INTEGRACIÓN DE SERVICIOS GNU/LINUX Y SEGURIDAD DE RED MEDIANTE ENDIAN FIREWALL

Ediver Andres Obando Cruz
Eaobandoc@unadvirtual.edu.co
Carlos Dairo Herrán Castañeda
cdherranc@unadvirtual.edu.co
Dainer Camilo Cortes Ramírez
dccortesra@unadvirtual.edu.co
Noe Villegas Castro
nvillegascas@unadvirtual.edu.co

RESUMEN: Este trabajo presenta el proceso de instalación, configuración y validación de una infraestructura de seguridad perimetral basada en GNU/Linux Endian Firewall, implementada en un entorno virtualizado mediante VirtualBox. Se establecieron las zonas Verde (LAN), Roja (WAN) y Naranja (DMZ), garantizando una segmentación lógica adecuada. Se configuraron reglas NAT para permitir la comunicación controlada desde la LAN y la DMZ hacia la red WAN simulada. Además, se habilitaron servicios HTTP y FTP en la DMZ, aplicando restricciones al protocolo ICMP para reforzar la seguridad. Se desarrollaron reglas de acceso interzonales para permitir y denegar tráfico según los requerimientos, verificando su funcionamiento mediante pruebas de conectividad y monitoreo del tráfico. Finalmente, se implementó un proxy HTTP no transparente con autenticación por usuario y listas negras de navegación, evaluando su correcto funcionamiento desde la LAN. Los resultados confirman la eficacia de Endian Firewall como plataforma de filtrado y control de tráfico en redes segmentadas.

PALABRAS CLAVE: Firewall, NAT, DMZ, Endian

1 INTRODUCCIÓN

El creciente panorama de amenazas informáticas exige la implementación de arquitecturas de red robustas que integren mecanismos de defensa perimetral, en este contexto, las plataformas firewall de código abierto, como GNU/Linux Endian, nos ofrecen herramientas avanzadas para la segmentación, inspección y control del tráfico en entornos corporativos y educativos, su implementación en escenarios virtualizados proporciona una estrategia eficaz para el aprendizaje práctico de conceptos de seguridad de red.

Este proyecto se enfoca en la construcción de una infraestructura segmentada mediante las zonas Verde, Roja y Naranja, acompañada de la configuración de reglas NAT y políticas de acceso para garantizar comunicaciones seguras y controladas. Las pruebas realizadas incluyen habilitación de servicios en la DMZ, restricciones de protocolos, redirección de puertos y validación del tráfico entre zonas, permitiendo evaluar el comportamiento del firewall ante distintos flujos de red.

Además, se implementó un proxy HTTP no transparente con autenticación y filtrado por listas negras, reforzando las políticas de navegación y control de usuarios. La integración de estos mecanismos permite valorar la capacidad de Endian Firewall como solución integral para la administración del acceso y la protección del perímetro en arquitecturas de red segmentadas.

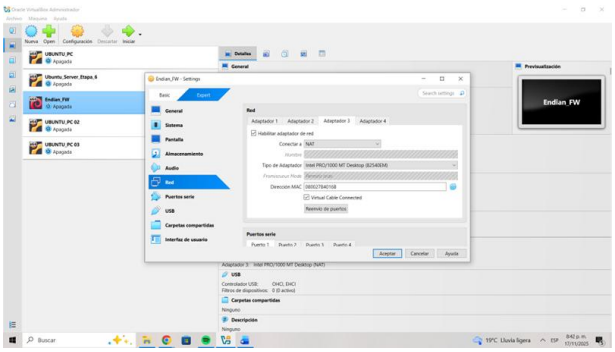
2 DESARROLLO DE LAS TEMÁTICAS

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

En la etapa inicial luego de haber descargado la ISO de Endian Firewall se definen las tarjetas de red correspondientes a las zonas Verde, Roja y Naranja, garantizando su correcta asignación antes de proceder con la instalación del sistema. Esta base técnica permite asegurar que el firewall funcione adecuadamente y que las zonas operen de forma aislada y controlada desde el inicio.

Antes de instalar la ISO procedemos a configurar las interfases de red para la red roja, verde y naranja, la primera será la roja, la cual tendrá acceso a internet, por tanto, la configuramos en un adaptador tipo NAT con DHCP para que asigne automáticamente las ip a las maquinas que se conecten.

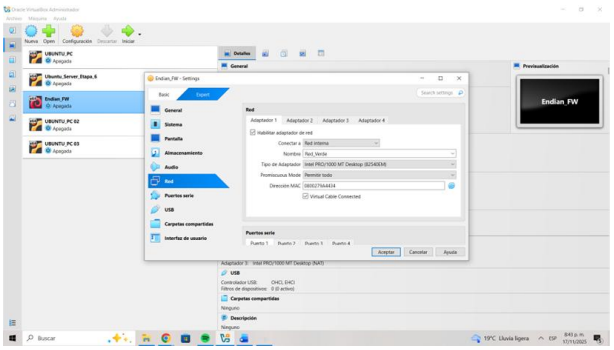
Ilustración 1Configuracion interfaz de red roja



Fuente: Autoría Propia

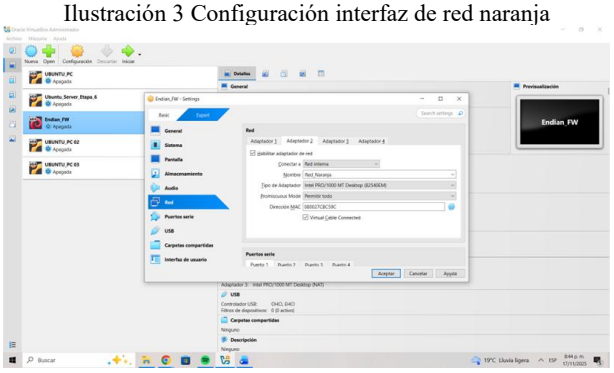
Para las redes Verde y Naranja, usaremos redes internas, nombrándolas con sus colores correspondientes.

Ilustración 2 Configuración interfaz de red verde



Fuente: Autoría Propia

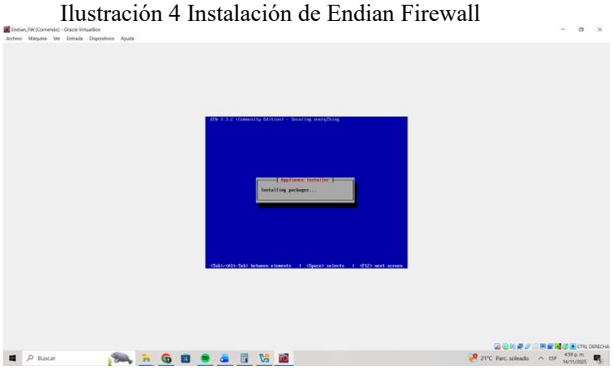
Ilustración 3 Configuración interfaz de red naranja



Fuente: Autoría Propia

Luego de configurar las interfaces de red procedemos a crear la máquina virtual destinada para Endian habilitando los 3 adaptadores para cada una de las redes, se procede a realizar la instalación siguiendo las instrucciones del menú interactivo.

