DISEÑO DE UN LABORATORIO VIRTUAL PARA SEGURIDAD Y GESTIÓN DE RED

Edwin Orlando Chavarro Rivera
e-mail: eochavarror@unadvirtual.edu.co
Juan Carlos Fuelgas Chungana
e-mail: jcfuelpasc@unadvirtual.co
Adriana María Cano Silva
e-mail: amcanos@unadvirtual.edu.co
Luis Felipe Mazuera Martínez
e-mail: lfmazueram@unadvirtual.edu.co
Angela Lizbeth Arteaga López
e-mail: alarteagal@unadvirtual.edu.co

RESUMEN: *La protección de redes perimetrales es fundamental para salvaguardar las infraestructuras tecnológicas. Este proyecto busca asegurar la protección de los servidores dentro de una red interna (LAN) y externa (WAN) mediante la creación de una zona DMZ utilizando Endian UTM. La implementación de un firewall Endian, junto con la aplicación de políticas de acceso, asegura una comunicación segura entre las distintas áreas de la red. Las tareas incluyen la configuración de traducción de direcciones de red (NAT), la habilitación de servicios en la zona DMZ, y la integración de un proxy HTTP con autenticación para filtrar el tráfico web.*

PALABRAS CLAVE: Autenticación proxy, Endian Firewall, NAT, Seguridad DMZ.

1 INTRODUCCIÓN

La seguridad en redes informáticas representa un desafío crítico para organizaciones de todos los tamaños. Este trabajo aborda la implementación de un sistema de seguridad robusto utilizando GNU/Linux Endian Firewall, una distribución especializada que integra múltiples herramientas de protección [3]. El objetivo principal es crear un entorno seguro que permita la segregación del tráfico de red y el control granular de las comunicaciones entre diferentes segmentos, implementando un modelo de defensa en profundidad.

La implementación se desarrolla en un entorno virtualizado utilizando VirtualBox [6], donde se configuran tres zonas de seguridad fundamentales: la zona verde (LAN) para usuarios internos, la zona roja (WAN) para la conexión a Internet y la zona naranja (DMZ) para albergar servidores accesibles externamente. Esta segmentación permite estructurar la red de manera que cada zona tenga niveles de acceso y reglas específicas.

A lo largo del trabajo se implementan diversas técnicas de seguridad, incluyendo la traducción de direcciones de red (NAT), reglas de filtrado de tráfico inter-zona, control de servicios específicos y un sistema de proxy HTTP con autenticación. Cada uno de estos componentes se configura y gestiona desde el sistema GNU/Linux, aprovechando herramientas administrativas presentes en distribuciones como Ubuntu Server y Debian [1][2]. Además, se aplican comandos GNU y Unix esenciales para la administración del sistema y la seguridad [5], apoyados por buenas prácticas descritas en literatura especializada sobre administración de servidores Ubuntu [4].

Esta arquitectura de red controlada busca minimizar la superficie de ataque y proporcionar mecanismos eficaces para gestionar las comunicaciones y proteger los activos digitales.

2 IMPLEMENTACIÓN

Endian UTM es una distribución GNU/Linux especializada en seguridad de redes, basada en CentOS, y enfocada en proporcionar funcionalidades avanzadas de firewall, control de contenidos y protección contra intrusiones [3]. Su versatilidad permite su despliegue tanto en hardware físico como en plataformas virtuales, como Oracle VM VirtualBox [6].

Para esta implementación, se utilizó VirtualBox para crear una máquina virtual con las siguientes características: Sistema operativo base: Linux (Oracle Linux 64-bit) Método de arranque: ISO

La instalación de la máquina virtual con GNU/Linux Endian incluye la configuración de tres interfaces de red, lo cual permite la segmentación lógica de las siguientes zonas de seguridad.

Zona verde (LAN), destinada a los usuarios internos de la red, la zona roja (WAN), utilizada para la conexión con Internet y la zona naranja (DMZ), diseñada para alojar servidores accesibles desde el exterior.

