“IMPLEMENTACIÓN DE SERVICIOS Y SEGURIDAD PERIMETRAL EN GNU/LINUX UTILIZANDO ENDIAN FIREWALL”

Integrante 1 Esthephanie Castellanos Pérez
e-mail: eycastellanosp@unadvirtual.edu.co
Integrante 2 Yarlin Danilo Calpa Guancha
e-mail: ydcalpag@unad.virtual,edu.co
Integrante 3Mayerly Orjueluea Navarrete
e-mail:morjuelan@unadvirtual.edu.co
Integrante 4 Diana Milena Pachón Velásquez
e-mail:dmpachonv@unadvirtual.edu.co
Integrante 5 Yulian Ardila Maldonado
e-mail:yamaldonado@unadvirtual.edu.co

RESUMEN: *El desarrollo de la presente actividad permitió implementar diferentes mecanismos de seguridad en entornos GNU/Linux mediante el uso de Endian Firewall Community y herramientas de virtualización en Oracle VirtualBox. Inicialmente se trabajó el reconocimiento de aspectos básicos relacionados con arquitectura de sistemas Linux, procesos de arranque, acceso remoto y configuración de hardware necesarios para la administración de sistemas operativos GNU/Linux.*

Posteriormente, se implementó una infraestructura de red segmentada en zonas GREEN, RED y ORANGE, permitiendo establecer comunicación entre clientes, servidores y acceso a Internet dentro de un entorno virtualizado. A partir de esta configuración se desarrollaron diferentes temáticas relacionadas con la administración y seguridad de redes, incluyendo configuración NAT, implementación de servicios HTTP y FTP, creación de reglas de acceso y filtrado de tráfico, restricción del protocolo ICMP y configuración de un proxy HTTP con políticas de autenticación y control de navegación.

Las pruebas realizadas durante la práctica permitieron validar el funcionamiento de las reglas configuradas, la comunicación entre las diferentes zonas de red y el comportamiento de los servicios implementados dentro de la infraestructura virtualizada. Asimismo, la actividad permitió fortalecer conocimientos relacionados con seguridad perimetral, virtualización, administración de redes y gestión de servicios en sistemas GNU/Linux.

PALABRAS CLAVE: Endian Firewall, GNU/Linux, NAT, Proxy HTTP, seguridad perimetral, reenvío de puertos, reglas de acceso, FTP y NAT.

1 INTRODUCCIÓN

Actualmente, la seguridad informática juega un papel muy importante dentro de cualquier infraestructura tecnológica, especialmente por la gran cantidad de amenazas y riesgos que existen en internet. El crecimiento de ataques dirigidos a redes, servidores y servicios web ha hecho necesario implementar mecanismos que permitan controlar el tráfico de red y proteger la información que circula entre los diferentes dispositivos conectados a una infraestructura informática.

En este sentido, los sistemas GNU/Linux se han convertido en una de las alternativas más utilizadas para la administración de servidores y servicios de red, gracias a su estabilidad, flexibilidad y capacidad de configuración. Del mismo modo, herramientas como Endian Firewall Community permiten implementar soluciones de seguridad perimetral mediante el control y filtrado del tráfico entre diferentes zonas de red, facilitando la administración de políticas de acceso y comunicación dentro de un entorno protegido.

Para el desarrollo de esta actividad se implementó un entorno virtualizado utilizando Oracle VirtualBox, en el cual se configuraron máquinas virtuales con Ubuntu Desktop, Ubuntu Server y GNU/Linux Endian Firewall Community. A partir de esta infraestructura se realizó la segmentación de la red en zonas GREEN, RED y ORANGE, permitiendo establecer la comunicación entre clientes, servidores y acceso a Internet dentro de un mismo entorno de práctica.

A lo largo del trabajo se desarrollaron diferentes temáticas relacionadas con configuración NAT, implementación de servicios HTTP y FTP, administración de reglas de acceso, filtrado de tráfico y configuración de un proxy HTTP con autenticación para navegación en Internet. Asimismo, durante las pruebas realizadas fue posible validar la conectividad entre las diferentes zonas de red y verificar el funcionamiento de las políticas de seguridad configuradas en el firewall.

Además de la parte técnica, el desarrollo de la actividad permitió fortalecer conocimientos relacionados con virtualización, administración de redes y seguridad perimetral en sistemas GNU/Linux, enfrentando situaciones reales de configuración, validación de servicios y solución de problemas de conectividad dentro del entorno implementado.

2 METODOLOGIA

Para el desarrollo de las prácticas se implementó un entorno virtualizado en Oracle VirtualBox utilizando Ubuntu Desktop, Ubuntu Server y Endian Firewall Community. La infraestructura fue segmentada en las zonas GREEN, ORANGE y RED, permitiendo establecer comunicación entre clientes, servidores y acceso a Internet mediante NAT.

Posteriormente, se configuraron interfaces de red, direccionamiento IP y reglas básicas de conectividad para garantizar la comunicación entre las diferentes zonas implementadas. A partir de esta estructura se desarrollaron las temáticas relacionadas con configuración NAT, servicios HTTP y FTP, reglas de firewall y proxy HTTP con autenticación y filtrado web.

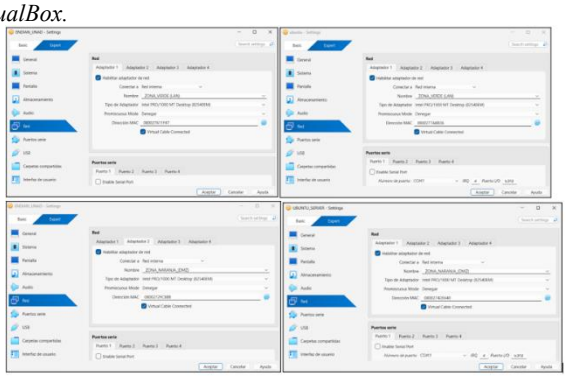
Finalmente, se realizaron pruebas de conectividad, navegación y validación de servicios mediante comandos de red y acceso desde navegador web, permitiendo comprobar el correcto funcionamiento de las políticas de seguridad implementadas dentro del entorno GNU/Linux virtualizado.

3 CONFIGURACION DEL ENTORNO VIRTUALIZADO

Para el desarrollo de las prácticas se configuró una infraestructura virtualizada en Oracle VirtualBox utilizando Ubuntu Desktop, Ubuntu Server y Endian Firewall Community. La red fue segmentada en las zonas GREEN, ORANGE y RED, permitiendo la comunicación entre clientes, servidores y acceso a Internet mediante NAT.

Asimismo, se configuraron las interfaces de red y el direccionamiento IP correspondiente para cada máquina virtual, garantizando conectividad entre las diferentes zonas implementadas dentro del entorno virtualizado.

Figura 1 Configuración de adaptadores de red para la segmentación de zonas GREEN, RED y ORANGE en VirtualBox.



Fuente: autoría propia

Dispositivo	Zona de red	Dirección ip	Función
Endian Firewell	GREEN (LAN)	192.168.10.1	Puerta de enlace red clientes
Ubuntu Desktop	GREEN (LAN)	192.168.10.2	Equipo cliente
Endian Firewell	ORANGE (DMZ)	192.168.20.1	Puerta de enlace DMZ
Ubuntu Server	ORANGE (DMZ)	192.168.20.2	Servidor DMZ
Endian Firewell	RED (WAN)	DHCP	Salida a internet

4 DESARROLLO POR TEMATICAS

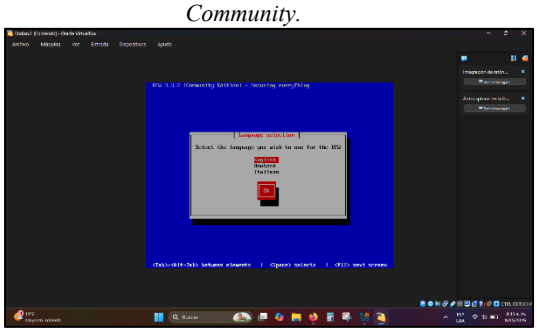
4.1 TEMATICA 1: CONFIGURACION DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX E INTALACION EFECTIVA DEL MISMO.

La temática desarrollada estuvo orientada a la implementación y configuración de GNU/Linux Endian Firewall Community Edition en un entorno virtualizado utilizando Oracle VirtualBox. El propósito principal de la práctica consistió en comprender el funcionamiento básico de un firewall dentro de una infraestructura segmentada y la manera en que este permite controlar la comunicación entre diferentes zonas de red dentro de un entorno GNU/Linux.

Para el desarrollo de la actividad fue necesario crear una máquina virtual dedicada exclusivamente al firewall Endian, asignando recursos básicos de hardware como memoria RAM, almacenamiento y adaptadores de red virtuales. La configuración de las interfaces de red representó una de las etapas más importantes de la práctica, debido a que cada adaptador debía cumplir una función específica dentro de la segmentación planteada en la actividad. En este caso, se trabajó con las zonas GREEN, RED y ORANGE, correspondientes a la red interna LAN, la salida hacia Internet y la zona DMZ destinada a los servidores.

