IMPLEMENTACIÓN DE UNA RED SEGMENTADA CON ENDIAN FIREWALL Y SERVICIOS EN DMZ EN ENTORNO LINUX VIRTUALIZADO

Leidy Johanna Rodríguez Delgado
e-mail: ljrodriguezde@unadvirtual.edu.co
Daniel Medina Villamizar
e-mail: dmedinavi@unadvirtual.edu.co
Óscar Fernando Montañez Corredor
e-mail: ofmontanezc@unadvirtual.edu.co
Ferney Alexander Garzón Capacho
e-mail: fagarzonca@unadvirtual.edu.co
Mayerly Janne Ballén González
e-mail: mjballeng@unadvirtual.edu.co

RESUMEN: Este artículo describe la implementación de una red segmentada utilizando máquinas virtuales Linux en VirtualBox, con el firewall GNU/Linux Endian. Se configuraron tres zonas de red: verde (LAN), roja (WAN) y naranja (DMZ), garantizando una separación lógica de servicios y niveles de acceso. Se instaló un servidor Ubuntu en la zona DMZ con servicios HTTP y FTP, accesibles bajo políticas de control definidas. Se validó la conectividad entre zonas, incluyendo la navegación desde la LAN hacia Internet y desde la DMZ hacia la WAN. Además, se aplicaron reglas para permitir o denegar tráfico HTTP, y se configuró un proxy HTTP no transparente con autenticación de usuarios y listas negras. Los resultados demuestran una arquitectura funcional y segura, útil para fines educativos y de pruebas.

PALABRAS CLAVE: Endian, firewall, segmentación de red, VirtualBox, FTP, DMZ, Ubuntu Server.

1 INTRODUCCIÓN

En el presente trabajo se documenta la implementación de una red virtualizada basada en sistemas GNU/Linux, con el propósito de simular un entorno seguro, funcional y segmentado mediante el uso del firewall de código abierto Endian, desplegado sobre la plataforma de virtualización VirtualBox. La arquitectura diseñada contempla tres zonas de seguridad: zona verde (LAN), zona naranja (DMZ) y zona roja (WAN), lo cual permite un control granular del tráfico y una administración centralizada de las políticas de acceso.

El proyecto se desarrolló de forma colaborativa, dividiendo el proceso en cinco temáticas específicas que abarcan desde la instalación inicial del firewall hasta la configuración de reglas NAT, servicios en DMZ, proxy con autenticación, y gestión de accesos, con el fin de emular escenarios reales de seguridad perimetral. Esta implementación no solo permite reforzar conceptos clave de redes y seguridad informática, sino también validar, mediante pruebas controladas, la conectividad, segmentación y gestión eficiente del tráfico en entornos educativos o empresariales simulados.

2 CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN, SUS ZONAS EN VIRTUALBOX E INSTALACIÓN

La correcta instalación y configuración del sistema GNU/Linux Endian es fundamental para la implementación de una arquitectura de red segmentada. En esta sección se describe el proceso técnico llevado a cabo para crear la máquina virtual del firewall en VirtualBox, asignar los recursos necesarios, configurar sus adaptadores de red e instalar el sistema operativo.

2.1 INSTALACIÓN Y CONFIGURACIÓN INICIAL DE ENDIAN FIREWALL

Para implementar un esquema de red segmentado en entornos virtualizados, se utilizó la distribución GNU/Linux Endian en una máquina virtual configurada mediante VirtualBox. Esta herramienta permite simular distintas zonas de red, facilitando pruebas de seguridad y conectividad.

La máquina virtual de Endian fue creada con las siguientes especificaciones mínimas: 1024 MB de RAM, disco duro de 8 GB en formato VDI, y tres adaptadores de red habilitados para representar las zonas Verde (LAN), Naranja (DMZ) y Roja (WAN).

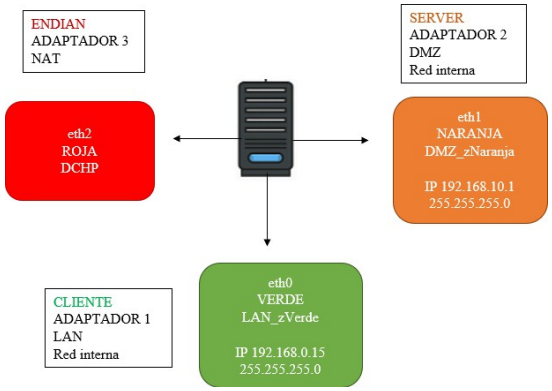
El proceso inició con la descarga del archivo ISO desde el sitio oficial, el cual se montó en la unidad de almacenamiento virtual para proceder con la instalación. El asistente guió la selección de idioma, la aceptación de licencia y la instalación en todo el disco disponible. Una vez completado, se asignaron direcciones IP según el rol de cada zona:

Zona verde (eth0): 192.168.0.15
Zona naranja (eth1): 192.168.10.1
Zona roja (eth2): por DHCP

La configuración inicial continuó desde el navegador accediendo a https://192.168.0.15:10443, donde se asignaron usuarios, contraseñas y se definieron las interfaces correspondientes a cada zona.

Como se muestra en la Figura 1, el diseño contempla tres zonas de red interconectadas mediante Endian Firewall.

Figura 1. Diseño de red segmentada con zonas Verde, Naranja y Roja conectadas a través de Endian Firewall.



Fuente: Autoría propia.

La red está compuesta por una zona LAN interna conectada a través de la interfaz verde, una zona DMZ protegida conectada a través de la interfaz naranja, y una zona WAN simulada con NAT que representa el acceso a Internet. El firewall Endian permite controlar el tráfico entre estas zonas, asegurando los servicios críticos en DMZ como servidores web o bases de datos.

2.2 CREAR LA MAQUINA VIRTUAL ENDIAN EN VIRTUALBOX

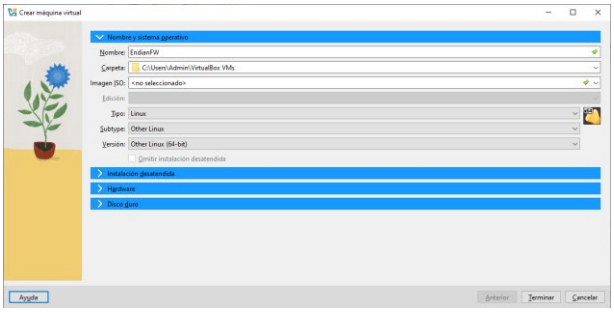
Para llevar a cabo la instalación de Endian Firewall, fue necesario crear previamente una máquina virtual con parámetros específicos en VirtualBox. Los siguientes pasos describen el proceso desarrollado:

En la interfaz de VirtualBox, se seleccionó la opción Nueva, asignando como nombre EndianFw, con tipo de sistema Linux y versión Linux 2.6 / 3.x / 4.x (64-bit).

Se asignó una memoria mínima de 1024 MB y un disco duro de al menos 8 GB, en formato VDI y con asignación dinámica de espacio.

En la Figura 2 se puede observar el proceso de creación inicial de la máquina virtual en VirtualBox.

Figura 2. Creación y configuración inicial de la máquina virtual Endian en VirtualBox.



Fuente: Autoría propia

Posteriormente, se configuraron los tres adaptadores de red necesarios para simular las zonas:

Adaptador 1: Tipo Adaptador interno, nombre de red LAN_zVerde (Zona Verde).

Adaptador 2: Tipo Adaptador interno, nombre de red DMZ_zNaranja (Zona Naranja).

Adaptador 3: Tipo Adaptador puente o NAT, para la Zona Roja (Internet simulada).

2.3 INSTALACIÓN DEL SISTEMA OPERATIVO ENDIAN

Una vez creada la máquina virtual, se procedió a montar la imagen ISO del sistema operativo Endian, previamente descargada desde su repositorio oficial [1]. Esta imagen fue cargada en el apartado de almacenamiento de VirtualBox para iniciar el proceso de instalación.

El asistente gráfico de instalación guió la configuración inicial, que incluyó:

Selección de idioma, aceptación de los términos de licencia, instalación completa en el disco detectado y reinicio del sistema para aplicar los cambios.

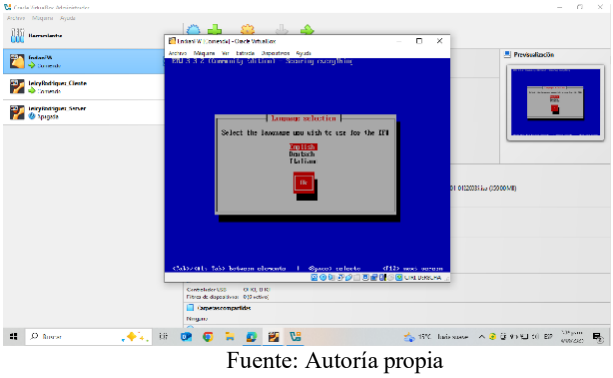
Tras reiniciar, el sistema solicitó la configuración de red. En esta etapa, se asignaron direcciones IP a las interfaces asociadas a cada zona:

Zona verde (eth0): 192.168.0.15
Zona naranja (eth1): 192.168.10.1
Zona roja (eth2): asignación automática por DHCP.

Finalizada la instalación, se accedió a la consola web de administración de Endian desde el navegador, mediante la dirección https://192.168.0.15:10443. Desde allí se definieron las zonas, se establecieron credenciales administrativas y se completó la configuración básica del sistema.