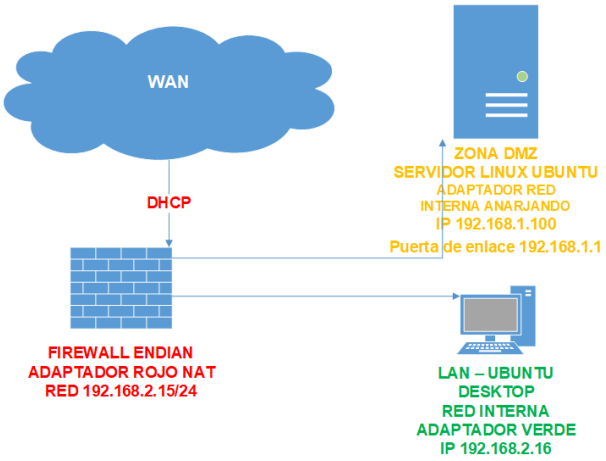
Esta estructura de red segmentada es fundamental para aplicar políticas específicas de seguridad, facilitando el control del tráfico y reduciendo la exposición a posibles amenazas.

LAN: Conjunto de dispositivos interconectados para recibir información.

WAN: Red que permite la conexión del dispositivo.

DMZ: Muestra la conexión entre el servidor y la red.

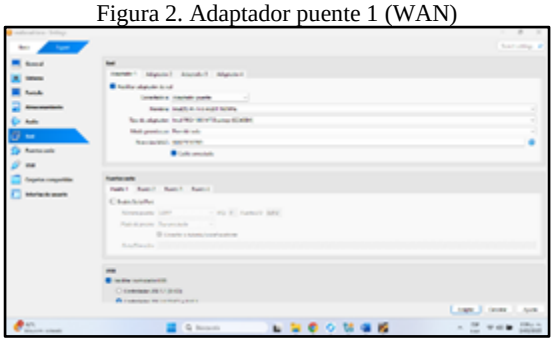
Figura 1: Escenario base.



Fuente: Autoría propia

Se configura el adaptador 1 de Endian como adaptador puente (WAN).

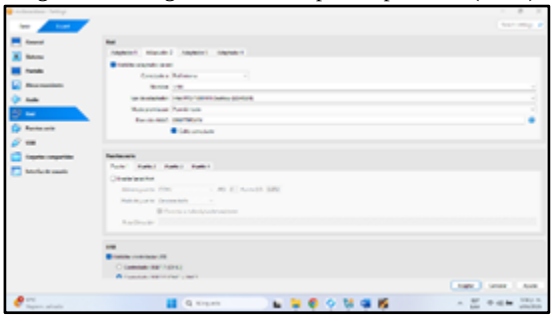
Figura 2. Adaptador puente 1 (WAN)



Fuente: Autoría propia

Se configura el adaptador 2 de Endian como red interna (LAN).

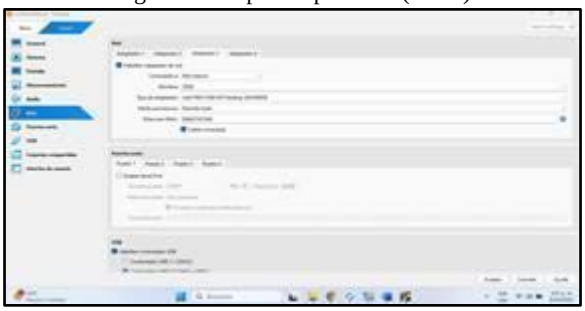
Figura 3. Configuración de adaptador puente 2 (LAN)



Fuente: Autoría propia

Se realizó la configuración el adaptador 3 de Endian como red interna (DMZ), validando cada punto y funcionamiento.

Figura 4. Adaptador puente 3 (DMZ)

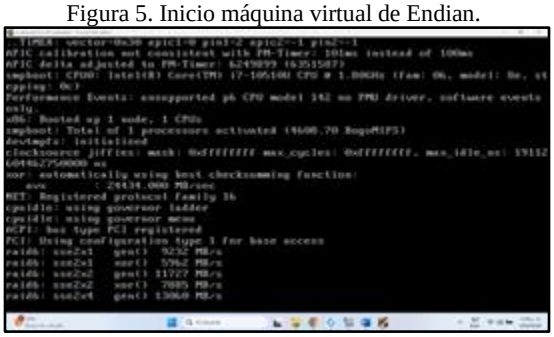


Fuente: Autoría propia

3 PROCESOS DE INSTALACIÓN

Con la configuración de las tarjetas de red establecida en cada una de las zonas de la máquina virtual de Endian, se procede a iniciar el equipo. Este se configuró para arrancar desde la unidad óptica virtual que apunta a la imagen ISO del sistema operativo. A continuación, comienza el proceso de instalación con la selección del idioma, como se muestra en la figura siguiente.