Inicialmente se realizó el montaje de la imagen ISO de Endian Firewall Community Edition para iniciar el proceso de instalación dentro de VirtualBox. Durante esta etapa se configuraron parámetros básicos relacionados con idioma, preparación del disco virtual y reconocimiento del hardware asignado a la máquina virtual. Posteriormente, se llevó a cabo la configuración de la interfaz GREEN asignando el direccionamiento IP principal que sería utilizado para la administración del firewall y la comunicación con el cliente Ubuntu Desktop implementado durante la práctica.

Figura 2 Inicio del proceso de instalación de Endian Firewall Community.



Fuente: autoría propia

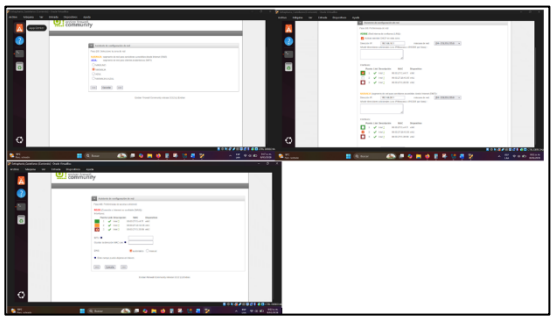
Una vez finalizada la instalación básica del sistema, se procedió a realizar la configuración inicial desde el panel administrativo web de Endian Firewall. El acceso se realizó desde el navegador del cliente Ubuntu utilizando la dirección IP configurada previamente para la interfaz GREEN. A través del asistente de configuración se definieron las interfaces activas,

los parámetros de red y la segmentación de las zonas utilizadas durante la implementación.

Durante esta etapa también se configuraron las interfaces GREEN, RED y ORANGE, permitiendo separar correctamente el tráfico correspondiente a la red interna, la salida hacia Internet y la zona DMZ. La configuración de estas zonas permitió comprender la importancia de la segmentación de red dentro de infraestructuras que requieren control y administración del tráfico entre diferentes servicios y dispositivos conectados.

Aunque inicialmente la configuración parecía sencilla, durante las pruebas surgieron algunos inconvenientes relacionados con la comunicación entre las máquinas virtuales. Uno de los principales problemas encontrados estuvo relacionado con el orden de los adaptadores de red configurados en VirtualBox, ya que algunas interfaces se encontraban invertidas, impidiendo la correcta comunicación entre el cliente Ubuntu y el firewall. Después de revisar nuevamente la configuración de red y reorganizar las interfaces virtuales, fue posible restablecer la conectividad y continuar con el proceso de validación.

Figura 3 Configuración de interfaces y segmentación de zonas de red en Endian Firewall.



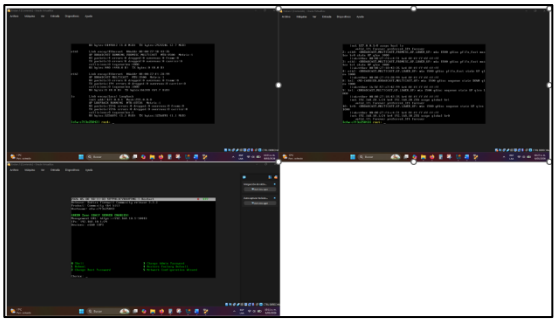
Fuente: autoría propia

Posteriormente, se realizaron diferentes pruebas de conectividad desde consola utilizando comandos básicos de red como ping e ip route. Estas validaciones permitieron comprobar el direccionamiento IP asignado, el reconocimiento de las interfaces activas y la comunicación correcta entre el cliente Ubuntu y la interfaz GREEN del firewall. De igual manera, desde el dashboard principal de Endian Firewall fue posible monitorear el estado de las interfaces y verificar el tráfico generado durante las pruebas realizadas en la red virtualizada.

Además de las pruebas de conectividad, también se verificó el correcto funcionamiento del panel administrativo web, permitiendo evidenciar que las configuraciones realizadas durante la práctica habían sido aplicadas correctamente. La validación tanto desde consola como desde la interfaz gráfica permitió tener una visión más completa sobre el comportamiento del firewall dentro del entorno implementado.

Finalmente, el desarrollo de esta temática permitió fortalecer conocimientos relacionados con virtualización, administración de redes y seguridad perimetral en entornos GNU/Linux. Asimismo, la práctica ayudó a comprender de manera más aplicada la importancia que tiene la segmentación de redes y el control de tráfico dentro de infraestructuras donde se administran servicios y servidores conectados entre diferentes zonas de red.

Figura 4 Validación de interfaces y parámetros de red desde la consola de Endian Firewall.



Fuente: autoría propia

Finalmente, el desarrollo de esta temática permitió fortalecer conocimientos relacionados con virtualización, administración de redes y seguridad perimetral en entornos GNU/Linux. Además de comprender la función de un firewall dentro de una infraestructura segmentada, la práctica permitió identificar la importancia que tienen las configuraciones de red y la correcta administración de interfaces para garantizar la comunicación y seguridad entre diferentes zonas dentro de un entorno informático virtualizado.

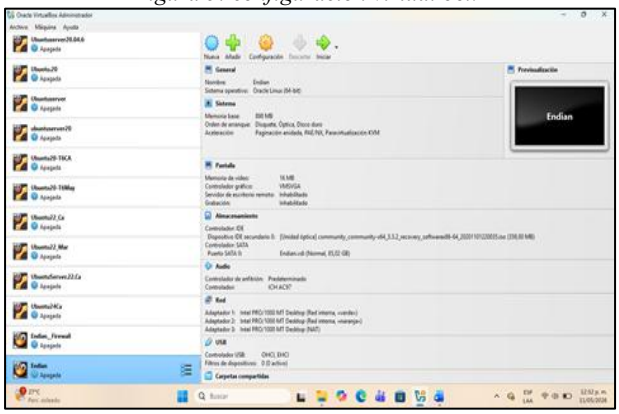
4.2 TEMÁTICA 2: CONFIGURACIÓN NAT.

La temática desarrollada estuvo orientada a la configuración y validación del mecanismo NAT (Network Address Translation / Traducción de Direcciones de Red) dentro de GNU/Linux Endian Firewall Community Edition, implementado previamente en un entorno virtualizado mediante Oracle VirtualBox. El propósito principal de esta práctica consistió en comprender el funcionamiento del proceso de traducción de direcciones IP dentro de una infraestructura segmentada, permitiendo el establecimiento de comunicación entre las diferentes zonas de red y la WAN simulada de Internet.

Mientras trabajamos en la actividad, mejoramos la infraestructura pre-split actualizando las zonas GREEN, RED, adn ORANGE en el Firewall de Endian La zona verde es donde los clientes se conectan a nuestra red interna, la zona roja es donde simulamos nuestra conexión a Internet, y la zona naranja es donde alojamos nuestros servidores y servicios en un espacio virtual.

La implementación del servicio NAT permitió comprender la importancia de la traducción de direcciones dentro de entornos GNU/Linux orientados a la administración de redes y seguridad informática. Este mecanismo posibilita que múltiples dispositivos pertenecientes a redes privadas puedan acceder a redes externas mediante un proceso de enmascaramiento y traducción de direcciones IP administrado directamente por el firewall.

Figura 5: configuración virtual box



Fuente: autoría propia

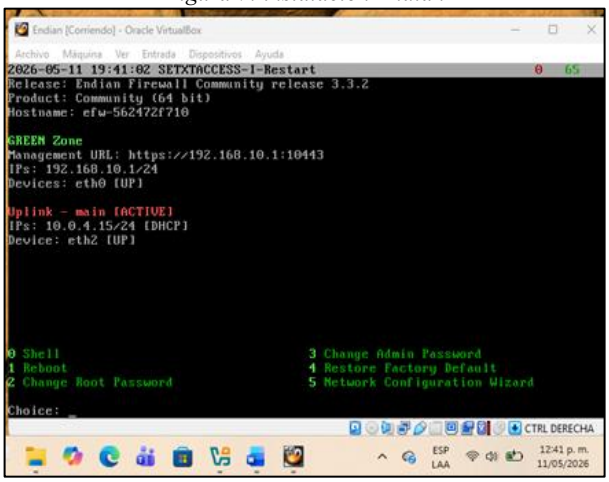
Se configuran las tres zonas de red: LAN, DMZ y WAN en el firewall Endian Firewall Community dentro del entorno virtualizado implementado en Oracle VM VirtualBox. La red LAN fue destinada para la comunicación interna entre los equipos virtuales, la DMZ se empleó para la publicación y validación de servicios como HTTP y FTP, mientras que la WAN permitió simular la conexión externa hacia otras redes. Esta segmentación permitió aplicar políticas de seguridad, filtrado de tráfico y control de acceso entre las diferentes zonas de la infraestructura, garantizando un entorno de pruebas seguro y funcional para la validación de reglas del firewall.

Figura 6: configuración direcciones ip

Fuente: autoría propia

Se configura la interfaz de red GREEN en Endian Firewall Community con la dirección IP 192.168.10.1 y máscara de subred 255.255.255.0, correspondiente a la red LAN interna del entorno virtualizado. Esta interfaz fue destinada para la comunicación segura entre los equipos de la red local, permitiendo la administración de los dispositivos conectados y el control del tráfico interno mediante las políticas de seguridad implementadas.

