Implementación de Seguridad Perimetral en un Entorno LAN–DMZ–WAN Utilizando GNU/Linux Endian Firewall

Félix Rosales Gómez
frosalesg@unadvirtual.edu.co
Damaris Prada Mejía
depradam@unadvirtual.edu.co
Isaac Daniel Benítez Marmolejo
idbenitezb@unadvirtual.edu.co
Deison Barreto Montes
Djbarretomo@unadvirtual.edu.co
Neider Ureche
nfurechet@virtual.edu.co

RESUMEN: Este artículo presenta la implementación colaborativa de una solución de seguridad perimetral basada en la distribución GNU/Linux Endian como plataforma UTM, empleada para proteger una infraestructura de red compuesta por zonas Green (LAN), Red (WAN) y Orange (DMZ). Cada integrante del grupo desarrolló una temática específica, incluyendo configuración de red, reglas de NAT, habilitación de servicios en la DMZ, políticas de acceso inter-zona e implementación de un proxy HTTP no transparente con autenticación. La metodología se basó en prácticas experimentales dentro de entornos virtualizados configurados en VirtualBox, siguiendo lineamientos de administración de redes y seguridad en GNU/Linux. Los resultados evidencian la correcta segmentación de la red, la aplicación funcional de reglas de control de tráfico y la operación del proxy con políticas de restricción y autenticación. Se demuestra que Endian constituye una herramienta efectiva para fortalecer la seguridad perimetral en arquitecturas educativas o de laboratorio.

PALABRAS CLAVE: Endian, Firewall, VirtualBox, GNU/Linux, DMZ, LAN, WAN, virtualización, seguridad perimetral.

1 INTRODUCCIÓN

La seguridad perimetral es un componente fundamental en redes modernas, especialmente en entornos donde coexisten servidores internos, servicios expuestos y estaciones de trabajo. El uso de un firewall perimetral permite controlar el flujo de información entre distintas zonas de la red, garantizando la protección de servicios críticos y minimizando riesgos de acceso no autorizado.

Este artículo presenta la implementación de un entorno LAN–DMZ–WAN utilizando Endian Firewall, una solución UTM basada en GNU/Linux que permite integrar firewall, NAT, proxy, filtrado de contenido, VPN e IDS/IPS en un mismo lugar.

El proyecto se estructura en cinco temáticas: instalación y configuración de Endian en VirtualBox, configuración NAT, habilitación selectiva de servicios en la DMZ, reglas de acceso inter-zonas e implementación de un proxy HTTP no transparente.

Estas tareas permiten evaluar y aplicar conceptos prácticos de administración de redes seguras en GNU/Linux. El uso de entornos de virtualización, como Oracle VirtualBox, permite recrear y evaluar dichas soluciones sin afectar infraestructuras reales.

2 MARCO TEÓRICO

La virtualización constituye una técnica que permite ejecutar varios sistemas operativos sobre un único hardware físico. Oracle VM VirtualBox proporciona capacidades avanzadas para la creación de laboratorios de red mediante máquinas virtuales aisladas. La seguridad perimetral se fundamenta en el uso de firewalls, NAT, filtrado de tráfico, IDS/IPS y VPN, con el propósito de controlar y proteger el flujo de información entre redes internas y externas. Endian Firewall integra estas funciones bajo un enfoque UTM, gestionando tráfico y servicios mediante zonas: verde (LAN), roja (WAN), naranja (DMZ) y azul (WLAN). La segmentación permite aplicar controles específicos y contener posibles vulnerabilidades.

La DMZ constituye un área semipública donde se alojan servicios expuestos a Internet, reduciendo riesgos para la red interna. NAT, DHCP y reglas de firewall complementan la arquitectura, facilitando la administración y protección del entorno. La virtualización de Endian en VirtualBox posibilita la simulación de escenarios reales mediante adaptadores configurados para cada zona, resultando especialmente útil en contextos formativos y de experimentación.

3 METODOLOGÍA/DESARROLLO

La metodología aplicada en este trabajo consistió en la instalación, configuración y evaluación progresiva de diferentes funciones de seguridad dentro de la plataforma Endian Firewall, implementada sobre un entorno virtualizado con VirtualBox. Cada temática se abordó de manera independiente, pero manteniendo coherencia con el diseño general de la red segmentada en zonas Verde, Naranja y Roja. De esta forma, se garantizó que los resultados obtenidos en cada fase correspondieran al comportamiento real de la solución UTM, como se evidencia a continuación.

