Implementación de Reglas de Acceso para el Control de Tráfico en Redes Segmentadas

Victor Hugo Conto Carvajal
vhcontoc@unadvirtual.edu.co
Maira Alejandra Franco Perez
Mafrancop@unadvirtual.edu.co
Sergio Alexander Segura Salazar
saseguras@unadvirtual.edu.co
Jorge Duvan Velásquez Ramirez
jdvelasquezra@unadvirtual.edu.co

Resumen: En entornos de red segmentados, el control del tráfico mediante reglas de acceso es esencial para garantizar la seguridad y la funcionalidad entre zonas. Este artículo describe la implementación de políticas de filtrado utilizando Endian Firewall, enfocándose en la gestión del tráfico entre zonas específicas (Verde, Naranja, DMZ e Internet). Se detalla la configuración de reglas para permitir o bloquear servicios como HTTP y FTP, empleando la interfaz web de Endian. Además, se documenta la verificación del tráfico Inter-Zona y la validación funcional a través de navegadores web, considerando criterios de seguridad, conectividad y buenas prácticas en redes protegidas.

PALABRAS CLAVE: firewall, FTP, HTTP, reglas de acceso, segmentación de red, tráfico Inter-Zona.

1. INTRODUCCIÓN

El control del tráfico de red mediante reglas de acceso es una práctica esencial para la protección de los recursos informáticos. En arquitecturas de red con múltiples zonas —como LAN (zona Verde), zona Naranja, DMZ e Internet (WAN)—, se requiere un diseño cuidadoso de políticas que permitan solo el tráfico legítimo. Este estudio describe la implementación y verificación de dichas reglas usando servicios comunes como HTTP y FTP.

A medida que avanza la tecnología las compañías tienden a crecer su infraestructura informática esto hace que sean mas vulnerables a los ataques informáticos, ya que por medio de alguna conexión sin filtrado se corre el riesgo de ser vulnerados, es por eso la importancia de tener la red segmentada y con diferentes políticas de conexión en la organización ya que se tiene control del perímetro de salida y entrada, a continuación veremos como por medio de herramientas de código libre logramos implementar las acciones requeridas y así poder cumplir con la disponibilidad, integridad y confidencialidad de la información.

2. ARQUITECTURA DE RED Y ESCENARIO

La implementación del Endian FW, se llevó a cabo en un entorno de virtualización tratando de emular en lo posible un entorno empresarial, por consiguiente, el Endian actuara como un host perimetral de filtrado de trafico de red y también habrá dos máquinas Linux más una haciendo las veces de servidor y la otra de host, en cuanto a la red esta se compone de las siguientes zonas:

- Zona Verde (LAN): Red interna confiable
- Zona Naranja: DMZ
- Zona Roja: Internet (WAN)

A su vez se definió el direccionamiento IP a las zonas de la siguiente manera: la zona WAN (roja) con la dirección 192.168.1.100/24, la zona LAN (verde) con la red 192.168.100.0/24 y la zona DMZ (naranja, para servidores) con la red 192.168.200.0/24.

En lo que respecta al hardware la máquina que soporta el firewall debe tener dos interfaces físicas, por lo que bastara con agregar el hardware en la máquina virtual, una de estas interfaces estará destinada a la red WAN la cual emulará la conexión a la red foránea dada por el proveedor de internet, la otra interface será configurada como red LAN y dentro de esta red destinaremos unas de direcciones ip disponibles la cual será configurada de manera estática ya que mediante esta dirección se acceso la administración web del recurso.

Es importante señalar: i) En cuanto a configuraciones en el entorno virtual, la interface WAN debe estar configurada en modo brige (puente), mientras que la red LAN debe ir en la red interna. ii) Tanto la maquina servidor como el host deben estar en la red interna.

2.1 INSTALACIÓN Y CONFIGURACIÓN

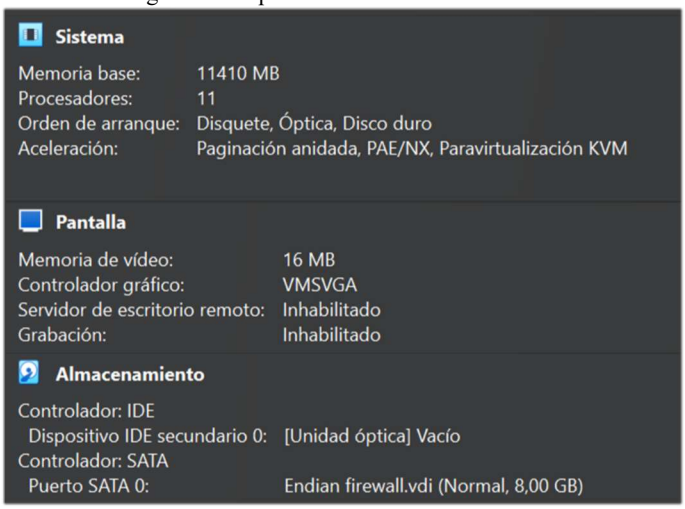
2.1.1 CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX (TARJETAS DE RED) E INSTALACIÓN EFECTIVA DEL MISMO

El Endian Firewall es un software de código abierto diseñado para la gestión unificada de amenazas de red (UTM), proporcionando una solución robusta y flexible para la seguridad perimetral. Esta distribución destaca por su amplia gama de funcionalidades, que incluyen desde el control de accesos hasta la protección avanzada contra ciberataques. Para los propósitos de este proyecto, se implementaron los servicios de NAT, firewall y proxy, configurados específicamente para optimizar la segmentación de red, filtrar el tráfico de manera granular y garantizar una navegación segura mediante la inspección y control de contenidos. Además, se aprovecharon las capacidades de monitoreo y registro de eventos de Endian para

mantener un control proactivo sobre las actividades de la red, asegurando una administración eficiente y una respuesta rápida ante posibles incidentes de seguridad.

A diferencia de otras distribuciones de seguridad, Endian Firewall no está disponible como un paquete instalable directamente desde los repositorios estándar de Linux, lo que lo distingue por su enfoque dedicado y especializado. En su lugar, los usuarios deben descargar la imagen en formato ISO desde el sitio oficial del fabricante para proceder con su instalación, ya sea en hardware físico o en un entorno virtualizado. Para este proyecto, se optó por un entorno de simulación controlada utilizando el software de virtualización VirtualBox, versión 7.1.6, donde se desplegó la versión Endian Firewall Community. Los requisitos mínimos para este entorno virtual incluyeron 11 GB de RAM, una asignación de 10 a 20 núcleos de CPU y 20 GB de espacio disponible en disco. Sin embargo, es importante destacar que en un entorno productivo, donde el tráfico de red puede ser significativamente mayor, estos requisitos podrían incrementarse para garantizar un rendimiento óptimo y una gestión eficiente de las cargas de trabajo. La instalación se llevó a cabo siguiendo un proceso de montaje de la ISO, configurando cuidadosamente las interfaces de red virtuales y ajustando los parámetros del sistema para alinearse con las necesidades específicas del proyecto, asegurando así una plataforma estable para la implementación de los servicios de NAT, firewall y proxy.