Figura 7: instalación Endian



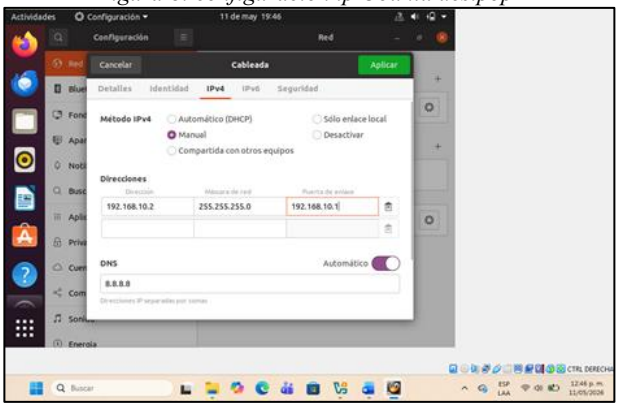
Fuente autoría propia

En la pantalla se visualiza el estado de las interfaces de red configuradas en el firewall, evidenciando la correcta asignación de direcciones IP tanto para la zona GREEN como para la interfaz WAN.

La zona GREEN presenta la dirección IP 192.168.10.1/24, correspondiente a la red LAN interna utilizada para la comunicación segura entre los equipos del laboratorio virtual. Asimismo, se observa la interfaz WAN configurada con la dirección IP 10.0.4.15/24 obtenida mediante DHCP, permitiendo la conexión hacia redes externas o acceso a Internet.

Esta verificación permitió confirmar el correcto funcionamiento de las interfaces de red y la adecuada segmentación entre las zonas internas y externas del firewall. Además, desde esta consola administrativa fue posible acceder a opciones de configuración, reinicio y administración del sistema, necesarias para la implementación y validación de las políticas de seguridad y filtrado de tráfico dentro del entorno virtualizado.

Figura 8: configuración ip Ubuntu destpop

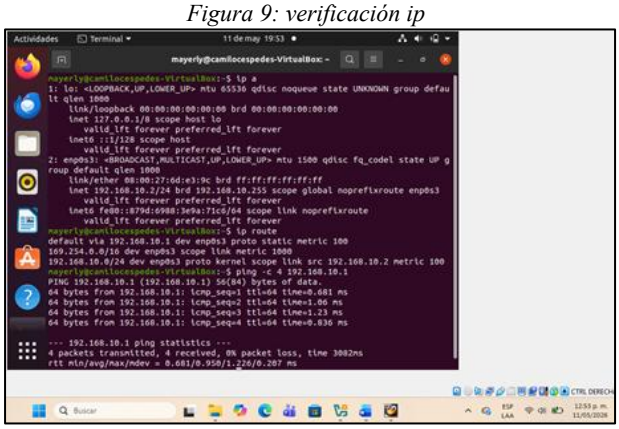


Fuente: autoría propia

Antes de iniciar la máquina virtual, accedemos a los ajustes de red para establecer el adaptador en modo Red Interna, seleccionando el nombre del segmento correspondiente (en este

caso, 'verde'). Una vez iniciada la sesión en el sistema operativo, nos dirigimos a la configuración de red cableada para cambiar el método de IPv4 de Automático (DHCP) a Manual. Procedemos a ingresar la dirección IP, la máscara de red y la puerta de enlace según los parámetros establecidos previamente en el esquema de direccionamiento. Finalmente, para asegurar que el sistema reconozca y aplique la nueva configuración, reiniciamos el servicio de red.

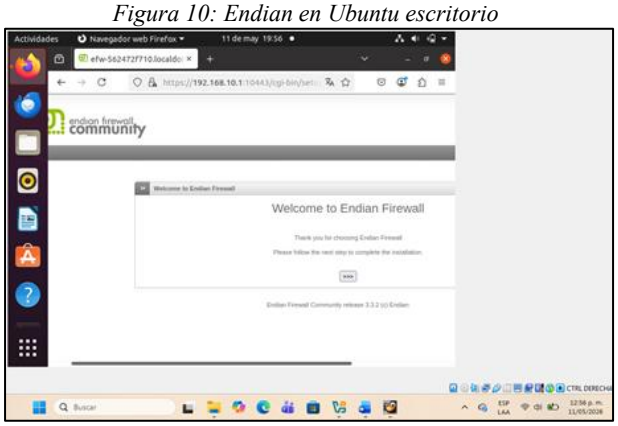
Figura 9: verificación ip



Fuente autoría propia

Tras aplicar los cambios en la configuración IP, procedimos a validar la comunicación dentro de la red interna. Ejecutamos el comando ping hacia la dirección del firewall Endian (192.168.10.1) para comprobar la conectividad entre ambos puntos. Los resultados confirman que existe una conexión estable y bidireccional, con una respuesta inmediata y sin pérdida de paquetes, lo que garantiza que la máquina virtual está correctamente integrada en el segmento de red establecido

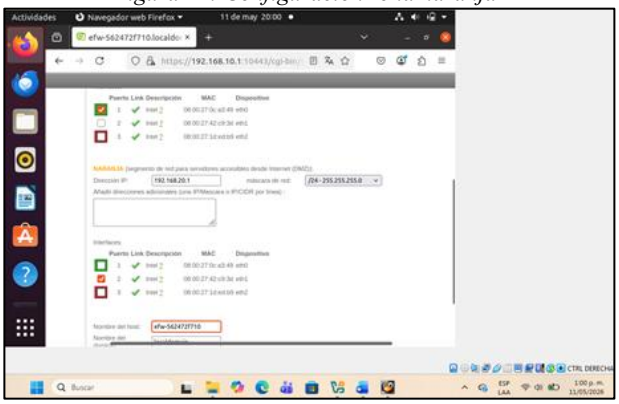
Figura 10: Endian en Ubuntu escritorio



Fuente autoría propia

Tras acceder con éxito al panel de administración de Endian Firewall desde el navegador, iniciamos el asistente de configuración para definir las zonas de red. En esta etapa, procedemos a configurar la red naranja (DMZ), la cual se utiliza para aislar los servidores que ofrecen servicios externos, garantizando una capa extra de seguridad. Definimos los parámetros de direccionamiento para este segmento de red, asegurando que la comunicación entre la zona verde y la naranja esté correctamente gestionada por las reglas del firewall.

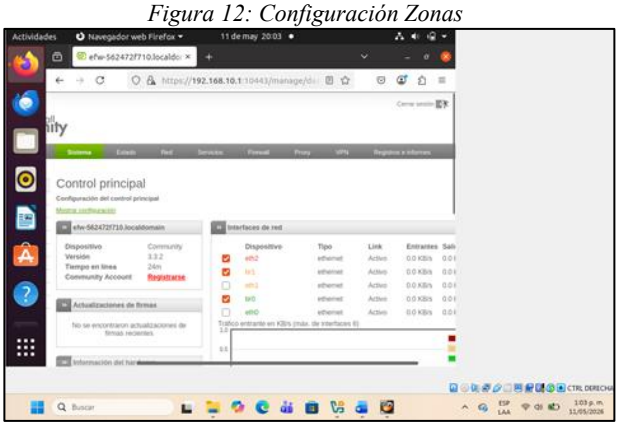
Figura 11: Configuración zona naranja



Fuente autoría propia

Configuramos nuestra red naranja con la IP 192.168.20.1, estableciéndola como la puerta de enlace predeterminada para el segmento de la DMZ (Zona Desmilitarizada). Al asignar esta dirección con una máscara de subred /24, definimos un espacio aislado para los servicios que requieren exposición controlada, permitiendo que el firewall Endian gestione de forma independiente el tráfico y las políticas de seguridad entre esta zona, la red interna (verde) y el acceso exterior

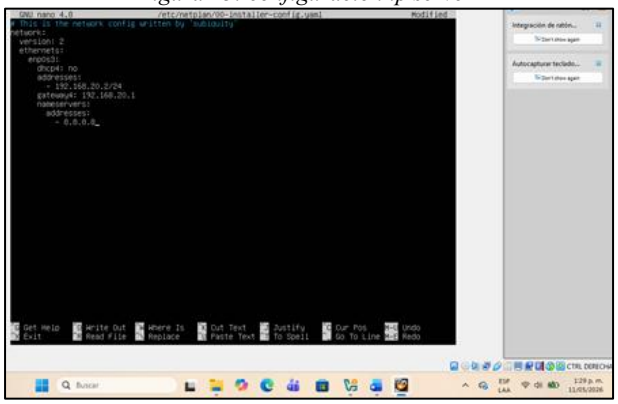
Figura 12: Configuración Zonas



Fuente autoría propia

Con las tres zonas de red (Verde, Naranja y Roja) correctamente configuradas y operativas en el firewall, procedemos a la implementación y configuración del servidor dentro del segmento correspondiente. Este paso consiste en asignar una dirección IP estática al servidor dentro del rango de la red naranja (DMZ), establecer su puerta de enlace apuntando a la interfaz del firewall y verificar que los servicios que alojará sean accesibles bajo las políticas de seguridad y reglas de tráfico que definiremos en el Endian.