3.1 INSTALACIÓN Y CONFIGURACIÓN INICIAL DE ENDIAN

Se utiliza Oracle VirtualBox y la imagen ISO de Endian Firewall. La máquina virtual se configura con tres adaptadores de red, asignados a las zonas Verde, Roja y Naranja respectivamente.

Configuración de Tarjetas de Red en VirtualBox

- Zona Roja (WAN): Adaptador configurado en modo NAT o Puente para acceso a Internet.
- Zona Verde (LAN): Adaptador en modo Red Interna, utilizado para la red interna.
- Zona Naranja (DMZ): Adaptador en modo Red Interna separado, destinado a servidores.

La instalación se realiza arrancando desde la ISO. Una vez instalado, se asignan las interfaces:

- eth0 → Zona Roja
- eth1 → Zona Verde
- eth2 → Zona Naranja

3.2 CONFIGURACIÓN NAT

Para esta práctica armé la red en Packet Tracer con el router, el switch y las dos redes internas (LAN y DMZ). Luego configuré las IP en cada interfaz y marqué cuáles eran internas y cuál sería la salida hacia la "Internet". Después creé las listas de acceso y las reglas de NAT para que ambas redes pudieran salir usando la misma dirección pública del router.

Cuando todo estuvo listo, hice pruebas de ping desde los equipos internos y revisé la tabla de NAT. Ahí pude ver las traducciones activas, lo que confirmó que la configuración estaba funcionando bien.

Finalmente, se verificó la conectividad con pings y se revisó la tabla de traducciones del router, confirmando que NAT estaba funcionando correctamente.

3.3 SERVICIOS PERMITIDOS DESDE LA DMZ

La metodología se centró en la configuración y verificación de servicios dentro de una zona DMZ utilizando un servidor Ubuntu y el firewall Endian. Primero, se creó una regla para permitir el acceso al servicio HTTP (puerto 80), seleccionando la opción *uplink main* para redirigir las solicitudes hacia el servidor ubicado en la DMZ. Luego, se configuró una regla similar para habilitar el servicio FTP (puerto 21). Una vez aplicadas las reglas, se comprobó el funcionamiento de ambos servicios utilizando la IP pública proporcionada por Endian, verificando el acceso exitoso al sitio web y al servicio FTP.

Posteriormente, se implementó una regla de bloqueo para el protocolo ICMP, específicamente para los puertos 8 y 30, con el fin de impedir respuestas al comando *ping* desde las zonas verde y naranja. Finalmente, se validó la correcta aplicación de las reglas mediante la revisión del tráfico en el panel de monitoreo de Endian, confirmando que ICMP era bloqueado mientras que los servicios HTTP y FTP permanecían operativos.

3.4 REGLAS DE ACCESO INTER-ZONAS

Gracias a la configuración de las reglas de cortafuegos inter-zonas en Endian Firewall, se pudo controlar y gestionar el tráfico entre las distintas áreas de red: zona Verde (LAN), zona Naranja (DMZ) y zona Roja (WAN). Por limitaciones del entorno virtual no fue posible visualizar la zona Roja desde el módulo "Inter-Zone Traffic", pero sí se pudieron configurar y probar reglas operativas con las zonas disponibles (Green y Orange) y la gestión NAT para simular el tráfico hacia la WAN.

En esta temática, las reglas configuradas se enfocaron en permitir y restringir el flujo de tráfico utilizando servicios específicos como HTTP (puerto 80) y FTP (puerto 21). La metodología realizada consistió en la generación de reglas de firewall entre zonas y la comprobación posterior desde un cliente Ubuntu conectado a la zona Green.

Las reglas inter-zonas creadas fueron:

- **Regla Green → Orange (HTTP)**: Se permitió el acceso al servidor web ubicado en la zona DMZ.
- **Regla Green → Orange (FTP)**: Se habilitó el tráfico FTP desde la zona Verde hacia el servidor de la DMZ.
- **Regla Orange → WAN (simulada mediante NAT)**
- **Regla WAN → DMZ**

La configuración de las normas para el acceso entre zonas hizo notar lo importante que es controlar pequeños partes del tráfico en arquitecturas divididas por zonas de seguridad. Por medio de Endian Firewall fue posible poner reglas que manejan cómo interactúa la zona verde (LAN), la zona naranja (DMZ) y la red exterior (WAN), asegurando que solo los servicios permitidos —mas que nada HTTP y FTP— podían moverse entre ellas.

