GUÍA COMPLETA PARA CONFIGURAR ENDIAN EN VIRTUALBOX: SEGURIDAD Y CONTROL DEL TRÁFICO EN RED

Hugo Bejarano Acosta
hbejaranoa@unadvirtual.edu.co
Mauricio Andrés Escobar López
maescobarlo@unadvirtual.edu.co
Julián Andrés Segura Guerra
jaseguragu@unadvirtual.edu.co
Clara Esther Martinez Abaúnza
cemartinezab@unadvirtual.edu.co
Fredy Jacob Gomez Fandiño
fjgomezf@unadvirtual.edu.co

RESUMEN: *El presente artículo detalla la implementación y configuración del firewall Endian sobre una máquina virtual en VirtualBox, estructurado en cinco ejes temáticos. En primer lugar, se establece una arquitectura de red segmentada mediante zonas verde (LAN), roja (WAN) y naranja (DMZ), orientada a fortalecer la seguridad perimetral y optimizar la comunicación interzonal. En segundo lugar, se configuran reglas SNAT y DNAT para permitir la publicación controlada de servicios internos, como servidores web, sin comprometer la integridad de la red LAN. La tercera temática aborda la activación de servicios HTTP y FTP desde la DMZ hacia otras zonas, junto con el bloqueo del protocolo ICMP como medida preventiva. Posteriormente, se definen reglas de acceso que filtran el tráfico en función de parámetros como dirección IP, puerto, interfaz y estado de conexión. Finalmente, se implementa un proxy HTTP no transparente con autenticación, permitiendo el control del tráfico web*.

PALABRAS CLAVE: DMZ (Zona Desmilitarizada), NAT (Network Address Translation), SNAT (Source NAT), DNAT (Destination NAT), ICMP (Internet Control Message Protocol).

1 INTRODUCCIÓN

Desde los años setenta aproximadamente, durante el auge del internet y el crecimiento incansable del desarrollo tecnológico, se ha visto la necesidad de poder proteger y brindar seguridad a las comunicaciones y a la información. En un entorno digital cada vez más expuesto a amenazas y vulnerabilidades, se hace necesario hallar y contar con soluciones eficientes de seguridad para las redes y dispositivos que se conectan a ellas.

Endian Firewall, una distribución de código abierto basada en Linux, ofrece una solución integral de seguridad unificada (UTM), que permite proteger, controlar y gestionar el tráfico en redes corporativas o domésticas. En el desarrollo de cada una de las temáticas aquí trabajadas, se dan pautas que pueden ayudar a instalar y configurar Endian en una máquina virtual, utilizando VirtualBox, proporcionando un entorno seguro, flexible y fácil de administrar.

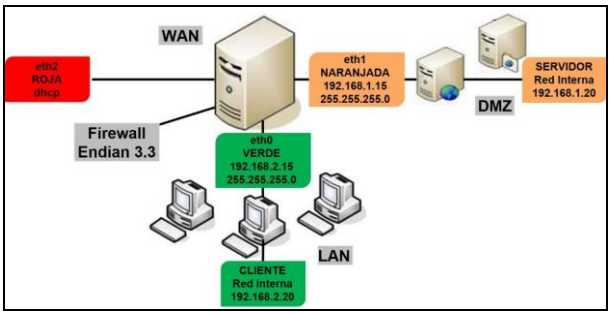
De igual forma, a lo largo del desarrollo de estas actividades, se abordará el paso a paso desde la creación de la máquina virtual, hasta la configuración de las interfaces de red, las reglas de firewall, los servicios de filtrado y las herramientas de monitoreo. Todo esto, con el objetivo de brindar el conocimiento necesario para implementar una solución de seguridad, mejorar la visibilidad del tráfico en la red y, asegurar la integridad de los sistemas y diferentes datos, propios de la comunicación y de los dispositivos conectados.

2 DESARROLLO DE CONTENIDOS

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

Diseño del diagrama de red que se utilizaremos para la implementación y configuración de las zonas verde, naranja y roja en Endian Firewall 3.3.

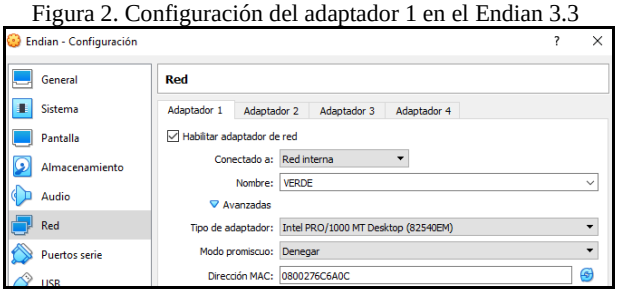
Figura 1. Diagrama de red en Endian 3.3



Fuente: Autoría Propia

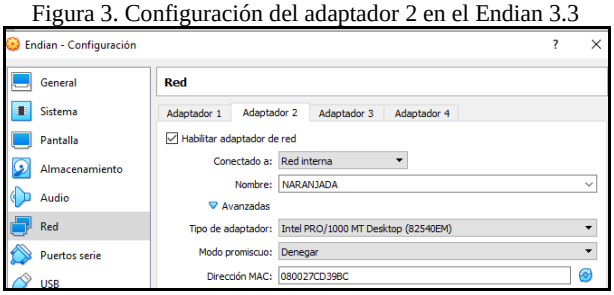
Descarga del Endian 3.3, desde su página oficial, https://sourceforge.net/projects/efw/. Y configuración del programa y los sistemas operativos (Ubuntu Desktop Cliente, Ubuntu Server Servidor) a utilizar para el desarrollo de la actividad. Iniciamos configurando las tarjetas de red. Adaptador 1, red interna y la llamo la red VERDE. Adaptador 2, red interna y la llamo la red NARANJADA. Adaptador 3, es el internet, lo dejo en NAT, vendría siendo la red ROJA.

Figura 2. Configuración del adaptador 1 en el Endian 3.3



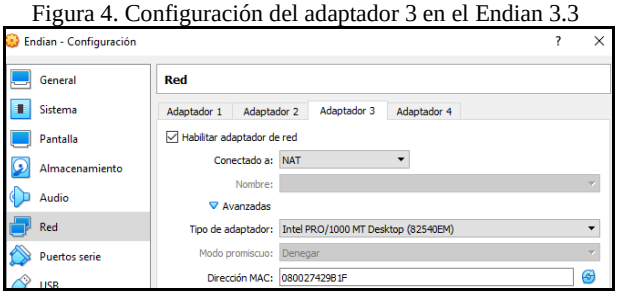
Fuente: Autoría Propia

Figura 3. Configuración del adaptador 2 en el Endian 3.3



Fuente: Autoría Propia

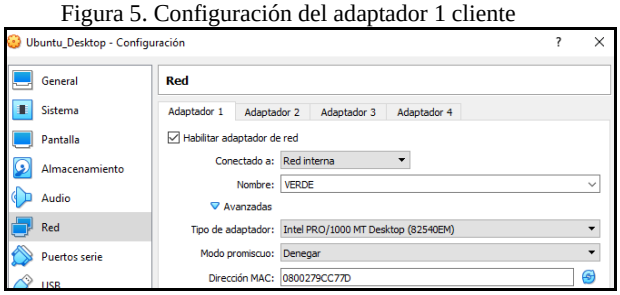
Figura 4. Configuración del adaptador 3 en el Endian 3.3



Fuente: Autoría Propia

Configuración de la tarjeta de red en Ubuntu Desktop (Cliente). Adaptador 1, red interna, va a utilizar la red VERDE.

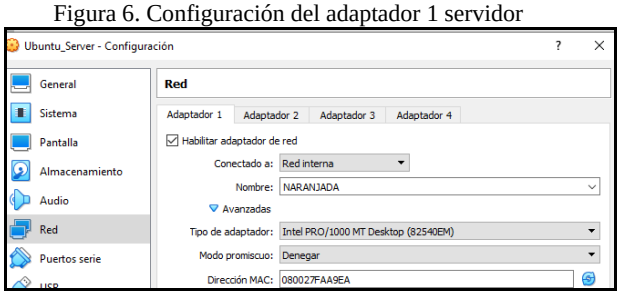
Figura 5. Configuración del adaptador 1 cliente



Fuente: Autoría Propia

Configuración de la tarjeta de red en Ubuntu Server (Servidor). Adaptador 1, red interna, va a utilizar la red NARANJADA.

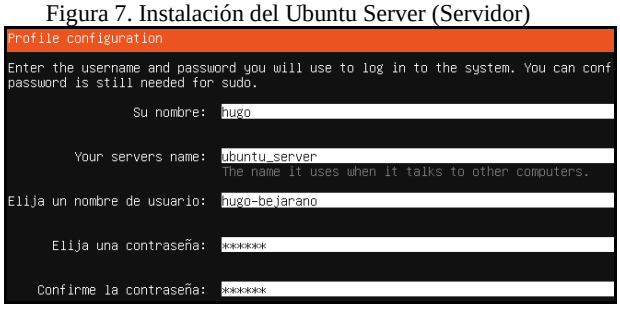
Figura 6. Configuración del adaptador 1 servidor



Fuente: Autoría Propia

Instalación de los sistemas operativos Ubuntu Server (Servidor), Ubuntu Desktop (Cliente) y Endian Firewall 3.3.