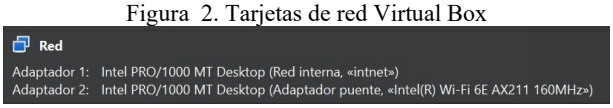
Figura 1. Requisitos Hardware Virtual Box



Fuente: Autoría Propia

En la fase de aprovisionamiento, se llevaron a cabo una serie de configuraciones clave para garantizar la operatividad y la correcta integración del Endian Firewall en el entorno de red diseñado. Como se mencionó previamente, se procedió a la incorporación de dos tarjetas de red virtuales con funciones específicas: una dedicada al enlace WAN para la conexión a Internet y otra asignada al entorno LAN para la comunicación interna. La primera tarjeta, destinada a la interfaz WAN, se configuró en modo bridge, permitiendo que el Endian Firewall accediera directamente a la red externa y gestionara el tráfico de Internet de manera transparente y eficiente. Por su parte, la segunda tarjeta, correspondiente a la interfaz LAN, se estableció en modo de red interna, lo que facilitó la interconexión segura y controlada entre los hosts y servidores dentro de la red local, asegurando una comunicación fluida y protegida.

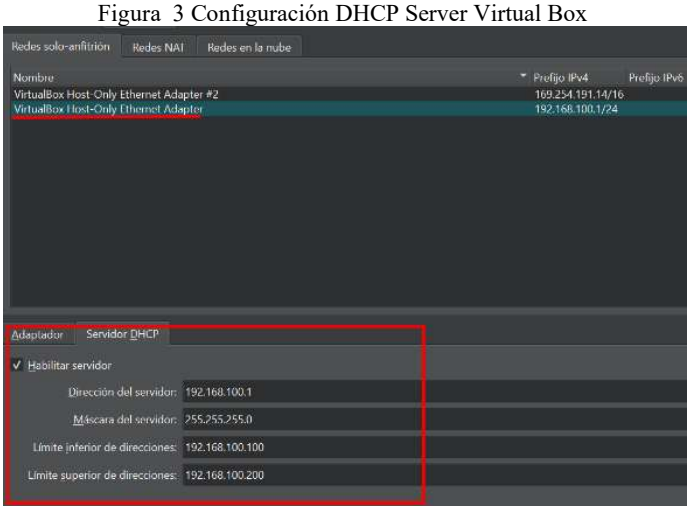
Figura 2. Tarjetas de red Virtual Box



Fuente: Autoría Propia

Adicionalmente, se habilitó y configuró el servicio DHCP en la interfaz de la red interna, una decisión estratégica orientada a simplificar la gestión del direccionamiento IP. Este servicio permite que los dispositivos conectados a la red LAN obtengan automáticamente una dirección IP válida, reduciendo la necesidad de configuraciones manuales y agilizando la incorporación de nuevos hosts al entorno. La configuración del DHCP se ajustó cuidadosamente para definir un rango de direcciones adecuado al tamaño de la red simulada, garantizando que no se presentaran conflictos de IP y que los dispositivos pudieran comunicarse sin interrupciones. Esta estructura de red, combinada con las configuraciones mencionadas, sentó las bases para un entorno funcional y escalable, permitiendo no solo la implementación efectiva de los servicios de NAT, firewall y proxy, sino también la realización de pruebas exhaustivas para evaluar el rendimiento y la seguridad del sistema.

Figura 3 Configuración DHCP Server Virtual Box



Fuente: Autoría Propia

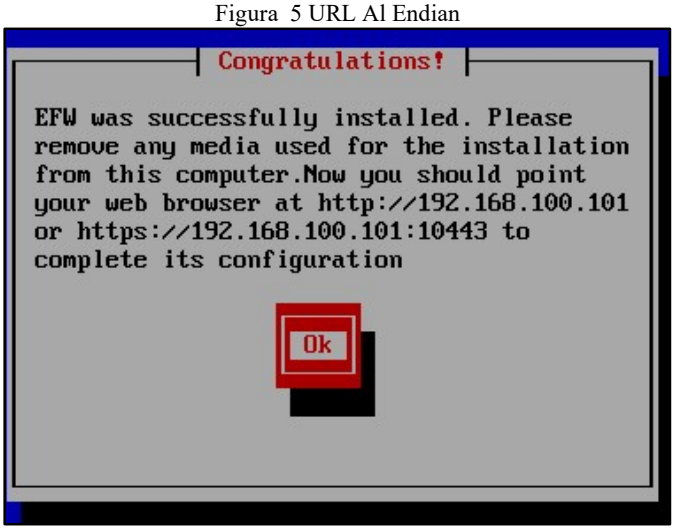
El proceso de instalación de Endian Firewall se caracteriza por su simplicidad y eficiencia, diseñado para ser accesible incluso para usuarios con experiencia técnica moderada. Este procedimiento se lleva a cabo en un entorno TUI (Text User Interface), que ofrece una interfaz basada en texto, clara y estructurada, con un flujo de pasos intuitivo que minimiza la posibilidad de errores. Durante la instalación, el sistema guía al usuario a través de una serie de configuraciones básicas, solicitando información esencial para poner en marcha la distribución. Entre estos pasos, destaca la configuración de la dirección IP asignada a la red LAN, que en la terminología de Endian Firewall corresponde a la "zona verde" (green zone). Esta zona representa el segmento de red interna considerado seguro y confiable, donde se conectan los dispositivos y servidores de la organización.

Figura 4. Configuración de red proceso de instalación

Fuente: Autoría Propia

La configuración de la IP de la zona verde requiere especial atención, ya que no solo define el esquema de direccionamiento para los dispositivos conectados a la LAN, sino que también establece el punto de acceso principal para la interfaz gráfica de administración de Endian Firewall. Una configuración incorrecta en este parámetro podría resultar en problemas de conectividad o en la imposibilidad de acceder al panel de control web, lo que dificultaría la gestión posterior de los servicios UTM. Por ello, durante este proceso, se recomienda verificar cuidadosamente la dirección IP asignada, la máscara de subred y la puerta de enlace, asegurándose de que sean coherentes con la topología de red planificada. En el caso de este proyecto, se optó por una dirección IP estática dentro de un rango privado, garantizando compatibilidad con el servicio DHCP previamente configurado y facilitando la integración con los hosts de la red interna.

Figura 5 URL Al Endian



Fuente: Autoría Propia

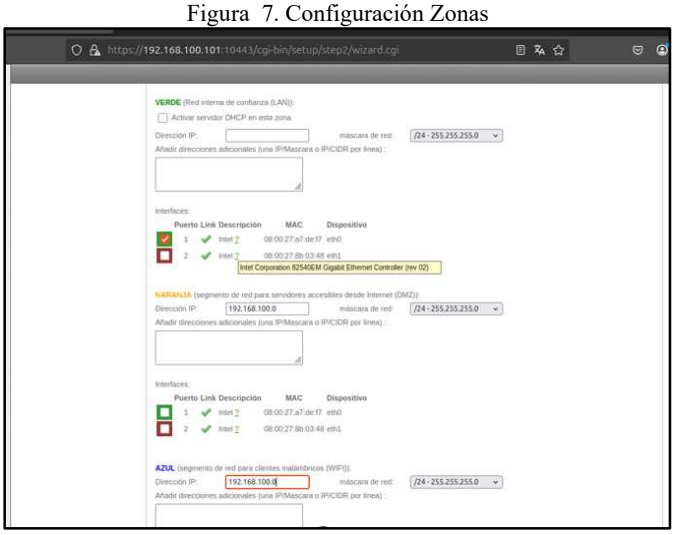
Una vez completada la instalación de Endian Firewall, los primeros pasos en el aplicativo se centran en la configuración inicial a través de su interfaz web, un entorno intuitivo y bien estructurado que facilita la administración del sistema. Como es común en plataformas de gestión basadas en web, al acceder por primera vez al panel de control mediante un navegador, utilizando la dirección IP de la zona verde configurada durante la instalación, se despliega un asistente de configuración guiado. Este asistente, diseñado para agilizar la puesta en marcha, comienza solicitando la creación de un usuario con privilegios de administrador. Este paso es crucial, ya que el usuario administrador será responsable de gestionar todas las funcionalidades del sistema, incluyendo la configuración de políticas de seguridad, el monitoreo de la red y la resolución de incidentes. Se recomienda establecer una contraseña robusta y cumplir con buenas prácticas de seguridad para proteger el acceso al panel de control.

