Implementación de un perímetro seguro en GNU/Linux: Endian Firewall, NAT y proxy HTTP no transparente

Efrain Enrique González Hernández
eegonzalezhe@unadvirtual.edu.co
Deyvi Ferney Medina Sosa
dfmedinaso@unadvirtual.edu.co
Daniel Steven Monroy Casas
danielsmonroyc@unadvirtual.edu.co

RESUMEN: *En este artículo se indica la forma de instalar y realizar la configuración de Endian, un firewall Linux, de código abierto, el cual consta de herramientas de seguridad para la protección y administración del tráfico de la red. En primer lugar, se establece una arquitectura segmentada de la red, compuesta por tres zonas: una zona roja (WAN), una zona verde (LAN) y una zona naranja (DMZ), cuya finalidad es controlar el tráfico a través de la aplicación de reglas o políticas de seguridad específicas como. NAT para la comunicación desde LAN y DMZ hacía WAN, Habilitación de servicios HTTP y denegación de protocolo ICMP, comunicación de la zona verde con la naranja y la implementación de un proxy HTTP (no trasparente) con políticas de autenticación para navegar en la web.*

ABSTRACT: *This article describes the implementation and configuration of the GNU/Linux Endian Firewall in a virtualized environment using Oracle VirtualBox. The network architecture was segmented into WAN, LAN, and DMZ zones to control traffic and apply security policies such as NAT, HTTP proxy, and port forwarding.*

Palabras clave— Firewall, GNU/Linux Endian, virtualización, seguridad en redes, segmentación de red, Oracle VirtualBox, puertos.

Keywords— Firewall, GNU/Linux, virtualization, network security, Endian.

1 INTRODUCCIÓN

La seguridad en los equipos y redes se ha convertido en un factor vital para la protección de los activos, no solo en las empresas, sino a también a nivel de redes pequeñas en hogar. Por lo que es necesario tener claridad sobre cuáles son las zonas de confianza y las que generan riesgo. El firewall con Endian permite segmentar estas zomas mediante la utilización de colores como: zona roja (WAN), zona verde (LAN – red interna) y zona naranja (DMZ – servidores).

Los firewalls basados en GNU/Linux permiten ser flexibles y tener una capacidad para la implementación de controles de seguridad, como son la traducción de direcciones NAT, filtrado de políticas, control de tráfico en la red y sobre todo tener una administración del sistema centralizado.

En este artículo se describe la configuración y comprobación del tráfico de la red mediante NAT y reenvió de puertos, habilitación de servicios como HTTP y FTP, reglas de acceso entre las zonas y reforzando la navegación a través de un proxi no transparente que requiere autenticación y políticas de filtrado., documentándose cada una de las actividades desarrolladas.

2 OBJETIVOS

1.1 OBJETIVO GENERAL

Implementación y configuración de un firewall perimetral con Endian Firewall Community en una arquitectura WAN, LAN y DMZ, empleando políticas de NAT, filtrado inter-zonas y proxi HTTP autenticado para controlar el acceso y trafico a internet.

1.2 OBJETIVOS ESPECIFICOS

- Diseñar y desplegar la configuración de Endian en VirtualBox con las correspondientes interfaces.
- Configurar y verificar reglas de SNAT para permitir conectividad entre la red LAN y WAN.
- Habilitar NAT / reenvió de puertos para permitir la salida o publicación controlada de servicios desde la zona DMZ hacía la WAN.
- Implementar y validar reglas DNAT para la publicación controlada de servicios en la zona DMZ, como habilitación de los puertos 80 (HTTP) y 21 (FTP), denegación de ping (ICMP).
- Implementar y evaluar un proxi HTTP no transparente con autenticación y políticas de filtrado.

3 IMPLEMENTACIÓN DE GNU/LINUX ENDIAN

Para el desarrollo de esta implementación se requiere elaborar previamente la arquitectura que tendrá la red, donde se establecen los parámetros necesarios que garanticen no solo el

funcionamiento, sino la debida segmentación de la red, como se muestra en la figura 1 que tiene como nombre arquitectura de la red.