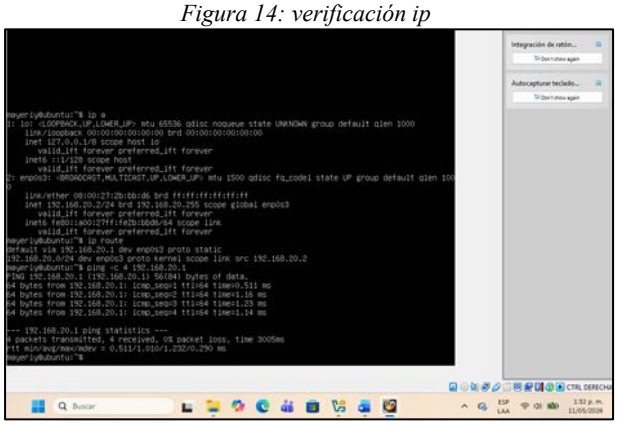
Figura 13: configuración ip server



Fuente autoría propia

Una vez definidas las zonas en el firewall, procedemos a la configuración de red en el Ubuntu Server. Accedemos al archivo de configuración de Netplan (o mediante la interfaz de red correspondiente) para asignar de forma estática la dirección IP, la máscara de subred y la puerta de enlace dentro del segmento de la red naranja. Tras guardar los parámetros, ejecutamos el comando.

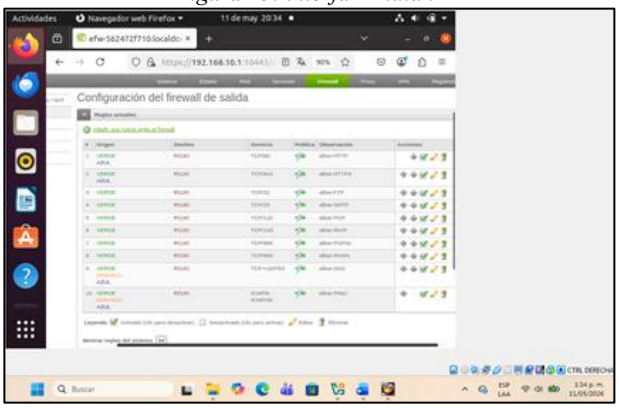
Figura 14: verificación ip



Fuente autoría propia

En este punto, las tres zonas de red (Verde, Naranja y Roja) se encuentran plenamente operativas y comunicadas con el firewall Endian. Este escenario base garantiza que la infraestructura de red está lista para la siguiente fase: la configuración de políticas de acceso, reglas de firewall y el despliegue de servicios seguros dentro de la DMZ.

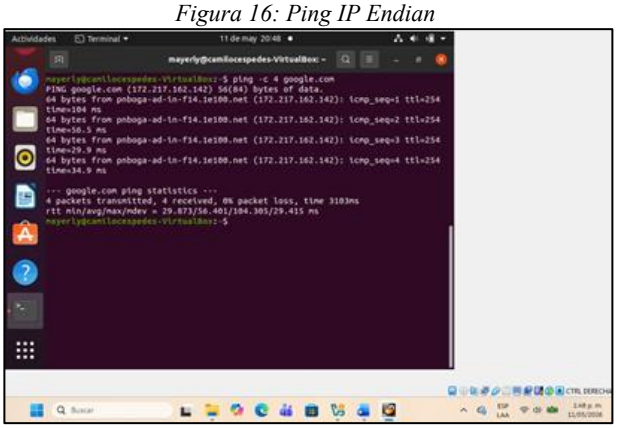
Figura 15: interfaz Endian



Fuente autoría propia

En la sección de tráfico de salida, verificamos que las reglas para la zona verde vienen configuradas de forma predeterminada, permitiendo el acceso hacia la zona roja. Gracias a esta configuración de fábrica, los equipos de la red interna cuentan con permisos automáticos para navegar por Internet. Esto nos permite validar de inmediato que el enrutamiento y la función de NAT (Network Address Translation) del Endian están operando correctamente, facilitando la salida de paquetes sin necesidad de intervenciones manuales adicionales en esta etapa inicial.

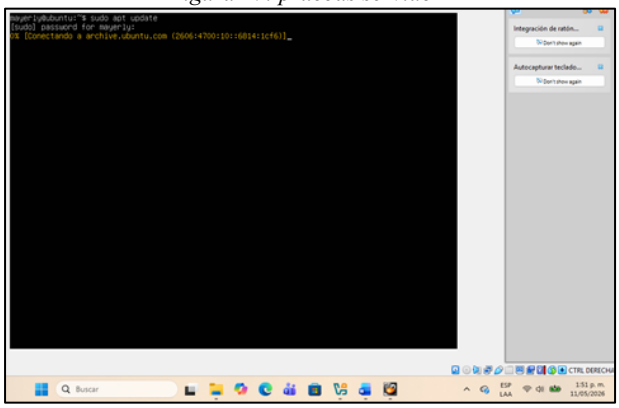
Figura 16: Ping IP Endian



Fuente autoría propia

Realizamos un ping a google.com desde la terminal y confirmamos que tenemos conectividad hacia el exterior, validando que la resolución de nombres (DNS) es funcional. Con este resultado, se demuestra que la NAT (Network Address Translation) ya está configurada correctamente en el firewall Endian, permitiendo que las direcciones IP privadas de nuestra red interna se traduzcan de forma transparente a una dirección pública para navegar por Internet sin comprometer la seguridad de la estructura local.

Figura 17: pruebas servidor

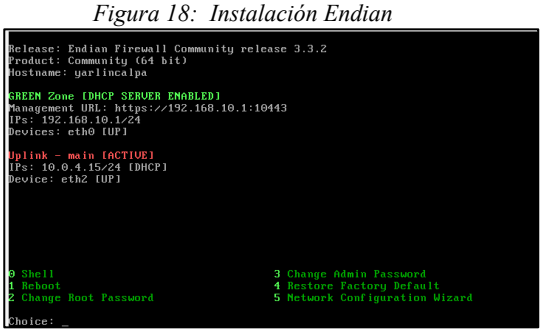


Fuente autoría propia

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

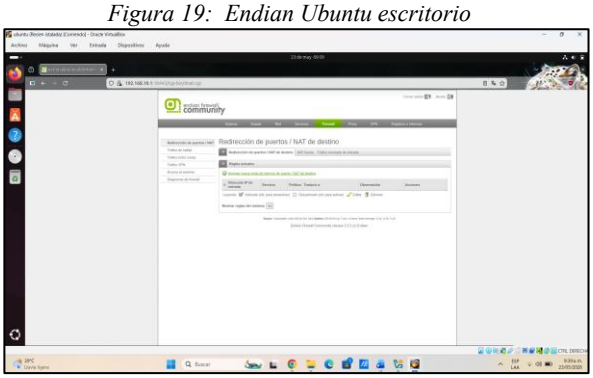
Para el desarrollo de esta temática es necesario realizar previamente la configuración de red de cada una de las máquinas virtuales dentro de VirtualBox. En Ubuntu Desktop, el adaptador 1 será configurado en la zona verde (GREEN), asignándole la dirección IP 192.168.10.2 con máscara de subred 255.255.255.0 y puerta de enlace predeterminada 192.168.10.1, correspondiente a la interfaz GREEN configurada en Endian Firewall Community. Por otra parte, en Ubuntu Server el adaptador 1 será asociado a la zona naranja (ORANGE/DMZ), configurando la dirección IP 192.168.20.2 y estableciendo como gateway la dirección 192.168.20.1. Finalmente, en Endian se configurarán tres interfaces de red: el adaptador 1 para la zona verde, el adaptador 2 para la zona naranja y el adaptador 3 configurado bajo NAT, el cual permitirá la salida hacia internet. Una vez establecida toda la segmentación de red y el direccionamiento IP, el orden correcto de inicialización de las máquinas virtuales será primero Endian, posteriormente Ubuntu Server y finalmente Ubuntu Desktop, garantizando así el correcto enrutamiento y funcionamiento de los servicios dentro de la infraestructura virtualizada.

Figura 18: Instalación Endian



Fuente: autoria propia

Figura 19: Endian Ubuntu escritorio



Fuente: autoria propia

4.3.2 CONFIGURACIÓN INICIAL

En la sección 3.3 configuración de Endian se establecieron los tres adaptadores de red que serán implementados en esta temática

Zona GREEN (verde – cliente)

Zona ORANGE (naranja - DMZ)

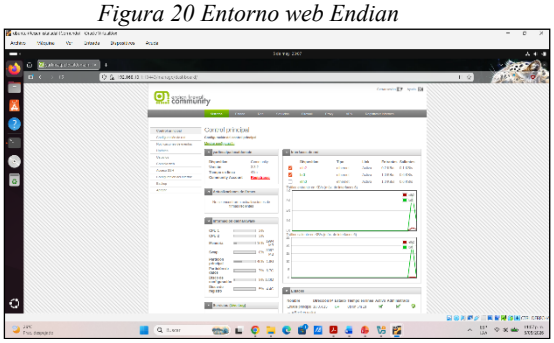
Zona RED (roja – internet)

De igual manera se configuro las direcciones IP y para ello quedaron establecidas de la siguiente manera

Ubuntu desktop	192.168.10.2
Ubuntu server	192.168.20.2
Endian	192.168.10.1
Mascara de subred	255.255.255.0
Puerta de enlace	192.168.10.1 y 192.168.20.1

Después de haber realizado toda la configuración de red y encendido las máquinas virtuales, se procede a administrar el firewall de Endian Firewall Community mediante su interfaz web de administración. Para acceder a esta interfaz, desde Ubuntu Desktop se ingresa en el navegador la dirección IP 192.168.10.1, correspondiente a la interfaz configurada en la zona verde (GREEN) de Endian, permitiendo así gestionar las políticas de seguridad, reglas de firewall y servicios de red de la infraestructura virtualizada.