La asignación de interfaces y parámetros iniciales durante la instalación se detalla en la Figura 3.

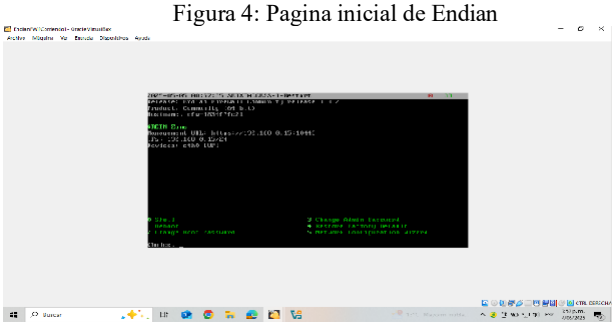
Figura 3. Asistente de instalación de Endian y definición de interfaces de red.



Fuente: Autoría propia

La interfaz de inicio de Endian una vez instalado se muestra en la Figura 4

Figura 4: Pagina inicial de Endian



Fuente: Autoría propia

3 TEMATICA 1: CONFIGURACIÓN DE LAS ZONAS DE RED EN ENDIAN FIREWALL

Como parte de la temática 1, se abordó la implementación de las zonas de red dentro de la arquitectura virtualizada con Endian Firewall. Estas zonas corresponden a distintos segmentos de seguridad: la zona verde (LAN), la zona naranja (DMZ) y la zona roja (WAN). Su correcta configuración es fundamental para garantizar la segmentación del tráfico, el aislamiento de servicios críticos y la implementación de políticas de seguridad.

La configuración se realizó desde VirtualBox, asignando un adaptador de red específico para cada zona. En esta sección se detallan los pasos seguidos para establecer las interfaces correspondientes a cada segmento.

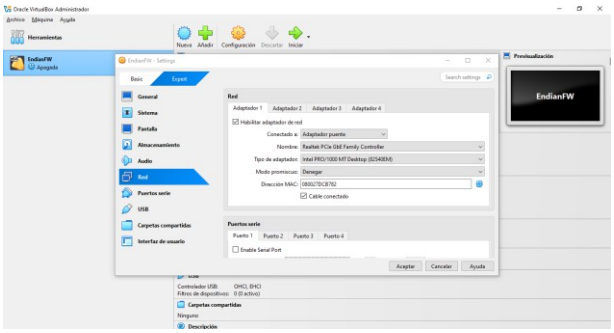
3.1 ZONA VERDE: RED INTERNA (LAN)

La zona verde representa la red interna segura, donde residen los equipos cliente. En VirtualBox, se configuró el Adaptador 1 como tipo Adaptador interno, con el nombre de red LAN_zVerde.

En Endian, esta zona se asoció a la interfaz eth0, a la cual se le asignó la dirección IP 192.168.0.15 con su respectiva máscara de subred. Esta configuración permite que los dispositivos internos (como el equipo cliente) puedan comunicarse a través del firewall y, posteriormente, acceder a servicios o a internet según las reglas definidas.

La configuración del adaptador de red para la zona verde se ilustra en la Figura 5.

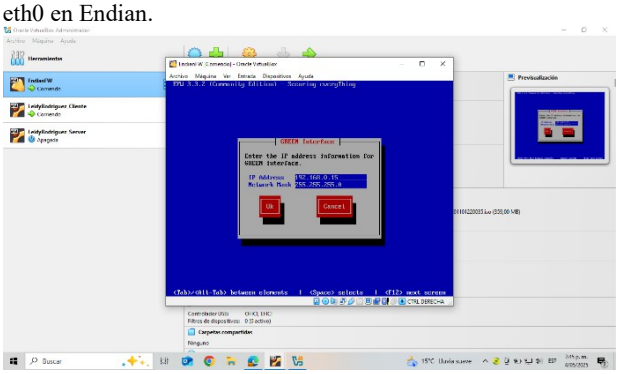
Figura 5. Configuración del adaptador de red para la zona verde en VirtualBox.



Fuente: Autoría propia.

La asignación de la IP 192.168.0.15 a eth0 se muestra en la Figura 6.

Figura 6. Asignación de la IP 192.168.0.15 a la interfaz eth0 en Endian.



Fuente: Autoría propia.

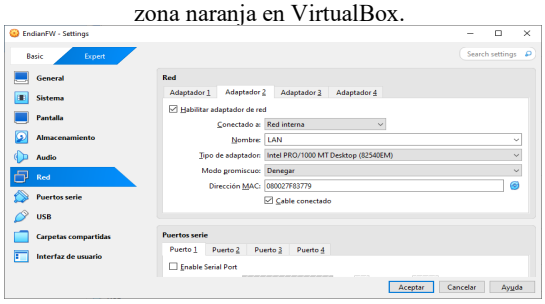
3.2 ZONA NARANJA: SERVIDORES EN DMZ

La zona naranja fue configurada para alojar servicios públicos como un servidor web o FTP, aislándolos de la red interna pero permitiendo su acceso controlado desde el exterior. En VirtualBox, se asignó el Adaptador 2 como Adaptador interno, bajo el nombre de red DMZ_zNaranja.

Dentro del asistente de configuración de Endian, esta zona fue asociada a la interfaz eth1, a la cual se le asignó la dirección IP estática 192.168.10.1. Esta red se utilizará más adelante por la máquina virtual que actúa como servidor, que debe tener su IP dentro del mismo rango para establecer comunicación directa.

La configuración del adaptador de red para la zona naranja puede verse en la Figura 7.

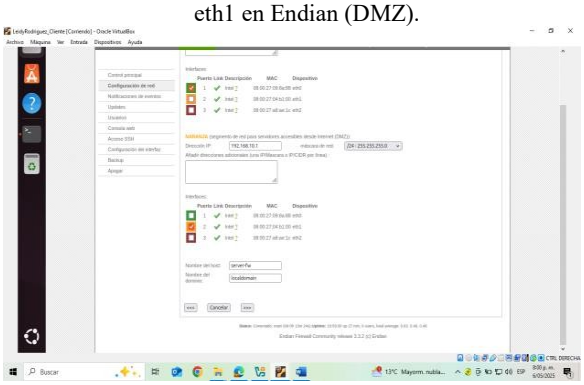
Figura 7. Configuración del adaptador de red para la zona naranja en VirtualBox.



Fuente: Autoría propia.

En la figura 8 se presenta la IP asignada a eth1 en la DMZ

Figura 8. Asignación de IP 192.168.10.1 a la interfaz eth1 en Endian (DMZ).



Fuente: Autoría propia.

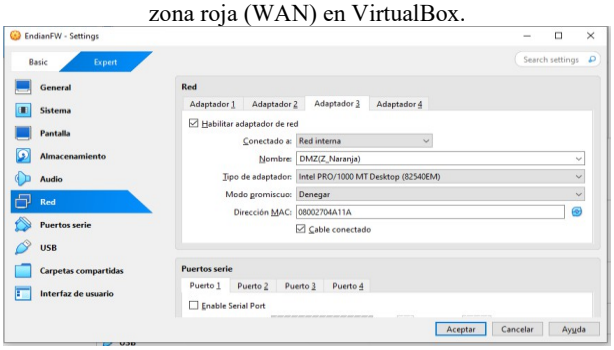
3.3 ZONA ROJA: CONEXIÓN SIMULADA A INTERNET (WAN)

La zona roja representa el acceso externo, es decir, la simulación de Internet. Para esta zona, se configuró el Adaptador 3 en VirtualBox como Adaptador puente (o NAT, según disponibilidad), lo que permite que Endian reciba una IP automáticamente por DHCP desde la red real del host.

En la configuración de Endian, esta zona fue asociada a la interfaz eth2, sin necesidad de definir manualmente una dirección IP. Esta conexión permitirá realizar pruebas de navegación desde la LAN y actualizaciones desde el servidor en DMZ, siempre que se establezcan reglas de red apropiadas.

La configuración del adaptador de red para la zona roja está representada en la Figura 9.

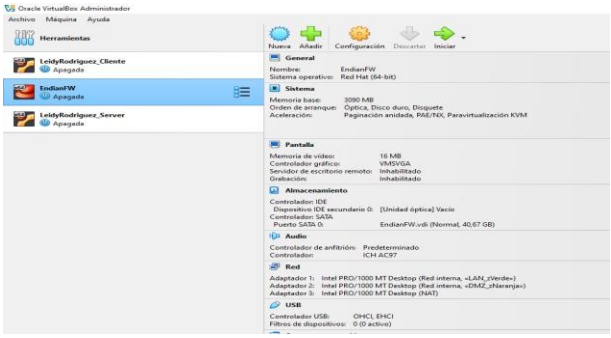
Figura 9. Configuración del adaptador de red para la zona roja (WAN) en VirtualBox.



Fuente: Autoría propia.

El estado final de las tres interfaces configuradas se muestra en la Figura 10.

Figura 10. Estado final de las tres interfaces de red en Endian.



Fuente: Autoría propia.