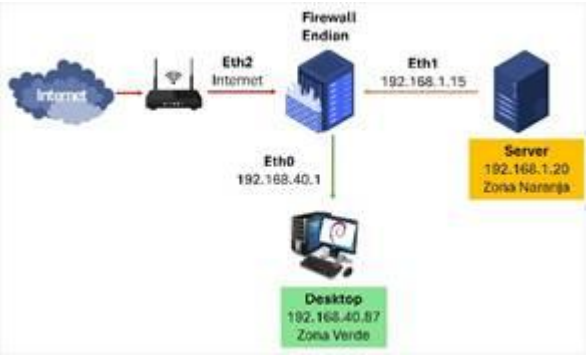

Fig. 1. Arquitectura de la red.

En la Fig. 1, arquitectura de la red podemos observar que la zona roja, corresponde a la que tiene acceso a internet, a través del router, la zona naranja al servidor y este se comunica con el firewall a través de una IP que actúa como puerta de enlace. Y finalmente la zona verde corresponde a la red local, al igual que la naranja, se comunica a través de una puerta enlace con el firewall. Para que exista una comunicación entre la zona verde y la naranja, se deben establecer permisos, al igual que para que estas zonas puedan acceder a internet.

Para la implementación del firewall basado en GNU/Linux Endian se utiliza la herramienta de virtualización Oracle VirtualBox y poder realizar la segmentación del tráfico y la gestión de las diferentes interfaces.

Inicialmente, se procedió con la creación de una máquina virtual asignando recursos adecuados como memoria RAM, procesador y almacenamiento. Posteriormente, se configuró el sistema operativo como "Other/Unknown (64-bit)" para garantizar compatibilidad con la arquitectura del sistema.

Fig. 2. Creación de la máquina virtual en VirtualBox.

Se asignan los recursos básicos para la instalación del sistema Endian.

Se configuran los adaptadores de red necesarios para simular la estructura de red. Definición de las múltiples interfaces, incluyendo una interfaz conectada a NAT para salida a internet y otras interfaces en red interna para representar zonas como LAN (zona verde) y DMZ (zona Naranja).

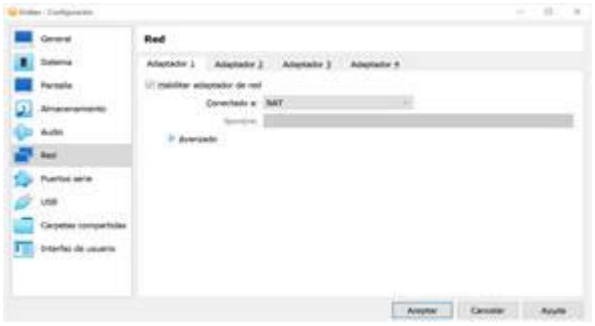

Fig. 3. Configuración de adaptadores de red en VirtualBox

Se procede a la instalación del sistema operativo Endian a partir de una imagen ISO. Durante el proceso, se configuraron parámetros básicos como idioma, particionamiento del disco y asignación de interfaces de red.

Fig. 4. Proceso de instalación de GNU/Linux Endian.

Durante la configuración de red, se asignó una dirección IP a la interfaz GREEN (LAN), estableciendo la dirección 192.168.10.1 con máscara de subred 255.255.255.0, permitiendo la comunicación dentro de la red interna.

Fig. 5. Configuración de la interfaz GREEN.

En la figura 5, configuración de la interfaz green, se define la dirección IP para la red local.

Finalizada la instalación, se accede al sistema mediante consola, donde se realizan pruebas de verificación utilizando

comandos básicos como “ip a” para validar la correcta configuración de las interfaces de red.

Fig. 6. Verificación de interfaces mediante comando en consola.

En la figura 6, verificación de interfaces mediante comando en consola, se observan las interfaces de red activas y la dirección IP asignada.

4 CONFIGURACIÓN NAT EN GNU/LINU GNU/LINUX ENDIAN FIREWALL

En este tema se configura NAT (Network Address Translation) sobre GNU/Linux Endian Firewall Community 3.3.2 en un entorno virtualizado con Oracle VirtualBox. Se estableció una arquitectura de tres zonas: zona Roja (WAN, DHCP), zona Verde (LAN, 192.168.10.0/24) y zona Naranja (DMZ, 192.168.20.0/24), permitiendo que los equipos de ambas redes privadas compartieran la IP pública del firewall para acceder a Internet.