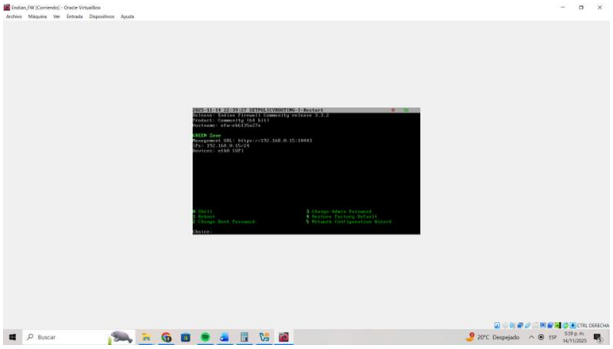
Ilustración 4 Instalación de Endian Firewall



Fuente: Autoría Propia

Al terminar, se reiniciará y podremos ver la consola de Endian donde nos indica la ip para realizar la conexion por navegador web para la administración y opciones como cambiar la contraseña de administración, por defecto la contraseña es “endian” para este caso la cambié por “12345678”; el siguiente paso es configurar nuestras redes a través de la consola de endian.

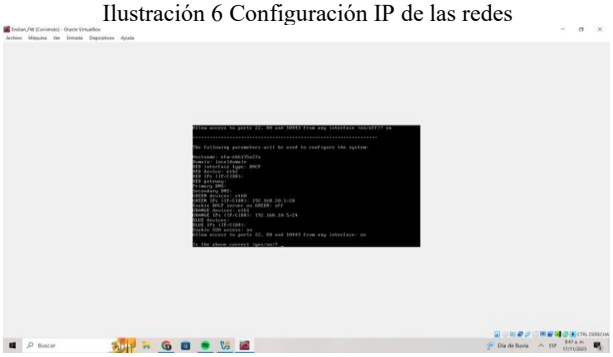
Ilustración 5 Consola Endian Firewall



Fuente: Autoría Propia

En esta interfaz podemos configurar las diferentes redes que vamos a utilizar a través de la opción No. 5; para la red Roja una red NAT con DCHP, para la red Verde una red interna con rango de ip 192.168.20.1/24 y para la red naranja de igual manera red interna con rango 192.168.10.5/24.

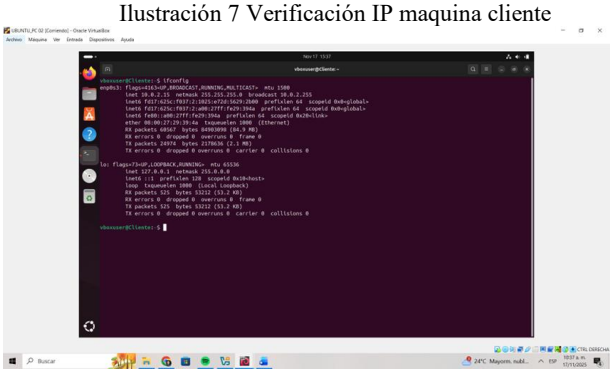
Ilustración 6 Configuración IP de las redes



Fuente: Autoría Propia

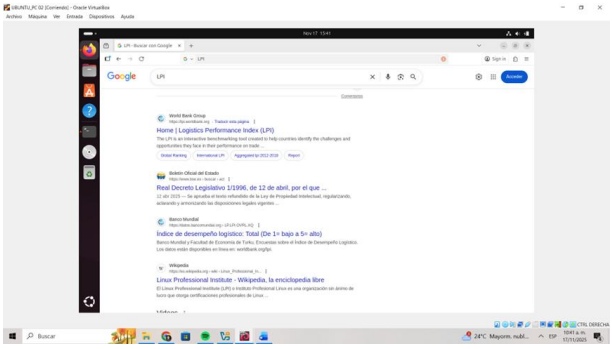
Iniciamos la máquina virtual cliente conectada a la zona Roja y verificamos que obtiene correctamente una dirección IP asignada por el servicio DHCP del adaptador NAT de VirtualBox, que actúa como la red simulada de Internet. Esta máquina cuenta únicamente con una interfaz de red configurada en modo NAT, lo que permite que funcione como un equipo externo al firewall. Finalmente, comprobamos la conectividad hacia Internet desde esta red simulada, confirmando que la comunicación opera sin inconvenientes.

Ilustración 7 Verificación IP maquina cliente



Fuente: Autoría Propia

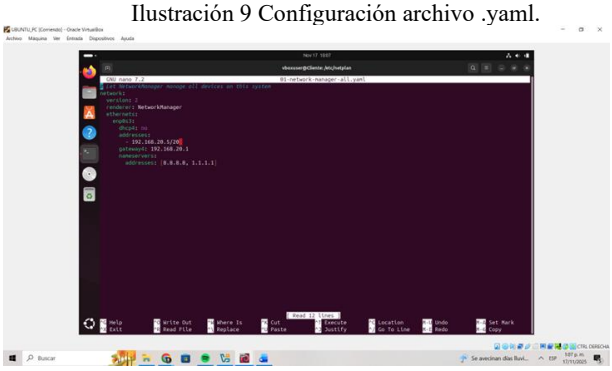
Ilustración 8 Verificación conexión a internet



Fuente: Autoría Propia

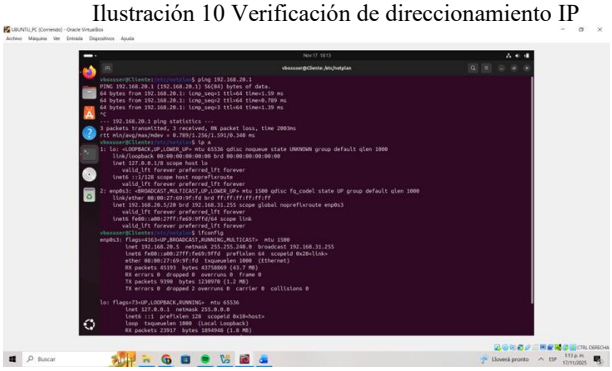
Iniciamos otra máquina cliente conectada a la Red_Verde y procedemos a configurar su archivo *.yaml* con el segmento de red asignado en Endian. En este caso, la dirección IP correspondiente es 192.168.20.5. Tras aplicar los cambios mediante el comando netplan apply, verificamos que la máquina haya tomado la IP configurada. Posteriormente, comprobamos la comunicación con el firewall y, finalmente, accedemos a la interfaz web de administración a través de la dirección 192.168.20.1:10443, donde se encuentra la configuración principal de Endian.