Figura 7. Instalación del Ubuntu Server (Servidor)



Fuente: Autoría Propia

Figura 8. Instalación del Ubuntu Desktop (Cliente)

Fuente: Autoría Propia

Figura 9. Instalación del Endian Firewall 3.3

Fuente: Autoría Propia

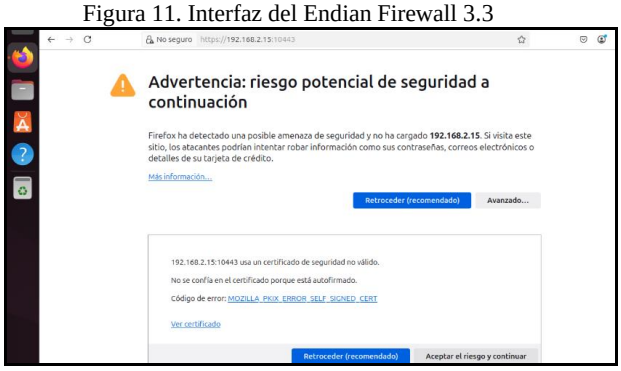
Al culminar la instalación de Endian 3.3, nos presenta la siguiente interfaz, donde se puede observar, que ya están activas la zona VERDE y la zona ROJA, zonas que quedaron configuradas, durante el proceso de instalación de cada sistema operativo.

Figura 10. Interfaz del Endian Firewall 3.3

Fuente: Autoría Propia

Complementación de la configuración del Endian 3.3, para lo cual nos dirigimos al Ubuntu Desktop (Cliente), se abre navegador y se escribe la url https://192.168.2.15 o simplemente la dirección IP 192.168.2.15. Aparece un mensaje de alerta por que el sitio no es seguro, clic en Avanzado y, en Aceptar el riesgo y continuar.

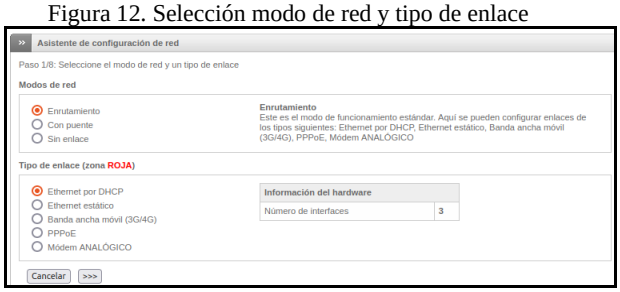
Figura 11. Interfaz del Endian Firewall 3.3



Fuente: Autoría Propia

Recibimos una bienvenida a Endian Firewall. Seleccionamos un idioma y una ubicación para la instalación y aceptamos la licencia de uso del programa. Luego de lo anterior, se presenta la siguiente interfaz, la cual nos brinda cierta información, primero, que debo realizar 8 pasos para la configuración. Me dice que el internet, modo de red es por enrutamiento, que el tipo de enlace es a través de ethernet por DHCP y que tengo 3 tarjetas de red a configurar en el servidor de Endian. Clic en las flechas para continuar.

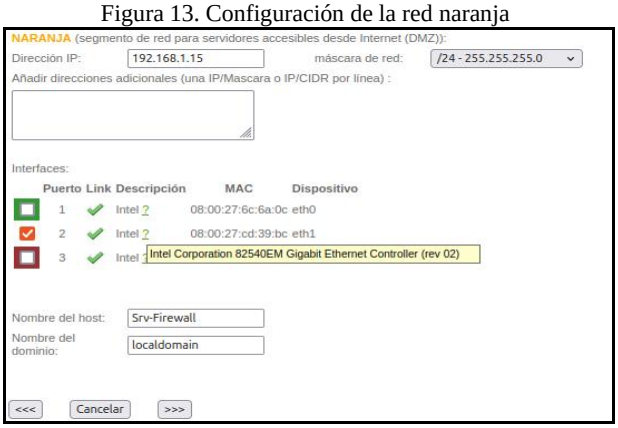
Figura 12. Selección modo de red y tipo de enlace



Fuente: Autoría Propia

Nos encontramos en la interfaz más importante, nos muestra que la red VERDE y ROJA, están configuradas. Que debemos configurar la red NARANJA, digitamos la IP 192.168.1.15, damos clic en el puerto link descripción 2. Asignamos nombre al servidor y al dominio. Clic en las flechas para continuar.

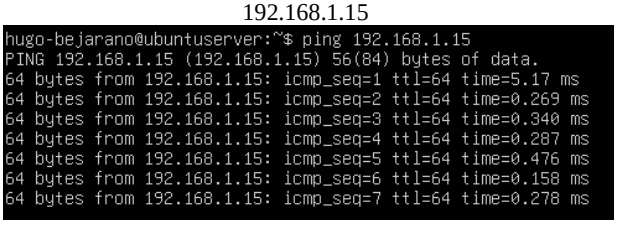
Figura 13. Configuración de la red naranja



Fuente: Autoría Propia

Dejamos todo por defecto en los pasos 4 al 7. La interfaz final; el paso 8 de 8, nos dice que se ha guardado la configuración, que puede tardar unos segundos, para que disfrutemos de nuestras configuraciones. Finalmente, podemos hacer la comprobación de la instalación y configuraciones efectivas, haciendo un ping desde nuestro Ubuntu Server (Servidor), a la dirección IP 192.168.1.15, para verificar si hay conexión, evidenciando que hay respuesta de manera correcta.

Figura 14. Comprobación efectiva pin desde servidor a IP 192.168.1.15



Fuente: Autoría Propia

O ingresando desde nuestro Ubuntu Desktop (Cliente) a una página de internet.

Figura 15. Comprobación efectiva ingreso a página de internet

Fuente: Autoría Propia

2.2 TEMÁTICA 2: CONFIGURACIÓN NAT E IMPLEMENTACIÓN DE REGLAS EN ENDIAN FIREWALL PARA CONECTIVIDAD SEGURA ENTRE LAN, DMZ Y WAN

Para la implementación de las reglas NAT, se utilizó una instancia de Endian Firewall 3.3 configurada en VirtualBox con tres interfaces de red: eth0 (VERDE/LAN: 192.168.2.0/24), eth1 (NARANJA/DMZ: 192.168.1.0/24) y eth2 (ROJA/WAN: NAT hacia Internet), como se detalla en la Sección 2.1. Esta arquitectura permitió aplicar reglas de traducción de direcciones (SNAT) para garantizar conectividad segura entre las zonas.

La validación incluyó pruebas de conectividad desde la LAN (Ubuntu Desktop: 192.168.2.16) mediante ping a 8.8.8.8 y resolución DNS (google.com), así como acceso HTTP desde el servidor en la DMZ (Ubuntu Server: 192.168.1.20) a servicios externos. Se confirmó que las políticas del firewall permitían el tráfico NAT sin restricciones indebidas, cumpliendo con los objetivos de conectividad segura.

Esta sección detalla la implementación de reglas NAT en Endian Firewall 3.3 para permitir comunicación segura entre la LAN (192.168.2.0/24), DMZ (192.168.1.0/24) y WAN (Internet). Se validó mediante pruebas de conectividad y reenvío de puertos.

2.2.1 CONFIGURACIÓN INICIAL

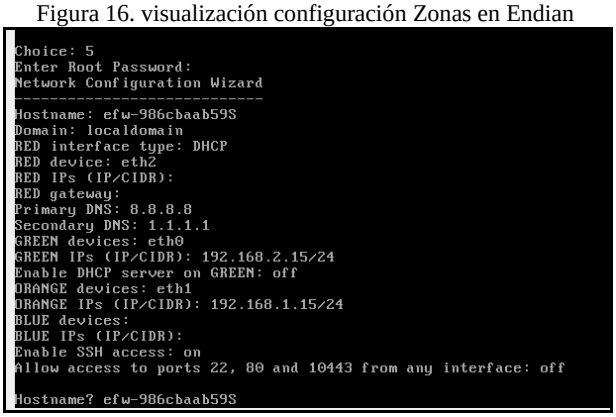
Como se muestra en el Diagrama de red en Endian 3.3 (ver **Fig. 1**), el firewall Endian actúa como puente entre las zonas, con interfaces eth0 (LAN: 192.168.2.0/24, Zona Verde), eth1 (DMZ: 192.168.1.0/24, Zona Naranja) y eth2 (WAN: DHCP, Zona Roja).

