxy HTTP no transparente con autenticación y lista negra permitió aplicar políticas de navegación desde la LAN, bloqueando sitios definidos sin impedir el acceso a otros destinos. Esto demuestra la utilidad del proxy como mecanismo de control de usuarios y filtrado de contenido en entornos administrados.

La práctica fortaleció competencias de administración GNU/Linux, redes, virtualización y seguridad perimetral, debido a que exigió relacionar configuración de servicios, direccionamiento, reglas de firewall, pruebas de conectividad y documentación técnica con evidencias verificables.

REFERENCIAS

[1] Linux Professional Institute, “Learning Materials 101-500,” LPI. [En línea]. Disponible: https://learning.lpi.org/es/learning-materials/101-500/. Accedido: 24-may-2026.

[2] Canonical, “Ubuntu Server Documentation,” Canonical. [En línea]. Disponible: https://ubuntu.com/server/docs. Accedido: 24-may-2026.

[3] Debian Project, “El manual del administrador de Debian,” Debian. [En línea]. Disponible: https://www.debian.org/releases/stable/amd64/index.es.html. Accedido: 24-may-2026.

[4] Oracle, “Oracle VM VirtualBox User Manual,” Oracle. [En línea]. Disponible: https://www.virtualbox.org/manual/. Accedido: 24-may-2026.

[5] Endian, “Endian UTM 3.2 Reference Manual,” Endian, 2016. [En línea]. Disponible: http://docs.endian.com/3.2/utm/index.html. Accedido: 24-may-2026.