Ilustración 9 Configuración archivo .yaml.



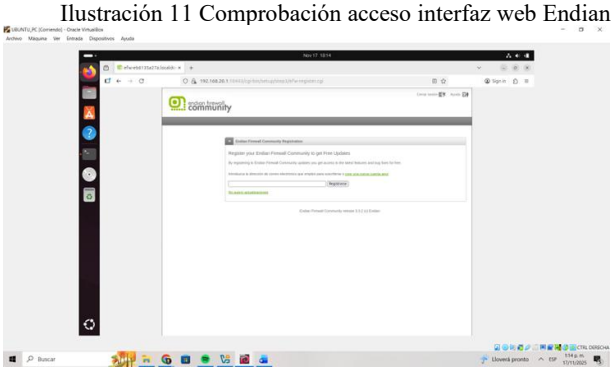
Fuente: Autoría Propia

Ilustración 10 Verificación de direccionamiento IP



Fuente: Autoría Propia

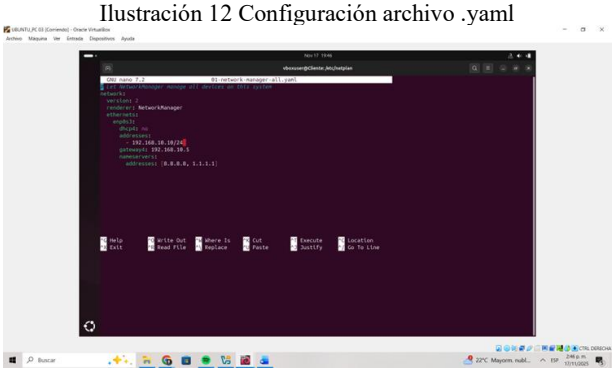
Ilustración 11 Comprobación acceso interfaz web Endian



Fuente: Autoría Propia

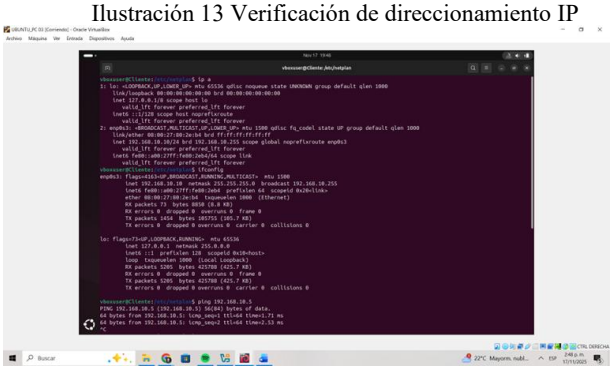
Continuamos con la máquina cliente conectada a la Red_Naranja y, de la misma manera que en la máquina anterior, configuramos su archivo *.yaml* con el segmento de red asignado en Endian. En este caso, la dirección IP establecida es 192.168.10.10. Tras aplicar los cambios mediante el comando netplan apply, verificamos que la máquina haya tomado la IP correspondiente y, posteriormente, confirmamos la comunicación con el firewall.

Ilustración 12 Configuración archivo .yaml



Fuente: Autoría Propia

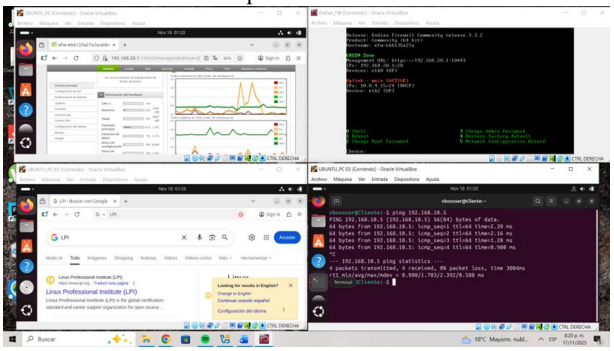
Ilustración 13 Verificación de direccionamiento IP



Fuente: Autoría Propia

Finalmente, con todas las interfaces configuradas, procedemos a encender todas las máquinas virtuales y verificar su correcto funcionamiento. La máquina conectada a la Red_Verde accede sin inconvenientes a la interfaz gráfica de Endian a través de la dirección mostrada en la consola. La máquina conectada a la Red_Naranja presenta comunicación estable con su interfaz de red, y aunque no dispone de acceso a Internet, este podría habilitarse si fuera necesario. Por último, la máquina conectada a la Red_Roja cuenta con navegación a Internet gracias a la dirección IP asignada por el servicio DHCP del adaptador NAT de VirtualBox, que actúa como la red WAN simulada.

Ilustración 14 Comprobación funcionamiento simultanea



Fuente: Autoría Propia

2.2 TEMÁTICA 2: CONFIGURACIÓN NAT

La traducción de direcciones de red (NAT) es un mecanismo utilizado en dispositivos perimetrales como enrutadores y firewalls para permitir la comunicación entre redes privadas y redes públicas, especialmente internet. Este servicio suele implementarse en la interfaz WAN del enrutador perimetral, lo que es común en infraestructuras como centros de datos, campus y sucursales, donde se requiere un control eficiente del tráfico externo [1].

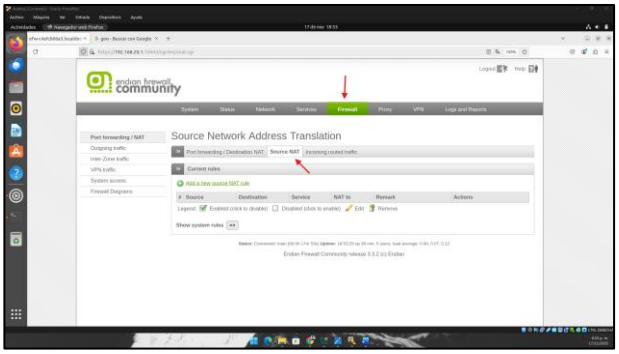
Mediante NAT, una organización puede utilizar una sola dirección IP pública, o un conjunto reducido de ellas, para representar a numerosos dispositivos internos. En este proceso también interviene la Traducción de Direcciones de Puerto (PAT), que permite que varios hosts compartan la misma IP mediante la asignación dinámica de puertos, optimizando el uso de direcciones disponibles [1].

En el contexto del firewall Endian, NAT se vuelve un componente clave para garantizar que las redes internas puedan comunicarse con la red externa. Para ello, se configuran reglas específicas que autorizan a zonas como la verde y la naranja a enviar tráfico hacia internet utilizando la interfaz roja como punto de salida principal hacia la WAN.