Después de realizar la descargar e instalación de firewall Endian 3.3 (ver Figura 10), se procede a configurar las zonas en el servidor firewall Endian 3.3 en el cual se implementó las tres interfaces de red, cada una asociada a una zona específica:

- eth0 (VERDE/LAN): Configurada con IP estática 192.168.2.15/24, conectada a la red interna donde reside el cliente Ubuntu Desktop (192.168.2.16).
- eth1 (NARANJA/DMZ): IP estática 192.168.1.15/24, destinada al servidor Ubuntu Server (192.168.1.16) que aloja servicios expuestos.
- eth2 (ROJA/WAN): Configurada con DHCP (IP: 10.0.2.15), proporcionando acceso a Internet a través del NAT de VirtualBox.

Esta disposición permitió aislar el tráfico y aplicar políticas de seguridad diferenciadas por zona.

Figura 16. visualización configuración Zonas en Endian

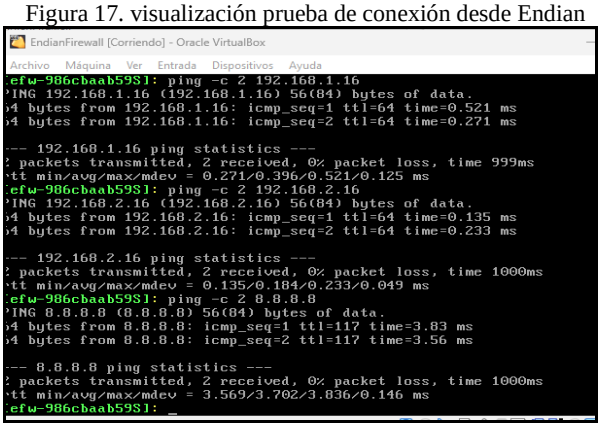


Fuente: Autoría Propia

2.2.2 VERIFICACIÓN DE CONECTIVIDAD BÁSICA

Como paso preliminar a la configuración NAT, se verificó la conectividad del firewall mediante ping a la LAN (192.168.2.16 - Zona Verde), ping a la DMZ (192.168.1.20 - Zona Naranja), y ping a 8.8.8.8 (WAN), obteniendo respuesta exitosa en todos los casos y validando así la correcta configuración de las interfaces y rutas básicas.

Figura 17. visualización prueba de conexión desde Endian



Fuente: Autoría Propia

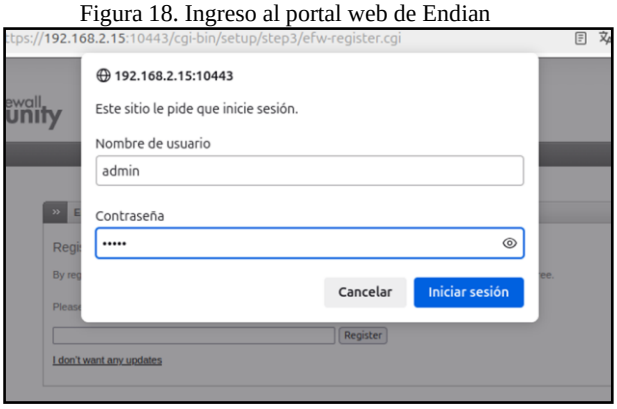
2.2.3 CONFIGURACIÓN DE REGLAS NAT

Para permitir el acceso a Internet desde la red local, se realizó la siguiente configuración mediante la interfaz web de administración del Endian Firewall:

Desde el Ubuntu Desktop (192.168.2.20), se ingresó al portal web del firewall mediante, https://192.168.2.15:10443

Utilizando las credenciales de administrador, en este caso para el usuario “admin” y la contraseña que se cambio por “12345678”

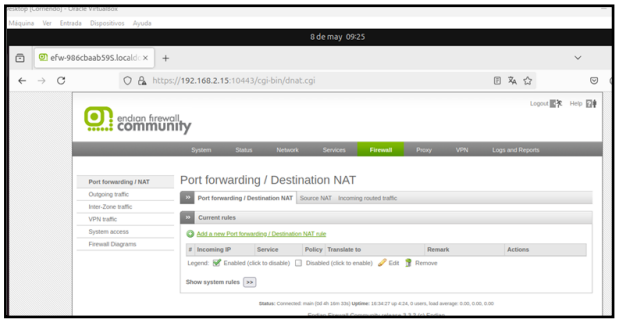
Figura 18. Ingreso al portal web de Endian



Fuente: Autoría Propia

Desde el panel web de administración del Endian Firewall, se navega al módulo NAT seleccionando Firewall > NAT > Source NAT (SNAT), donde se configura una nueva regla con los parámetros: Source Type: Network/IP (red 192.168.2.0/24 - VERDE/LAN), Destination Type: Zone/VPN/Uplink (interfaz Uplink main - RED), NAT Action: Auto (Masquerading), Position: First, y Remark: "NAT para tráfico LAN a Internet", finalizando con la creación y aplicación de la regla mediante los botones Add a new source NAT rule → Create Rule → Apply.

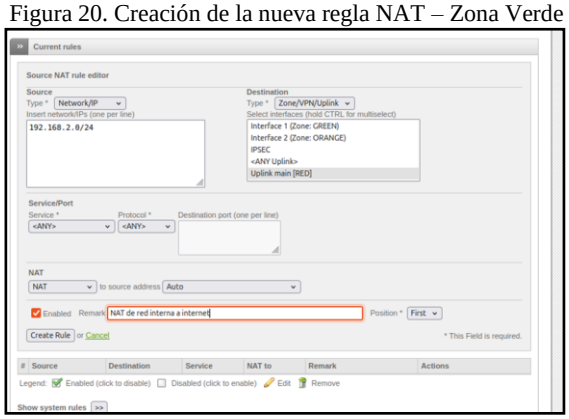
Figura 19. Ingreso al módulo firewall para configuración NAT



Fuente: Autoría Propia

Se procede configurar y crear la regla para la zona Verde (LAN) dentro del formulario que se abre en la opción de crear nueva regla en la opción “**Add a new source NAT**”.

Figura 20. Creación de la nueva regla NAT – Zona Verde



Fuente: Autoría Propia

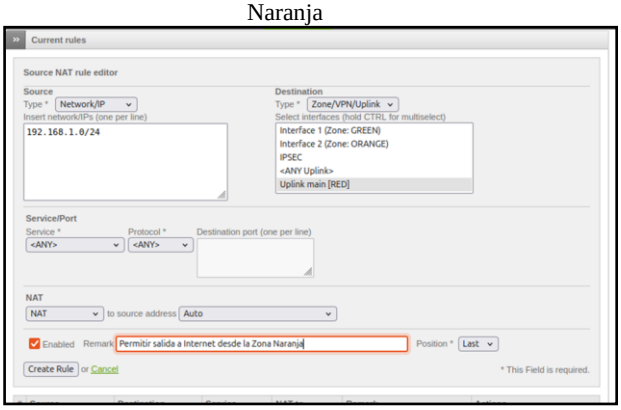
Luego de aplicar la regla nos muestra la regla ya activa dentro del panel de la opción de Source NAT, en donde podemos observar la regla ya creada y configurada.

Figura 21. Verificación de la regla creada y activada

Fuente: Autoría Propia

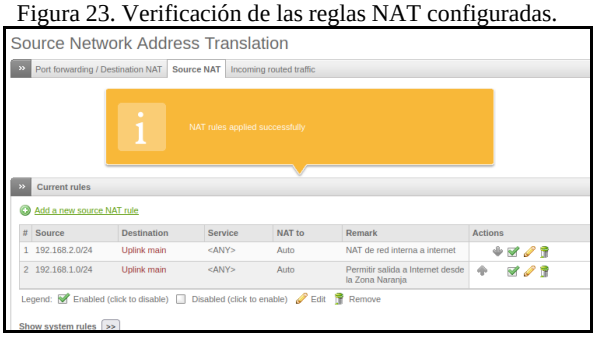
Luego dentro de la misma interfaz Source NAT, se implementó una regla adicional para la DMZ estableciendo como parámetros: campo Source con Network/IP: 192.168.1.0/24 (correspondiente a la zona NARANJA/DMZ), Destination en Uplink main (RED), selección de Auto (Masquerading) en NAT Action, posición Last en la tabla de reglas para mantener la prioridad del tráfico LAN, y el comentario "NAT para tráfico DMZ a Internet" en Remark, ejecutando posteriormente los botones Add a new source NAT rule → Create Rule → Apply para activar la configuración.

Figura 22. Creación de la nueva regla NAT – Zona Naranja



Fuente: Autoría Propia

Figura 23. Verificación de las reglas NAT configuradas.