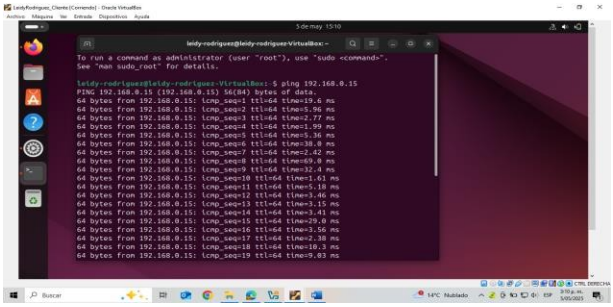
3.4 VERIFICACIÓN DE CONECTIVIDAD ENTRE ZONAS

Finalizada la configuración de las interfaces de red en Endian, se procedió a validar la conectividad entre las máquinas virtuales de cada zona. La prueba inicial consistió en ejecutar el comando ping desde la máquina cliente (zona verde) hacia la IP del firewall Endian en esa misma red (192.168.0.15), comprobando que el tráfico fluye correctamente a través del adaptador correspondiente.

De igual manera, se validó la conectividad desde el servidor (zona naranja) hacia su gateway asignado (192.168.10.1). Ambas pruebas arrojaron respuestas exitosas, lo que confirma que las redes internas están correctamente enlazadas.

La Figura 11 muestra el resultado de la prueba de conectividad mediante ping desde la zona verde.

Figura 11. Resultado del comando ping desde el cliente hacia el firewall en la zona verde.

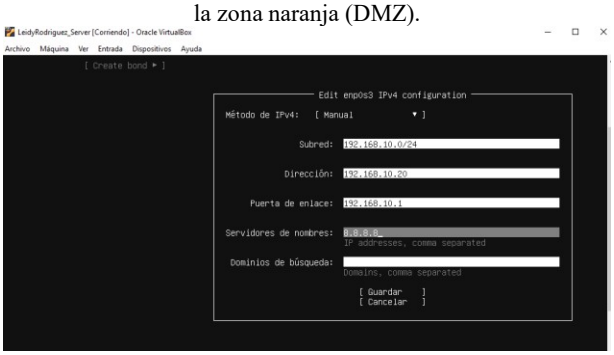


Fuente: Autoría propia.

Durante la instalación de la máquina virtual asignada como servidor, ubicada en la zona naranja (DMZ), se recomienda establecer una dirección IP estática. Esto se debe a que el adaptador de red utilizado corresponde a una red interna, sin asignación automática por DHCP. Definir una IP fija dentro del rango 192.168.10.0/24 garantiza que el servidor mantenga conectividad constante con el firewall Endian y pueda ser accedido de forma estable para futuras pruebas o servicios.

La IP estática del servidor en la zona naranja fue configurada como se muestra en la Figura 12.

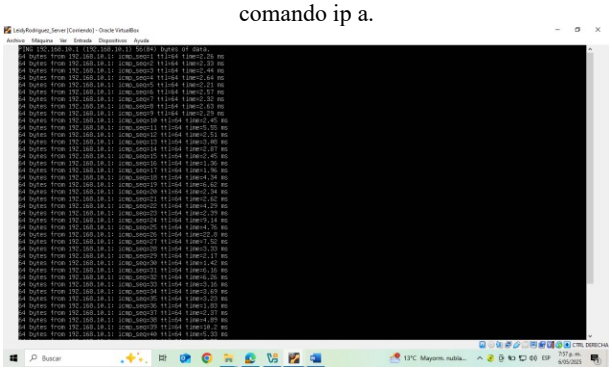
Figura 12. Configuración de IP estática en el servidor de la zona naranja (DMZ).



Fuente: Autoría propia.

La verificación de la IP mediante el comando `ip a` está documentada en la Figura 13.

Figura 13. Verificación de la IP del servidor mediante el comando ip a.



Fuente: Autoría propia.

La correcta configuración de las zonas de red en Endian Firewall constituye la base fundamental para una segmentación efectiva y segura. Establecer adaptadores específicos para cada zona, asignar direcciones IP adecuadas y validar conectividad asegura el flujo controlado de datos entre segmentos internos y externos. Esta infraestructura permite que el resto del equipo implemente funciones como NAT, proxy y control de servicios desde una arquitectura confiable.

4 TEMÁTICA 2: CONFIGURACIÓN NAT EN ENDIAN

Esta parte del proceso tiene como propósito dar acceso a internet al host cliente de la zona verde y al servidor de la zona naranja, mediante la configuración de las reglas NAT en el panel de Endian y la máquina virtual Endian será el 'puente' entre cada equipo e internet. Se debe comprobar acceso de Endian a internet, con un comando ping, por ejemplo, para estar seguros del estado inicial. Igualmente, se comprueba la conexión entre redes internas verde y naranja, entre las (2) ip, la del adaptador de red de Endian en esa zona, y su otro elemento, máquina virtual escritorio o máquina virtual servidor.

Tabla 1. Distribución de direcciones de red

Host	Zona	ip
Endian	Roja	192.168.0.119
	Verde	192.168.2.15
	Naranja	192.168.1.15
Cliente	Verde	192.168.2.20
Servidor	Naranja	192.168.1.20

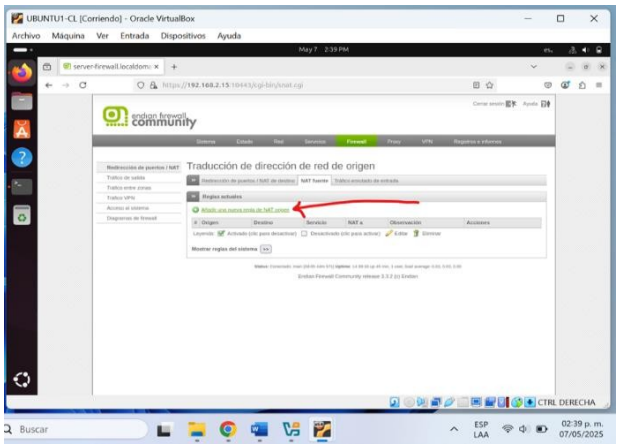
Fuente: Autoría Propia

4.1 CONFIGURAR REGLA NAT PARA LA COMUNICACIÓN DE LA LAN HACIA LA WAN

Para crear la regla NAT, se debe ir al panel superior Firewall>NAT fuente en la cinta de opciones horizontal y luego, dar clíck en la opción Añadir nueva regla NAT origen [4].

La ruta de configuración para añadir reglas NAT está descrita en la Figura 14.

Figura 14 . Ruta de configuración Firewall>Nat fuente>Añadir regla de NAT origen



Fuente: Autoría propia.

Posteriormente, en la ventana emergente para configurar la regla NAT, se deben llenar los campos con los valores, teniendo en cuenta que la dirección de la red verde es 192.168.2.0:

Panel Origen:
Tipo: Red/IP
En la caja de texto izquierda: 192.168.2.0 /24

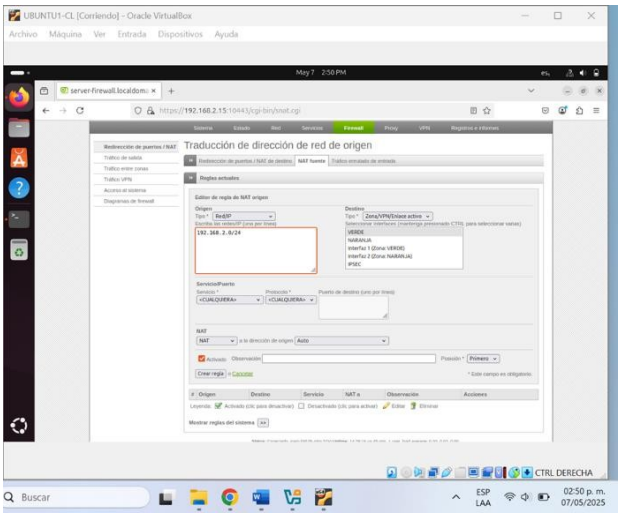
Panel Destino:
Tipo*: Zona/VPN/enlace Activo
En la caja de texto derecha: VERDE

En el panel Servicio/Puerto:
Servicio: <CUALQUIERA>
Protocolo: <CUALQUIERA>

El resto de los campos inferiores, se dejan por defecto y se da clíck en el botón Crear Regla

La regla NAT de la red verde hacia internet está detallada en la Figura 15.

Figura 15. Valores de la regla NAT que establece conexión de la red verde hacia internet



Fuente: Autoría Propia

A continuación, se debe dar clíck en un botón llamado Aplicar, que aparece al salir de la ventana de la regla NAT, para hacer efectivos los cambios.

4.2 CONFIGURAR REGLA NAT PARA LA COMUNICACIÓN DE LA DMZ HACIA INTERNET

En este paso se procede a hacer lo mismo para la red naranja, teniendo en cuenta su dirección de red 192.168.1.0/24.

Panel Origen:
Tipo: Red/IP
En la caja de texto izquierda: 192.168.1.0 /24

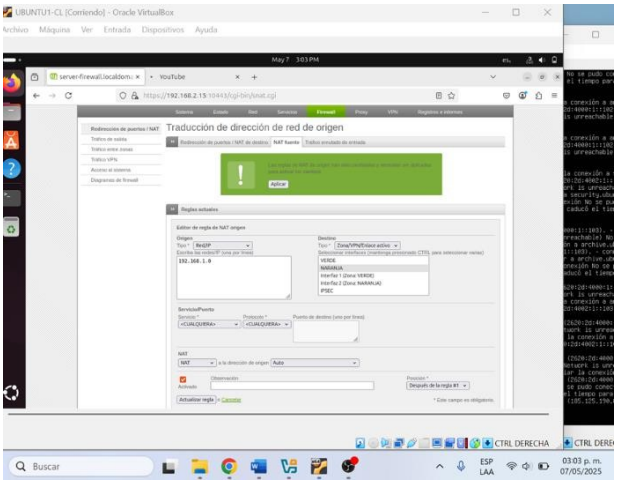
Panel Destino:
Tipo*: Zona/VPN/enlace Activo
En la caja de texto derecha: NARANJA
En el panel Servicio/Puerto:

Servicio: <CUALQUIERA>
Protocolo: <CUALQUIERA>

El resto de los campos inferiores, se dejan por defecto y se da clíck en el botón Crear Regla.