2.2.1 ACCESO AL MODULO NAT EN ENDIAN FIREWALL

La configuración inicio ingresando a la consola de administración web del firewall de Endian. Una vez dentro, se navegó hasta el menú: Firewal – Source NAT

Ilustración 15 Consola de adminstración de Endian



Fuente: Autoría Propia

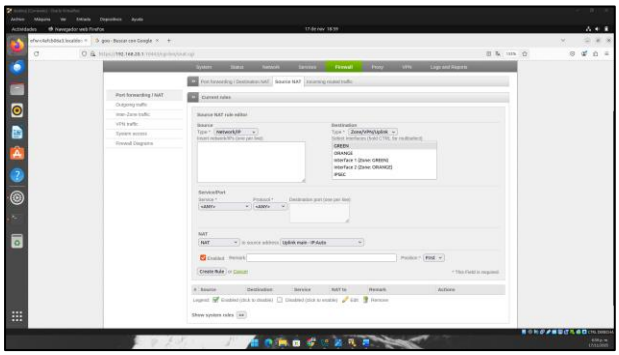
Desde este apartado se gestionaron las reglas necesarias para que las redes internas puedan realizar solicitudes hacia internet bajo una dirección pública única.

2.2.2 CREACIÓN DE REGLA SNAT PARA LA ZONA VERDE

Con el propósito de habilitar la comunicación de la LAN hacia la red WAN, se creó una regla de Source NAT. Se estableció de la siguiente forma:

- Destino: GREEN (LAN)
- Source address: : Uplink main (interfaz roja encargada del enlace hacia Internet).

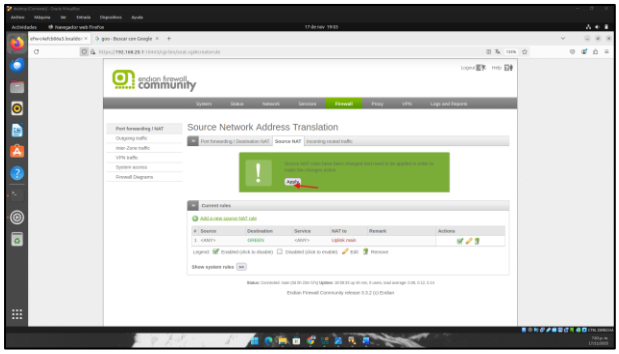
Ilustración 16 Menu Firewall - Source NAT



Fuente: Autoría Propia

Luego de definir estos campos, la regla fue guardada y activada.

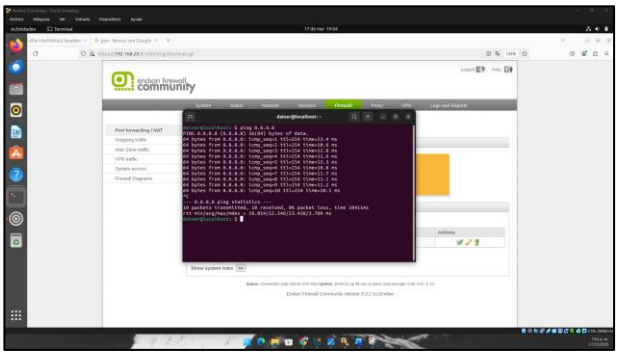
Ilustración 17 Menu Firewall - Source NAT



Fuente: Autoría Propia

Como resultado, los dispositivos de la zona verde pueden acceder a recursos externos empleando la dirección publica asociada a la interfaz Uplink main.

Ilustración 18 Consola de Ubuntu



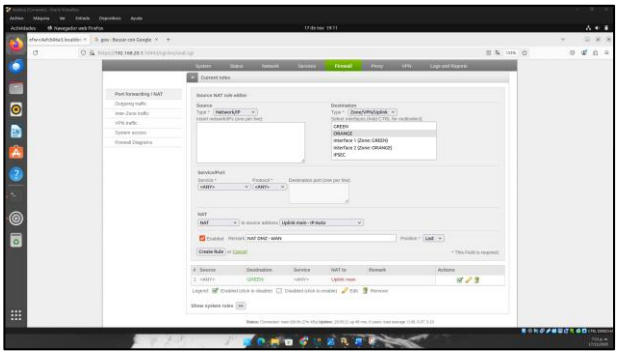
Fuente: Autoría Propia

2.2.3 CREACIÓN DE REGLA SNAT PARA LA ZONA NARANJA

Posteriormente, se elaboró una segunda regla con la finalidad de permitir que los equipos ubicados en la DMZ también pudieran conectarse a la red WAN. Para ello se realizó a siguiente configuración.

- Destino: ORANGE (DMZ)
- Source address: Uplink main (interfaz de salida hacia la WAN).

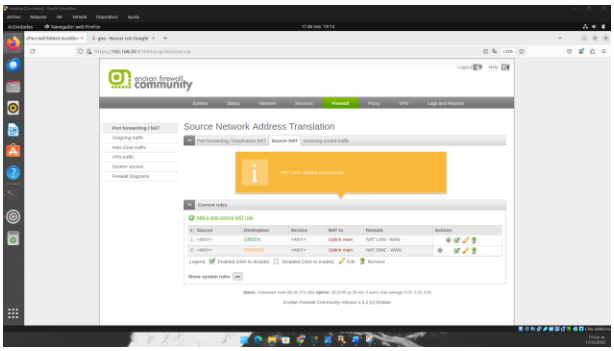
Ilustración 19 Menu Firewall - Source NAT



Fuente: Autoría Propia

Luego de definir estos campos, la regla fue guardada y activada.

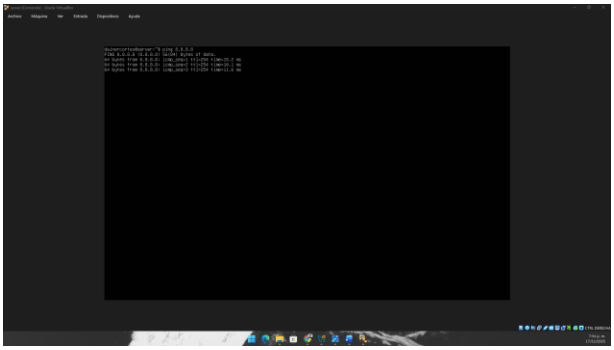
Ilustración 20 Menu Firewall - Source NAT



Fuente: Autoría Propia

Una vez aplicada la regla, los dispositivos en la zona naranja quedaron autorizados para conectarse a internet, utilizando igualmente la dirección publica proporcionada por la interfaz de salida, sin que las direcciones privadas sean expuestas.

Ilustración 21 Consola de Ubuntu Server



Fuente: Autoría Propia

2.2.4 VERFICACION DE REGLAS APLICADAS

Luego de finalizar la creación y aplicación de las reglas NAT, se procedió a realizar la revisión del módulo correspondiente para confirmar que cada regla hubiese sido registrada correctamente y estuviera operando según lo previsto.

Durante la revisión se comprobó que la regla asociada a la zona verde (LAN) estaba activa y los equipos podían comunicarse sin problemas con la red WAN.