Fuente: Autoría Propia

De igual forma que en el caso de la regla aplicada en la Zona Verde, al finalizar la configuración, se puede observar que la nueva regla se encuentra activa dentro del panel de la opción Source NAT, donde es posible visualizar todas las reglas creadas y configuradas

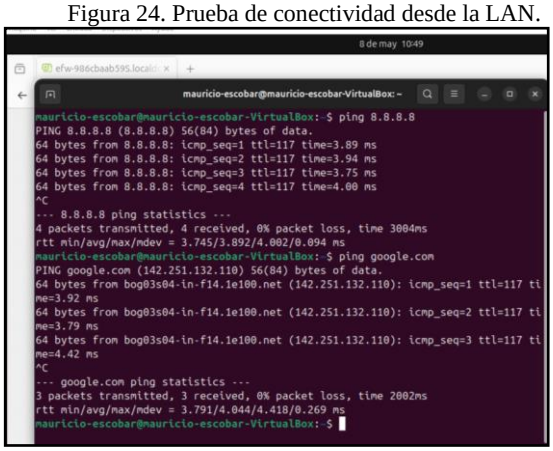
Se debe tener en cuenta que la correcta priorización de las reglas NAT es fundamental, donde la regla LAN (posición First) tiene mayor precedencia que la DMZ (posición Last); el mecanismo de Masquerading automático emplea la dirección IP pública asignada dinámicamente a la interfaz WAN (eth2), y todos los cambios de configuración requieren confirmación mediante el botón Apply para su activación permanente en el firewall.

2.2.4 RESULTADOS Y VALIDACIÓN

Con el objetivo de verificar la correcta implementación de las reglas NAT y la política de seguridad en el entorno de red configurado con Endian Firewall 3.3, se llevaron a cabo diversas pruebas de conectividad y acceso entre las zonas LAN, DMZ y WAN. Estas pruebas permitieron evaluar el cumplimiento de los objetivos establecidos en cuanto a conectividad segura, aislamiento de zonas y funcionalidad del reenvío de puertos.

Prueba de conectividad desde la LAN hacia Internet: Se realizaron pruebas desde el equipo Ubuntu Desktop (192.168.2.16), ejecutando comandos ping hacia la dirección IP pública 8.8.8.8 y pruebas de resolución de nombres DNS hacia google.com, confirmando exitosamente la salida del tráfico a través del firewall.

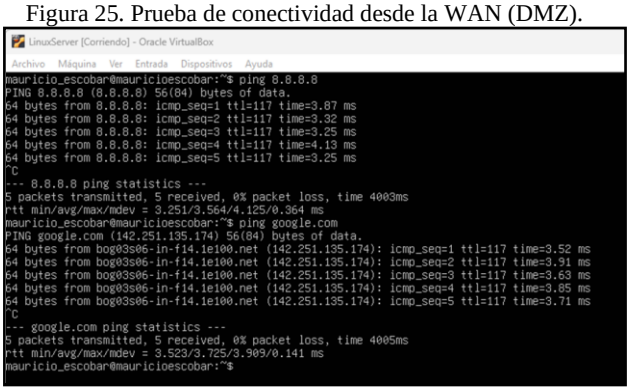
Figura 24. Prueba de conectividad desde la LAN.



Fuente: Autoría Propia

Prueba de conectividad desde la DMZ hacia Internet: Desde el servidor Ubuntu ubicado en la zona Naranja (DMZ), se ejecutaron pruebas de conectividad mediante comandos ping a la dirección IP 8.8.8.8 y al dominio google.com, confirmando tanto el acceso a Internet como la correcta resolución de nombres DNS a través del firewall.

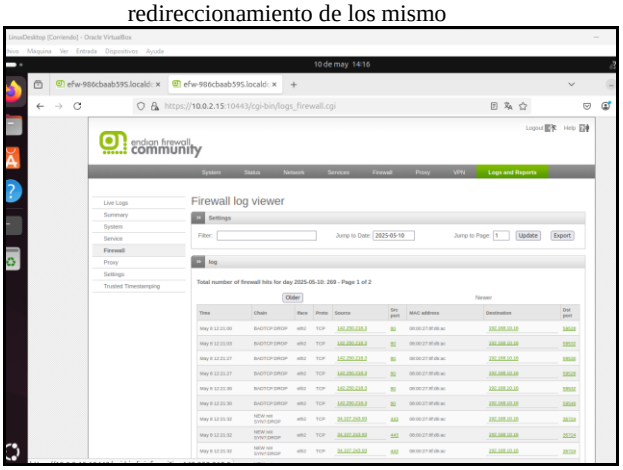
Figura 25. Prueba de conectividad desde la WAN (DMZ).



Fuente: Autoría Propia

Pruebas de NAT y redirección de puertos (DNAT): Desde una red externa simulada en VirtualBox, se realizaron accesos al servidor web ubicado en la zona DMZ mediante la dirección IP pública asignada a la interfaz WAN del firewall (10.0.2.15). Las solicitudes fueron redirigidas correctamente hacia el servidor interno, validando la correcta implementación de las reglas de DNAT y la disponibilidad del servicio desde el exterior permitiendo el tráfico por los puertos en este caso validando el puerto 80 y 443 desde el servidor DMZ (192.168.1.16).

Figura 25. Validación de trafico por los puertos y redireccionamiento de los mismo



Fuente: Autoría Propia

La configuración de Endian Firewall con las reglas de NAT y el enmascaramiento de direcciones ha logrado establecer una red segura y funcional entre las zonas LAN, DMZ y WAN. Se han implementado correctamente políticas de filtrado de tráfico que permiten el acceso controlado a los servicios internos y públicos, asegurando una segmentación adecuada y protección frente a accesos no autorizados.

La configuración de DNAT ha garantizado que los servicios externos, como el servidor web en la DMZ, sean accesibles de manera segura desde la WAN, mientras que el SNAT ha permitido a los dispositivos en la LAN acceder a Internet sin exponer sus direcciones internas.

Las pruebas de conectividad realizadas confirmaron que la red opera de acuerdo con las expectativas, validando que los servicios sean accesibles según las reglas definidas, a la vez que se mantienen los controles de seguridad. En general, este enfoque de configuración permite una administración eficiente de la red y refuerza las políticas de seguridad perimetral en la infraestructura de red.

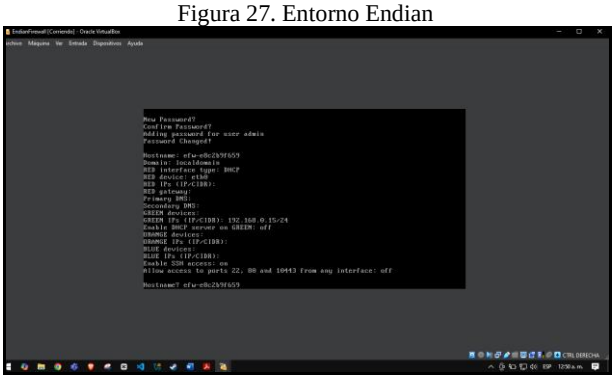
2.3 TEMÁTICA 3: PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED.

Para la implementación de esta temática, se utilizó una instancia de Endian Firewall 3.3 configurada en VirtualBox, empleando tres interfaces de red: eth0 (VERDE/LAN: 192.168.2.0/24), eth1 (NARANJA/DMZ: 192.168.1.0/24) y eth2 (ROJA/WAN: NAT hacia Internet). El objetivo principal fue habilitar servicios específicos (HTTP y FTP) para ser accedidos desde otras zonas, y simultáneamente aplicar políticas que restrinjan otros tipos de tráfico, como el ICMP, para aumentar la seguridad entre zonas.

Figura 26. Entorno Ubuntu

Fuente: Autoría Propia

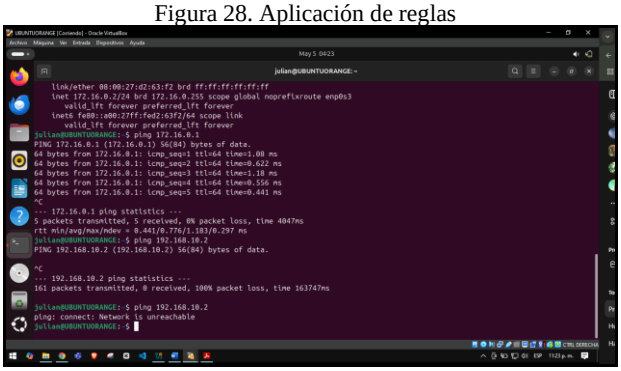
Figura 27. Entorno Endian



Fuente: Autoría Propia

La validación incluyó pruebas de acceso desde la LAN a servicios ubicados en la DMZ (HTTP y FTP), así como la comprobación del bloqueo de paquetes ICMP mediante comandos ping. Esto aseguró que solo los servicios permitidos estuvieran accesibles y que se respetaran las restricciones establecidas por las reglas del firewall.