Figura 6. Cambio contraseñas de acceso

Fuente: Autoría Propia

A continuación, el proceso avanza hacia un segundo asistente dedicado a la configuración de red, un componente esencial para definir la estructura operativa del Endian Firewall. En este asistente, se requiere configurar las zonas de red características de Endian: la zona verde (LAN, red interna segura), la zona roja (WAN, conexión a Internet), y, opcionalmente, la zona naranja (DMZ, para servidores accesibles desde el exterior). Cada zona debe asociarse a una interfaz de red específica y configurarse con un direccionamiento IP adecuado, ya sea estático o dinámico, según las necesidades del entorno. Para este proyecto, se asignó la interfaz WAN al modo bridge, previamente configurada para garantizar acceso a Internet, y la interfaz LAN a la zona verde, con una dirección IP estática que coincide con el esquema definido en la fase de aprovisionamiento. La configuración de estas zonas es un paso crítico, ya que establece las bases para el enrutamiento del tráfico, la aplicación de reglas de firewall y la segmentación de la red, asegurando que los dispositivos en la zona verde puedan comunicarse de manera segura mientras el tráfico hacia y desde la zona roja es estrictamente controlado.

Figura 7. Configuración Zonas



Fuente: Autoría Propia

El asistente de red también permite ajustar parámetros adicionales, como la configuración de la puerta de enlace predeterminada y los servidores DNS, que son fundamentales para garantizar la conectividad externa y la resolución de nombres de dominio. Una vez completados estos pasos, el sistema guarda las configuraciones y reinicia los servicios de red para aplicar los cambios, tras lo cual la interfaz web queda completamente operativa. Para verificar la correcta configuración, se realizaron pruebas de conectividad desde la zona verde hacia la zona roja, confirmando el acceso a Internet, y se revisaron los registros del sistema para asegurar que no hubiera errores en la asignación de interfaces o en el direccionamiento. Este proceso inicial, aunque sencillo gracias al diseño del asistente, requiere precisión para evitar problemas en la comunicación entre zonas o en la aplicación de políticas de seguridad.

En los apartados siguientes, se detallarán las configuraciones específicas de las características clave de Endian Firewall implementadas en este proyecto, incluyendo la gestión de reglas de NAT para el enrutamiento de tráfico, la definición de políticas de firewall para el filtrado granular y la configuración del proxy para el control de contenidos web. Además, se explorarán las herramientas de monitoreo y análisis integradas en la plataforma, que permiten supervisar en tiempo real el rendimiento de la red y detectar posibles amenazas, consolidando así la funcionalidad de Endian como una solución UTM robusta. Este enfoque metódico en los primeros pasos asegura no solo una integración efectiva del sistema en el entorno de red, sino también una base sólida para la implementación de configuraciones avanzadas y la evaluación de su comportamiento en escenarios simulados y productivos.

3. CONFIGURACIÓN NAT

El uso de direcciones IP privadas obliga a aplicar técnicas de traducción para permitir la conectividad con redes públicas. El NAT actúa como un intermediario, el cual traduce las direcciones privadas en públicas y viceversa. Esta técnica no solo garantiza el acceso a Internet desde redes internas, sino que también proporciona una capa básica de seguridad. En este ensayo se describe el proceso de configuración de reglas NAT para dos escenarios: acceso desde LAN hacia WAN y publicación de servicios desde DMZ hacia Internet.

3.1 LAN HACIA WAN

Las configuraciones NAT descritas en este documento fueron realizadas principalmente a través del panel gráfico de Endian, el cual permite aplicar reglas de traducción de direcciones sin necesidad de comandos de línea.

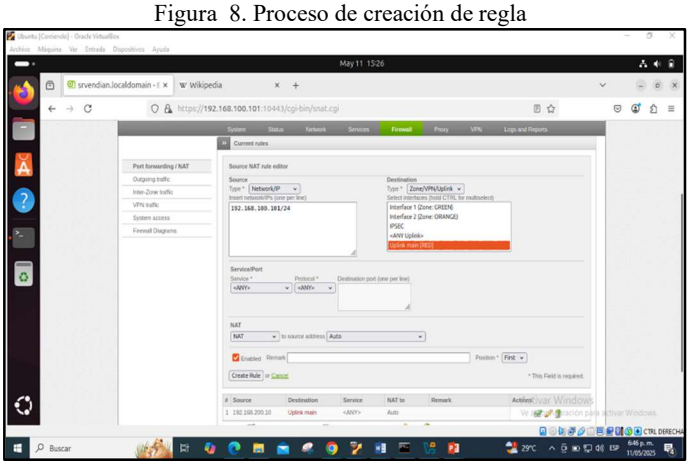
Network Address Translation (NAT) permite traducir direcciones IP privadas a direcciones IP públicas, facilitando la comunicación entre redes internas y el exterior. Existen diferentes tipos de NAT, como NAT estático, NAT dinámico y PAT (Port Address Translation), también conocido como sobrecarga de NAT

Esta técnica es fundamental para el ahorro de direcciones IPv4 y para mantener un cierto nivel de seguridad al ocultar la estructura interna de una red. Para esta práctica, se trabajó con Endian Firewall, una solución de seguridad de red que permite configurar reglas NAT desde una interfaz web gráfica, dentro de un entorno Ubuntu Desktop

El primer paso consistió en establecer la conectividad desde la red local hacia una red externa simulada (Internet). Para ello, se definió una regla de NAT la cual permite a múltiples dispositivos de la LAN compartir una única dirección IP pública.

La red interna (LAN) con direcciones 192.168.100.101/24 necesita acceder a Internet a través de un router Linux con una interfaz de salida WAN . Para esto se realiza la siguiente regla en Endian

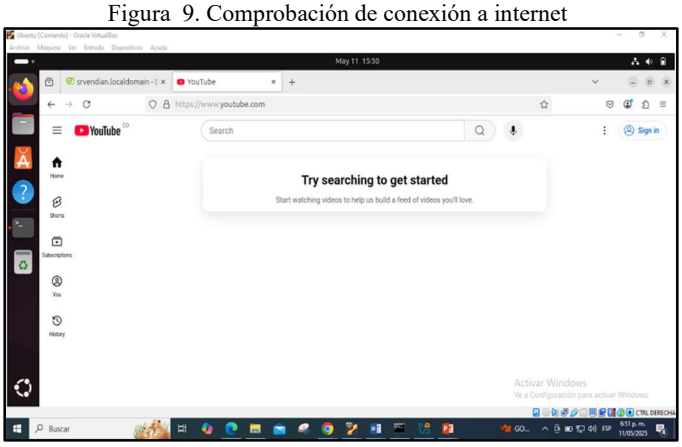
Figura 8. Proceso de creación de regla



Fuente: Autoría Propia

La conectividad puede validarse realizando un ping a una IP externa puede ser al la IP 8.8.8.8 o accediendo a un sitio web desde un navegador. Para este caso se comprueba que hay conexión a internet ingresando al sitio web Yotube :

Figura 9. Comprobación de conexión a internet



Fuente: Autoría Propia

Por defecto, Endian Firewall restringe completamente el tráfico entre las distintas zonas de red por razones de seguridad. Para permitir que los equipos ubicados en la red interna (zona verde) puedan establecer conexión con sistemas ubicados en la red de servidores (zona naranja), se configuró una regla personalizada en el firewall.