De igual formar, se verifico el comportamiento de la regla de la zona naranja (DMZ), confirmando que los servidores ubicados en la red podían acceder a servicios externos. Esta validación permitió confirmar que las reglas NAT operan correctamente y que la segmentación entre zonas se mantiene protegida.

2.3 TEMÁTICA 3: PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED.

Como parte de la formación práctica en Administración de Servicios en Red, se ejecutaron diversas actividades orientadas a comprender el funcionamiento de redes segmentadas y la implementación de políticas de seguridad utilizando herramientas basadas en GNU/Linux. Para ello, se configuró una infraestructura de red por medio del firewall Endian, proceso que incluyó desde la instalación del sistema hasta la verificación del tráfico autorizado y las restricciones aplicadas entre las distintas zonas.

2.3.1 CREACIÓN DE LA MÁQUINA VIRTUAL ENDIAN

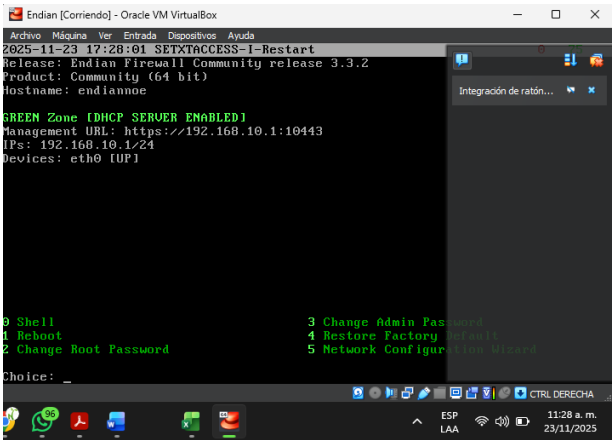
Para la creación de máquina virtual Endian se utilizó la herramienta de VirtualBox, configurada con sistema operativo Linux (64-bit), 4282 MB de RAM y disco duro 25 GB con 2 procesadores.

1. Adaptador 1: red interna llamada LAN
2. Adaptador 2: red interna llamada DMZ
3. Adaptador 3: modo NAT para salida de internet

2.3.2 INSTALACIÓN DEL SISTEMA ENDIAN FIREWALL

Se realizo el cargue de la imagen ISO EFW-COMMUNITY-3.3.2.iso en la máquina virtual y se realizó el proceso de instalación correspondiente. En la fase de configuración inicial, se estableció la zona verde con una dirección IP estática 192.168.10.1/24. Posteriormente, se accedió a la interfaz gráfica de administración mediante un navegador web desde un equipo perteneciente a la red LAN.

Ilustración 22 Consola de Ubuntu Server



Fuente: Autoría Propia

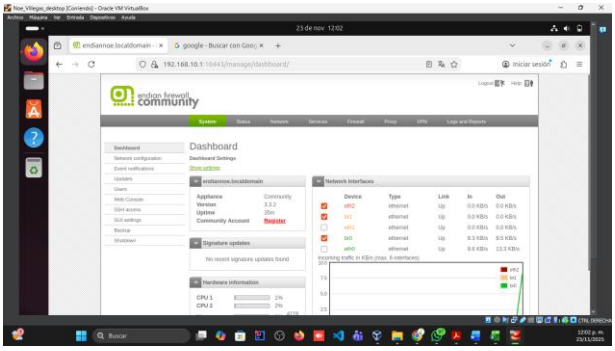
2.3.3 ACCESO AL DASHBOARD Y CONFIGURACIÓN BÁSICA

Desde el navegador de un equipo cliente con dirección IP 192.168.10.2, se ingresó a la URL https://192.168.10.1:10443

para acceder al panel de administración de Endian. Una vez dentro, se completó el asistente de configuración inicial, definiendo la zona roja en la interfaz ETH02, la zona verde en ETH00 y la zona naranja en ETH01. Posteriormente, se asignaron las direcciones IP correspondientes a cada una de las interfaces de red.

1. Verde: 192.168.10.1
2. Naranja: 192.168.20.1
3. Roja: automática por DHCP

Ilustración 23 Consola de Ubuntu Server

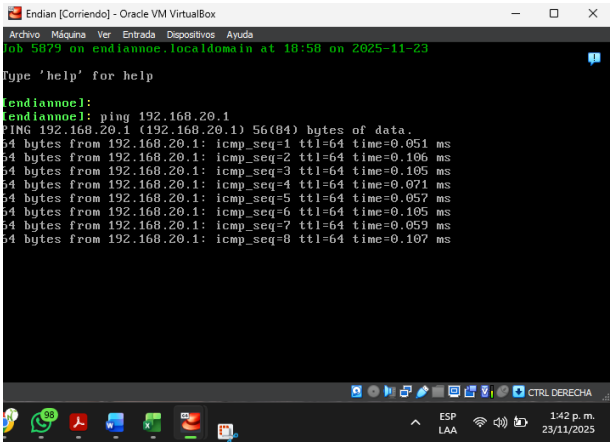


Fuente: Autoría Propia

2.3.4 PRUEBAS DE CONECTIVIDAD

Se realizó exitosamente el ping desde Endian con la IP 192.168.20.1 del DMZ

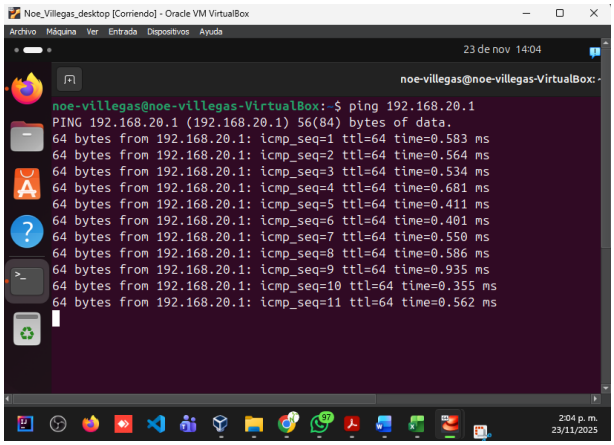
Ilustración 24 Consola de Ubuntu Server



Fuente: Autoría Propia

Se realizó exitosamente el ping desde el cliente 192.168.10.2 al 192.168.20.1 del DMZ