Figura 28. Aplicación de reglas



Fuente: Autoría Propia

2.3.1 CONFIGURACIÓN INICIAL

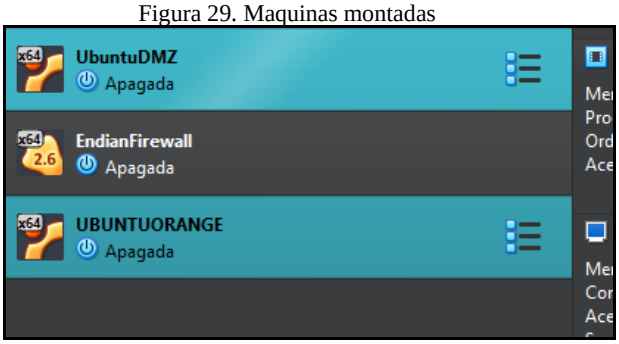
Como se detalla en la sección 2.1, Endian fue configurado con las tres zonas de red: VERDE (LAN), NARANJA (DMZ) y ROJA (WAN). Las direcciones IP asignadas a los servidores fueron:

Ubuntu Desktop en la LAN: 192.168.2.16

Ubuntu Server en la DMZ: 192.168.1.16

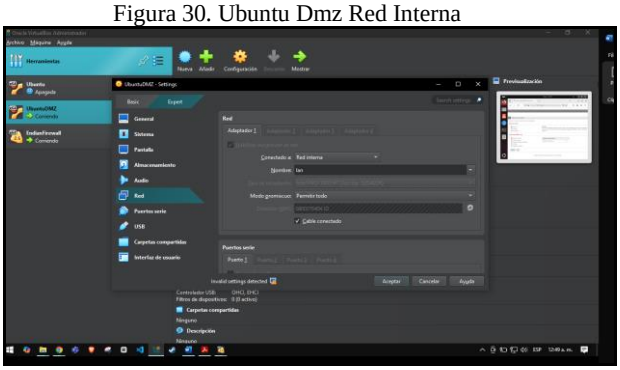
El firewall se administró desde la interfaz web de Endian accediendo a https://192.168.2.15:10443 desde el cliente en la zona VERDE.

Figura 29. Maquinas montadas



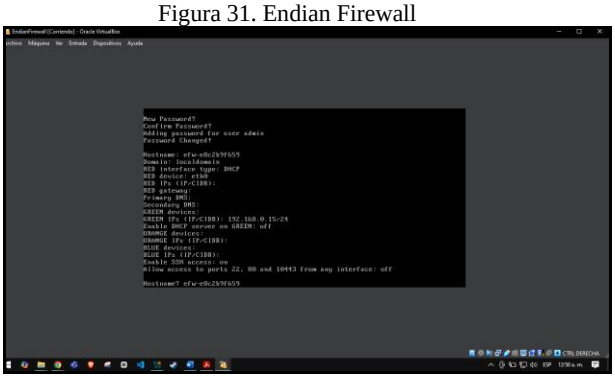
Fuente: Autoría Propia

Figura 30. Ubuntu Dmz Red Interna



Fuente: Autoría Propia

Figura 31. Endian Firewall



Fuente: Autoría Propia

2.3.2 ACTIVACIÓN DE SERVICIOS HTTP Y FTP

Para habilitar el acceso a los servicios web y FTP en la DMZ, se ingresó al panel Firewall > Port Forwarding (DNAT), donde se crearon dos reglas:

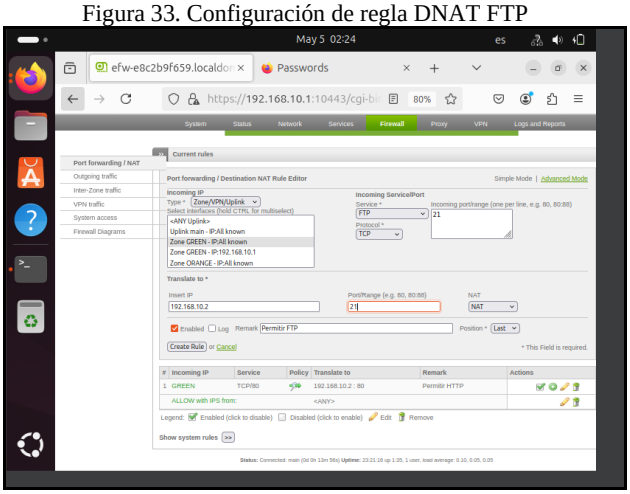
Regla DNAT HTTP:
Source: Any
Destination: IP WAN (10.0.2.15)
Port: 80
Forward to: 192.168.1.16 (Ubuntu Server)
Regla DNAT FTP:
Source: Any
Destination: IP WAN (10.0.2.15)
Port: 21
Forward to: 192.168.1.16 (Ubuntu Server)

Ambas reglas fueron activadas y aplicadas correctamente. Posteriormente se realizó la validación accediendo al servicio web desde un navegador y al servidor FTP usando FileZilla desde una red externa simulada.

Figura 32. Configuración de regla DNAT HTTP

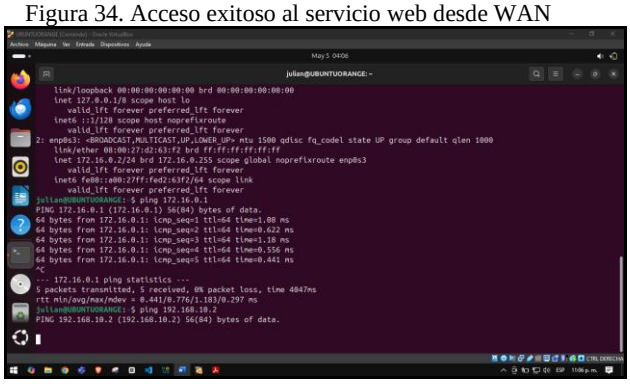
Fuente: Autoría Propia

Figura 33. Configuración de regla DNAT FTP



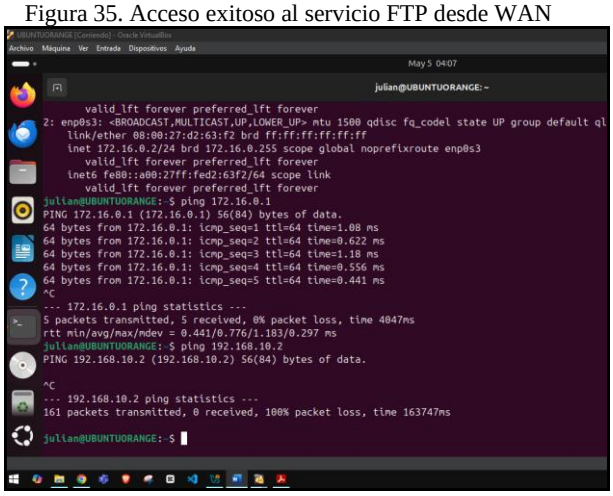
Fuente: Autoría Propia

Figura 34. Acceso exitoso al servicio web desde WAN



Fuente: Autoría Propia

Figura 35. Acceso exitoso al servicio FTP desde WAN



Fuente: Autoría Propia

2.3.3 BLOQUEO DE ICMP DESDE LAN A DMZ

Desde el mismo panel del firewall, se accedió a Firewall > Packet Filter para crear una nueva regla con las siguientes condiciones:

Source: Zona VERDE

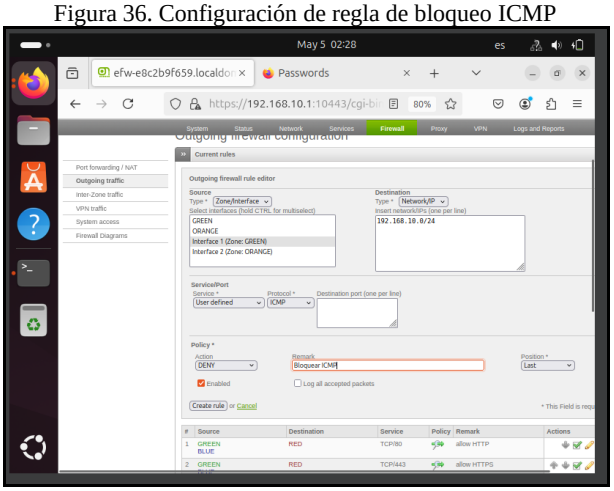
Destination: Zona NARANJA

Protocol: ICMP

Action: Drop

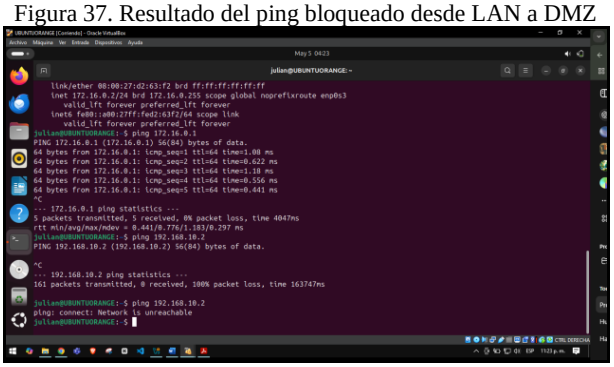
La regla fue agregada y aplicada. Para verificar su efectividad, se ejecutó el comando ping desde el cliente Ubuntu Desktop (LAN) al servidor Ubuntu Server (DMZ), y se obtuvo como resultado el bloqueo del tráfico ICMP.