La configuración para la red naranja hacia internet se observa en la Figura 16.

Figura 16. Valores de la regla NAT que establece conexión de la red naranja hacia internet



Fuente: Autoría Propia

Posteriormente, al salir de la ventana, se despliega un mensaje en verde que indica que para que tomen efectos los cambios hay que dar click en aplicar, botón al cual se debe dar click.

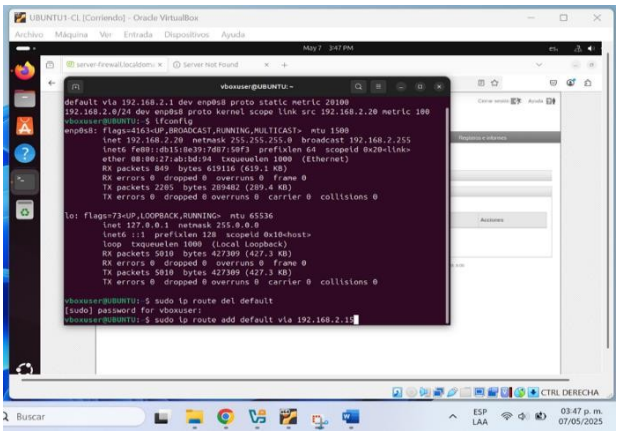
4.3 AJUSTE DE LA PUERTA DE ENLACE PREDETERMINADA EN LAS MÁQUINAS DE LAS REDES

Es necesario que las puertas de enlace predeterminadas, tanto en el cliente, como en el servidor sean las ip que tienen los adaptadores de red interna correspondientes de Endian para cada red, verde y naranja, para que por ahí se establezca la conexión hacia internet, a través de Endian. Por ello, se procede a cambiar manualmente la puerta de enlace por defecto (default Gateway) del cliente, que ahora no será 192.168.2.1, sino la ip de la zona verde de Endian 192.168.2.15

Se usan los comandos:
sudo ip route del default
sudo ip route add default via 192.168.2.15

La Figura 17 ilustra los comandos utilizados para definir la puerta de enlace en el cliente.

Figura 17. Ejecución de comandos para configuración de puerta de enlace predeterminada en la máquina virtual del cliente.

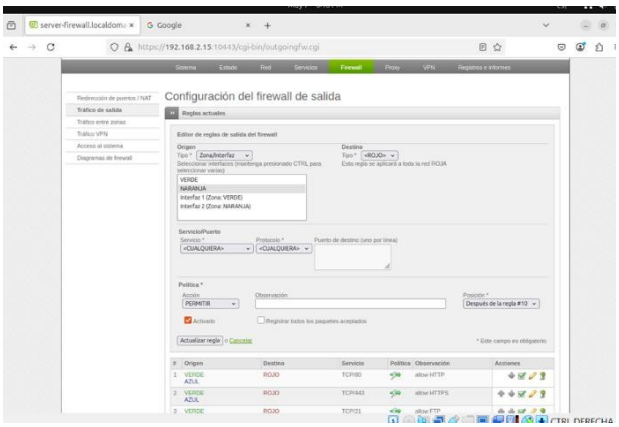


Fuente: Autoría Propia

Luego se puede ingresar a un sitio web, mediante el equipo de escritorio de la zona verde, en otra pestaña, aparte del panel web de Endian en 192.168.2.15:10443, por ejemplo, google:

El acceso a internet desde el navegador del cliente se muestra en la Figura 18.

Figura 18. Acceso a internet desde el navegador de la máquina virtual cliente en la zona verde



Fuente: Autoría Propia

Para cambiar la puerta de enlace predeterminada del servidor, se ejecuta el comando ip route default via [5], así:

sudo ip route add default via 192.168.1.15

Luego se debe verificar la configuración para el DNS, ejecutando el comando para editar:

sudo nano /etc/systemd/resolved.conf

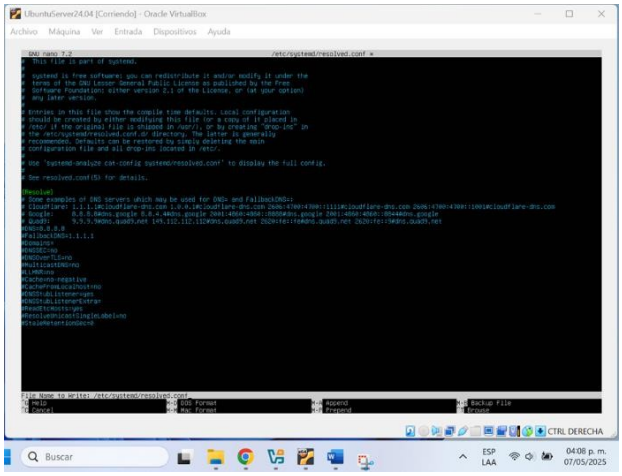
y agregar o cambiar el contenido para que quede así:

[Resolve]
DNS=8.8.8.8
FallbackDNS=1.1.1.1

La resolución de nombres en sistemas Linux modernos puede configurarse a través del archivo resolved.conf, el cual permite establecer DNS primarios y alternativos [6].

La edición del archivo resolved.conf con valores DNS está ilustrada en la Figura 19.

Figura 19. Edición de valores del DNS en el archivo resolved.conf



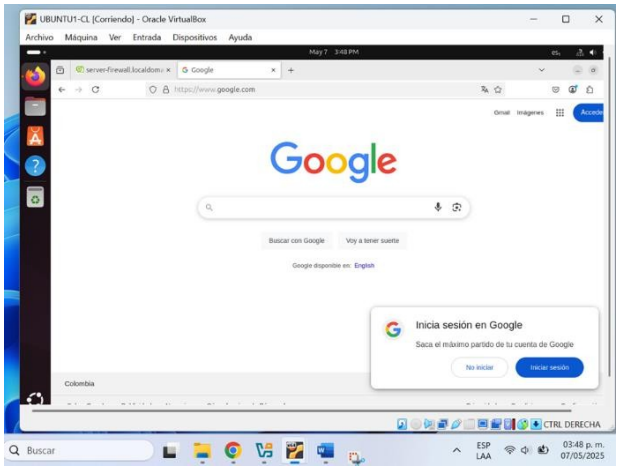
Fuente: Autoría Propia

Para que se apliquen los cambios, se reinicia el sistema con el siguiente comando:
sudo systemctl restart systemd-resolved

Fue necesario también, añadir una regla de tráfico de salida, con los valores que se muestran en la figura x, para conectar la red naranja hacia la red roja (internet)

En la Figura 20 se presenta la regla de salida para permitir conexión de la DMZ hacia Internet.

Figura 20. Regla para permitir acceso a internet desde la zona naranja



Fuente: Autoría Propia

Para terminar, se puede confirmar el acceso del servidor hacia internet, através de Endian, con el comando sudo apt-get update, para confirmar el acceso a internet para actualizar los repositorios del sistema.

5 TEMATICA 3. PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

En continuidad de las temáticas adelantadas, realizamos la respectiva configuración para permitir los servicios de la zona DMZ para la red establecida. Para ello se instalaron en esta zona (DMZ) un servidor web que permita servicios HTTP por el puerto 80 y un servidor que permita servicios FTP por el puerto 21, todo esto bajo Ubuntu Server. Dicha configuración se realiza en el Firewall Endian, junto con la denegación de protocolo ICMP en los puertos 8 y 30, para no permitir la realización de ping en la red.

5.1 CONFIGURACIÓN DE RED

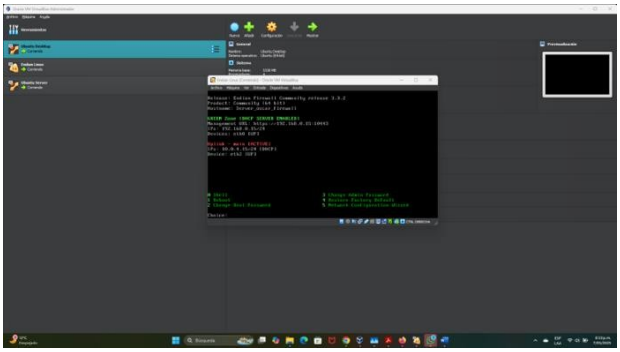
Tabla 2. Distribución de direcciones de red

Zona	Zona Roja	Zona verde	Zona Naranja
Gateway		192.168.0.15	192.168.10.1
Dirección IP		192.168.0.20/24	192.168.10.20/24
Host	Endian	Ubuntu Desktop 24.04	Ubuntu Server 24.04

Se definieron las direcciones IP´s y puertas de enlaces para establecer los parámetros de comunicación y definición de zonas.

La Figura 21 muestra la configuración de zonas verde y roja en Endian.