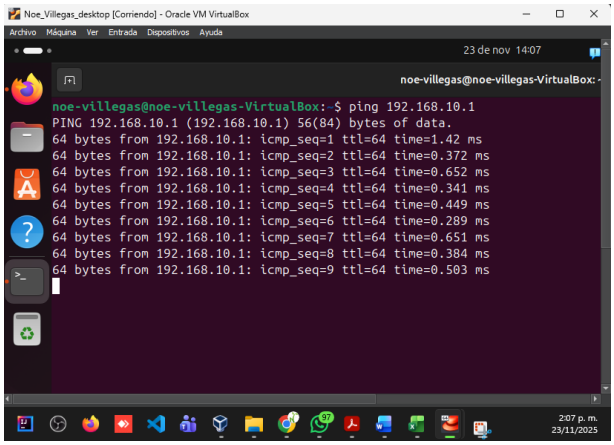
Ilustración 25 Consola de Ubuntu Server



Fuente: Autoría Propia

Se realizó exitosamente el ping desde el cliente 192.168.10.2 al 192.168.10.1 del DMZ

Ilustración 26 Consola de Ubuntu Server



Fuente: Autoría Propia

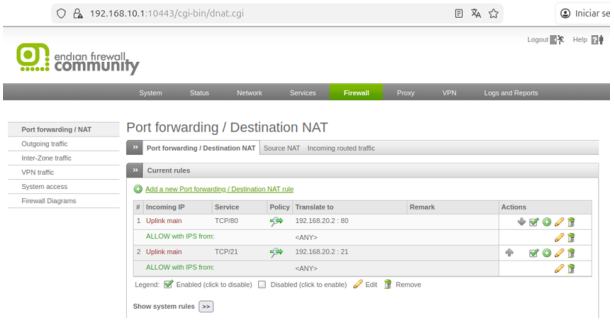
2.3.5 REGLAS DE FIREWALL Y FILTRADO DE SERVICIOS

Se activaron y se crearon las reglas para las zonas HTTP y FTP. Y adicional también se agrega la zona ICMP.

Regla 1: HTTP desde DMZ a LAN

Regla 2: FTP desde DMZ a LAN

Ilustración 27 Consola de Ubuntu Server



Fuente: Autoría Propia

Regla 3: Bloqueado ICMP (Puerto 8 y 30)

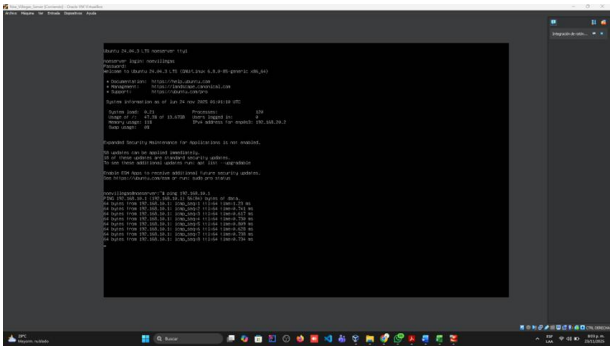
Ilustración 28 Consola de Ubuntu Server

Fuente: Autoría Propia

2.3.6 PRUEBAS REALIZADAS PARA CADA REGLA

Se realiza las respectivas pruebas en la LAN, así como se evidencia en las imágenes a continuación:

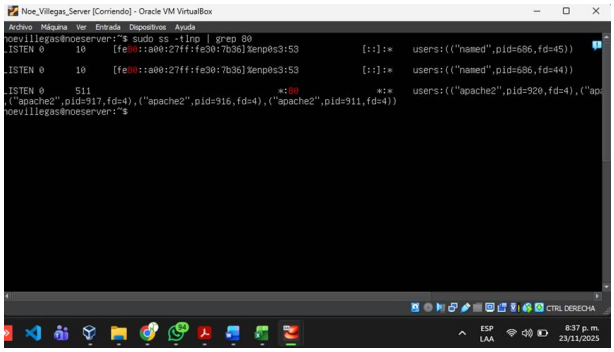
Ilustración 29 Consola de Ubuntu Server



Fuente: Autoría Propia

Regla 1:

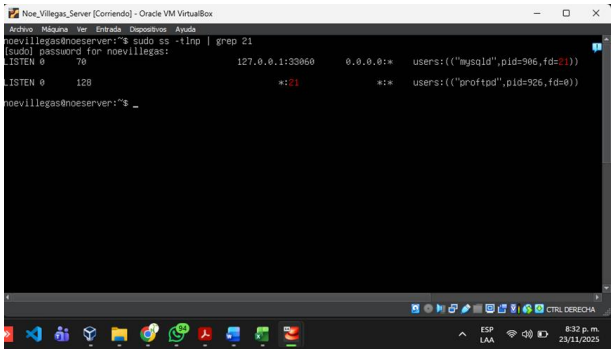
Ilustración 30 Consola de Ubuntu Server



Fuente: Autoría Propia

Regla 2:

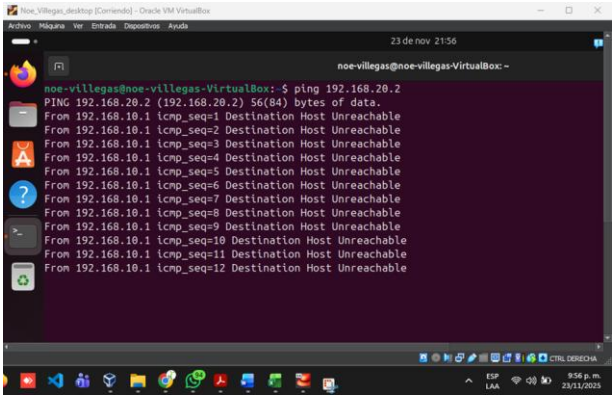
Ilustración 31Consola de Ubuntu Server



Fuente: Autoría Propia

Regla 3:

Ilustración 32 Consola de Ubuntu Server

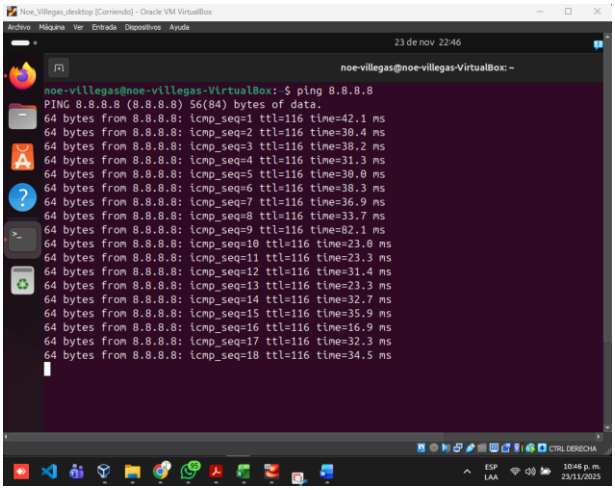


Fuente: Autoría Propia

2.3.7 RESULTADOS TEMÁTICA 3

Se realiza la prueba de ping 8.8.8.8 con la respectiva red del cliente LAN.