Figura 36. Configuración de regla de bloqueo ICMP



Fuente: Autoría Propia

Figura 37. Resultado del ping bloqueado desde LAN a DMZ



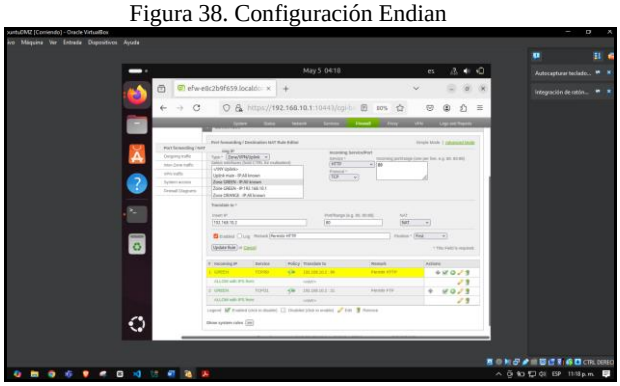
Fuente: Autoría Propia

2.3.4 RESULTADOS Y VALIDACIÓN

Las pruebas realizadas confirmaron que los servicios HTTP y FTP se encuentran disponibles desde el exterior (WAN), mientras que el tráfico ICMP proveniente de la LAN hacia la DMZ fue correctamente bloqueado. Esto garantiza un nivel de seguridad adecuado, asegurando que solo los servicios intencionalmente expuestos estén accesibles y que otros tipos de tráfico no deseados sean filtrados efectivamente.

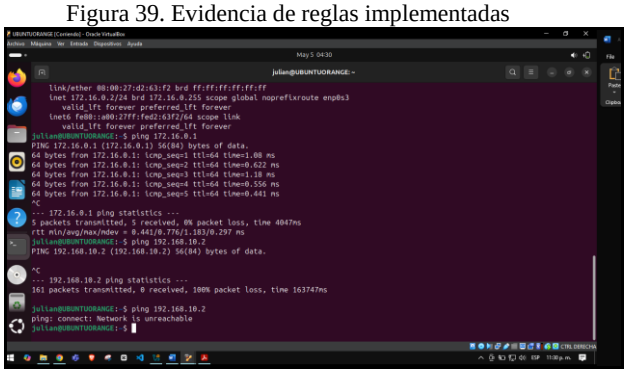
Estas configuraciones consolidan el uso de Endian Firewall como una herramienta robusta para la gestión segura del tráfico entre zonas, facilitando una administración detallada de las políticas de acceso y segmentación de la red.

Figura 38. Configuración Endian



Fuente: Autoría Propia

Figura 39. Evidencia de reglas implementadas

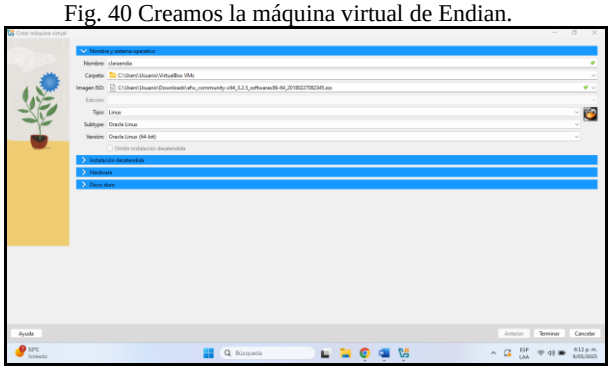


Fuente: Autoría Propia

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

Para la implementación de esta temática, se realizó la instalación de Endian, configurada en VirtualBox, empleando dos interfaces de red: eth1 (VERDE/LAN: 192.168.0.15/24), eth2 (NARANJA/Ubuntu Server: 192.168.1.1/24) con el fin de evitar bloqueos y tener el control adecuado del tráfico entrante y saliente.

Fig. 40 Creamos la máquina virtual de Endian.

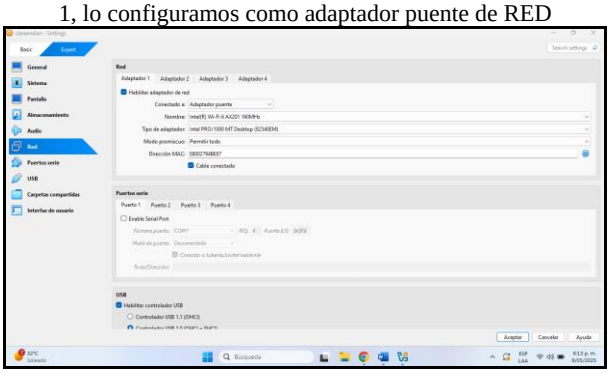


Fuente: Autoría propia

Fig. 41 Seleccionamos la cantidad de disco duro.

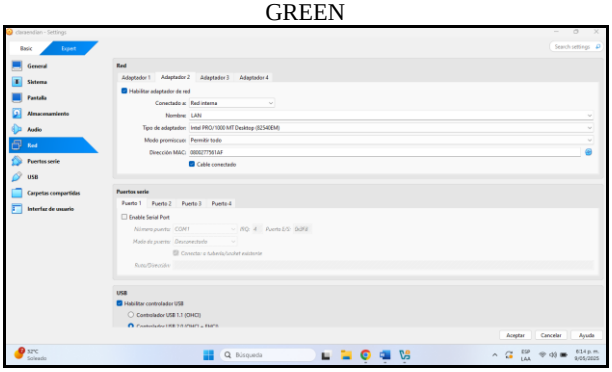
Fuente: Autoría propia

Fig. 42 Ingresamos a la opción Red, en la pestaña Adaptador 1, lo configuramos como adaptador puente de RED



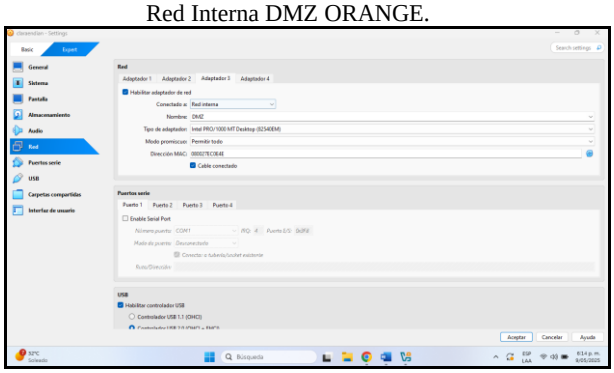
Fuente: Autoría propia

Fig. 43 Configuramos el Adaptador 2 como Red Interna LAN GREEN



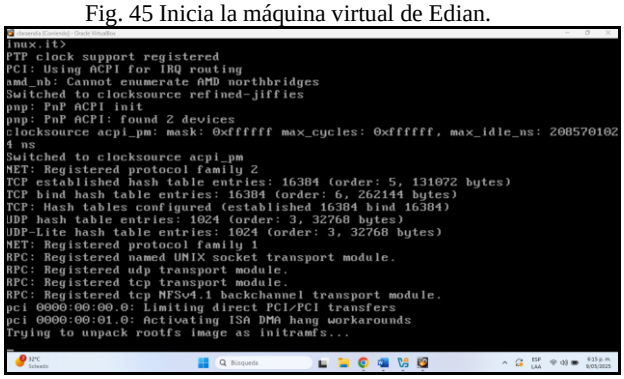
Fuente: Autoría propia

Fig. 44 Se realiza la configuración en el adaptador 3como Red Interna DMZ ORANGE.



Fuente: Autoría propia

Fig. 45 Inicia la máquina virtual de Edian.

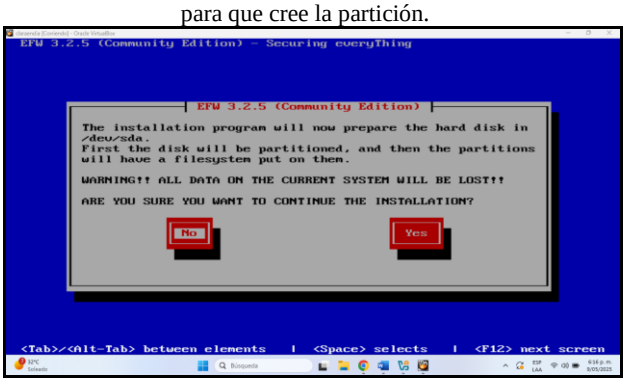


Fuente: Autoría propia

Fig. 46 Se selecciona el idioma.

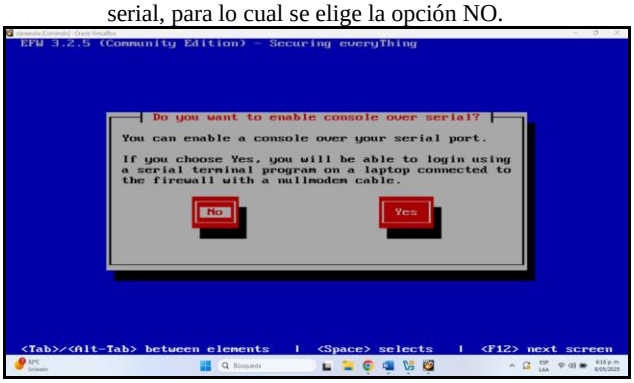
Fuente: Autoría propia

Fig. 47 para continuar con la instalación seleccionamos si, para que cree la partición.