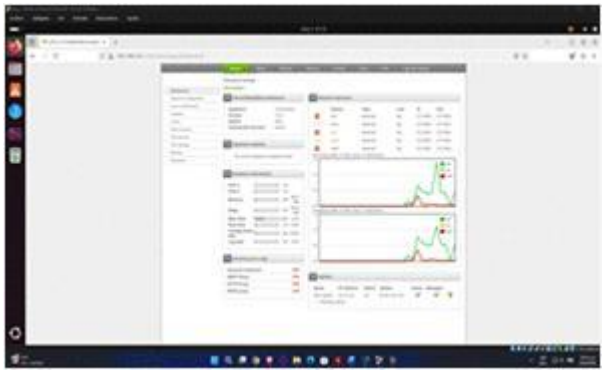

Fig. 7. Panel web de Endian Firewall — Dashboard con uplink activo.

Se accedió a Firewall → Source NAT en el panel web. Inicialmente la lista aparecía vacía, confirmando el estado previo sin reglas de enmascaramiento.

Fig. 8. Source NAT — estado inicial sin reglas (evidencia antes del NAT).

Se creó la regla de Source NAT para LAN→WAN (origen 192.168.10.0/24, destino Uplink main [RED]). El panel confirmó con "NAT rules applied successfully" y la regla quedó activa.

Fig. 9. Regla NAT LAN→WAN creada y aplicada exitosamente en Endian.

Se verificó la conectividad desde el cliente Ubuntu en la zona Verde con ping a 8.8.8.8 y google.com, obteniendo 0% de pérdida de paquetes, confirmando el correcto funcionamiento del NAT LAN→WAN.

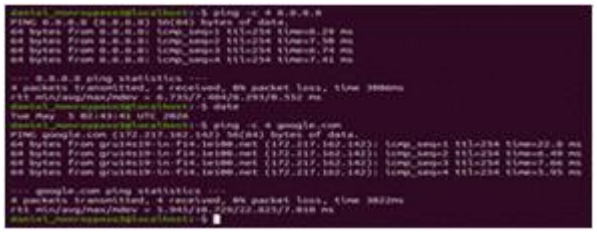

Fig. 10. Ping exitoso a 8.8.8.8 y google.com desde el cliente LAN.

Se configuró la IP estática del servidor DMZ (192.168.20.10/24) mediante netplan en Ubuntu Server, y se verificó su conectividad a Internet tras crear la segunda regla NAT para la zona Naranja→WAN (origen 192.168.20.0/24).

Fig. 11. IP estática DMZ configurada y ping exitoso a 8.8.8.8 desde el servidor DMZ.

El traceroute desde el cliente LAN confirmó que el primer salto es 192.168.10.1 (Endian Firewall), demostrando que todo el tráfico pasa por el firewall antes de salir a Internet. Ambas reglas NAT quedaron activas y verificadas.

Fig. 12. Traceroute confirmando Endian como primer salto hacia Internet.

5 PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

Con el fin de exteriorizar los servicios de la zona DMZ, sin que se comprometa la seguridad de la red interna, se procede a configurar en Endian el DNAT (destination NAT) o port forwarding. Esto permite mantener el aislamiento entre zonas habilitando únicamente los puertos requeridos. En este caso el servidor DMZ ofrece los servicios HTTP sobre TCP/80 y FTP sobre el TCP/21 (en entornos reales se recomienda SFTP o FTPS)

a. El servicio HTTP es el estándar utilizado en la navegación en la web sin cifrar. Cuando un usuario desde la zona verde o internet pretende ingresar al servidor mediante un navegador, el firewall recibe la petición a través del puerto 80, y la dirige hacía este. Si la regla o servicio no es activado, los usuarios no podrían acceder al servidor, debido a que el firewall bloquea la petición.

   Para la configuración el usuario accede desde la interfaz de endian, y en la pestaña de firewall, selecciona en el lado izquierdo Port forwarding / NAT y procede a crear o agregar una nueva regla, ingresando en los campos la información solicitada:

- Incoming IP: ANY Uplink o Uplink Main.
- Service: HTTP
- Protocol. TCP
- Incoming port: 80
- Insert IP: Ip del servidor
- Port. 80
- Nat: NAT

Fig. 13. Vista de la interfaz donde se configura el puerto 80 con la información antes relacionada.

b. El servicio FTP es configurado en la misma pestaña donde está configurada el servicio HTTP, realizando la activación o creación de la regla del FTP (file transfer Protocol), que permite la transferencia de archivos entre cliente y servidor, ya sea para subir o descargar, teniendo control sobre comandos y autenticación.