3.5 PROXY HTTP NO TRANSPARENTE

Para la implementación del Proxy HTTP no transparente en Endian Firewall se basó en un enfoque experimental guiado por la estructura del laboratorio. El proceso se dividió en las siguientes etapas:

3.5.1 PREPARACIÓN DEL ENTORNO

Se desplegó una máquina virtual con Endian Firewall actuando como dispositivo UTM, configurada con sus zonas predeterminadas: Red (WAN), Green (LAN) y Orange (DMZ). En la zona Green se instaló un cliente Ubuntu Desktop para realizar la configuración y validación del proxy.

3.5.2 ACTIVACIÓN Y CONFIGURACIÓN DEL PROXY HTTP

Dentro de la interfaz web de administración de Endian, se habilitó el servicio HTTP Proxy y se configuró como proxy no transparente en las zonas internas. Este modo no transparente obliga a que cada cliente configure manualmente la dirección del proxy en su navegador.

3.5.3 CREACIÓN DE PERFILES DE FILTRADO WEB

Se creó un perfil de filtrado denominado sitios_bloqueados, en el cual se personalizó la lista negra agregando los dominios de www.youtube.com, www.hotmail.com y www.elnuevodia.com. Este perfil se utilizaría posteriormente en las políticas de acceso para aplicar restricciones a los usuarios autenticados.

3.5.4 IMPLEMENTACIÓN DE AUTENTICACIÓN Y GRUPOS DE USUARIOS

Se configuró el módulo de autenticación local de Endian mediante la creación de un usuario y un grupo asociado (grupo_lan). Este mecanismo proporciona control de acceso basado en identidad, permitiendo que sólo los usuarios pertenecientes al grupo autorizado puedan utilizar el proxy.

3.5.5 DEFINICIÓN DE POLÍTICAS DE ACCESO

Finalmente, se diseñó una política de acceso que especifica:

- La zona desde la cual se permitirán solicitudes.
- El mecanismo de validación basado en grupos de usuarios.
- La aplicación del perfil de filtrado sitios_bloqueados.

Esta política representa la lógica final de control del tráfico HTTP saliente.

4 RESULTADOS

Los resultados obtenidos permiten validar el funcionamiento de cada una de las configuraciones implementadas dentro del entorno segmentado. A través de pruebas de conectividad, verificación de reglas, análisis de tráfico y revisión de los registros del firewall, se comprobó el comportamiento esperado para los servicios publicados en la DMZ, las reglas inter-zonas, el mecanismo NAT y el proxy HTTP no transparente. A continuación, se presentan los resultados específicos correspondientes a cada temática desarrollada.

4.1 INSTALACIÓN Y CONFIGURACIÓN INICIAL DE ENDIAN.

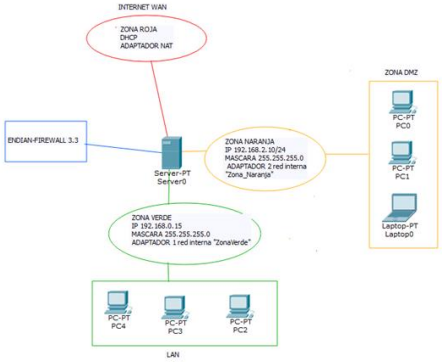

Fig 1 Arquitectura de la segmentación en Endian-Firewall.

- Funcionamiento correcto del envío de tráfico desde la zona verde hacia la zona roja mediante NAT.
- Aislamiento exitoso de la red interna frente a la DMZ.
- Asignación automática de direcciones IP a clientes de la LAN a través del servicio DHCP.
- Registros detallados del firewall que muestran la creación y aplicación de reglas configuradas.

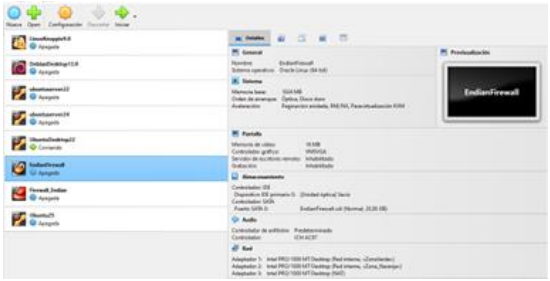

Fig. 2. Configuración de adaptadores de red en VirtualBox para Endian-Firewall.