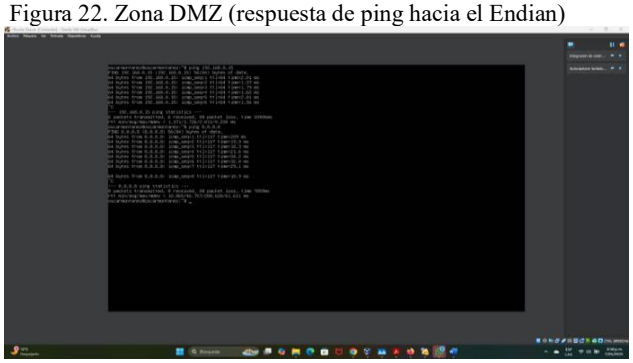
Figura 21. Zona verde (LAN) y zona roja (WAN) en Endian



Fuente: Autoría Propia

La respuesta de ping desde la zona DMZ se presenta en la Figura 22.

Figura 22. Zona DMZ (respuesta de ping hacia el Endian)



Fuente: Autoría Propia

5.2 SERVICIOS HTTP Y FTP

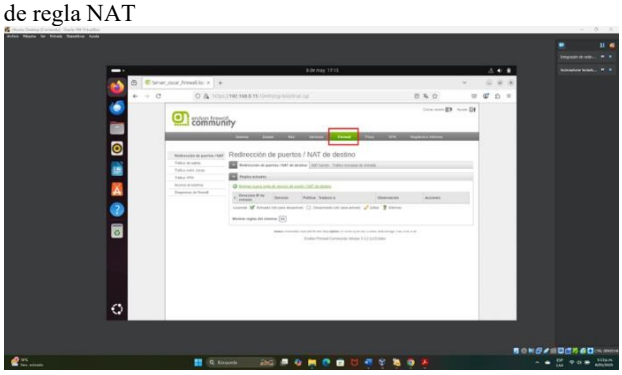
Para poder utilizar estos servicios, es preciso tener gestores de estos mismos en el servidor (DMZ), para ello realizamos primero la habilitación de acceso a internet al servidor (desde zona naranja hacia zona roja) para poder instalar los paquetes necesarios.

5.2.1 INSTALACIÓN Y CONFIGURACIÓN DE SERVICIOS

Primero accedemos desde el navegador del equipo en zona verde al Firewall Endian, ya alli iniciamos creando una regla NAT para poder hacer el puente de acceso entre las zonas especificadas (se especifica IP de servidor para su traducción a ip pública en zona roja).

La configuración de la regla NAT en el firewall se muestra en la Figura 23.

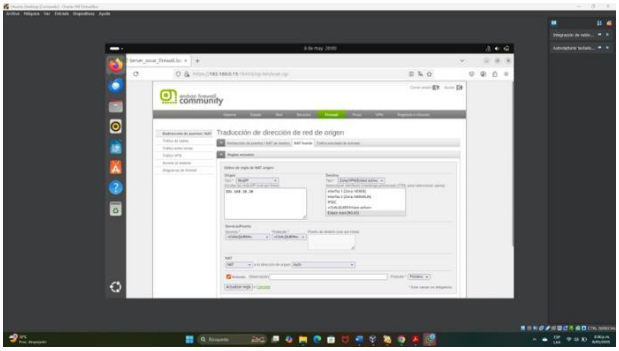
Figura 23. Acceso a la zona del firewall para la creación de regla NAT



Fuente: Autoría Propia

La Figura 24 detalla la IP del servidor redireccionada hacia la zona roja.

Figura 24. Desde la opción Fuente NAT, Indicamos la IP de nuestro servidor (origen) va hacia la zona roja (destino)

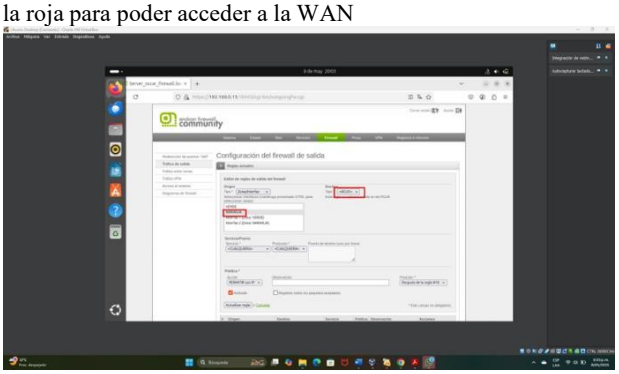


Fuente: Autoría Propia

Ahora que ya definimos la regla que nos permite el puente, definimos la salida en el firewall para que pueda pasar de LAN a WAN.

La regla para permitir el tráfico de la zona naranja hacia la roja se presenta en la Figura 25.

Figura 25. Indicamos que va desde la zona naranja hacia la roja para poder acceder a la WAN

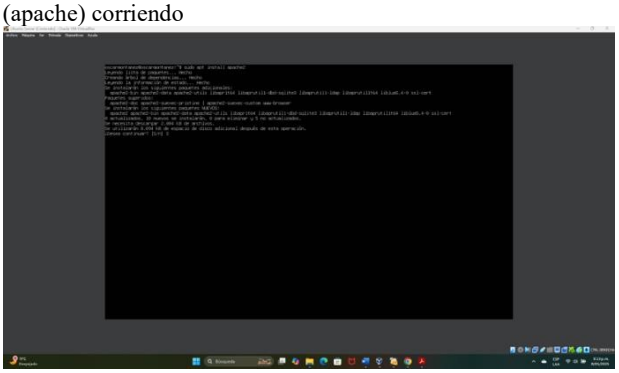


Fuente: Autoría Propia

Una vez habilitado el acceso desde el server hacia la red de internet, instalaremos el servidor web **Apache** y el servidor FTP **vsFTPd**

La instalación del servidor Apache se muestra en la Figura 26.

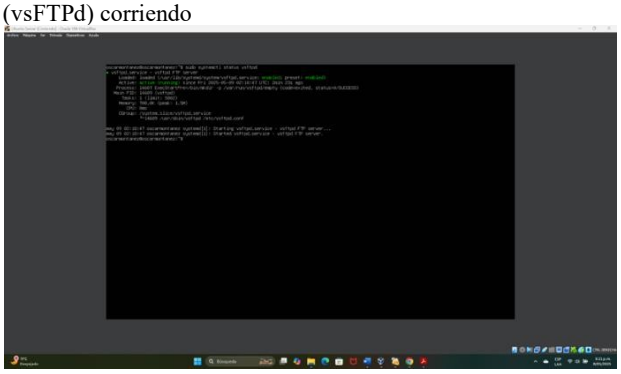
Figura 26: Instalación y verificación del servidor web (apache) corriendo



Fuente: Autoría Propia

La Figura 27 ilustra la instalación del servidor FTP (vsFTPd).

Figura 27: Instalación y verificación del servidor FTP (vsFTPd) corriendo



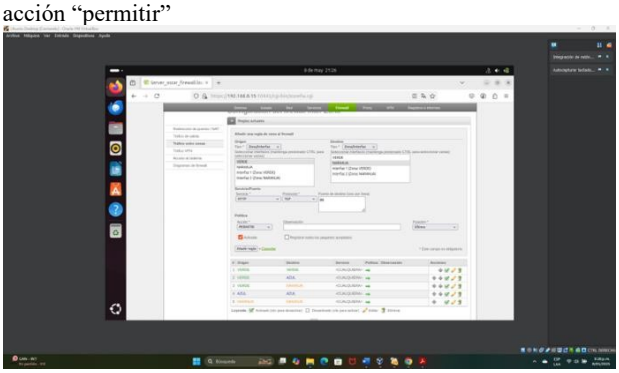
Fuente: Autoría Propia

5.2.2 CONFIGURACIÓN EN ENDIAN

Desde la interfaz gráfica del firewall Endian, creamos las reglas necesarias para que sea accesible los servicios descritos previamente, inicialmente en la sección de firewall – Trafico entre zonas, agregaremos las correspondientes reglas para permitir en primer caso, servicios HTTP por el puerto 80.

La creación de la regla para el servicio HTTP se observa en la Figura 28.

Figura 28: Desde la zona verde hacia la naranja, agregamos reglas de servicio http, por el puerto 80 (TCP), y en acción “permitir”

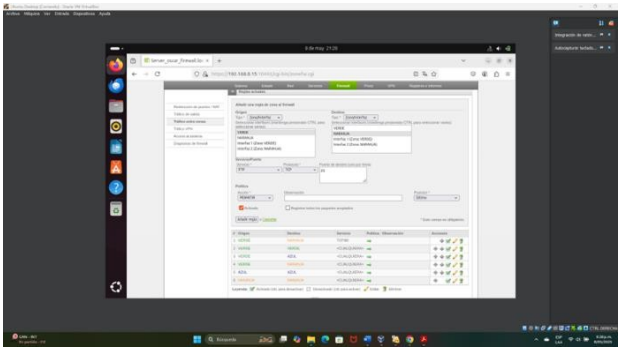


Fuente: Autoría Propia

Para el servicio FTP, agregaremos otra regla al igual que la anterior, pero en esta indicaremos que el servicio permitido será FTP, por el puerto 21

Las reglas para permitir el servicio FTP se presentan en las Figuras 29 y 30

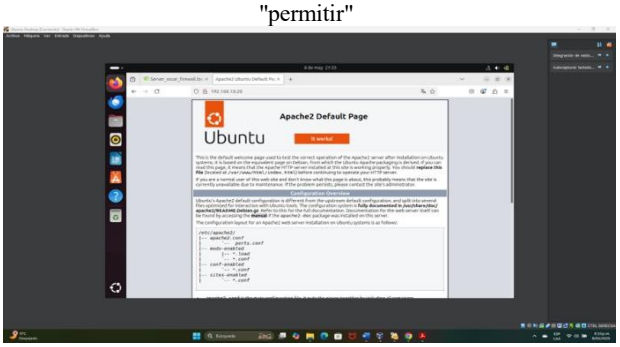
Figura 29: Servicio FTP, TCP por el puerto 21 y acción "permitir"



Fuente: Autoría Propia

Probamos desde el mismo equipo en zona verde, el acceso al servidor web por el puerto 80 y desde la terminal, acceso al servidor FTP.