Estas reglas DNAT (traducción de dirección de red de destino) son importantes porque traducen la IP pública y el número de puerto específico de las solicitudes que llegan al firewall a la IP privada de un host dentro de la red local, generando seguridad a partir de aislamiento, y definiendo quienes pueden acceder al servidor, además, permiten la visibilidad de archivos, documentos, etc., desde el exterior en forma controlada, evitando que el tráfico se pierda, toda vez que el firewall sabe a qué terminal enviar la petición de la web.

Para agregar la regla FTP, utilizamos los campos de la siguiente forma:

- Incoming IP: ANY Uplink o Uplink Main.
- Service: FTP
- Protocol. TCP
- Incoming port: 21
- Insert IP: Ip del servidor
- Port/range: 21
- Nat: NAT

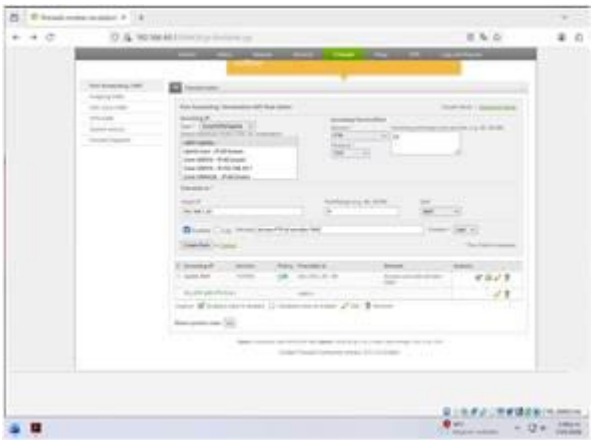

Fig. 14. Vista de la interfaz donde se configura el puerto 21 con la información antes relacionada.

Para la verificación de los servicios HTTP y FTP en el servidor podemos utilizar los siguientes comandos.

- ss –tunlp | grep –E ':80'
- ss –tunlp | grep –E ' :21'

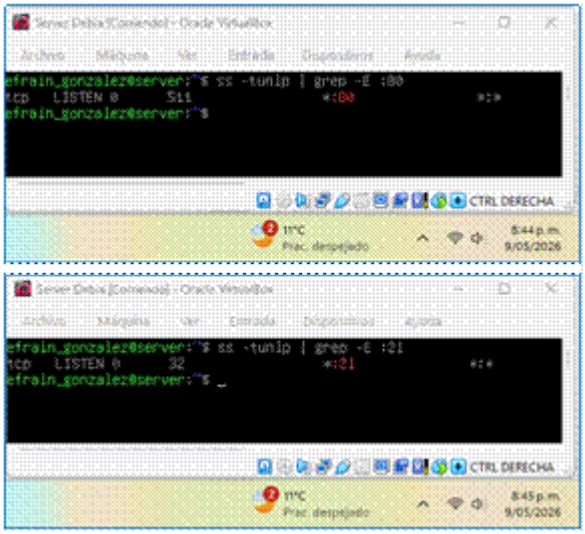

Fig. 15. Verificación de que el puerto esta activo en el servidor.

Desde la maquina local o desktop podemos realizarlo de la siguiente forma desde la terminal:

- curl –I IP_Servidor
- Ftp IP_Servidor

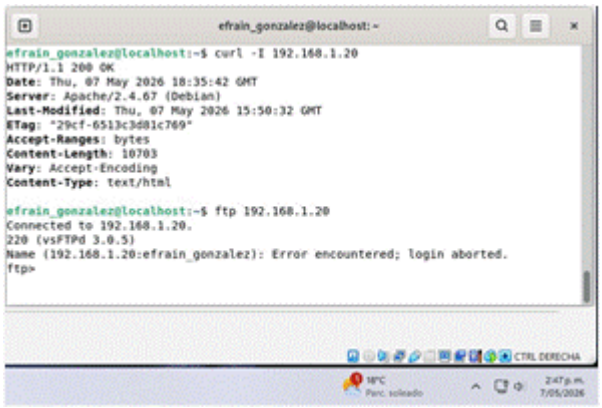

Fig. 16. La figura muestra la activación de los servicios HTTP y FTP desde una maquina local.