Figura 5. Inicio máquina virtual de Endian.



Fuente: Autoría propia

Figura 6. Elección de idioma.

Fuente: Autoría propia

En este caso, se selecciona el idioma inglés y se continúa con la instalación. Esta etapa proporciona una pantalla de bienvenida e indica que al presionar “Cancel” en cualquiera de las pantallas de instalación, el sistema se reiniciará, tal como se ilustra en la figura siguiente.

Figura 7. Partición instalación del sistema.

Fuente: Autoría propia

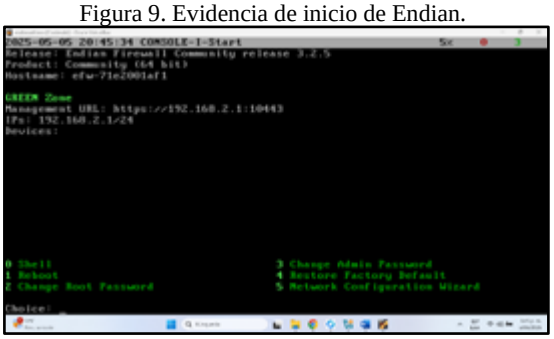
En la siguiente pantalla, se informa que toda la información del disco duro será eliminada debido a que se procederá a particionar y formatear. Es necesario aceptar esta condición para continuar con la instalación, como se muestra a continuación.

Figura 8. Establecimiento de ip GREEN.

Fuente: Autoría propia

Como último paso de la instalación, se solicita la configuración de la dirección IP y la máscara de GREEN.

Figura 9. Evidencia de inicio de Endian.



Fuente: Autoría propia

Se inició Endian de forma exitosa, donde se muestra la IP de GREEN.

Una vez finalizada la instalación, se accede a la interfaz gráfica de Endian a través de https://<IP_GREEN>:10443.

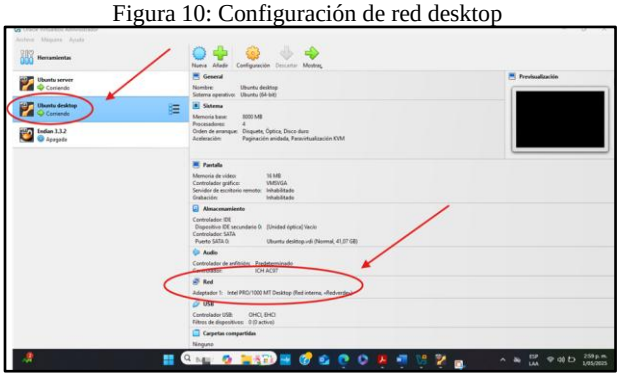
4 IMPLEMENTANDO SEGURIDAD EN GNU/LINUX

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

Configurar la instancia para GNU/Linux Endian en VirtualBox (tarjetas de red) e instalación efectiva del mismo. Implementando GNU/Linux Endian con las zonas verde, roja y naranja, así: Zona verde: Red interna (LAN), Zona roja: Acceso a internet (WAN) y Zona naranja: Servidores (DMZ).

Se realizó la configuración del Adaptador 1 en el desktop de la siguiente forma: (Red interna, <<RedVerde>>) para que se escuche por la misma tarjeta de red de Endian**.**

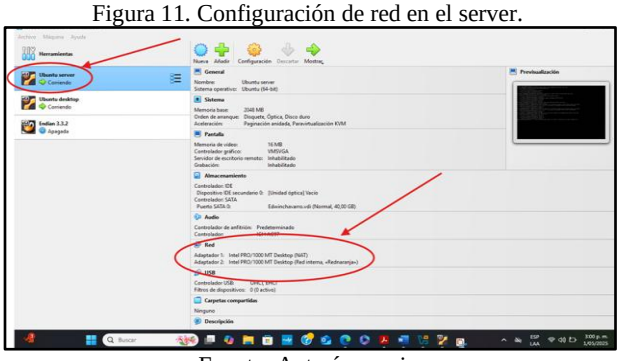
Figura 10: Configuración de red desktop



Fuente: Autoría propia

En la siguiente imagen se muestra la configuración de los adaptadores de la siguiente forma Adaptador 1: (NAT) Adaptador 2: (Red interna, << Red Naranja>>) el servidor va a tener la tarjeta de red anaranjada.