Figura 20 Entorno web Endian



Fuente: autoría propia

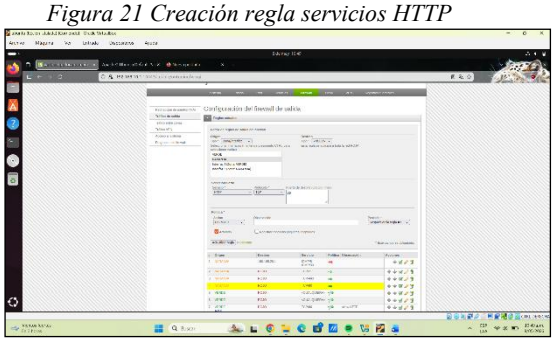
4.3.3 CREACIÓN REGLAS SERVICIOS HTTP Y FTP

En la interfaz gráfica de administración de Endian Firewall Community nos dirigimos al apartado de Firewall, donde procederemos a crear una nueva política de filtrado para permitir el acceso al servicio HTTP mediante el puerto 80, como se ilustra en la imagen 19. La configuración de la regla se realiza de la siguiente manera:

Origen: interfaz NARANJA (DMZ).
Destino: interfaz ROJO (Internet).
Servicio/Puerto: HTTP.
Protocolo: TCP.
Puerto: 80.
Política/Acción: Permitir.

Una vez realizada la configuración, procedemos a seleccionar la opción "Crear Regla" para aplicar la política dentro del firewall. Posteriormente, la regla será ubicada al inicio de la lista de políticas configuradas, permitiendo darle mayor prioridad dentro del procesamiento del tráfico y facilitando su identificación dentro de las reglas implementadas en el sistema.

Figura 21 Creación regla servicios HTTP



Fuente: autoría propia

Figura 22 Servicios HTTP Ubuntu server

Fuente: autoría propia

Figura 23 Servicios HTTP Ubuntu escritorio

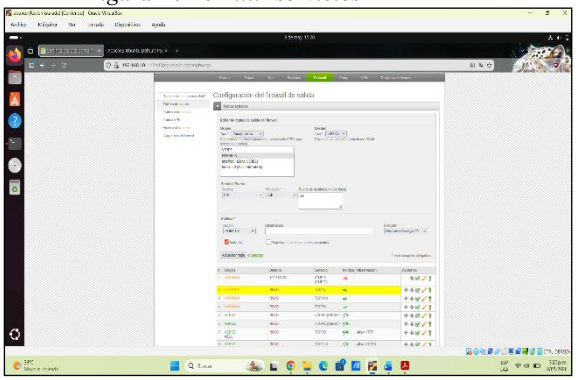
Fuente: autoria propia

Pasamos a crear la segunda regla que activación de los servicios FTP por el puerto 21. En la interfaz gráfica de Endian Firewall Community nos dirigimos al apartado Firewall → Tráfico de salida, donde procederemos a crear una nueva regla para permitir el acceso al servicio FTP mediante el puerto 21, como se ilustra en la imagen. La configuración de la política se realiza de la siguiente manera:

Origen: interfaz ORANGE (DMZ).
Destino: interfaz RED (Internet).
Servicio/Puerto: FTP.
Protocolo: TCP.
Puerto: 21.
Política/Acción: Permitir.

Una vez configurada la regla, procedemos a seleccionar la opción "Crear Regla" para aplicar la política dentro del firewall. Posteriormente, la regla será ubicada al inicio de la lista de políticas configuradas, permitiendo asignarle mayor prioridad dentro del procesamiento del tráfico de red y facilitando la identificación de la regla implementada dentro de la infraestructura de seguridad.

Figura 24 Permitir servicios FTP



Fuente: autoría propia

Figura 25 comprobación servicios FTP

Fuente: autoria propia

4.3.4 DENEGAR EL PROTOCOLO ICMP

En la interfaz gráfica de Endian Firewall Community nos dirigimos al apartado Firewall → Tráfico entre zonas, donde procederemos a crear una nueva política de filtrado con el objetivo de bloquear el protocolo ICMP dentro de la red, como se ilustra en la imagen. La configuración de la regla se realiza de la siguiente manera:

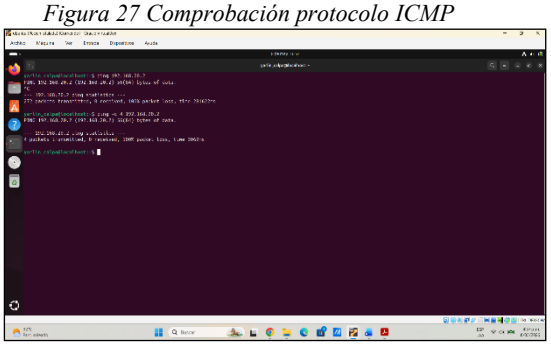
Origen: interfaz GREEN (Clientes).
Destino: interfaz ORANGE (DMZ – Ubuntu Server).
Servicio: Definido por el usuario.
Protocolo: ICMP.
Tipo ICMP: 8 y 0, configurados uno en cada línea.
Política/Acción: Denegar.

Una vez configurada la política, procedemos a seleccionar la opción “Crear Regla” para aplicar el bloqueo del tráfico ICMP dentro del firewall. Posteriormente, la regla será ubicada en la primera posición de la lista de políticas configuradas, permitiendo darle mayor prioridad dentro del procesamiento del tráfico y facilitando su identificación dentro de las reglas implementadas. Finalmente, se guardan los cambios y se aplica la nueva configuración de seguridad en la infraestructura de red virtualizada.

Figura 26 Creación regla protocolo ICMP

Fuente: autoría propia

Figura 27 Comprobación protocolo ICMP



Fuente: autoría propia

Cada una de las reglas configuradas en Endian Firewall Community funcionó correctamente durante el desarrollo de las pruebas realizadas, permitiendo validar la correcta implementación de las políticas de seguridad dentro de la infraestructura de red virtualizada. Los servicios HTTP y FTP operaron de manera satisfactoria al atravesar la zona desmilitarizada (DMZ), logrando establecer conectividad y transmisión de datos entre las diferentes redes configuradas. De igual manera, la política de denegación del protocolo ICMP fue aplicada correctamente, evidenciándose al realizar pruebas de conectividad mediante el comando ping hacia la dirección IP 192.168.20.2, donde el firewall bloqueó la transmisión y recepción de paquetes ICMP conforme a las reglas definidas. Con estos resultados, se comprobó el correcto funcionamiento del firewall de Endian en el control, filtrado y administración del tráfico de red implementado en el presente trabajo.

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

Para el desarrollo de la práctica se empleó una estructura segmentada por zonas de seguridad. La zona Verde representa la red local o LAN, la zona Naranja corresponde a la DMZ, donde se ubican los servicios publicados, y la zona Roja representa la conexión hacia Internet.

4.4.1 Servicios y puertos utilizados:

Los servicios configurados durante la práctica fueron HTTP y FTP. HTTP fue utilizado para validar el acceso web hacia el servidor Apache2, mientras que FileZilla fue considerado para la transferencia de archivos entre zonas.

4.4.2 Metodología:

La metodología utilizada se dividió en cuatro fases principales:

- Preparación del servidor ubicado en la DMZ.
- Instalación y activación del servicio Apache2.
- Creación de reglas de acceso en el firewall.
- Validación del acceso HTTP desde un navegador web.

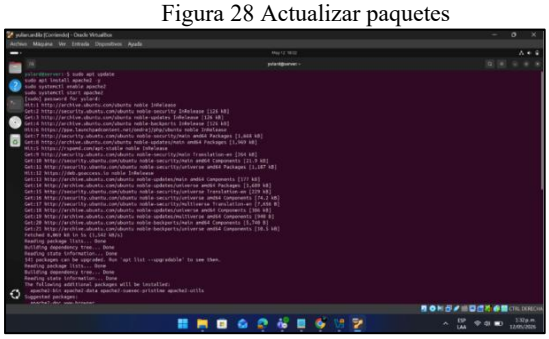
Donde 192.168.80.161 representa el equipo cliente y 192.168.80.151 corresponde al servidor web Apache2.