Desde el navegador podemos ingresar con http://IP_Servidor

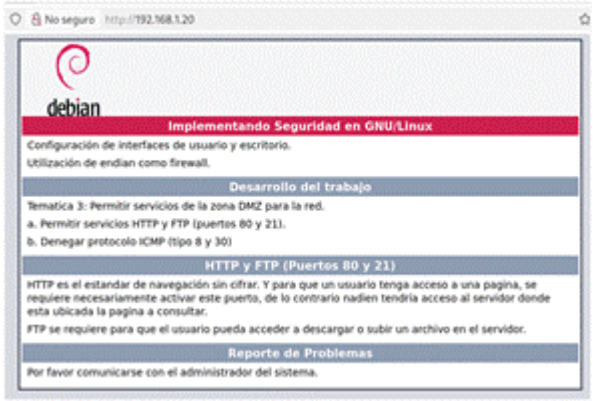

Fig. 17. La figura muestra la activación de los servicios HTTP y FTP desde una maquina local a través del navegador.

c. Con el fin de reducir la superficie de reconocimiento, se restringe o deniega el protocolo ICMP (tipo 8 y 30 o 0) hacia el servidor en DMZ, para no permitir hacer ping en la red.

El protocolo ICMP determina, si los datos llegan o no al destino. Se utilizan los tipos ICMP 8 y 30. El tipo 8 es una solicitud de eco, que permite diagnosticar si el servidor se encuentra encendido o apagado. Sin este deniega, el servidor aumenta la seguridad frente a escaneo de la red. El tipo 30 o 0 es respuesta de eco. Cuando un ciberdelincuente intenta rastrear una ruta hacía el servidor, envía paquetes ICMP y UDP, que expiran después del envió de cierta cantidad de datos, en este caso el tipo 30 se convierte en ese número para expirar.

El configurar este protocolo ICMP evita que ciberdelincuentes puedan obtener información de la red interna como cantidad de hosts, router y firewalls.

La creación de esta regla se realiza en la interfaz de endian, en la pestaña firewall - Inter-Zone Traffic llenando los campos:

- Source: IP del host (zona verde)

- Destination: orange
- Service: User defined
- Protocol: ICMP
- Destination port: 8, 30
- Policy – action: Deny
- Position: First

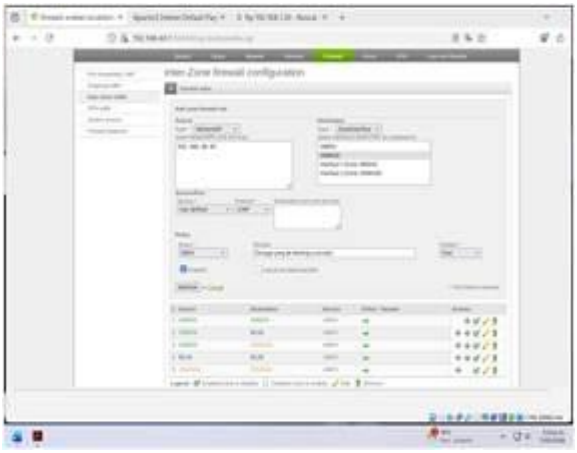

Fig. 18. Configuración del protocolo ICMP, tipo 8 y 30.

Fig. 19. Comprobación por consola o terminal de una terminal con ping –c 4 IP_Servidor, la no respuesta del comando ping hacia una IP de la red, señalando 100% paquetes perdidos.

En la figura 19 comprobación por consola, se considera correcta la política cuando el resultado muestra la pérdida del 100% de los paquetes, es decir, no hay respuesta. Adicionalmente se confirma esto al revisar el tráfico de salida y la creación de las reglas en la interfaz de endian en logs and reports – firewall log viewer, como se muestra en la figura 20 en la que se observa el tráfico de salida en el firewall, observándose la denegación en la columna chain, donde señala BADTCP-DROP.

Fig. 20. En la figura se observa el tráfico de salida en el firewall, observándose la denegación en la columna chain, donde señala BADTCP-DROP.

6 IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE) CON POLÍTICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET.