Segmentación exitosa de la red donde cada zona operó de forma independiente, respetando las reglas predeterminadas de seguridad y de acceso a Internet desde la zona verde. La interfaz roja, configurada como adaptador NAT, proporcionó conectividad externa, aislamiento adecuado d

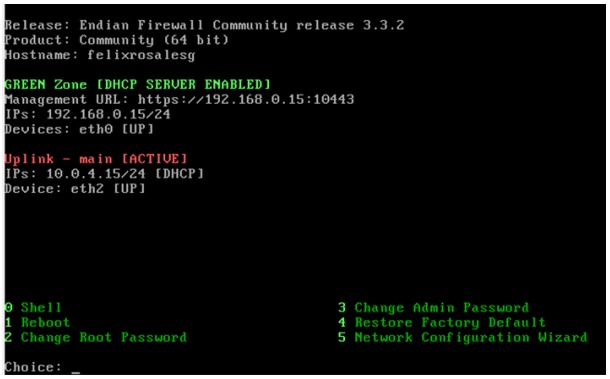

Fig 3. Configurado zona verde y DHCP zona roja.

Para permitir el acceso a los servicios alojados en el servidor dentro de la DMZ, se configuraron reglas específicas en el firewall Endian. Primero se habilitó el servicio permitiendo que cualquier IP conocida accediera al sitio web creado. Esta funcionalidad se comprobó ingresando a la página a través de la IP pública asignada por Endian, confirmando que el redireccionamiento operaba correctamente.

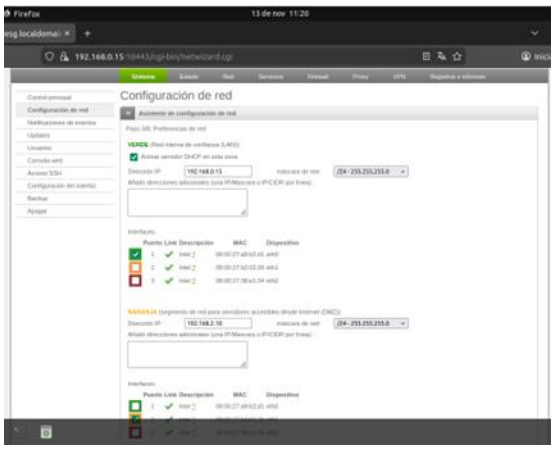

Fig 4. Interfaz gráfica de Endian-Firewall

Se verificó el acceso conectándose mediante la IP pública, evidenciando que el servicio FTP funcionaba sin inconvenientes. En conjunto, estas reglas permitieron que los servicios web y FTP del servidor ubicado en la DMZ fueran accesibles de manera segura desde el exterior.

4.2 CONFIGURACIÓN NAT

Una vez configurada la red, las pruebas empezaron a responder como se esperaba. Los equipos de la LAN y la DMZ pudieron comunicarse sin problema con el router, y al hacer pings hacia la red externa se generaron las traducciones NAT. Esto se confirmó revisando la tabla de NAT, donde aparecieron las entradas creadas por el tráfico de las PCs.

En pocas palabras, las pruebas mostraron que la comunicación desde ambas redes internas hacia la "Internet" simulada funcionó bien y que el NAT quedó trabajando como debía.

4.3 SERVICIOS PERMITIDOS DESDE LA DMZ

Después de analizar los servicios configurados en la DMZ, se comprobó lo siguiente:

1. Se permite el acceso al servicio HTTP (puerto 80) desde la red externa hacia el servidor ubicado en la DMZ, garantizando la disponibilidad pública del sitio web.

2. Se habilita el servicio FTP (puerto 21) únicamente desde la DMZ hacia las estaciones autorizadas, permitiendo la gestión controlada de archivos sin exponer el servidor interno.

3. No se permiten conexiones ICMP desde el exterior hacia la DMZ, lo que evita que los atacantes puedan hacer ping y descubrir información de la red.

4. Las reglas creadas en el firewall se verificaron mediante pruebas de tráfico, comprobando que solamente los servicios autorizados pasan y que todo lo no permitido es bloqueado.