Figura 11. Configuración de red en el server.

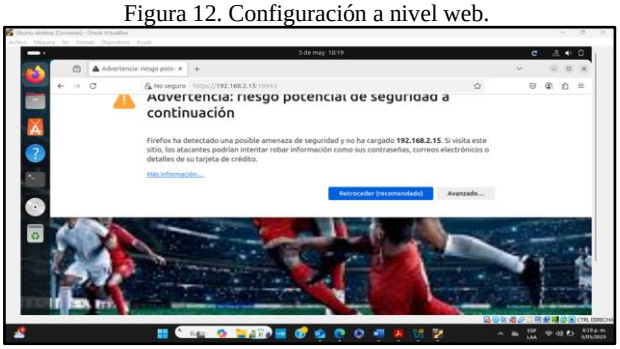


Fuente: Autoría propia

Una vez configurados los diferentes adaptadores Se inicia el Proceso de instalación y configuración endian a nivel web accediendo a la interfaz gráfica de Endian a través del navegador del cliente (desktop) que se encuentra en la red verde,

la cual tiene configurada la dirección ip https://IP:192.168.2.15:10443 haciendo uso del puerto10443.

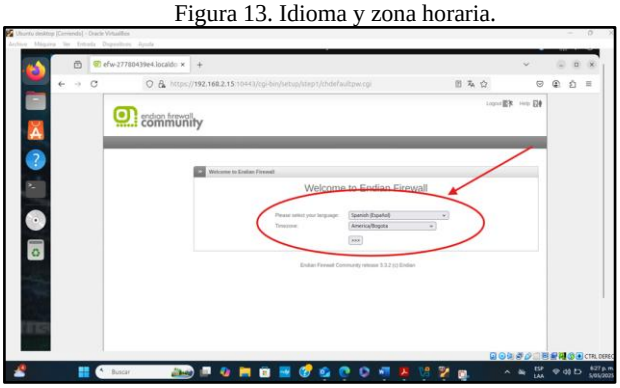
Figura 12. Configuración a nivel web.



Fuente: Autoría propia

Se configuró el idioma dando clic en siguiente, para este caso se selecciona “español” y la zona “America/Bogota” como se observa en la imagen de la Figura.

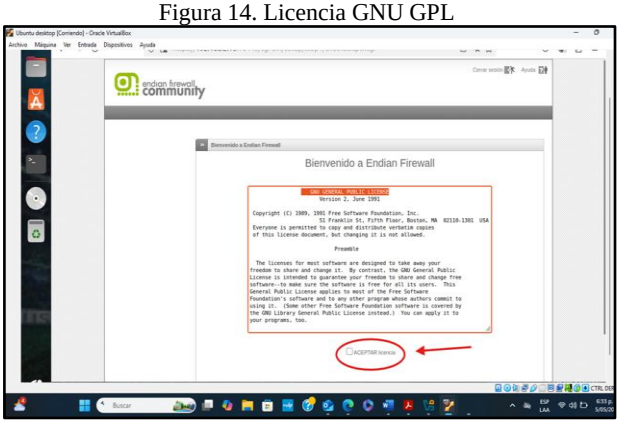
Figura 13. Idioma y zona horaria.



Fuente: Autoría propia

Posteriormente a la elección del idioma Se configura la contraseña del usuario “admin” y del usuario “root” , se aceptan los términos de licencia, tener presente que se deben aceptar los términos de licencia, también se debe elegir si se va a restaurar alguna copia de seguridad (para este caso se debe seleccionar “No” ya que el escenario es nuevo) observar Figura 14 y 15.

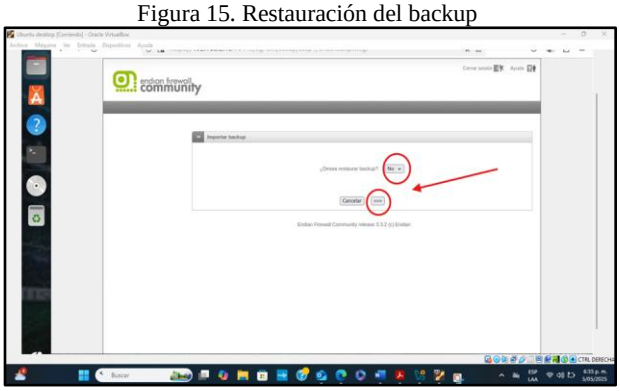
Figura 14. Licencia GNU GPL



Fuente: Autoría propia

se registró los datos y se validó en importar backup encontrando la opción restaurar si y no, para proceder y continuar.