Estando en la interfaz de endian firewall, En el menú superior (fondo gris), hacer clic sobre Proxy. Luego, activar la opción Habilitar Proxy HTTP y

1) hay que asegurar que la configuración para verde y naranja sea no transparente,

2) que el puerto que será usado sea el 8080. Lo demás se puede dejar como está, y la vista de estas opciones sería similar a esta

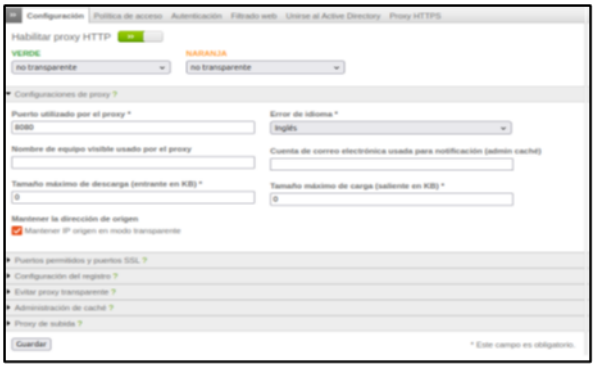

Fig. 21. Habilitación del modo no transparente.

Para crear un perfil y establecer una lista negra bloqueando los sitios:

www.hotmail.com
www.youtube.com
www.elnuevodia.com.co

Ir a Proxy

1. luego a HTTP
2. Filtrado web
3. Hacer clic en Añadir nuevo perfil, asignando el nombre.

4. hacer clic sobre Listas negra y blancas personalizadas y, en los sitios a bloquear, completar el trabajo. Fig.

Fig. 22. Estableciendo lista negra de sitios.

Se continua, con el establecimiento de la política de acceso, siguiendo estos pasos:

1) Proxy,
2) HTTP,
3) luego a Política de acceso y
4) hacer clic en Añadir política de acceso Endian aplicando configuración de política de acceso.

Fig. 23. Política de acceso creada exitosamente.

Al abrir una nueva pestaña, en un navegador, este informa que se requiere autenticación, como se muestra en la fig.

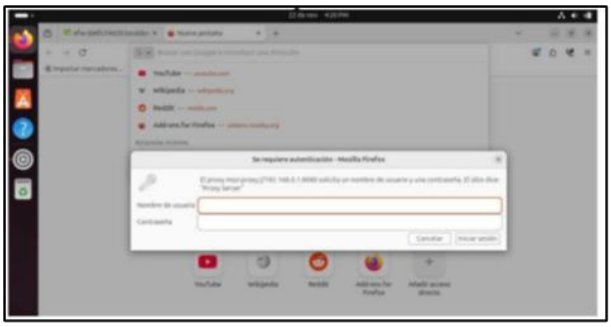

Fig. 24. Pestaña que solicita autenticación.

Finalmente, al intentar entrar a YouTube, se evidencia que el proxy deniega su acceso, devolviendo un error de tipo timeout.

Fig. 25. Error de tipo timeout.

7 CONCLUSIONES

La configuración de las reglas DNAT y el bloqueo del protocolo ICMP, coadyuvan a fortalecer la seguridad del sistema, especialmente en la zona DMZ o del servidor, traduciendo las direcciones hacía la IP privada, evitando que ciberdelincuentes tengan información sobre la estructura interna de la red.

La implementación de Endian Firewall Community permite establecer una solución efectiva de seguridad perimetral mediante la segmentación de redes LAN, WAN y DMZ.

El uso de un proxy HTTP no transparente con autenticación mejoró el control de acceso a Internet, permitiendo aplicar políticas de navegación y filtrado de contenido web.

Finalmente, el desarrollo de este documento permite comprender el funcionamiento de los firewalls GNU/Linux y la importancia de las políticas de seguridad dentro de las infraestructuras de redes empresariales.

2 REFERENCIAS

Canonical Ltd. (2023). Guía del escritorio Ubuntu 20.04 LTS. Help Ubuntu. https://help.ubuntu.com/

Debian Project. (2023). El manual del administrador de Debian 12.5.0. Debian. https://www.debian.org/releases/stable/amd64/index.es.html

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

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

Markova, V. *(2026). What is ICMP (Internet control message protocol)? ClouDNS Blog.* https://www.cloudns.net/blog/what-is-icmp-internet-service-message-protocol/

Pramatarov, M. (2026). FTP vs HTTP: Understanding the key differences. ClouDNS Blog. https://www.cloudns.net/blog/ftp-vs-http-file-transfer-protocol-hypertext-transfer-protocol/