4.4.3 Desarrollo de la configuración:

A. Actualización del sistema

En primer lugar, se actualizó la lista de paquetes del servidor Linux ubicado en la zona DMZ mediante el siguiente comando: sudo apt update

Figura 28 Actualizar paquetes

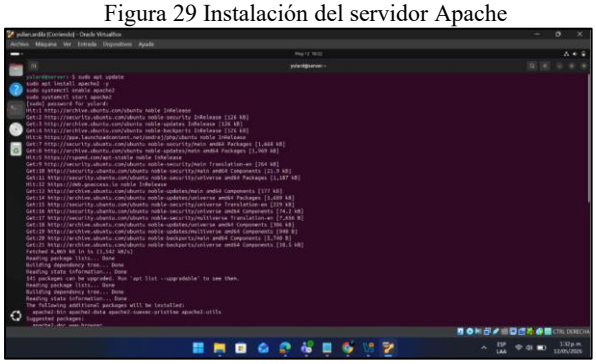


Fuente: autoría propia

B. Instalación del servidor web Apache2:

Apache2 permite convertir el equipo Linux en un servidor web capaz de responder solicitudes HTTP. El parámetro -y automatiza la confirmación de instalación, evitando que el sistema solicite aprobación manual durante el proceso.

Figura 29 Instalación del servidor Apache

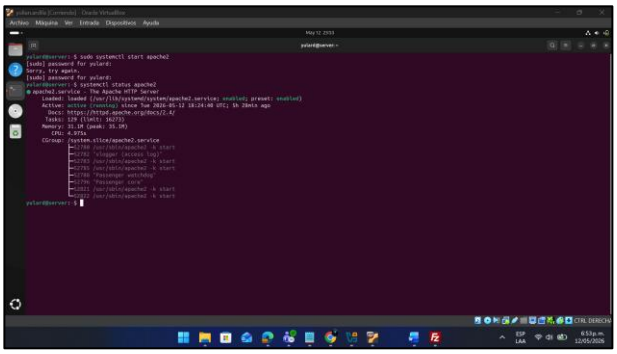


Fuente: autoría propia

C. Inicio del servicio Apache2:

Se inicia el servidor Apache con el siguiente comando: sudo systemctl start apache2, a partir de este momento el servidor quedó preparado para recibir solicitudes HTTP por el puerto TCP 80.

Figura 30 Inicio del servicio Apache2 y verificación del estado del servicio.



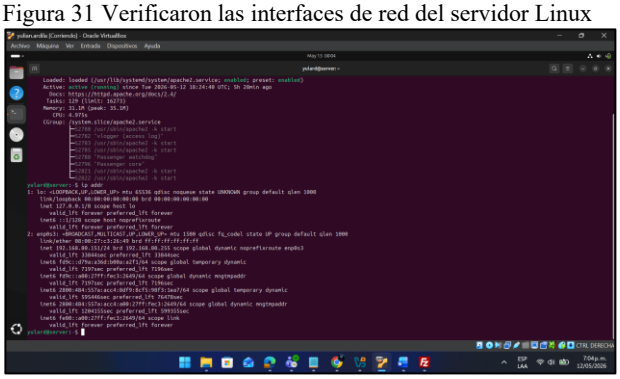
Fuente: autoría propia

4.4.4 Configuración de reglas de acceso:

Para permitir el tráfico HTTP desde la LAN hacia la DMZ, se configuró una regla de firewall con los siguientes parámetros:

Inicialmente se verificaron las interfaces de red del servidor Linux mediante el comando ip addr. El resultado permitió identificar la interfaz activa enp0s3, la cual tiene asignada la dirección IP 192.168.80.151/24. Esta dirección corresponde al servidor ubicado en la red de pruebas y será utilizada para validar el acceso al servicio HTTP publicado mediante Apache2.

Figura 31 Verificaron las interfaces de red del servidor Linux

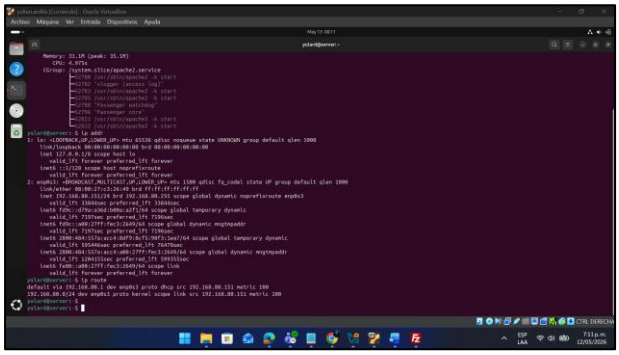


Fuente: autoría propia

4.4.5 Verificar conectividad básica desde este servidor:

Se verificó la tabla de enrutamiento del servidor mediante el comando ip route. El resultado permitió identificar que la interfaz activa enp0s3 utiliza la dirección IP 192.168.80.151, perteneciente a la red 192.168.80.0/24. Asimismo, se evidenció que la puerta de enlace predeterminada corresponde a 192.168.80.1, lo cual permite al servidor enviar tráfico hacia redes externas al segmento local.

Figura 32 Verificación de conectividad básica desde este servidor.



Fuente: autoría propia

4.4.7 Verificar conectividad entre el servidor Linux y el gateway.

Se ejecutó una prueba de conectividad hacia la puerta de enlace predeterminada mediante el comando ping -c 4 192.168.80.1. El resultado evidenció el envío de cuatro paquetes ICMP y la recepción de cuatro respuestas, obteniendo un 0% packet loss. Esta prueba permitió confirmar la comunicación exitosa entre el servidor Linux con dirección 192.168.80.151 y su gateway 192.168.80.1.

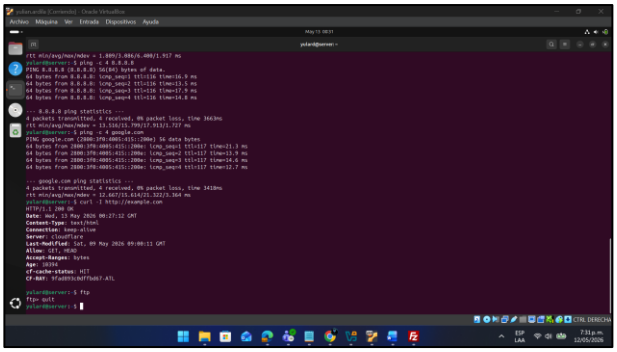
Figura 33 Verificación de conectividad con el gateway

Fuente: autoría propia

4.4.8 Verificar que el cliente FTP está instalado.

Se verificó la disponibilidad del cliente FTP mediante la ejecución del comando ftp. El sistema ingresó al modo interactivo del cliente, mostrando el indicador ftp>, lo cual confirmó que la herramienta se encontraba instalada y disponible para realizar pruebas de conexión mediante el protocolo FTP.

Figura 34 Disponibilidad del cliente FTP

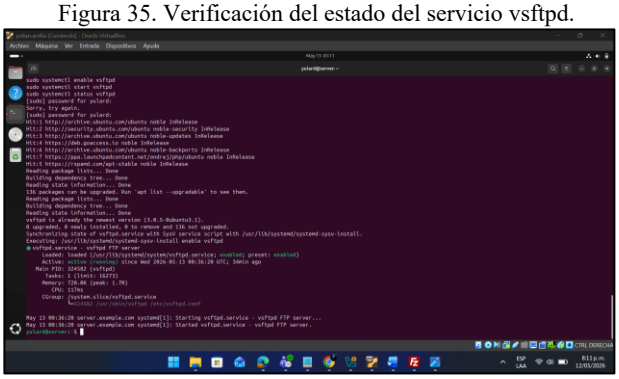


Fuente: autoría propia

4.4.9 Instalación y activación del servidor FTP.

Para complementar la validación del servicio FTP, se instaló y habilitó el servidor vsftpd en el equipo Linux ubicado en la zona DMZ. Este servicio permite recibir conexiones FTP mediante el puerto TCP 21, facilitando la transferencia de archivos entre las zonas definidas dentro de la infraestructura de red.

Figura 35. Verificación del estado del servicio vsftpd.

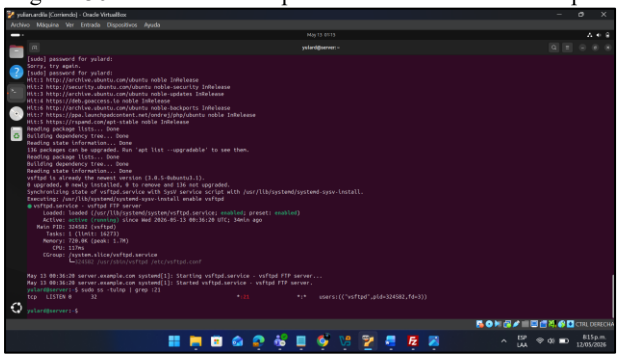


Fuente: autoría propia

4.4.10 Verificación del puerto FTP TCP 21.

Posteriormente, se verificó que el servicio FTP estuviera escuchando en el puerto TCP 21 mediante el comando, el resultado mostró el puerto *:21 en estado LISTEN, asociado al proceso vsftpd. Esto confirmó que el servidor FTP estaba preparado para recibir conexiones entrantes desde otros equipos de la red.

Figura. 36. Verificación del puerto TCP 21 asociado a vsftpd.