4.4 REGLAS DE ACCESO INTER-ZONAS

La verificación de las reglas de tráfico entre las zonas Green (LAN), Orange (DMZ) y la salida hacia la zona Red (WAN) fue posible gracias a la aplicación de las normas de acceso inter-zonas en Endian Firewall. Las pruebas confirmaron que la comunicación hacia Internet se manejó de manera adecuada por medio del mecanismo NAT configurado en el Uplink, a pesar de que el módulo "Inter-Zone Traffic" no ofrecía la zona Red.

Las reglas establecidas posibilitaron el análisis de la conducta del firewall al permitir exclusivamente los servicios requeridos, preservando el aislamiento estructural entre las áreas. Los hallazgos más importantes fueron:

- **Comunicación Green → Orange (HTTP).**
- **Comunicación Green → Orange (FTP).**
- **Acceso Orange → WAN mediante NAT.**
- **Acceso WAN → DMZ vía DNAT.**
- **Bloqueo selectivo de tráfico no permitido.**

En conjunto, los resultados evidencian que Endian Firewall aplicó correctamente las reglas definidas, permitiendo únicamente el tráfico aprobado entre zonas y bloqueando los servicios no autorizados. Esto refleja un comportamiento seguro, consistente y adecuado para entornos de práctica en seguridad perimetral.

4.5 PROXY HTTP NO TRANSPARENTE

Tras aplicar el perfil de filtrado web, el cliente en la zona Verde no pudo acceder a los dominios incluidos en la lista negra. Al intentar abrir alguno de los sitios bloqueados, el navegador presentó un mensaje de acceso denegado generado por el propio sistema de filtrado de Endian. Esto confirma que las reglas de filtrado funcionaron según lo previsto. Vea figuras 5, 6 y 7.

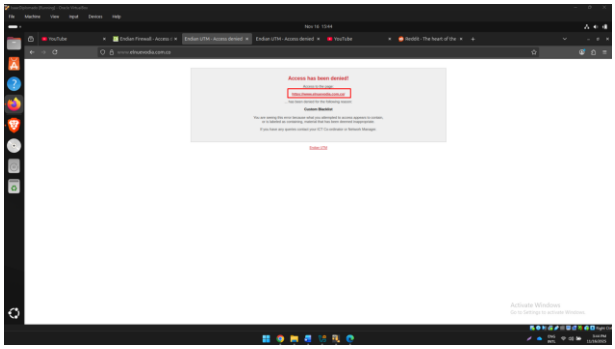

Fig 5. Acceso denegado a www.elnuevodia.com.co

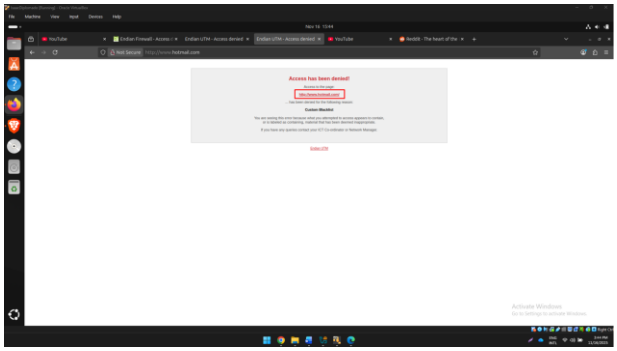

Fig 6. Acceso denegado a www.hotmail.com

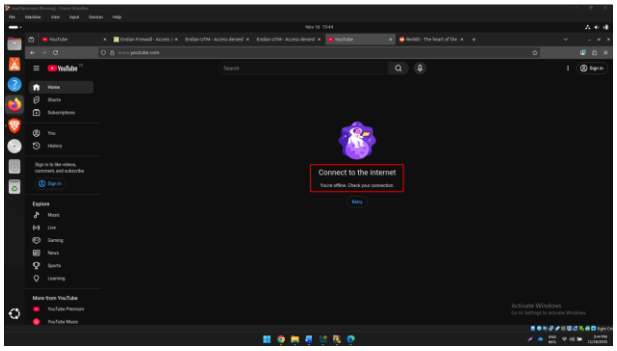

Fig 7. Acceso denegado para navegar en www.youtube.com

Al configurar el navegador con el proxy manual, se requirió autenticación previamente a permitir la navegación. Solamente los usuarios pertenecientes al grupo **grupo_lan** pudieron acceder a Internet, demostrando que el control de acceso basado en identidad se aplicó correctamente. Vea figura 8.