Esta regla fue definida a través de la interfaz gráfica de Endian, permitiendo establecer explícitamente la autorización del flujo de datos desde la zona verde hacia la naranja.

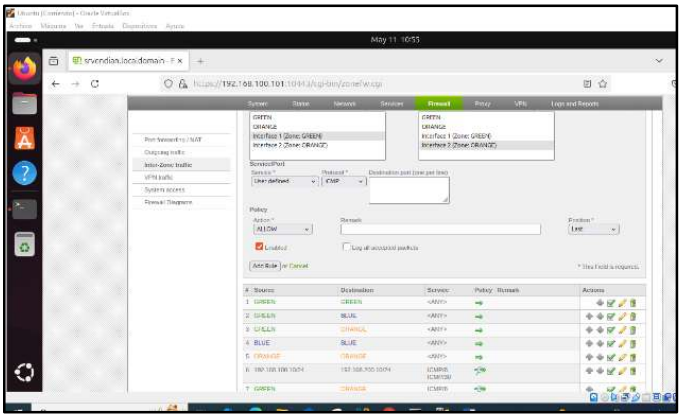


Figura 10. Proceso de creación de regla
Fuente: Autoría Propia

Una vez aplicada esta configuración, se procedió a validar la conectividad mediante herramientas de diagnóstico como ping.

La respuesta obtenida confirma la correcta implementación de la política de acceso, evidenciando que la traducción de direcciones se llevó a cabo de forma exitosa.

Figura 11. Comprobación de conectividad Desde LAN a DMZ

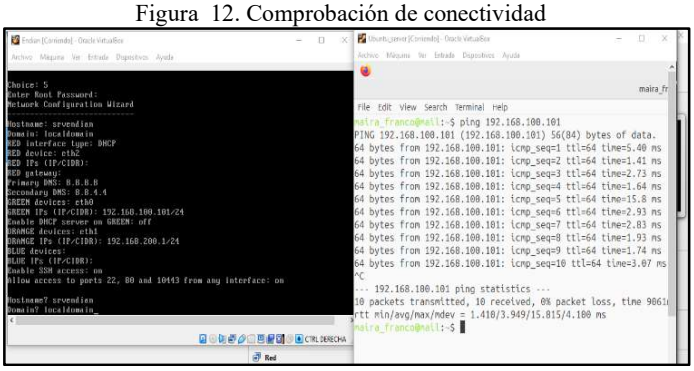
Fuente: Autoría Propia

Como parte del proceso de pruebas, también se evaluó la posibilidad de establecer comunicación desde la zona DMZ (naranja) hacia la red interna (verde).

Para permitir esta interacción, se implementó una nueva regla de firewall que habilita el tráfico saliente desde la zona naranja con destino a la verde, bajo protocolos específicos como ICMP y TCP

Posterior a la configuración, se realizaron pruebas funcionales que incluyeron comandos ping hesde un servidor ubicado en la DMZ hacia un equipo de la red interna. Los resultados confirmaron que la comunicación fue exitosa

Figura 12. Comprobación de conectividad



Fuente: Autoría Propia

3.2 DMZ HACIA WAN (PORT FORWARDING)

El Port Forwarding (reenvío de puertos) es una técnica utilizada para redirigir el tráfico entrante desde una dirección IP pública a una IP y puerto específicos dentro de una red privada. Esta funcionalidad es esencial para exponer servicios internos de manera controlada, como servidores web, FTP o SSH, sin comprometer la seguridad de toda la red.

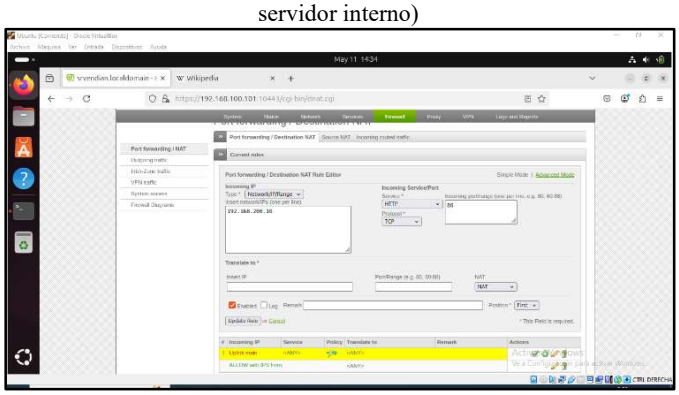
De acuerdo con esto, la zona DMZ (naranja), que aloja los servidores expuestos al exterior, necesita ser accesible desde la WAN (red pública) para que los usuarios puedan interactuar con estos servicios. Sin embargo, debido a que Endian Firewall bloquea por defecto todas las conexiones entrantes hacia la red interna, fue necesario configurar reglas de Port Forwarding para permitir el acceso controlado a estos servicios.

El proceso de configuración de NAT con Port Forwarding en Endian Firewall se realizó de la siguiente manera:

Creación de la regla de Port Forwarding: En la interfaz gráfica de Endian, se configuró una regla de NAT que redirige el tráfico HTTP (puerto 80) proveniente de la interfaz WAN hacia el servidor web ubicado en la DMZ. Los parámetros configurados fueron los siguientes:

- Interfaz de entrada: WAN
- Puerto público: 80 (HTTP)
- Destino interno: 192.168.200.1 (servidor web en la DMZ)
- Puerto destino: 80 (puerto del servidor web)

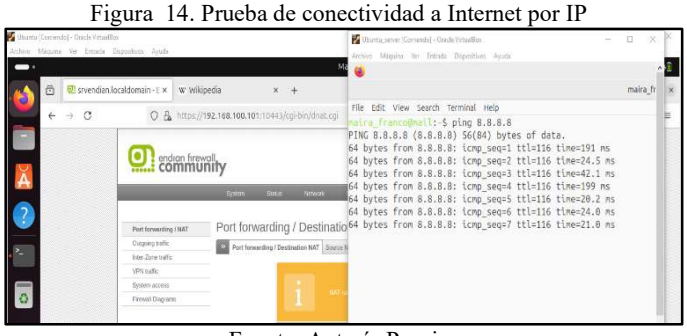
Figura 13. Configuración Port forwarding (redirigir puertos a un servidor interno)



Fuente: Autoría Propia

Este tipo de configuración permite que los usuarios externos accedan al servicio web alojado en la DMZ sin comprometer la red interna (LAN). Una vez realizada la configuración se utilizó la dirección IP 8.8.8.8 correspondiente a uno de los servidores DNS públicos de Google. La conexión fue exitosa, y se comprobó que el tráfico fue correctamente dirigido al servidor de la DMZ.

Figura 14. Prueba de conectividad a Internet por IP



Fuente: Autoría Propia

4. ARQUITECTURA DE RED

Las zonas de red son creadas con el fin de lograr tener una comunicación controlada es por eso que tenemos una zona desmilitarizada para así lograr tener ese perímetro cubierto con el fin de que nuestro de servidor cuente con la seguridad perimetral controlado y poder garantizar la disponibilidad, confidencialidad he integridad de la información, para los usuarios lo más importante es siempre contar con una data legitima y que se pueda acceder.

En primer lugar, es necesario habilitar los puertos específicos para garantizar la comunicación adecuada entre los servicios de red. En este caso, vamos a conceder acceso a los puertos 80 (HTTP) y 21 (FTP), que son fundamentales para la correcta operación de los servicios web y de transferencia de archivos en nuestra infraestructura de red.