Fuente: autoría propia

4.4.11 Validación de conexión FTP hacia el servidor DMZ.

Una vez verificado el servicio FTP, se realizó una conexión hacia el servidor ubicado en la dirección 192.168.80.151 mediante el comando: ftp 192.168.80.151. Inicialmente se evidenció la conexión con el servidor FTP a través del mensaje Connected to 192.168.80.151 y el banner 220 (vsFTPd 3.0.5). Posteriormente, se realizó la autenticación con un usuario válido del sistema, permitiendo acceder al modo interactivo del cliente FTP.

Figura 37. Conexión al servidor FTP ubicado en la DMZ.

Fuente: autoría propia

4.4.12 Configuración de reglas de reenvío de puertos.

Para permitir el acceso desde la zona WAN hacia el servidor ubicado en la DMZ, se configuraron reglas de reenvío de puertos en el gateway de red. El servidor interno utilizado fue 192.168.80.151, donde se encontraban activos los servicios Apache2 y vsftpd. Las reglas configuradas fueron las siguientes:

Figura 38. Reglas de reenvío de puertos para HTTP y FTP hacia 192.168.80.151.

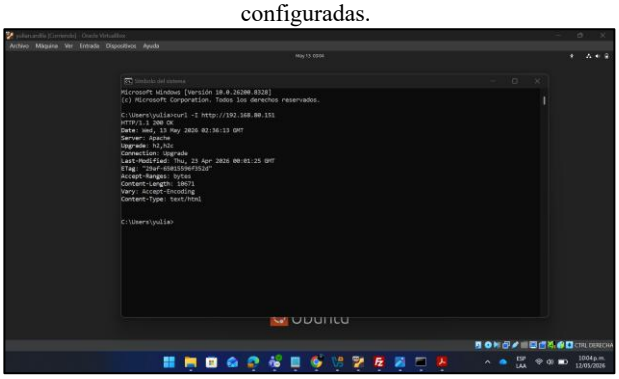
Fuente: autoría propia

La primera regla permite redirigir el tráfico HTTP que ingresa al gateway por el puerto TCP 80 hacia el servidor Apache2. La segunda regla permite redirigir el tráfico FTP que ingresa por el puerto TCP 21 hacia el servidor vsftpd. Esta configuración permite publicar los servicios de la DMZ hacia la zona externa de forma controlada.

4.4.13 Validación del tráfico HTTP por puertos configurados.

Una vez configurada las reglas con los puertos en el gateway, se realiza la validación del tráfico desde el servidor apache2 hacia zona externa de forma controlada.

Figura 39. Validación del tráfico HTTP con las reglas configuradas.



Fuente: autoría propia

4.5 TEMÁTICA 5: IMPLEMENTAR UN PROXY HTTP

Se desarrolla la implementación de un proxy HTTP no transparente utilizando la distribución GNU/Linux Endian Firewall Community, con el objetivo de fortalecer la seguridad perimetral en una infraestructura de red segmentada en zonas LAN, WAN y DMZ. La solución integra mecanismos de autenticación de usuarios, control de acceso basado en políticas y filtrado de contenido web mediante listas negras. Se validó el funcionamiento del sistema a través de pruebas de navegación, evidenciando el control del acceso a Internet, la restricción de sitios específicos y la correcta autenticación de usuarios.

4.5.1 Metodología

La implementación se realizó sobre una infraestructura virtualizada en Oracle VirtualBox, donde se configuraron las siguientes zonas de red:

- Zona Verde (LAN): 192.168.10.0/24
- Zona Naranja (DMZ): 192.168.20.0/24
- Zona Roja (WAN): DHCP mediante NAT

El firewall Endian se configuró como punto central de control del tráfico entre estas zonas.

4.5.2 Implementación del Proxy HTTP

A. Configuración del Proxy HTTP No Transparente

Se habilitó el servicio de proxy HTTP en Endian, configurándolo en modo no transparente para permitir la autenticación explícita de los usuarios.

Esta configuración garantiza que los dispositivos clientes deban utilizar manualmente el proxy, permitiendo mayor control del tráfico.

Figura 40 Configuración de proxy

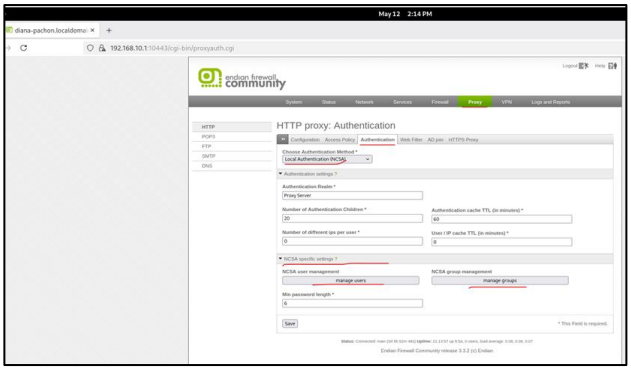
Fuente: autoría propia

B. Configuración de Autenticación

Se activó la autenticación tipo NCSA (Local Authentication), lo cual permitió la gestión de usuarios directamente en el firewall.
Se definieron parámetros como:

- Realm de autenticación
- Control de sesiones
- Longitud mínima de contraseña

Figura 41 Activación de autenticación



Fuente: autoría propia

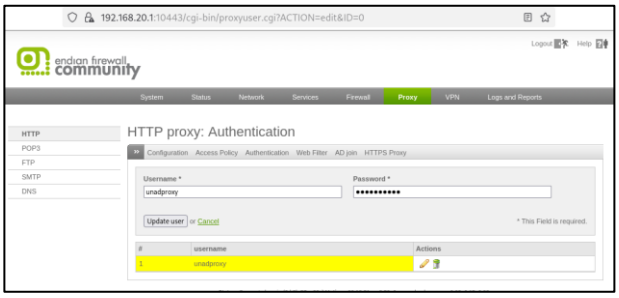
C. Creación de Usuarios y Grupos

Se implementó una estructura básica de control de acceso mediante:

- Usuario: unadproxy
- Grupo: admin_proxy

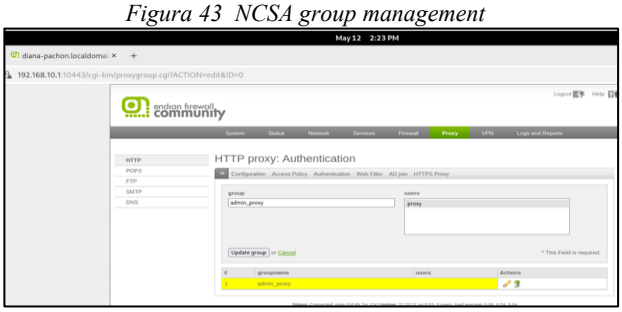
Posteriormente, el usuario fue asociado al grupo, permitiendo aplicar políticas específicas basadas en pertenencia a grupos.

Figura 42 NCSA user management



Fuente: autoría propia

Figura 43 NCSA group management



Fuente: autoría propia

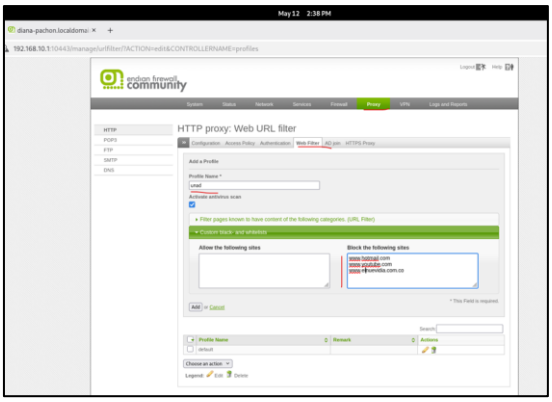
D. Configuración de Filtrado Web (Lista Negra)

Se creó un perfil de filtrado denominado “unad”, en el cual se definió una lista negra de sitios web restringidos, incluyendo:

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

Este perfil permite bloquear el acceso a dominios específicos desde la red interna.

Figura 44 Creación de perfil y lista negra



Fuente: autoría propia

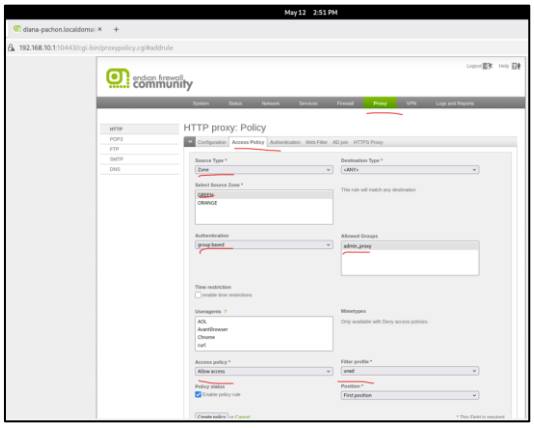
E. Creación de Políticas de Acceso

Se definió una política de acceso en el proxy HTTP con las siguientes características:

- Origen: Zona GREEN (LAN)
- Autenticación: Basada en usuario/grupo
- Acción: Permitir acceso
- Perfil de filtrado: "unad"
- Prioridad: Primera posición

Esta política garantiza que todo el tráfico de la red interna pase por el proxy, sea autenticado y sometido a filtrado.