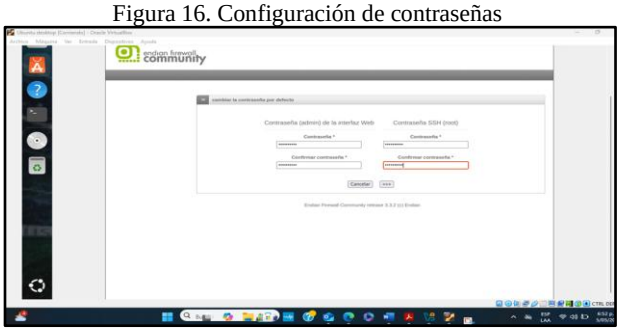
Figura 15. Restauración del backup



Fuente: Autoría propia

Se realiza la Asignación de contraseña para la interfaz web y SSH**.** (se encomienda una contraseña fuerte).

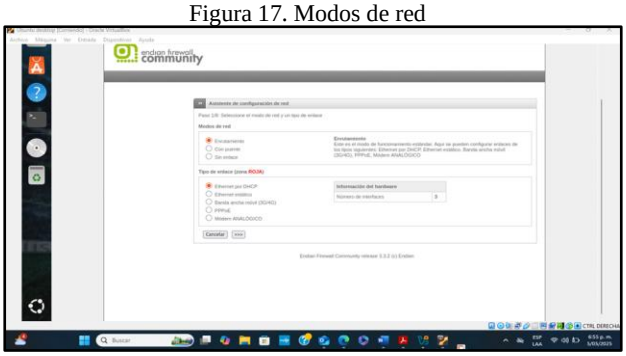
Figura 16. Configuración de contraseñas



Fuente: Autoría propia

Después de haber realizado la configuración de las contraseñas, tenemos el primer proceso, la instalación de las diferentes áreas, indica los modos de red por enrutamiento, Ethernet por DHCP, indica que tiene 3 tarjetas de red configuradas el servidor de Endian como se observa en la Figura 17.

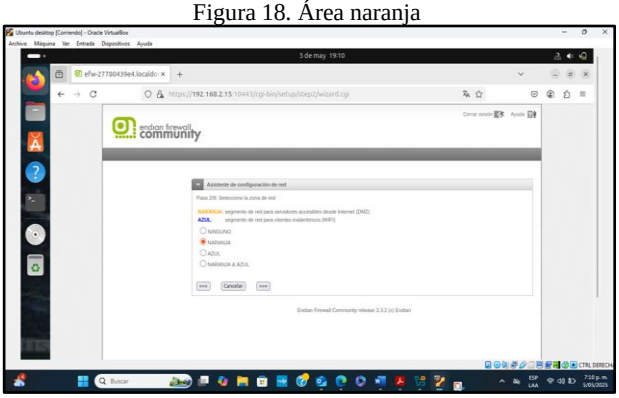
Figura 17. Modos de red



Fuente: Autoría propia

Se Muestra el proceso para configurar el área naranja, (ya tenemos una tarjeta verde que es con que estamos trabajando, roja que es la del internet) acá se selecciona el área naranja como se observa

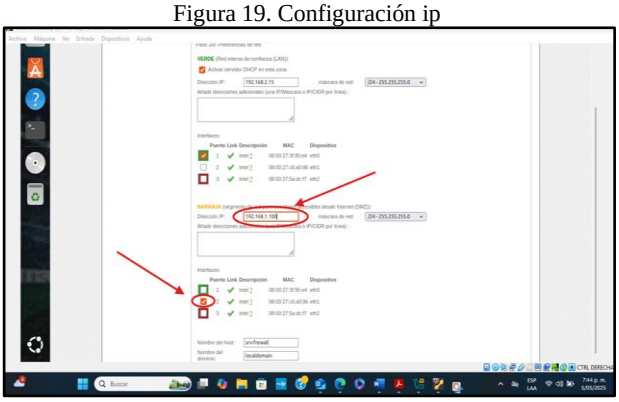
Figura 18. Área naranja



Fuente: Autoría propia

Configuración de la 192.168.1.100 de la red anaranjada asignada en la segmentación y selección de interfaz.