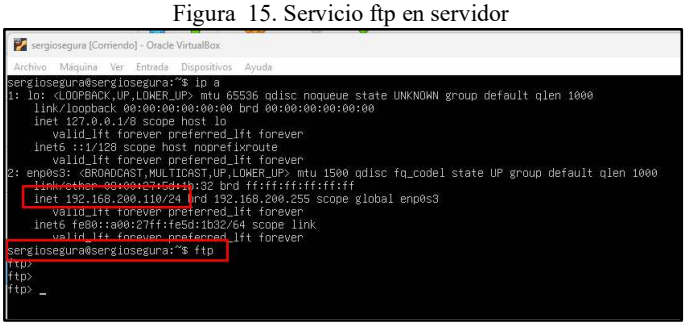
El puerto 80 se utiliza para el protocolo HTTP, esencial para la comunicación web estándar, que permite a los clientes acceder a los recursos de servidores web a través de navegadores.

El puerto 21, por su parte, se emplea para el protocolo FTP (File Transfer Protocolo), que facilita la transferencia de archivos entre sistemas en la red, permitiendo tanto la carga como la descarga de datos.

Se procede a validar los puertos del servidor en funcionamiento.

Primero, nos aseguramos de que el servicio FTP esté en funcionamiento en el servidor asignado. El puerto 21 debe estar accesible y escuchando por las solicitudes entrantes desde otras máquinas en la red. Para esto procedemos a instalar el servicio desde los repositorios oficiales, una vez descargados procedemos a instalarlos en el servidor y así lograr comunicación para saber que el servicio está funcionando correctamente en el servidor podemos realizar un telnet al localhost de la maquina con el puerto 21.

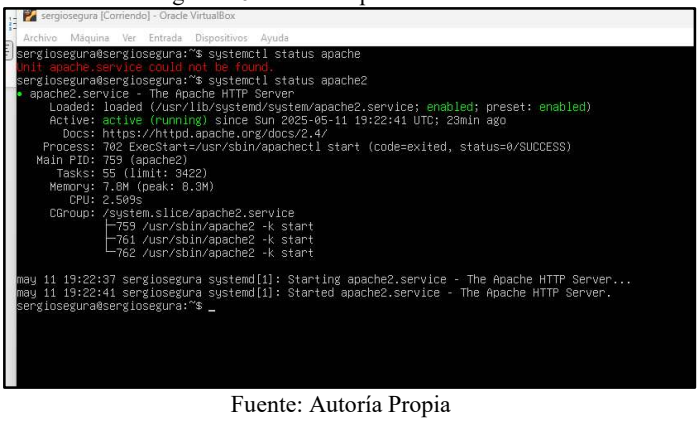
Figura 15. Servicio ftp en servidor



Fuente: Autoría Propia

De igual forma validamos que el servidor web Apache esté corriendo correctamente con el puerto 80 (HTTP) esté accesible para las conexiones entrantes. Este servicio es crucial para servir contenido web a través de los navegadores de los usuarios en la red también se debe realizar la prueba de conexión desde el mismo servidor a mirar el estatus del servicio con systemctl status apache2 y así tener la valides que el servicio se encuentra corriendo de manera correcta.

Figura 16. Servicio apache en servidor



Fuente: Autoría Propia

Tenemos el servicio instalado en el server, ahora procedemos habilitar la conexión de los servicios en la red que tenemos instalada. Se debe realizar unas políticas de comunicación entre zonas a nivel de firewall donde se ubica como origen la zona verde que es donde se encuentra la LAN del desktop y como destino tenemos la zona naranja donde se encuentra el servidor ubuntu, definimos los servicio de conexión que requerimos los cuales son el puerto 80 y el puerto 21 para así asegurar las conexiones estrictamente necesarias en el perímetro.

Además de eso debemos tener en cuenta que las políticas se validan secuencialmente el ingresa a la primera regla y si no cumple con el criterio de arriba continua con la siguiente regla y si cumplen en la primera regla ya no ingresa a la siguiente regla.

Figura 17. políticas del firewall

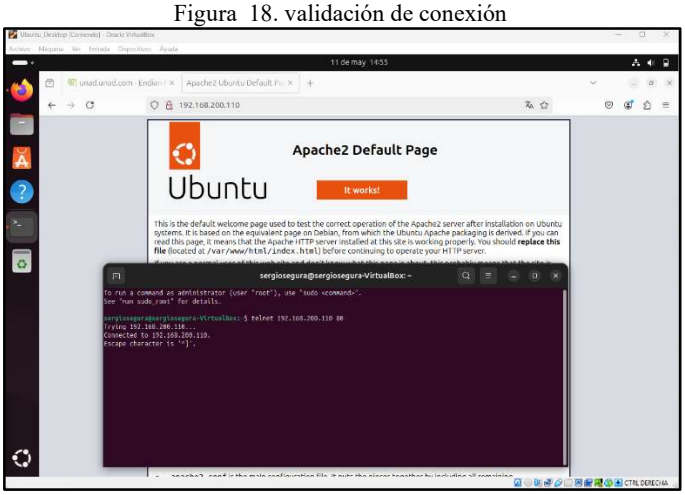
Fuente: Autoría Propia

Una vez que se han configurado las reglas necesarias, el siguiente paso es verificar la conectividad entre el desktop y el servidor.

Para ello, comenzamos validando que el puerto 80 esté correctamente habilitado y operativo para el servicio Apache. Esto asegura que el servidor web esté accesible a través de HTTP y que las solicitudes desde la red interna puedan ser procesadas adecuadamente.

Podemos observar en la siguiente figura la conexión correcta entre el equipo de escritorio y el servidor donde por medio del navegador ingresamos la direcion IP del servidor y el puerto así logrando visualizar la conexión exitosa, también podemos observar como segunda opción la conexión por medio de protocolo de conexión telnet, donde por medio de la línea de comendo de Linux se procede a realizar un telnet a la dirección Ip de destino la cual es el servidor y el puerto indicándonos que la conexión fue correcta. En caso de que no sea correcta este se queda conectando y no se obtiene respuesta y si el puerto en el servidor se encuentra en estado inactivo nos podemos dar cuenta por que indica que esta refuse.

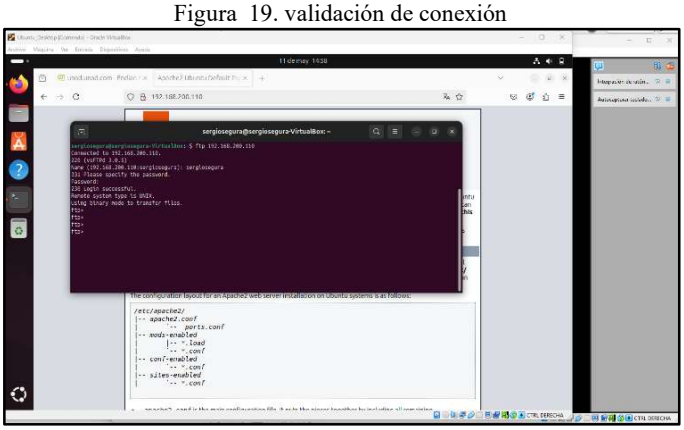
Figura 18. validación de conexión



Fuente: Autoría Propia

Procedemos a verificar el estado del puerto 21 utilizado por el servicio FTP, el cual debe estar activo en el servidor para permitir la transferencia de archivos. Al realizar la validación, confirmamos que el puerto está correctamente abierto y escuchando solicitudes entrantes, garantizando así el correcto funcionamiento del servicio FTP en el servidor

Figura 19. validación de conexión



Fuente: Autoría Propia

El ping es una herramienta en las redes informáticas ya que por medio de este podemos obtener información de conexión, pero también es una puerta para los atacantes que por medio de una gran cantidad de solicitudes puede llegar a realizar una denegación de servicio es por eso por lo que vamos a bloquear este protocolo de comunicación, es muy importante saber que el ping es una herramienta muy útil, pero se debe usar con mucha prudencia ya que al traer información puede ser usando por cualquier atacante y generar conflicto.