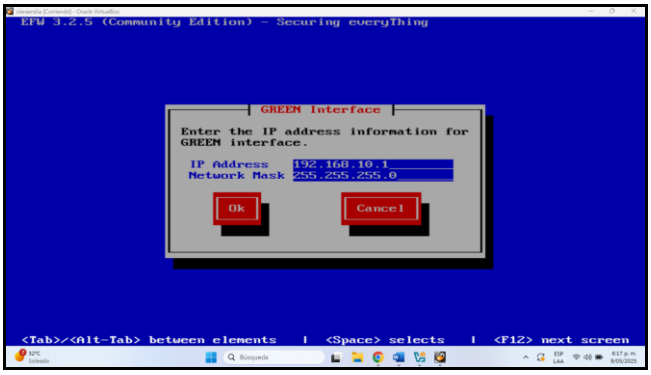
Fuente: Autoría propia

Fig. 48 Se habilita el acceso a Firewall a través de un puerto serial, para lo cual se elige la opción NO.



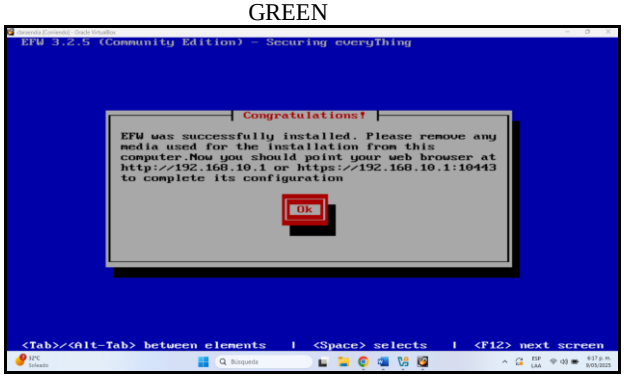
Fuente: Autoría propia

Fig. 49 Seleccionamos la opción OK para establecer la IP y la máscara de GREEN.



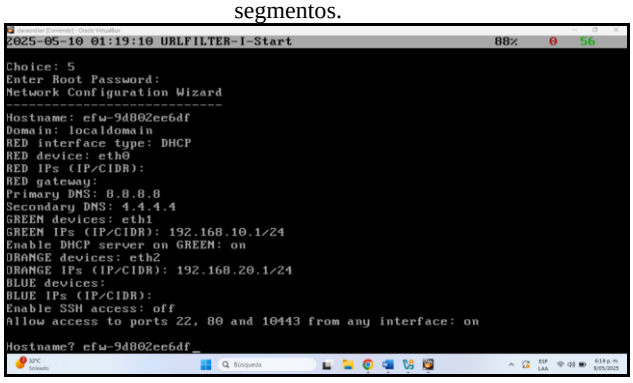
Fuente: Autoría propia

Fig. 50 Se evidencia la configuración exitosa de la IP GREEN



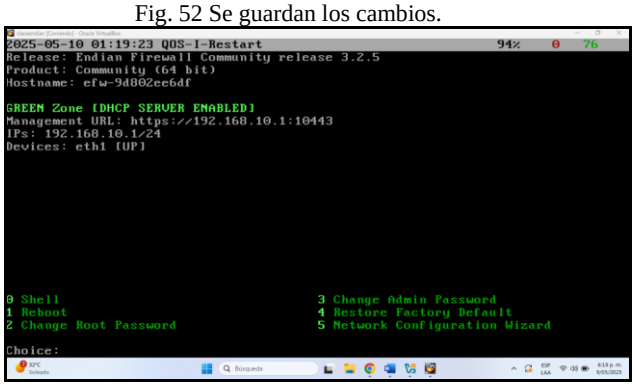
Fuente autoría propia

Fig. 51 Se configuran las zonas de acuerdo con los segmentos.



Fuente: Autoría propia

Fig. 52 Se guardan los cambios.



Fuente: Autoría propia

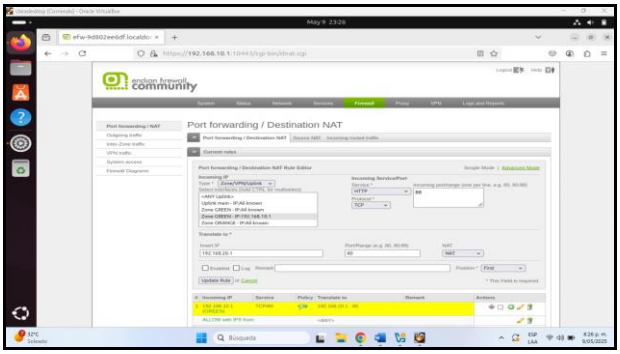
Se valida la configuración de la Red Ubuntu desktop y configuramos en adaptador 1 con red interna y con el nombre LAN GREEN, configuramos la red estática con la 192.168.10.20 verificando que los cambios se hayan guardado de manera correcta para acceder a Endian.

Fig. 53 Ingreso exitoso a Endian.

Fuente: Autoría propia

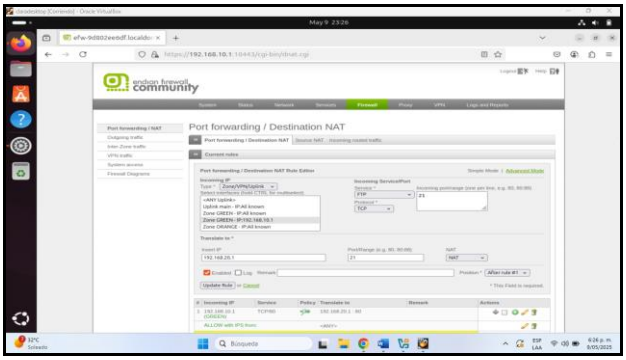
Se configura la RED de manera DHCP, para seleccionar las zonas del Firewall, seleccionando ORANGE que define el segmento de red el cual será accesible desde Internet (DMZ), se aceptan las opciones que nos van a permitir configurar las reglas de Port Forwarding para permitir tráfico HTTP (puerto 80) desde la LAN hacia la DMZ en un firewall Endian que es la que nos permite el tráfico HTTP (puerto 21) desde la LAN hacia la DMZ.

Fig. 54 Configuración de reglas de Port Forwarding para permitir tráfico HTTP (puerto 80) desde la LAN hacia la DMZ en un firewall Endian.



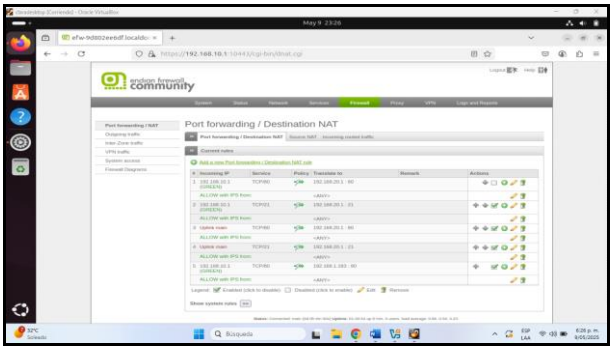
Fuente: Autoría propia

Fig. 55 Configuración de reglas de Port Forwarding para permitir tráfico HTTP (puerto 21) desde la LAN hacia la DMZ en un firewall Endian.



Fuente: Autoría propia

Fig. 56 Reglas NAT aplicadas para permitir el tráfico HTTP (puerto 80) y FTP (puerto 21) hacia la IP interna en la zona DMZ.

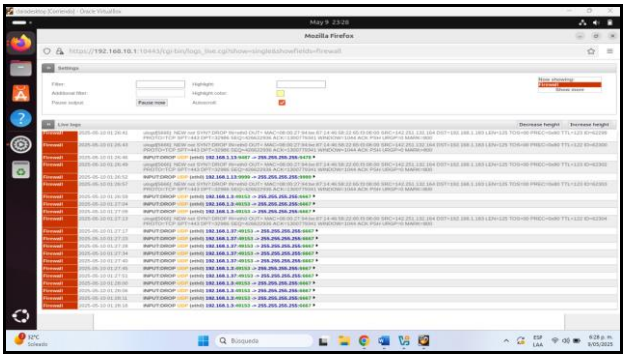


Fuente: Autoría propia

2.4.1 RESULTADOS Y VALIDACIÓN

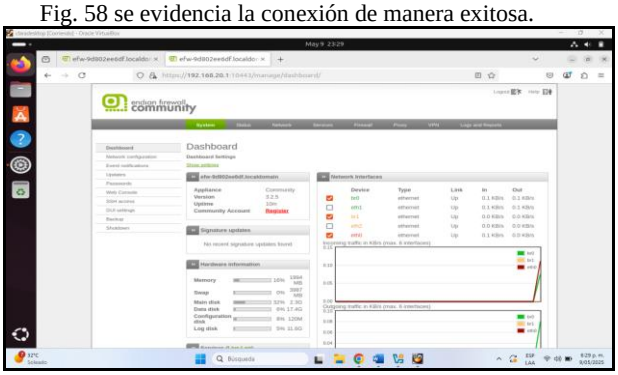
De manera correcta se evidencia que se configuraron correctamente las reglas de NAT y Firewall para permitir el acceso HTTP desde la LAN hacia la WAN. Tras aplicar las reglas, se verificó que el tráfico HTTP se estaba gestionando adecuadamente sin bloqueos, lo que indica que las configuraciones fueron exitosas

Fig. 57. configuraron correctamente las reglas de NAT y Firewall



Fuente: Autoría propia

Fig. 58 se evidencia la conexión de manera exitosa.