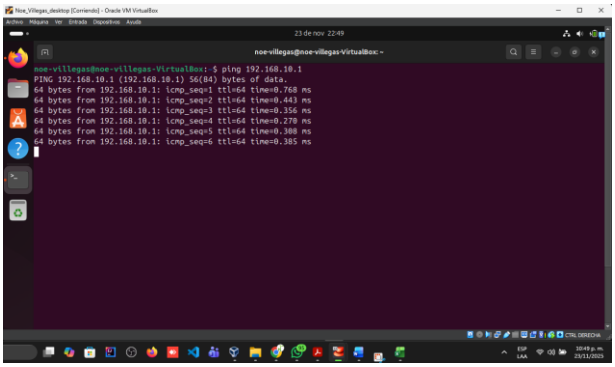
Ilustración 33 Consola de Ubuntu Server



Fuente: Autoría Propia

Se realiza la prueba de ping 192.168.10.1 con el puerto del firewall.

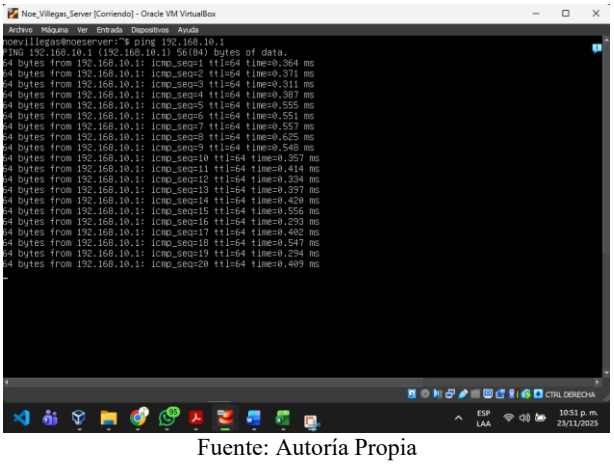
Ilustración 34 Consola de Ubuntu Server



Fuente: Autoría Propia

Se realiza la prueba de ping 192.168.10.1 desde el Ubuntu Server al puerto del firewall.

Ilustración 35 Consola de Ubuntu Server



Fuente: Autoría Propia

2.4 TEMÁTICA 4: REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO.

Las reglas de acceso son instrucciones o normas que determinan el tipo de tráfico que queremos que circule dentro de una red, como también cuales conexiones deben ser bloqueadas. Permiten controlar el flujo de información según su origen, destino o servicio involucrado.

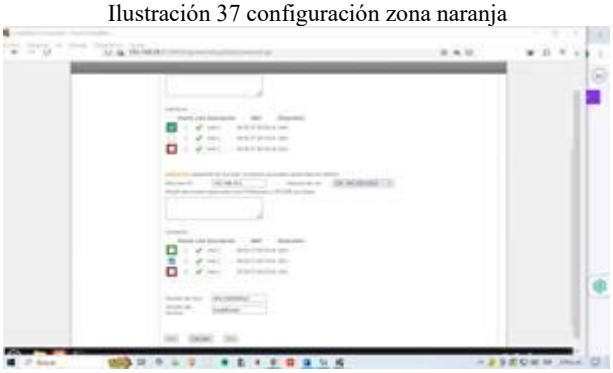
En esta etapa se aborda la configuración de las reglas de acceso en endian para gestionar el tráfico entre las zonas LAN, DMZ, WAN. Definiendo un enfoque de cuales servicios están permitidos y cuáles serán restringidos. Con el fin de tener una comunicación controlada y reducir riesgos en la red. Mas adelante se explica y configura la temática.

Ilustración 36 Configuración de red

Fuente: Autoría Propia

Este paso es fundamental porque indica al sistema endian como debe operar dentro de la red y como se debe conectar a internet se escogió enrutamiento por lo que endian actuara como un enrutador. Se valida que estén las tres tarjetas de red.

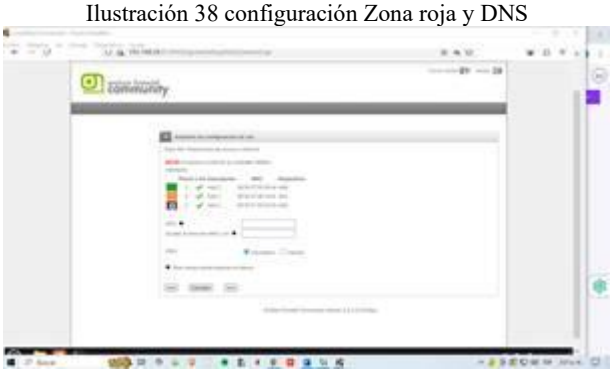
Ilustración 37 configuración zona naranja



Fuente: Autoría Propia

La imagen muestra la configuración de la zona naranja mejor conocida como la zona DMZ (zona desmilitarizada) tiene como propósito aislar los servicios públicos de la red interna de la zona verde y al mismo tiempo protegerlos de ataques de la zona roja.

Ilustración 38 configuración Zona roja y DNS



Fuente: Autoría Propia

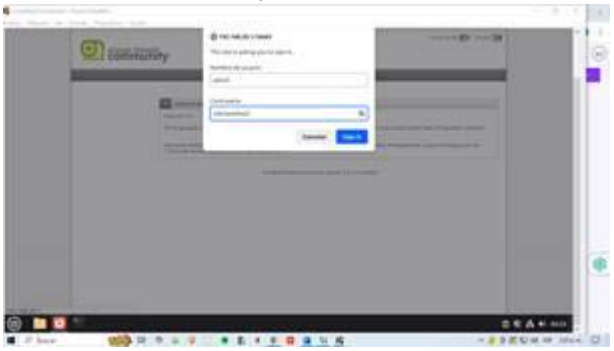
Esta parte de la configuración tiene como propósito la configuración de la zona roja, asegurar que el firewall pueda comunicarse con internet y manejar el tráfico externo

Ilustración 39 Aplicar configuración

Fuente: Autoría Propia

Aplicando la configuración se guardará todos los pasos que ya realizamos se esperan unos segundos para que estas se empleen.

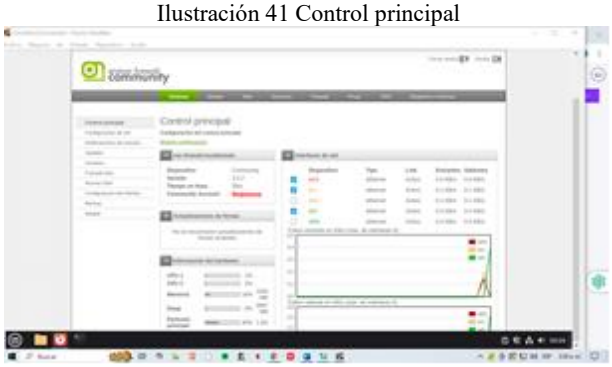
Ilustración 40 Validador de Usuario



Fuente: Autoría Propia

Previamente en el sistema endian ya se había configurado el usuario y contraseña con el que vamos a acceder al apartado de control principal de endian en forma gráfica.