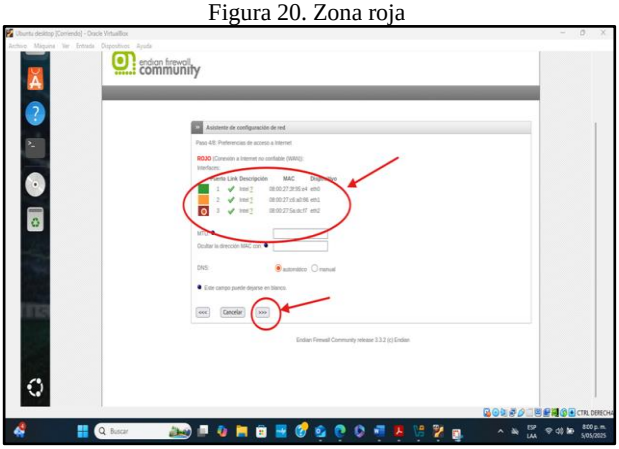
Figura 19. Configuración ip



Fuente: Autoría propia

Se finaliza la configuración de la zona roja y nos muestra la configuración de las 3 zonas verde, naranja, internet (NAT), se confirma la configuración de servidores DNS automática para el presente escenario como se observa en la figura 20.

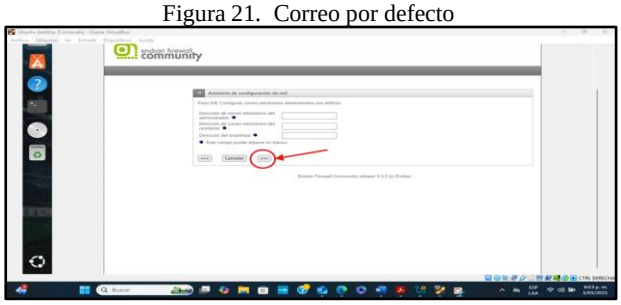
Figura 20. Zona roja



Fuente: Autoría propia

Una vez configuradas las 3 zonas, solicita la creación de un correo por defecto, como se observa en la Figura 21.

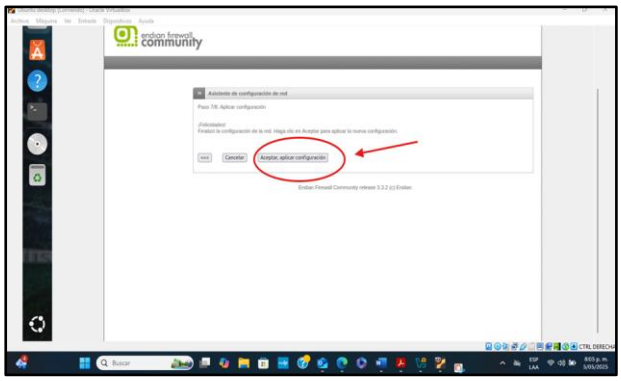
Figura 21. Correo por defecto



Fuente: Autoría propia

Se configuró el asistente de configuración de red, paso 7 y 8 donde se finalizó el proceso realizado, y se valida la opción para cancelar y también para aceptar y aplicar la respectiva configuración.

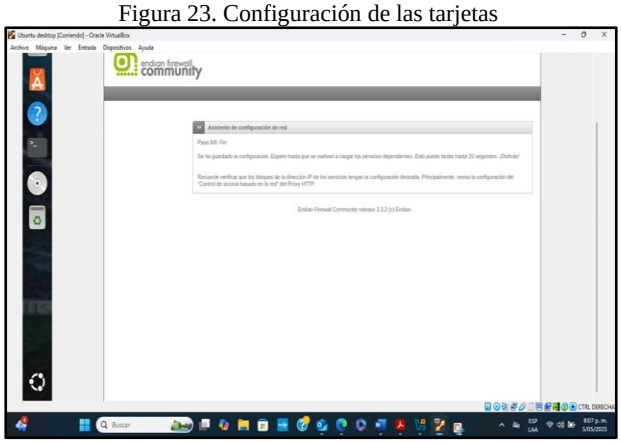
Figura 22. Aceptación para aplicar la configuración.