Fuente: Autoría propia

Fig. 59 evidenciamos la conexión HTTP desde la LAN hacia la WAN.

Fuente: Autoría propia

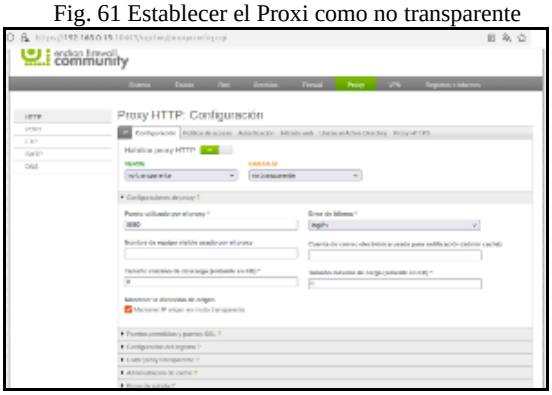
2.5 TEMÁTICA 5: IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE) CON POLÍTICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET.

Para la implementación de esta temática, se utilizó una instancia de Endian Firewall 3.3 configurada en VirtualBox, empleando tres interfaces de red: eth1 (VERDE/LAN: 192.168.0.15/24), eth2 (NARANJA/Ubuntu Server: 192.168.1.1/24) y eth3 (ROJA/WAN: NAT hacia Internet). El objetivo de la temática se encamino a aplicar políticas de restricción y autenticación de usuarios evitando la salida a sitios que se encuentran en lista negra permitiendo la optimización de recursos, cumplimiento de normatividad y disminuyendo el riesgo de ingreso de malware a la red.

Fig. 60 Máquinas virtuales Instaladas

Fuente: Autoría propia

Fig. 61 Establecer el Proxi como no transparente



Fuente: Autoría propia

Al configurar el proxy como no transparente, es posible exigir una configuración explícita del proxy en los clientes, lo cual permitió implementar mecanismos de autenticación robustos y un control más preciso sobre las conexiones salientes.

Fig. 62 Creación Perfil y restricciones

Fuente: Autoría propia

La creación de perfiles y listas negras dentro del Proxi HTTP
Permitió la aplicación de políticas de salida a sitios maliciosos, de phishing o que contengan malware mediante listas negras, se reduce el riesgo de infecciones y brechas de seguridad.

Fig. 63 Creaciones políticas

Fuente: Autoría propia

Mediante políticas, se puede definir quién puede acceder, cuándo, y a qué contenido, evitando el uso anónimo o no autorizado de los servicios de Internet.

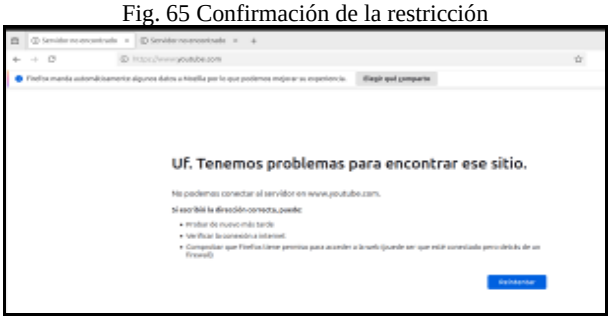
2.5.1 RESULTADOS Y VALIDACIÓN

Se confirmo que no hay acceso a sitios web no permitidos, en la práctica, se utilizó el usuario estudiante1 y se intentó ingresar a uno de los sitios almacenados en la lista negra y se confirma que no hay acceso.

Fig. 64 Usuario creado con restricción asignada

Fuente: Autoría propia

Fig. 65 Confirmación de la restricción



Fuente: Autoría propia

3 Conclusiones.

Se consigue aprender a configurar la arquitectura del sistema operativo GNU/Linux, instalando y administrando los diferentes paquetes, a través de los comandos y las pantallas graficas. Logrando implementar una arquitectura de red segmentada mediante la distribución GNU/Linux Endian, configurando la zona verde (LAN), roja (WAN) y naranja (DMZ), en pro del fortalecimiento de la seguridad de una red; optimizando la gestión del tráfico de red, de manera controlada y confiable entre dispositivos internos, servidores y el acceso a internet de los sistemas operativos utilizados durante el proceso.

El desarrollo de la temática 2 ha permitido adquirir una comprensión más profunda sobre la configuración de firewalls, NAT y políticas de seguridad en redes, utilizando Endian Firewall como herramienta clave. A lo largo de este proceso, se aprendió a implementar reglas de filtrado para asegurar las zonas LAN, DMZ y WAN, y se comprendió la importancia de segmentar redes eficientemente para proteger los recursos internos y garantizar una conectividad segura hacia el exterior. La configuración de SNAT y DNAT resultó fundamental para proporcionar acceso controlado a los servicios internos y asegurar que los recursos externos fueran accesibles de forma adecuada, sin comprometer la seguridad de la red interna. Las pruebas realizadas confirmaron que las configuraciones implementadas cumplen con los objetivos de conectividad y protección, destacando la efectividad de las políticas de seguridad aplicadas, lo que fortaleció las habilidades en la configuración de redes y firewalls y permitió comprender la importancia de aplicar medidas de seguridad adecuadas en entornos corporativos o de producción.

La implementación de servicios controlados desde la zona DMZ, mediante el uso de Endian Firewall, permitió no solo asegurar la exposición de servicios clave como HTTP y FTP, sino también restringir adecuadamente protocolos no deseados como ICMP. Esta práctica consolidó la comprensión de segmentación de redes y políticas de seguridad, fortaleciendo habilidades en la administración de sistemas GNU/Linux. La experiencia adquirida reafirma la importancia del uso de firewalls para la protección perimetral, demostrando la efectividad de una configuración estructurada y estratégica en entornos virtualizados.

Las pruebas de conectividad HTTP y FTP demostraron que es crucial revisar minuciosamente las reglas de firewall y NAT para garantizar que los servicios estén disponibles en la red. Los registros de tráfico mostraron que algunas conexiones fueron rechazadas, lo que indica que las reglas aún deben ajustarse para permitir ciertos tipos de tráfico. Garantizar una configuración correcta en las interfaces y servicios mejora tanto el acceso como la seguridad de la red, evitando bloqueos innecesarios y asegurando un control adecuado del tráfico entrante y saliente.

La implementación de un proxy HTTP no transparente con políticas de autenticación utilizando la herramienta Endian Firewall permitió establecer un control efectivo sobre el acceso a Internet dentro de la red local. A través de esta solución, se logró garantizar que únicamente los usuarios autorizados puedan navegar, fortaleciendo la seguridad y facilitando la trazabilidad de las actividades realizadas en línea. El uso de autenticación previa al acceso, además de ofrecer una capa adicional de protección, permitió aplicar políticas diferenciadas según grupos de usuarios, optimizando la gestión de recursos y el cumplimiento de normativas internas.

4 REFERENCIAS

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

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

[3] LaCroix, J. (2020). *Mastering Ubuntu Server: Gain expertise in the art of deploying, configuring, managing, and troubleshooting Ubuntu Server*. Packt Publishing. https://research-ebsco-com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b41952

[4] Linux Professional Institute (LPI). (2022). *Tema 102: Comandos GNU y Unix*. https://learning.lpi.org/es/learning-materials/101-500/102/

[5] Canonical. (2023). *Guía del Ubuntu Desktop 20.04 LTS*. https://help.ubuntu.com/20.04/ubuntu-help/index.html

[6] Debian Project. (2023). *Manual del administrador de Debian 12.5.0*. https://www.debian.org/releases/stable/amd64/index.es.html

[7] Endian. (2008). *Endian topologies*. https://help.ewon.biz/legacydocumentation/Oldies%20-%20Application%20User%20Guide/AUG-027-0-EN-%28ENDIAN%20topologies%29.pdf

[8] Endian. (2013). *Endian Firewall Community features*. https://www.endian.com/community/features/

[9] Endian. (2017). *Endian Firewall Community download*. https://sourceforge.net/projects/efw/

[10] Wikipedia contributors. (2023). *Endian Firewall*. Wikipedia. https://de.wikipedia.org/wiki/Endian_Firewall