Vamos a realizar la política en el firewall donde vamos a poner cualquier origen y cualquier destino es como decir una regla de origen all y destino all negando como servicio el protocolo ICMP esta regla lo que indica es que si vamos a realizar un ping desde la red verde a la red naranja no se pueden realizar ping. Después de que cualquier host del segmento indicado cumpla con la política se procede a denegar.

Figura 20. política de denegación

Fuente: Autoría Propia

Una vez completadas las validaciones de conexión, los registros logs de las herramientas de seguridad proporcionan una visión clara de cómo este servicio es bloqueado de manera efectiva. Estos logs detallan de forma contundente cómo las políticas de seguridad implementadas impiden el acceso no autorizado, evidenciando las acciones de bloqueo realizadas por el sistema ante los intentos de conexión no permitidos

Como se observa en la siguiente imagen donde el registro que tiene la herramienta endian nos muestra que desde el origen 192.168.100.0/24 con destino 192.168.200.0/24 desean realizar una peticion de ping (ICMP) la regla del firewall la deniega, esta regla funciona de forma bidireccional.

Figura 21. registro de actividades

Fuente: Autoría Propia

5. FUNDAMENTOS DE NAT Y REENVÍOS DE PUERTOS

Con el objetivo de establecer una arquitectura de red segura y funcional, se definieron reglas específicas de comunicación entre zonas dentro del entorno de pruebas basado en Endian Firewall. Las reglas se diseñaron conforme a principios de segmentación de red y control de acceso por servicio, permitiendo únicamente el tráfico necesario para los servicios definidos y reduciendo la superficie de ataque.

Se definieron las siguientes reglas de acceso en el firewall para cumplir con los requisitos de comunicación:

1. Comunicación de la Zona Verde a la Zona Naranja:
   A. Permitir tráfico HTTP (puerto 80) desde la Zona Verde a la Zona Naranja
   B. Permitir tráfico FTP (puertos 21) desde la Zona Verde a la Zona Naranja

   Esta configuración permite a los usuarios internos acceder a servidores web y servicios de transferencia de archivos alojados en la Zona Naranja, sin exponer dichos recursos directamente a la red externa.

2. Comunicación de la Zona Internet a la Zona DMZ:
   A. Permitir tráfico HTTP (puerto 80) desde la Zona Roja a la Zona DM
   B. Permitir tráfico FTP (puertos 21) desde la Zona Roja a la Zona DMZ.
3. Redirección de puertos desde Zona roja a la DMZ

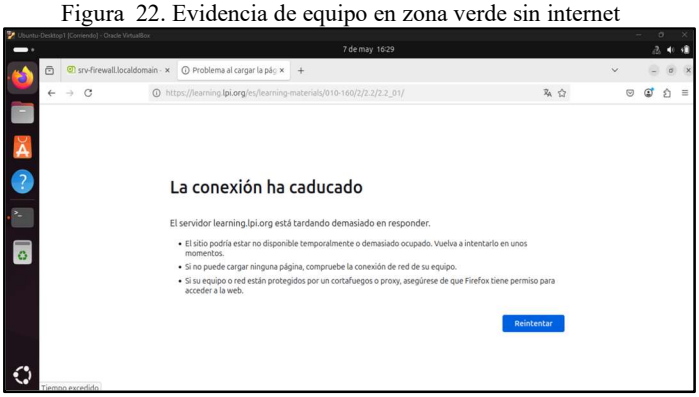
   Esta medida garantiza que solo los servicios públicos específicos sean accesibles desde el exterior, manteniendo el resto de la infraestructura aislada.

   Adicionalmente, se configuró la redirección de puertos desde la Zona Roja hacia la DMZ, a fin de dirigir solicitudes entrantes hacia los servidores correspondientes sin comprometer la estructura interna. Esta técnica permite exponer servicios seleccionados mediante port forwarding, mientras se conserva el control centralizado del tráfico entrante.

Estas configuraciones reflejan un enfoque de defensa en profundidad, permitiendo la operación de servicios públicos bajo criterios controlados, a la vez que se preserva la segmentación y se limita la exposición de las redes internas

La configuración de las reglas de acceso en Endian Firewall se realiza completamente desde su interfaz gráfica basada en web. A continuación, se describen los pasos que se deben seguir para implementar las reglas de tráfico entre zonas:

Figura 22. Evidencia de equipo en zona verde sin internet

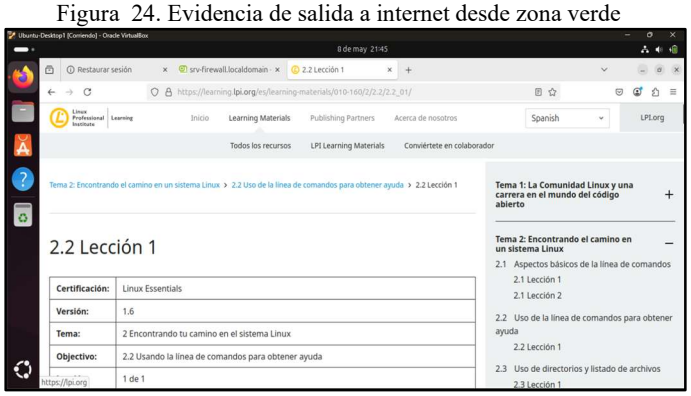


Fuente: Autoría Propia

Figura 23. Configuración salida internet en zona roja

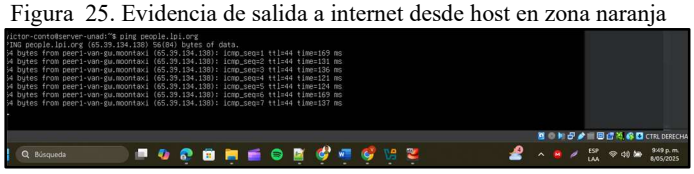
Fuente: Autoría Propia

Figura 24. Evidencia de salida a internet desde zona verde



Fuente: Autoría Propia

Figura 25. Evidencia de salida a internet desde host en zona naranja



Fuente: Autoría Propia

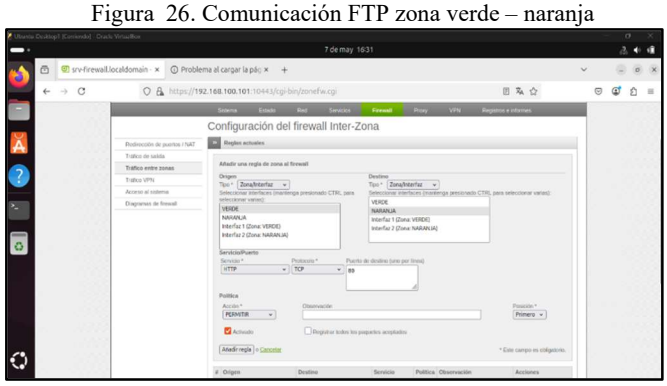
Una vez que se ha establecido con éxito la salida a Internet desde las zonas Verde (LAN) y Naranja (DMZ), es posible configurar la comunicación directa entre estas dos zonas internas, específicamente para los protocolos HTTP (puerto 80) y FTP (puerto 21). Esta etapa es fundamental cuando los usuarios en la red LAN requieren acceso a servicios internos desplegados en la DMZ, como servidores web o servicios de intercambio de archivos.