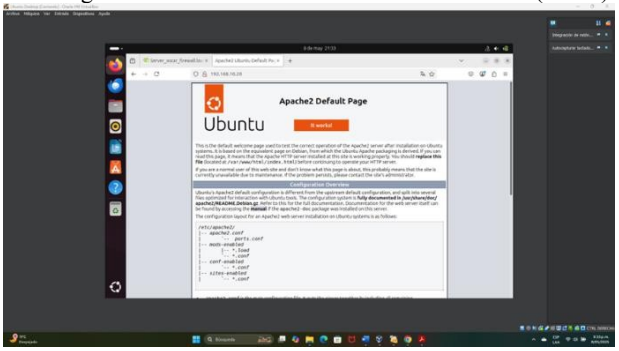
Figura 30: Servicio FTP, TCP por el puerto 21 y acción "permitir"



Fuente: Autoría Propia

El acceso desde la zona verde al servidor HTTP se muestra en la Figura 31.

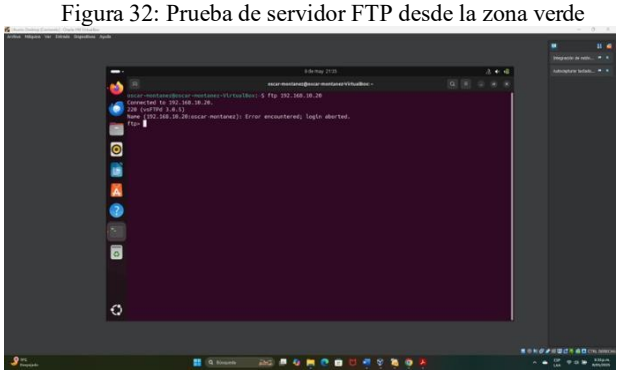
Figura 31: Prueba en zona verde del servidor web (HTTP)



Fuente: Autoría Propia

La conexión FTP desde la zona verde se valida en la Figura 32.

Figura 32: Prueba de servidor FTP desde la zona verde



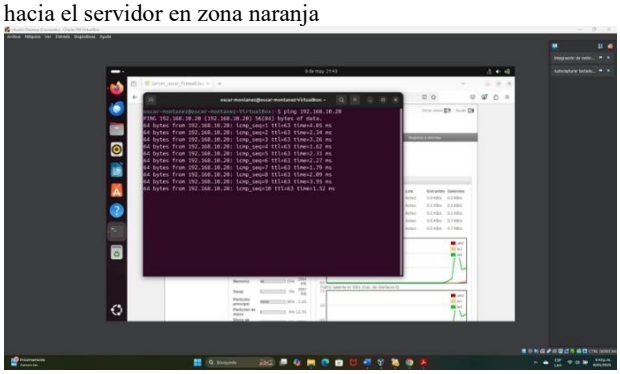
Fuente: Autoría Propia

5.3 DENEGAR EL PROTOCOLO ICMP (PUERTO 8 Y PUERTO 30)

Desde el firewall Endian, se puede restringir la comunicación entre los hosts de la red. Para ello se agregan reglas entre las zonas sobre el protocolo indicado. Inicialmente probaremos la respuesta del protocolo ICMP sobre la red.

El resultado del ping desde la zona verde a la DMZ se documenta en la Figura 33.

Figura 33: Prueba de ping desde equipo en zona verde hacia el servidor en zona naranja



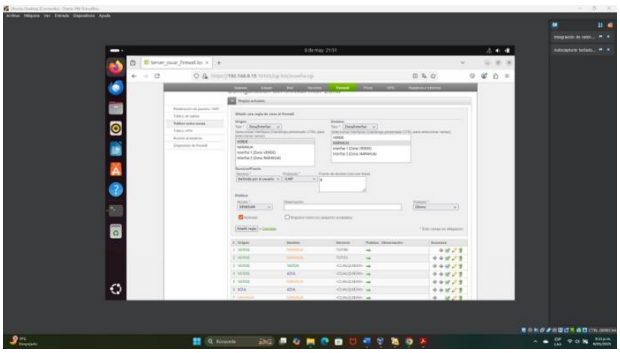
Fuente: Autoría Propia

5.3.1 CONFIGURACIÓN EN ENDIAN – TRÁFICO ENTRE ZONAS

Desde el Endian, en la sección de firewall – Trafico entre zonas, agregaremos las correspondientes reglas para denegar el protocolo ICMP por los puertos 8 y 30.

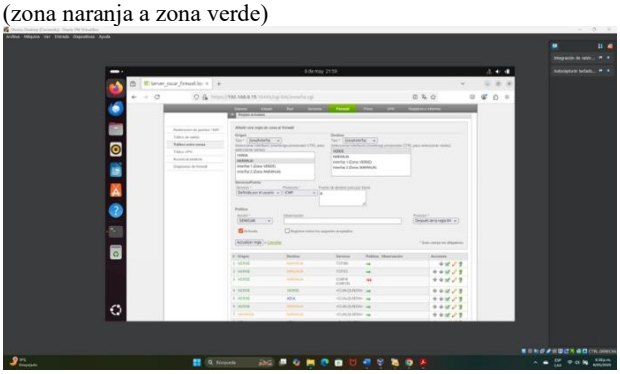
Las reglas para bloquear ICMP entre zonas están representadas en las Figuras 34 y 35.

Figura 34: Agregamos regla desde zona verde hacia zona naranja bajo protocolo ICMP puerto 8 y 30 con la acción "denegar"



Fuente: Autoría Propia

Figura 35: Agregamos la misma regla en sentido inverso (zona naranja a zona verde)



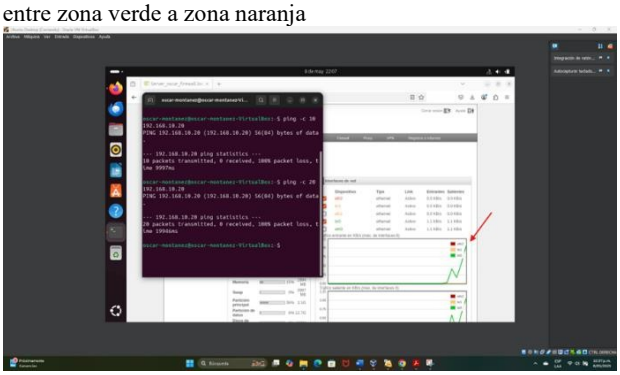
Fuente: Autoría Propia

5.3.2 PRUEBAS DE DENEGACIÓN Y REGISTRO DE INFORME

Una vez aplicadas las reglas, se realizan las pruebas desde la terminal tanto del equipo en zona verde, como desde la consola del servidor.

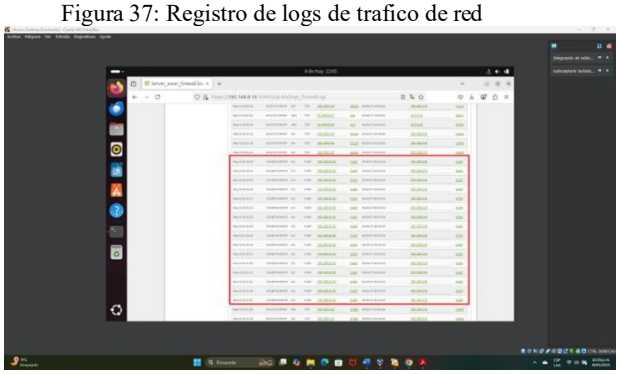
La denegación de tráfico y el registro en logs se muestra en las Figuras 36 y 37.

Figura 36: Gráfico y registro de denegación del servicio entre zona verde a zona naranja



Fuente: Autoría Propia

Figura 37: Registro de logs de trafico de red



Fuente: Autoría Propia

6 TEMATICA 4. REGLAS DE ACCESOS PARA PERMITIR O DENEGAR EL TRÁFICO.

6.1 RESUMEM.

En esta fase del proyecto se implementó una red segmentada utilizando Endian Firewall con el objetivo de controlar el tráfico entre tres zonas bien definidas: Verde, Naranja y Roja. El entorno fue desplegado en máquinas virtuales a través de VirtualBox. Un servidor Ubuntu alojado en la zona DMZ brindó servicios HTTP y FTP, mientras que un equipo cliente con Linux Mint en la zona LAN permitió realizar pruebas de acceso. Se configuraron reglas específicas en el firewall para permitir o denegar tráfico, y también se implementaron redirecciones desde la zona ROJA. Durante el proceso se presentaron diversos retos de conectividad y configuración, que fueron resueltos aplicando comandos, ajustes de red y pruebas con herramientas como ping, curl y ftp. El resultado fue una infraestructura funcional y segura, que permite comprender de manera práctica el manejo de reglas entre zona.

6.2 ARQUITECTURA DE RED

La red fue organizada en tres zonas conectadas a través de Endian Firewall:

Zona VERDE (LAN): Representada por una máquina Linux Mint con IP 192.168.2.20. Esta máquina simuló a un usuario interno que accede a servicios dentro y fuera de la red.