Fig 8. Requisito de autenticación en el proxy para navegación

Todas las solicitudes HTTP generadas por el cliente Ubuntu pasaron por el servicio de proxy de Endian. Esto se verificó mediante los registros del sistema, donde se observó el log completo de peticiones HTTP realizadas por el usuario autenticado. Vea figura 9.

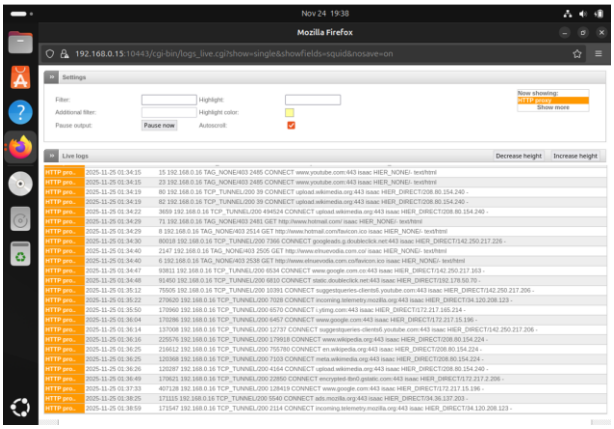

Fig 9. Log de solicitudes que pasan por el Proxy HTTP

Los resultados obtenidos confirman que el Proxy HTTP no transparente permite:

- Gestionar centralizadamente la navegación web
- Aplicar filtrado de contenido
- Autenticar usuarios antes de permitir el acceso
- Registrar las solicitudes de manera detallada.

5 DISCUSIÓN

El desarrollo de toda la actividad permitió ver de manera práctica cómo Endian Firewall actúa como una plataforma UTM capaz de integrar diferentes mecanismos de seguridad dentro de una misma solución. Trabajar cada temática de forma individual y luego observar cómo interactúan entre sí ayudó a entender mejor el papel que cumplen las zonas segmentadas (Verde, Naranja y Roja) dentro de un entorno de red. Esta separación, que inicialmente se aprecia como algo técnico, en la práctica demostró ser clave para controlar el flujo del tráfico y proteger los servicios más sensibles, especialmente aquellos ubicados en la DMZ.

A lo largo de las temáticas relacionadas con NAT, políticas interzona y publicación de servicios, se evidenció que la gestión adecuada de las reglas permite comunicar las redes sin comprometer su seguridad. El uso de NAT, por ejemplo, resultó esencial para permitir conexiones hacia Internet sin exponer directamente los equipos internos, mientras que las reglas entre la LAN y la DMZ facilitaron el acceso a los servicios web y FTP manteniendo los límites bien definidos.

La implementación del Proxy HTTP no transparente añadió otra capa importante. Con él, se pudo controlar el tráfico saliente desde la LAN, aplicar autenticación por usuario y configurar listas negras, lo que mostró cómo un proxy bien configurado se convierte en un apoyo tanto para la seguridad como para la administración del uso de Internet en una organización.

Finalmente, el uso de VirtualBox permitió recrear todo este entorno sin requerir infraestructura física adicional. La flexibilidad para configurar múltiples adaptadores de red hizo posible construir una topología realista donde fue sencillo probar, fallar y ajustar cada configuración. En conjunto, la experiencia confirmó que Endian es una herramienta útil tanto para aprender conceptos de seguridad perimetral como para visualizar cómo interactúan los distintos servicios y políticas dentro de una red segmentada.

6 CONCLUSIONES

La implementación de una instancia GNU/Linux Endian en VirtualBox constituye una estrategia eficaz para la enseñanza y experimentación en seguridad perimetral. La arquitectura multi zona facilita la comprensión de conceptos como segmentación, DMZ y reglas de firewall y los resultados obtenidos demuestran que Endian permite gestionar de manera centralizada servicios UTM esenciales y ofrece una plataforma confiable para pruebas de laboratorio. Entonces se concluye que el uso de entornos virtualizados con Endian proporciona versatilidad, seguridad y facilidad de administración.

7 REFERENCIAS

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

Oracle (2020). Manual de usuario VirtualBox . VirtualBox. https://www.virtualbox.org/manual/

Cisco Systems, “Comprender el orden de funcionamiento de NAT,” *Cisco Support*, nov. 2025. Disponible: https://www.cisco.com/c/es_mx/support/docs/ip/network-address-translation-nat/6209-5.html

Endian (2016), Endian UTM 3.2 Manual referencia . Endian.
http://docs.endian.com/3.2/utm/index.html