Fuente: Autoría propia

La configuración ha sido aceptada y está lista para ser aplicada. Con esta acción, se implementan las reglas y ajustes establecidos en el firewall

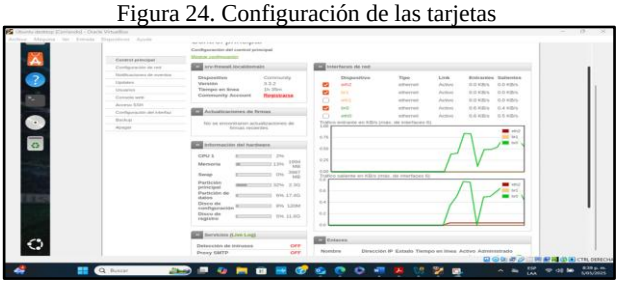
Figura 23. Configuración de las tarjetas



Fuente: Autoría propia

La figura 24 muestra la configuración de todas las tarjetas de red. red roja, red naranja, red verde.

Figura 24. Configuración de las tarjetas



Fuente: Autoría propia

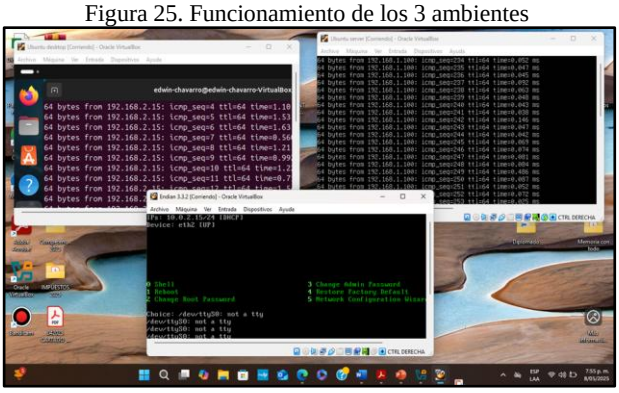
La figura 25 muestra el funcionamiento y la instalación y los 3 ambientes.

Endian con sus configuraciones.

Ubuntu Server con su configuración y conexión con el servidor.

Ubuntu desktop (cliente) con su configuración respondiendo al servidor.

Figura 25. Funcionamiento de los 3 ambientes



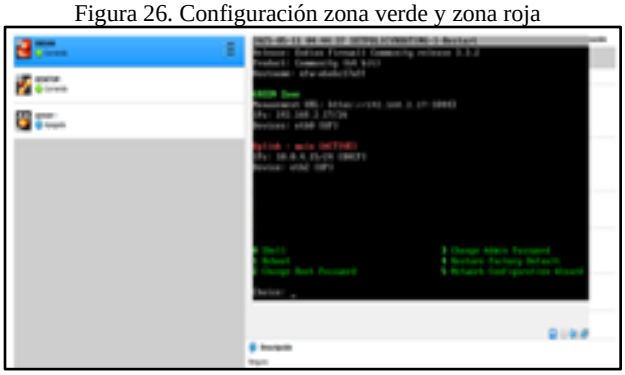
Fuente: Autoría propia

4.2 CONFIGURACIÓN NAT

Configurar las reglas NAT, con el establecimiento de comunicación desde la LAN, hacia la WAN, además establecer relación de la zona DMZ, ejecutando y estableciendo la DMZ hacia la internet con el servidor Ubuntu y las respectivas configuraciones de Endian Firewall.

Se configuró cada zona, pasamos a restaurar valores predeterminados, finalizada la instalación en máquina Endian Firewall, se evidencio la interfaz de las zonas verde y roja respectivamente por sus colores., se tuvo en cuenta https://192.168.2.17:10443