Zona NARANJA (DMZ): Ubuntu Server con IP 192.168.3.10, configurado para ofrecer servicios web (Apache) y FTP (vsftpd). Esta zona es un puente controlado entre la red interna y el exterior.

Zona ROJA (WAN): Equivale al acceso a Internet. Se implementó mediante un adaptador puente en Endian que recibió una IP de la red real, usada para simular peticiones externas.

Tabla 3 Estructura de red con sus respectivas zonas.

Verde	Cliente	Linux Mint	192.168.2.20	Navegar, acceder a servicios internos/externos
Naranja	Servidor	Ubuntu Server	192.168.3.10	Servidor HTTP (Apache) y FTP (vsftpd)
Rojo	Interfaz	Endian Firewall	192.168.0.12	Acceso simulado a Internet desde el exterior
	Firewall		3 interfaces (una por zona)	Control de tráfico entre zonas y reglas NAT

Fuente: Autoría Propia

6.3 CONFIGURACION DE SERVICIOS

Para brindar servicios reales y comprobables:

Apache2: Instalado en Ubuntu Server para servir una página web. Se accedió desde la LAN y desde el exterior usando un navegador y comandos como curl.

vsftpd: Servidor FTP instalado y configurado con el usuario pruebaftp, permitiendo pruebas de conexión desde distintas zonas.

Se comprobó el funcionamiento correcto de los puertos 21 (FTP) y 80 (HTTP) mediante comandos y análisis del tráfico.

6.4 REGLAS DE ACCESO EN ENDIAN

Una parte fundamental del trabajo fue definir qué tipo de tráfico estaba permitido entre zonas:

Accesos permitidos: Se autorizaron conexiones HTTP y FTP desde la zona VERDE a la NARANJA.

Redirección desde la Zona ROJA: Se configuró NAT para redirigir tráfico de Internet (ROJA) hacia el servidor Ubuntu en la DMZ, tanto para HTTP como para FTP.

Accesos restringidos: Se bloquearon paquetes ICMP (ping) desde ciertas zonas para aumentar la seguridad y reducir visibilidad innecesaria.

6.5 PRUEBAS REALIZADAS

Se llevaron a cabo pruebas prácticas para comprobar que las reglas funcionaban como se esperaba, cada una de estas pruebas fue acompañada por capturas y validaciones que sirvieron como evidencia del cumplimiento técnico del objetivo y que se muestran a continuación.

- Acceso HTTP desde Linux Mint hacia Ubuntu Server (DMZ).
- Acceso desde Mint a sitios web externos usando curl.
- Validación de conexión desde Ubuntu hacia Internet.
- Acceso desde Mageia (host real) al Apache de Ubuntu usando IP pública de Endian.
- Pruebas FTP desde Mint hacia servidores externos.
- Pruebas FTP desde Mageia hacia el servidor Ubuntu redirigido por NAT.

La Figura 38 presenta la configuración de reglas inter-zona.

Figura 38. Configuración de reglas Inter - Zona

Fuente: Autoría Propia

La configuración del firewall de salida se muestra en la Figura 39.

Figura 39. Configuración Firewall de salida

Fuente: Autoría Propia

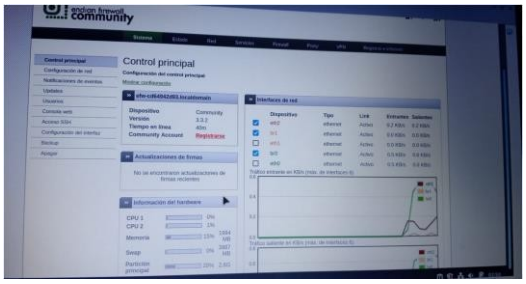
La configuración de puertos y reglas NAT se representa en la Figura 40.

Figura 40. Configuración de Puertos / NAT

Fuente: Autoría Propia

El control principal de Endian se visualiza en la Figura 41.

Figura 41. Visualización control principal Endian



Fuente: Autoría Propia

El entorno final reflejó un sistema segmentado funcional, en el que se pudo controlar el tráfico de forma precisa usando Endian. Las reglas aplicadas permitieron filtrar, redirigir y limitar accesos entre zonas, y los servicios instalados fueron visibles y accesibles solo según lo previsto. Se cumplieron todos los puntos exigidos en la temática.

7 TEMÁTICA 5: IMPLEMENTACIÓN DEL PROXY NO TRANSPARENTE CON POLÍTICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET

7.1 RESUMEN

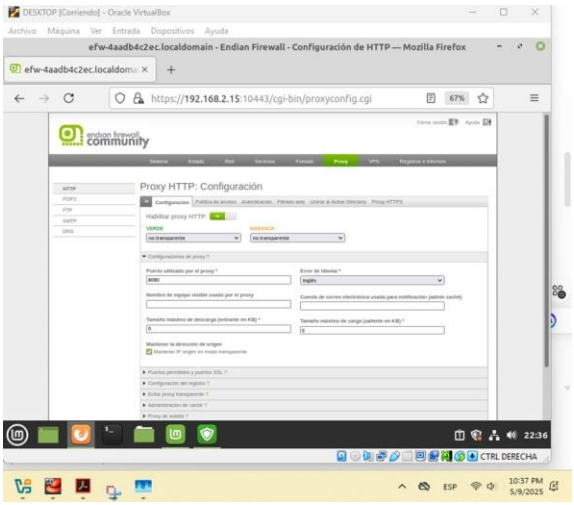
En esta etapa se configuró un proxy HTTP no transparente en el firewall Endian, con el fin de controlar el acceso a Internet desde la red interna (zona verde). Se creó un perfil de filtrado con una lista negra de sitios web restringidos (como YouTube, nuevodia y Hotmail), y se implementó un sistema de autenticación por usuario mediante el método local (NCSA). Los usuarios deben autenticarse para navegar, y las políticas aplicadas permiten o bloquean el acceso según el perfil asignado. La prueba se realizó desde una máquina cliente configurada con el proxy, verificando el correcto funcionamiento del control de acceso.

7.2 ACTIVACION DE PROXY

Se habilitó el proxy HTTP en modo no transparente en Endian, configurando el puerto 8080 y activando la autenticación local para controlar el acceso desde la red interna (zona verde).

La interfaz de configuración del proxy HTTP se presenta en la Figura 42.

Figura 42. Visualización panel de configuración proxy HTTP



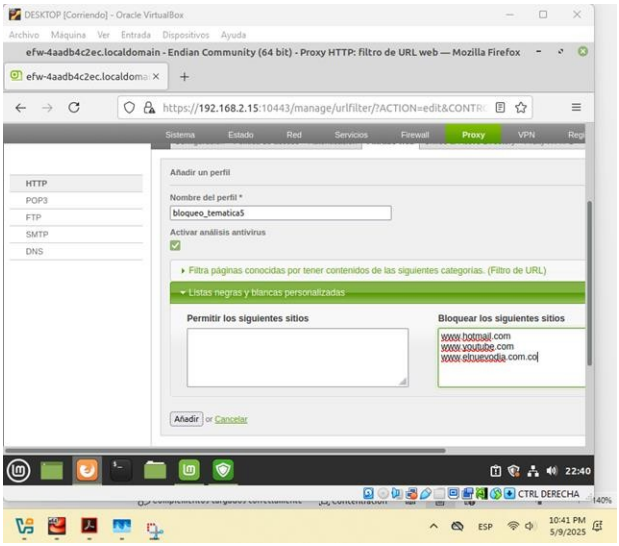
Fuente: Autoría Propia

7.3 CREACION DE PERFIL (LISTA NEGRA)

Se creó un perfil de filtrado en el proxy de Endian con una lista negra que bloquea sitios como YouTube, Hotmail y El Nuevo Día, aplicando restricciones de navegación a los usuarios autenticados.

La creación del perfil de filtrado se muestra en la Figura 43.

Figura 43. Visualización panel de configuración filtro URL



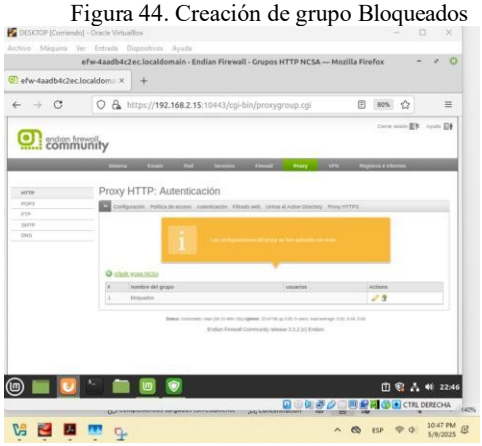
Fuente: Autoría Propia

7.4 CREACION DE USUARIOS Y GRUPOS PARA EL PROXY

Se crea un grupo llamado bloqueados, luego se genera un usuario y se asocia a ese grupo. Posteriormente, se configura una política de acceso vinculando al grupo y al perfil de filtrado con los sitios prohibidos.

La creación del grupo de usuarios bloqueados está documentada en las Figuras 44 y 45.