Figura 45 Creación de política de acceso



Fuente: autoría propia

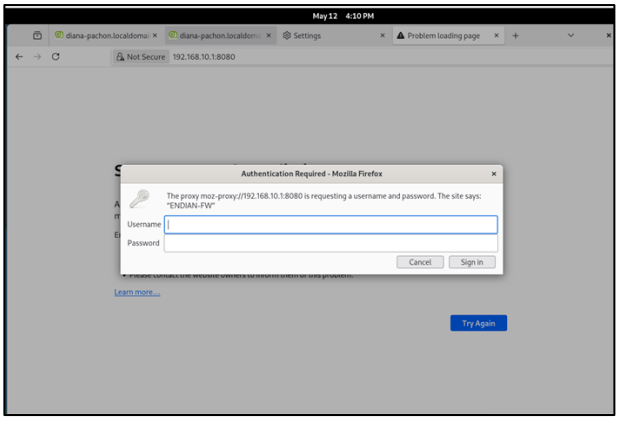
4.5.2 Pruebas y Resultados

A. Validación de Autenticación

Al realizar la prueba de navegación, el sistema solicitó credenciales de usuario, evidenciando que:

- El tráfico pasa por el proxy
- Se requiere autenticación previa
- Las políticas son aplicadas correctamente

Figura 46 Prueba de navegación por el proxy



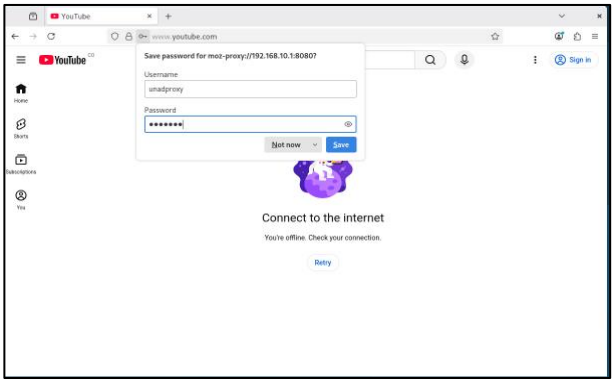
Fuente: autoría propia

B. Validación de Bloqueo de Sitios

Se realizaron pruebas accediendo a sitios incluidos en la lista negra, obteniendo como resultado:

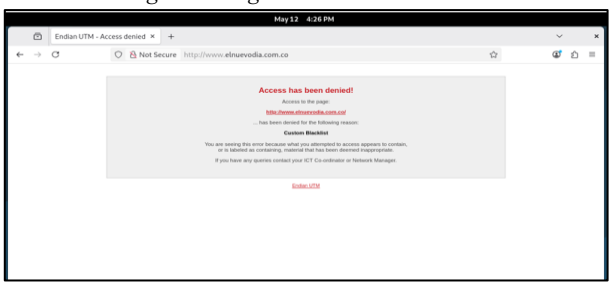
- Bloqueo exitoso con mensaje "Access Denied"
- Confirmación del funcionamiento del filtro web

Figura 47 Ingreso a YouTube



Fuente: autoría propia

Figura 48 Ingreso www.elnuevodia.com.co



Fuente: autoría propia

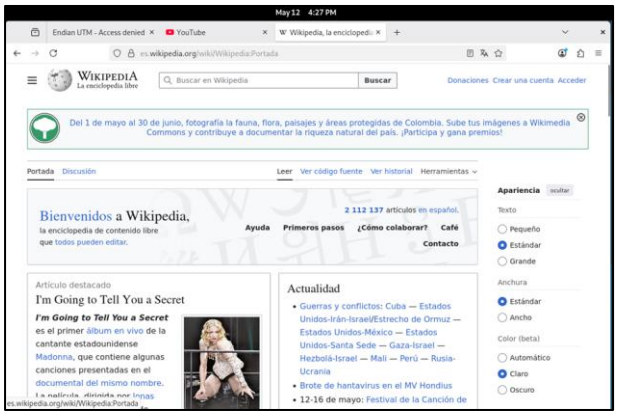
C. Validación de Navegación Permitida

Se verificó el acceso a sitios no restringidos (ej. Wikipedia), evidenciando que:

- La navegación es permitida cuando no hay coincidencia con la blacklist

- El sistema distingue correctamente tráfico permitido y restringido

Figura 49 Navegación permitida



Fuente: autoría propia

5 LIMITACIONES Y DIFICULTADES

Durante el desarrollo de las prácticas se presentaron algunas dificultades relacionadas con la configuración de adaptadores de red en Oracle VirtualBox, comunicación entre las zonas GREEN y ORANGE, validación de reglas de firewall y acceso a servicios dentro de la infraestructura virtualizada.

Asimismo, durante la configuración de NAT, DNS y Proxy HTTP fue necesario realizar diferentes pruebas y ajustes relacionados con direccionamiento IP, gateways y políticas de tráfico para garantizar la conectividad entre clientes, servidores y acceso a Internet.

A pesar de los inconvenientes presentados, estas situaciones permitieron fortalecer el proceso de aprendizaje y comprender la importancia de la correcta configuración de interfaces, segmentación de red y políticas de seguridad dentro de entornos GNU/Linux orientados a la administración de servicios y seguridad perimetral.

Durante el desarrollo de la Temática 4 se presentaron algunas dificultades relacionadas con la identificación correcta del rol de cada equipo dentro de la infraestructura de red. Inicialmente fue necesario diferenciar entre el servidor Linux ubicado en la DMZ y el equipo que actuaba como gateway o firewall, debido a que el servidor 192.168.80.151 solo contaba con una interfaz de red activa, mientras que las reglas de reenvío y control de tráfico debían aplicarse sobre el dispositivo de puerta de enlace 192.168.80.1.

También fue necesario verificar de forma independiente que los servicios HTTP y FTP estuvieran realmente activos antes de validar las reglas de acceso. Para ello se utilizaron comandos como systemctl status apache2, systemctl status vsftpd y ss –tulnp.

6 CONCLUSIONES.

El desarrollo de las temáticas permitió fortalecer conocimientos relacionados con virtualización, administración de redes y seguridad perimetral en entornos GNU/Linux mediante la implementación de Endian Firewall Community en Oracle VirtualBox.

En la temática 1 se logró instalar y configurar correctamente Endian Firewall, estableciendo las zonas GREEN, ORANGE y RED y validando la comunicación entre clientes, servidores y acceso a Internet dentro de la infraestructura virtualizada.

La temática 2 permitió comprobar el funcionamiento de NAT y la traducción de direcciones IP, validando conectividad, resolución DNS y acceso a redes externas desde las diferentes zonas configuradas en el firewall.

En la temática 3 se implementaron políticas de acceso y reglas de firewall para permitir servicios HTTP y FTP, además de restringir tráfico ICMP entre zonas de red. Las pruebas realizadas permitieron verificar el correcto control y filtrado del tráfico dentro de la infraestructura implementada.

La temática 4 permitió evidenciar el funcionamiento y la importancia de las reglas de acceso implementadas en Endian Firewall Community dentro de una infraestructura de red segmentada. A través de la configuración y habilitación de los servicios HTTP (puerto TCP 80) y FTP (puerto TCP 21) en el servidor Ubuntu Server con dirección IP 192.168.80.151, fue posible validar el acceso controlado desde la red cliente hacia la zona DMZ.

En la temática 5 se configuró un proxy HTTP no transparente con autenticación de usuarios y filtrado web mediante listas negras, evidenciando el correcto funcionamiento de las políticas de acceso y restricción de navegación.

Durante el desarrollo de las prácticas se presentaron dificultades relacionadas con configuración de adaptadores de red, comunicación entre zonas, reglas de firewall y validación de servicios. Sin embargo, estas situaciones permitieron fortalecer habilidades relacionadas con análisis de errores, solución de problemas y administración de servicios Linux.

7 REFERENCIAS

Apache Software Foundation. (2023). *Apache HTTP Server documentation*. https://httpd.apache.org/docs/

Canonical. (2023). *Guía de Ubuntu Desktop 20.04 LTS*. https://help.ubuntu.com/

Canonical. (2023). *Netplan documentation*. https://netplan.io/reference

Canonical. (2023). *Ubuntu Server documentation*. https://ubuntu.com/server/docs

Cisco. (2022). *Network Address Translation (NAT)*. https://www.cisco.com/

Debian Project. (2023). *Manual del administrador de Debian 12.5.0.*

https://www.debian.org/releases/stable/amd64/index.es.html

Endian. (2016). *Endian UTM 3.2 manual de referencia*. http://docs.endian.com/3.2/utm/index.html

Freedesktop.org. (2023). *systemd documentation*. https://www.freedesktop.org/wiki/Software/systemd/

Linux Foundation. (2023). *Linux documentation*. https://www.kernel.org/doc/html/latest/

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

Red Hat. (2022). *Linux networking and administration guide*. https://www.redhat.com/en/services/training/linux-system-administration

Squid Software Foundation. (2023). *Squid Proxy Server documentation.* http://www.squid-cache.org/Doc/

VMware. (2023). *Virtualization and virtual machine documentation*. https://docs.vmware.com/