Antes de establecer reglas interzonales, es imprescindible asegurar que tanto la zona Verde como la Naranja cuentan con acceso correcto a la red externa (zona Roja - WAN). Para ello, se verifica que:

- Las reglas de salida hacia Internet desde ambas zonas estén correctamente activas.
- El firewall esté enrutando el tráfico adecuadamente mediante reglas NAT (mascaramiento).
- Se pueda hacer ping a direcciones públicas desde ambas zonas.

Este paso garantiza que los clientes y servidores en la LAN o DMZ no solo están operativos localmente, sino que también tienen visibilidad y funcionalidad hacia el exterior, lo cual es vital en escenarios híbridos o actualizaciones remotas de sistemas.

Figura 26. Comunicación FTP zona verde – naranja

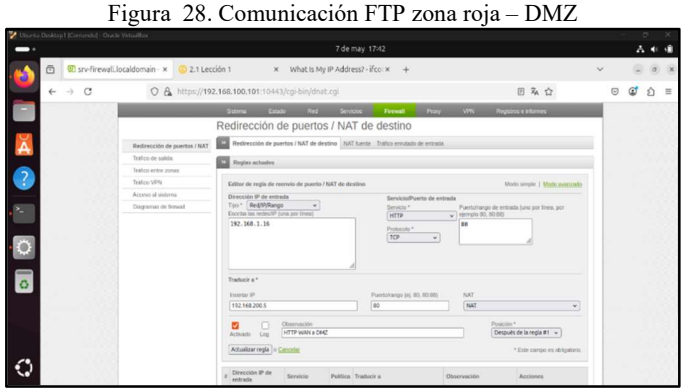


Fuente: Autoría Propia

Figura 27. Comunicación HTTP zona roja – DMZ

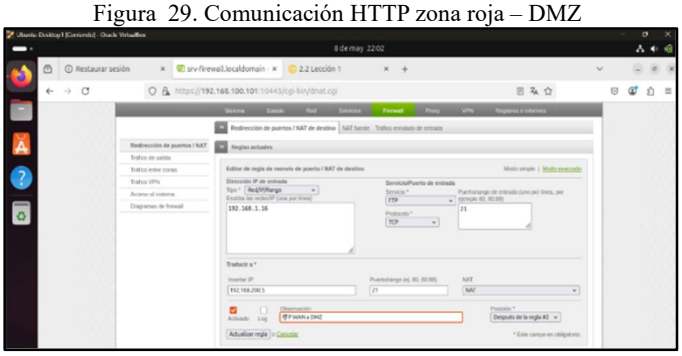
Fuente: Autoría Propia

Figura 28. Comunicación FTP zona roja – DMZ



Fuente: Autoría Propia

Figura 29. Comunicación HTTP zona roja – DMZ



Fuente: Autoría Propia

La redirección de puertos HTTP y FTP desde la zona roja (Internet) a la DMZ (zona desmilitarizada) en Endian permite exponer servicios públicos, como un servidor web (HTTP) o un servidor de archivos (FTP), a usuarios externos de forma controlada.

Con esta configuración, el firewall intercepta las solicitudes que llegan desde Internet a ciertos puertos (por ejemplo, 80 para HTTP y 21 para FTP) y las redirige hacia servidores ubicados en la DMZ, una red intermedia separada de la red interna para proteger los sistemas sensibles

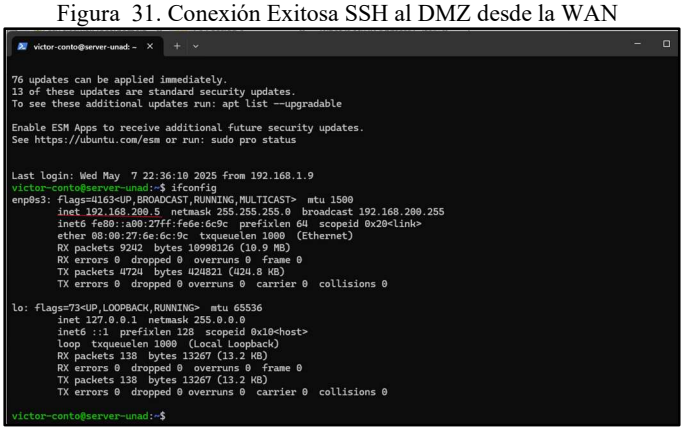
5.1 VALIDACIÓN Y PRUEBAS

Se realizaron pruebas desde navegadores web y clientes FTP para verificar la funcionalidad. Para ello, se implementa el servidor Apache en un equipo ubicado en la zona DMZ como prueba del servicio HTTP, y adicionalmente se activa un servidor FTP

Figura 30. Conexión SSH al DMZ desde la WAN

Fuente: Autoría Propia

Figura 31. Conexión Exitosa SSH al DMZ desde la WAN

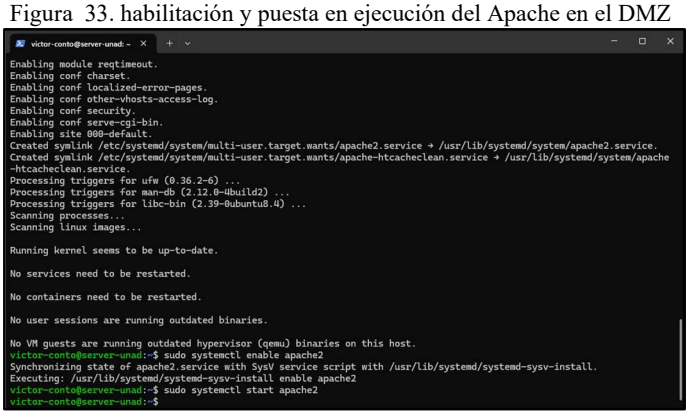


Fuente: Autoría Propia

Figura 32. Instalación exitosa de Apache en el DMZ desde la WAN

Fuente: Autoría Propia

Figura 33. habilitación y puesta en ejecución del Apache en el DMZ



Fuente: Autoría Propia

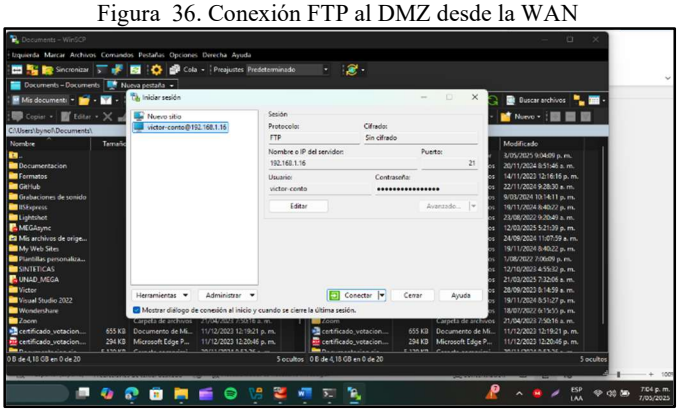
Figura 34. Instalación de servicio FTP en el DMZ