Figura 44. Creación de grupo Bloqueados

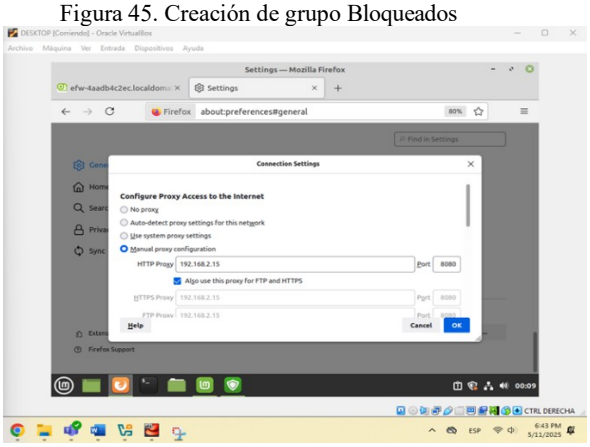


Fuente: Autoría Propia

7.5 CONFIGURACION DEL NAVEGADOR DEL CLIENTE (LINUXMINT) DESKTOP

En Firefox, se configura el uso del proxy. Al acceder a internet, se solicita el usuario y contraseña del proxy para autenticar. Una vez ingresados, permite la navegación según las políticas definidas.

Figura 45. Creación de grupo Bloqueados



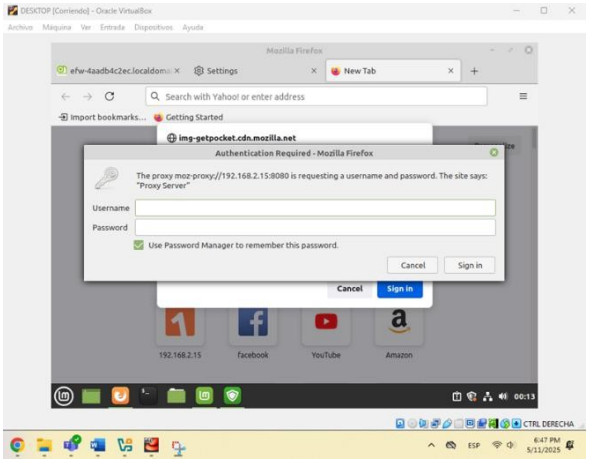
Fuente: Autoría Propia

7.6 REALIZACION DE PRUEBAS

Al intentar ingresar a sitios como Hotmail, YouTube o ElNuevodia.com.co, el navegador muestra un mensaje de acceso denegado, confirmando que la lista negra del proxy funciona correctamente.

La autenticación al acceder a Internet se valida en la Figura 46.

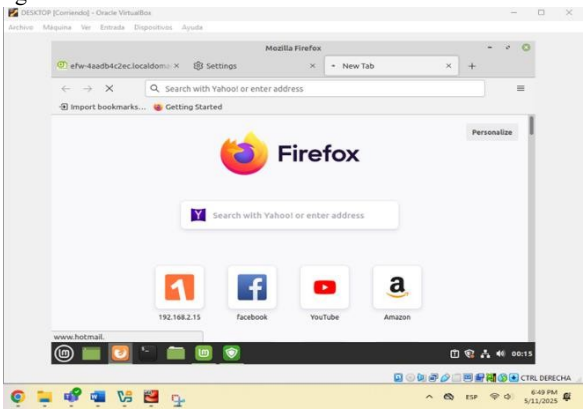
Figura 46. validamos que nos solicita usuario y contraseña previamente creadas



Fuente: Autoría Propia

El acceso exitoso a Google tras autenticarse se muestra en la Figura 47.

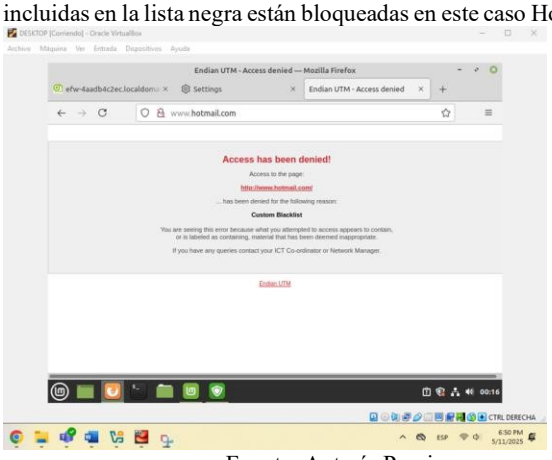
Figura 47. validamos que nos permite acceder a Google luego de suministrar las credenciales



Fuente: Autoría Propia

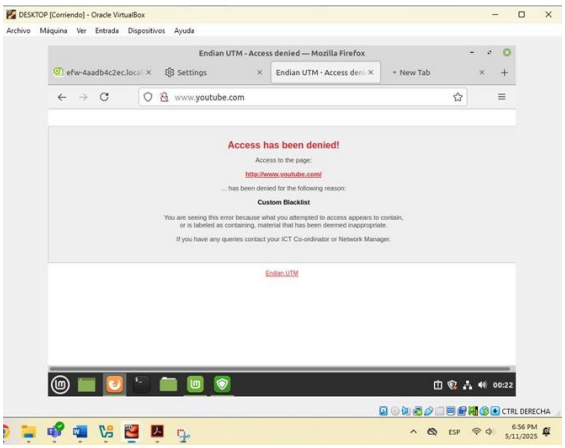
La denegación de acceso a sitios bloqueados se evidencia en las Figuras 48, 49 y 50.

Figura 48. validamos que efectivamente las paginas incluidas en la lista negra están bloqueadas en este caso Hotmail



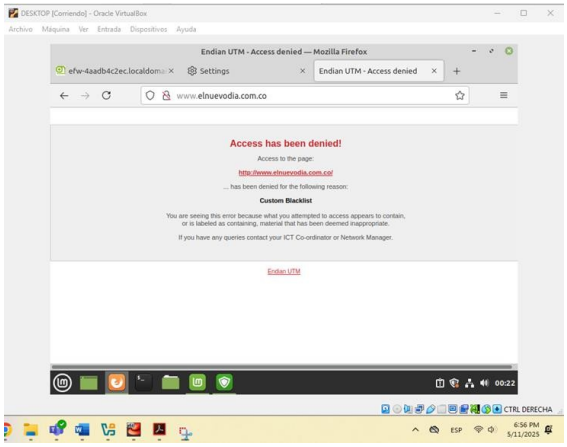
Fuente: Autoría Propia

Figura 49. validamos que efectivamente las paginas incluidas en la lista negra están bloqueadas en este caso Youtube



Fuente: Autoría Propia

Figura 50. validamos que efectivamente las páginas incluidas en la lista negra están bloqueadas en este caso Nuevodia.com.co



Fuente: Autoría Propia

7.1.1 CONCLUSIONES.

La instalación y configuración inicial de Endian Firewall permitió establecer la base de una arquitectura de red segmentada, funcional y segura, sobre la cual se desarrollaron las temáticas del presente artículo. A través de la creación de una máquina virtual con adaptadores correctamente asignados, se logró simular tres zonas de red —verde (LAN), naranja (DMZ) y roja (WAN)—, garantizando la separación lógica del tráfico.

La primera temática permitió evidenciar la importancia de asignar direcciones IP fijas, configurar correctamente cada adaptador en VirtualBox y validar la conectividad entre zonas mediante pruebas básicas como ping y verificación de puerta de enlace. Esta estructura inicial fue esencial para que las demás temáticas pudieran implementar servicios, reglas de acceso y mecanismos de seguridad de forma ordenada y efectiva. En conjunto, se demuestra que Endian es una herramienta útil para el aprendizaje y simulación de redes perimetrales en entornos virtualizados.

Durante el desarrollo de la temática se logró implementar y configurar el firewall Endian con sus respectivas zonas: verde (LAN), roja (WAN) y naranja (DMZ). Se permitió el acceso a los servicios HTTP y FTP desde el servidor Ubuntu en la DMZ, y se bloqueó el protocolo ICMP para mejorar la seguridad perimetral. Estas configuraciones permiten un control eficaz del tráfico entre zonas, fortaleciendo la protección de los recursos y servicios críticos.

Un entorno virtual correctamente estructurado puede simular con precisión el comportamiento de una red empresarial, incluyendo servicios HTTP, FTP, resolución DNS y control de tráfico por zonas.

8 CITAS Y/O REFERENCIAS

[1] Endian Team. (2023). Endian UTM Appliance Reference Manual. Endian S.r.l. Recuperado de https://docs.endian.com

[2] 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.

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

[4] Endian Team, "Endian UTM Appliance Reference Manual," Endian S.r.l., 2023. [Online]. Disponible en: https://docs.endian.com

[5] T. B. Smith, Linux Network Administration, 3rd ed., O'Reilly Media, 2020.

[6] L. Potter, Modern Linux Administration, Packt Publishing, 2021.

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

[8] Endian. (2016). Endian UTM 3.2 Manual de referencia. Endian Firewall. http://docs.endian.com/3.2/utm/index.html

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

• Cervelión, Á. J. (2023). Instalación de Nagios Core 4.4 en Ubuntu 22.04 . [Objeto_virtual_de_información_OVI]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/54230

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

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

• Guzman, D. (2022). VirtualBox con Endian 3.3.2, 3 Zonas_ Verde, Naranjada y Roja. Repositorio. Url: VirtualBox con Endian 3.3.2, 3 Zonas_ Verde, Naranjada y Roja.mp4

• Jay LaCroix. (2020). Mastering Ubuntu Server : Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting Ubuntu Server . Packt Publishing. https://research-ebsco-com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b41952

• LPI LPIC-1 Exam 101. (2022). Tema 102: Comandos GNU y Unix . https://learning.lpi.org/es/learning-materials/101-500/102/

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