Ilustración 41 Control principal



Fuente: Autoría Propia

Ingresando a este apartado podemos ver el monitoreo y estado general del firewall, este nos muestra la versión, el tiempo que lleva encendido el estado de la cuenta, el tráfico en tiempo real a través de las diferentes zonas.

Ilustración 42 Regla http

Fuente: Autoría Propia

Configurando la Inter-Zona en endian es esencial para establecer las políticas de tráfico y seguridad en la red, en esta interfaz agregamos la regla especifica como la administración del tráfico HTTP. Esta regla permite la comunicación de navegación web dentro de las zonas verde o naranja

Ilustración 43 Prueba Regla HTTP

Fuente: Autoría Propia

Se demuestra una prueba HTTP exitosa: el cliente accede sin problemas a la página por defecto de Apache en el servidor de la zona naranja esto verifica que la regla de Inter-

Zona para permitir el tráfico HTTP entre ambas zonas verde y naranja está configurada correctamente.

Ilustración 44 Regla FTP

Fuente: Autoría Propia

Se muestra la creación de una nueva regla enfocada en el servicio FTP. El objetivo es configurar la política permitir, tráfico FTP entre el origen verde y destino naranja lo que asegura que se pueda trasferir archivos usando FTP.

Ilustración 45 Prueba Regla FTP

Fuente: Autoría Propia

Como prueba, observamos la conexión FTP exitosa entre el cliente zona verde y servidor en la zona naranja esto verifica que la regla FTP del firewall Inter-Zona esta activa y permite la trasferencia de archivos.

Ilustración 46 Comunicación Internet y DMZ

Fuente: Autoría Propia

La función de esta regla es permitir selectivamente servicios esenciales para que los hosts de la red puedan acceder al exterior de forma segura cumpliendo con la política de seguridad.

Ilustración 47 Prueba Comunicación Internet y DMZ

Fuente: Autoría Propia

Como prueba, observamos la conexión a internet exitosa desde el servidor en la zona naranja (DMZ) hacia la zona roja. Esto verifica que la regla de salida está configurada correctamente.

Ilustración 48 Regla Tráfico Interzonal

Fuente: Autoría Propia

En la imagen nos muestra la configuración tráfico Inter-Zona permite el tráfico ICMP o ping entre zonas verde y naranja la política es permitir y servicio cualquiera es de gran utilidad para pruebas iniciales.

Ilustración 49 Prueba Servicio HTTP Desde LAN a WAN

Fuente: Autoría Propia

Como prueba, observamos el acceso HTTP exitoso desde Linux mint al dominio externo zona roja este resultado verifica la regla de firewall de salida para el tráfico HTTP.

Teniendo en cuenta las pruebas exitosas anteriores se puede confirmas que el firewall está filtrando y permitiendo solo el tráfico necesario; esto incluye la comunicación interna entre las computadoras de trabajo (Zona verde) y el servidor (Zona naranja), así como al internet (Zona roja) para sus propias tareas. Este control logra reducir el riesgo de ataques y garantizar que todos los servicios esenciales funcionen sin fallos.

3 CONCLUSIONES

3.1 TEMATICA 1

La implementación de GNU/Linux Endian dentro de un entorno virtualizado en VirtualBox permitió comprender de manera práctica la configuración de un sistema de seguridad perimetral basado en zonas. A través de la correcta asignación de las tarjetas de red y la instalación del sistema, fue posible estructurar las tres áreas fundamentales: la zona verde como red interna segura (LAN), la zona roja para la conexión hacia internet (WAN) y la zona naranja destinada a los servidores en la DMZ. Este proceso no solo evidenció la importancia de una segmentación adecuada para garantizar la protección y el control del tráfico, sino que también reforzó la relevancia de herramientas como Endian para la gestión eficiente y segura de infraestructuras de red. En conjunto, el ejercicio permitió afianzar conocimientos esenciales en administración de redes, virtualización y ciberseguridad.

3.2 TEMATICA 2

El proceso de configuración evidenció que NAT no solo facilita la comunicación entre redes privadas y externas, sino que además permite conservar una estructura de red escalable. Gracias a la aplicación de reglas diferenciadas para la LAN y la DMZ, se comprobó que Endian Firewall gestiona eficazmente múltiples orígenes de tráfico sin generar conflictos de enrute o duplicidad de direcciones IP.

3.3 TEMATICA 3

La configuración del Endian Firewall dentro del entorno virtualizado permitió entender de manera práctica cómo se gestionan las zonas de red y cómo se aplican reglas de seguridad entre ellas. Al habilitar únicamente los servicios HTTP y FTP hacia la zona DMZ, se comprobó cómo un firewall puede controlar de forma precisa qué tráfico es permitido según las necesidades del servicio. De igual manera, el bloqueo del protocolo ICMP evidenció cómo se pueden restringir funcionalidades que, aunque son útiles para diagnóstico, pueden representar un riesgo para la visibilidad interna de la red.

3.4 TEMATICA 4

Mediante la aplicación y pruebas de las reglas que realizamos en la temática 4 se demostró que el control de tráfico no solo nos permite a los usuarios acceder a los recursos y servicios necesarios (como la web o la transferencia de archivos) de manera eficiente, si no que permite mantener una red protegida al bloquear cualquier conexión que no esté autorizada y sea maliciosa.

4 REFERENCIAS

[1] «What Is Network Address Translation (NAT)?», Cisco. Accedido: 23 de noviembre de 2025. [En línea]. Disponible en: https://www.cisco.com/site/us/en/learn/topics/networking/what-is-network-address-translation-nat.html

[2] LPI LPIC-1 Exam 101. (2022). Tema 101: Determinar y configurar los ajustes de hardware. https://learning.lpi.org/es/learning-materials/101-500/101/101.1/

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

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

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

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

[7] Arsys. (s.f.). *Protocolos de Internet: HTTP y FTP*. Recuperado de https://www.arsys.es/blog/protocolos-de-internet-http-y-ftp

[8] cyberleon95. (s.f.). *Instalación y configuración de Firewall Endian* [Presentación en SlideShare]. SlideShare. https://es.slideshare.net/slideshow/instalacin-y-configurcin-firewall-endian/39219423

[9] Zapata Escobar, D. E., Gómez Tangarife, I. L., Acevedo Munera, J. D., Obando Ibarra, C. H., & García Arango, D. A. (2023). *Implementación de un sistema de control y seguridad informático Endian Firewall*. Ingeniería: Ciencia, Tecnología e Innovación, 10(1), 98–115. https://doi.org/10.26495/icti.v10i1.2401

[10] Install Linux Mint — Linux Mint Installation Guide documentation. (n.d.). Readthedocs.Io. Retrieved November 25, 2025, from https://linuxmint-installation-guide.readthedocs.io/en/latest/install.html