Fuente: Autoría Propia

Figura 35. Conexión HTTP al DMZ desde la WAN

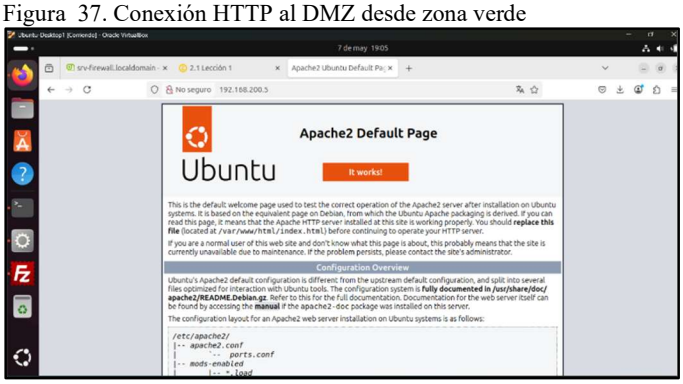
Fuente: Autoría Propia

Figura 36. Conexión FTP al DMZ desde la WAN



Fuente: Autoría Propia

Figura 37. Conexión HTTP al DMZ desde zona verde



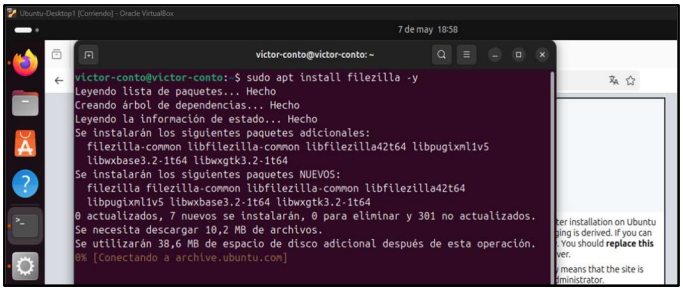
Fuente: Autoría Propia

La instalación del cliente FileZilla en un equipo con Ubuntu Desktop ubicado en la zona Verde (red LAN interna) representa una herramienta clave para llevar a cabo pruebas funcionales y diagnósticas en la implementación de reglas de acceso FTP entre zonas en el entorno de Endian Firewall.

El protocolo FTP (File Transfer Protocol), utilizado para la transferencia de archivos entre sistemas en red, requiere una conexión bidireccional con gestión de sesiones y puertos, lo cual puede verse afectado por políticas de firewall o configuraciones NAT.

Además, FileZilla ofrece una interfaz amigable y multiplataforma, ideal para usuarios técnicos y administradores de red que requieren una herramienta eficiente para realizar pruebas en entornos controlados. En este contexto, su instalación en un host Ubuntu Desktop dentro de la zona Verde resulta esencial para ejecutar pruebas de conectividad seguras y precisas, validando que el flujo FTP se comporta según lo definido por las reglas interzonales del firewall.

Figura 38. Instalación de Client Filezilla en host desktop en zona verde

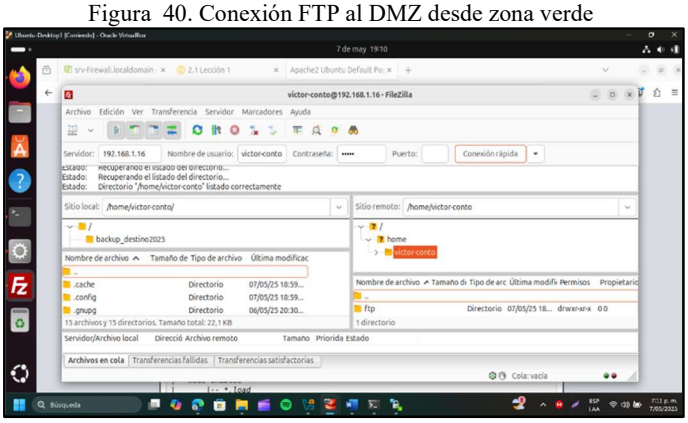


Fuente: Autoría Propia

Figura 39. Verificación de aplicación instalada

Fuente: Autoría Propia

Figura 40. Conexión FTP al DMZ desde zona verde



Fuente: Autoría Propia

5.2 RESULTADOS Y OBSERVACIONES

Con el propósito de evaluar la efectividad de las reglas de acceso configuradas en el entorno del Endian Firewall, se realizaron pruebas controladas orientadas a validar el enrutamiento, la aplicación de reglas NAT, y los mecanismos de seguridad entre las distintas zonas definidas (Verde, DMZ y WAN). Las observaciones descritas a continuación reflejan el comportamiento del sistema frente a diferentes escenarios de tráfico y modificación de reglas:

- El tráfico fue correctamente direccionado según las reglas configuradas.
- Se confirmó la creación automática de reglas NAT para tráfico saliente desde la zona Verde y DMZ hacia Internet.

- Se verificó que el acceso desde la WAN a la DMZ requiere reglas explícitas, lo que refuerza la seguridad por defecto

El acceso de la zona Verde hacia la Naranja debe estar cuidadosamente controlado. A diferencia del tráfico saliente a Internet, el tráfico entre zonas internas puede ser más susceptible a brechas si no se segmenta adecuadamente. Por este motivo, se recomienda:

- Limitar el acceso solo a los puertos y servicios necesarios (HTTP y FTP).
- Definir rangos de IP específicos como origen si se desea restringir aún más el acceso.
- Utilizar autenticación en el servidor FTP y evitar FTP anónimo.
- Activar monitoreo de tráfico con herramientas IDS/IPS si están disponibles.

6. CONCLUSIONES

La segmentación de red junto con reglas de acceso bien definidas permite controlar eficazmente el tráfico entre zonas, minimizando riesgos de seguridad. El acceso a servicios HTTP y FTP puede ser gestionado con precisión, asegurando la continuidad operativa sin comprometer la infraestructura. La validación mediante pruebas funcionales y técnicas demostró la correcta aplicación de las políticas definidas

La implementación de reglas NAT es indispensable para mantener la funcionalidad y seguridad de una red. Mientras que el NAT dinámico permite a los equipos internos acceder a Internet, el uso de port forwarding facilita la exposición de servicios controlados desde la DMZ. Ambas técnicas fueron probadas satisfactoriamente, validando tanto la conectividad como la configuración de reglas necesarias para una topología de red segura y eficiente.

Seguridad de la información es uh concepto clave para la informática, sabemos que en la actualidad los ataques a la infraestructura tecnología crece cada día más es por eso que existen los dispositivos de seguridad ya que la seguridad se basa en capas en esta oportunidad la seguridad perimetral es muy importante y el firewall es muy importante a la hora de concluir este tema y es porque el es que indica quien se conecta a los servicios expuestos tanto en origen como en destino.

La implementación de Endian Firewall facilita una administración eficiente de las políticas de acceso interzonales, fortaleciendo la postura de seguridad mediante la segmentación de la red y el control granular de protocolos. Los resultados obtenidos a partir de las pruebas confirman la efectividad de las reglas establecidas tanto en el tráfico interno como en el control del acceso externo. Asimismo, se resalta la relevancia de mantener auditorías periódicas sobre la configuración del sistema y de aplicar principios de seguridad por defecto, especialmente en zonas expuestas como la DMZ.

7. REFERENCIAS

[1] Endian Team. (s.f.). Endian Firewall Community (Versión 3.3.2) [Software de código abierto]. SourceForge. https://sourceforge.net/projects/efw/

[2] Ubuntu Documentation, "Ubuntu 20.04 Help", https://help.ubuntu.com/20.04/ubuntu-help/index.html.

[3] Oracle Corporation, "VirtualBox Documentation", https://www.virtualbox.org/wiki/Documentation.

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

[5] Endian Documentation, "The Zones – Endian UTM 3.2", http://docs.endian.com/3.2/utm/first.html#the-zones.

[6] Endian Documentation, "Firewall – In this page you find", https://docs.endian.com/3.2/utm/firewall.html#in-this-page-you-find.

[7] Endian Documentation, "Firewall – Inter-Zone Traffic", https://docs.endian.com/3.2/utm/firewall.html#inter-zone-traffic.

[8] Endian Documentation, "Firewall – Common Configuration Items", https://docs.endian.com/3.2/utm/firewall.html#common-configuration-items.

[9] Ubuntu, "Ubuntu Server Documentation", https://documentation.ubuntu.com/server/.

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