Figura 26. Configuración zona verde y zona roja



Fuente: Autoría propia

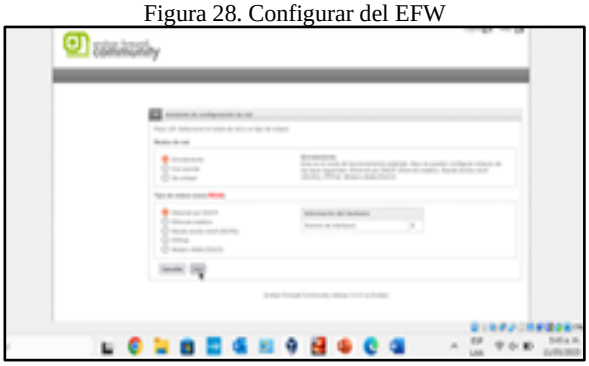
Continuando con el proceso se ejecutó el adaptador de red en la máquina, se hizo la confirmación de la IP asignada, que sea eficiente como se ve en la imagen y la respectiva configuración que comprende a 192.168.2.18 y también, 192.168.2.255, además se validó la subred, dirección y la puerta de enlace.

Figura 27. Adaptador de red

Fuente: Autoría propia

Se configuro a través del entorno web https://192.168.2.17:10443/, registro, datos y contraseña de interfaces web, y enrutar zona roja por Ethernet, validando tipo de enlace, modo red, completando todo el asistente de configuración red como se evidencia en la figura.

Figura 28. Configurar del EFW

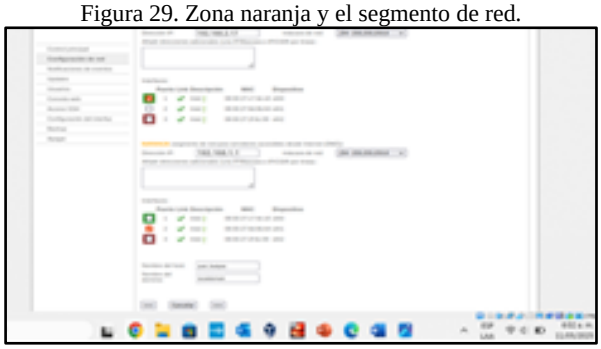


Fuente: Autoría propia

Se realizó el proceso de la zona verde y la red interna de confianza – LAN, activado el DHCP, teniendo en cuenta IP 192.168.2.17/24. la zona naranja, el segmento de red, para

servidores accesibles desde el internet y el DMZ con la configuración y la máscara de red evidenciando los puertos y las interfaces.

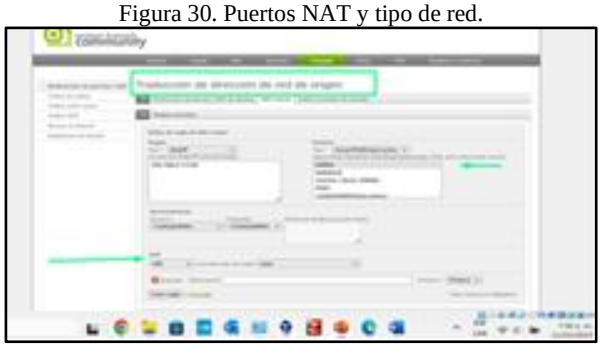
Figura 29. Zona naranja y el segmento de red.



Fuente: Autoría propia

Después de la validación de la zona roja y la conexión a Ethernet junto los datos como correo en el entorno http://192.168.2.17:10443/, se hizo la verificación del panel de control principal, interfaces de red, y la información del hardware, se configuró la regla NAT, con el establecimiento de comunicación desde LAN a WAN como de evidencia en la figura la traducción de dirección red de origen como se muestra en la dirección de puertos/ NAT.

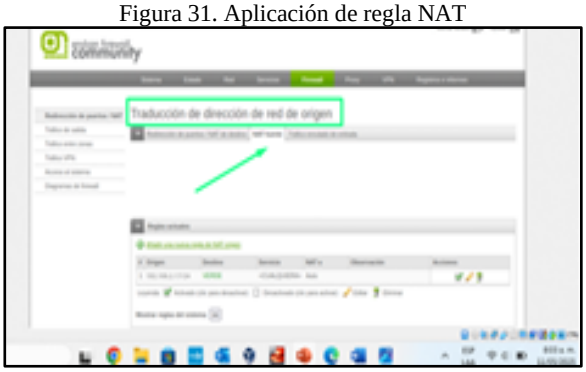
Figura 30. Puertos NAT y tipo de red.



Fuente: Autoría propia

Se procedió a configurar la regla NAT origen, y validar la zona verde estableciendo la conexión, la cual comprende el origen con 192.168.2.17/24 con un destino en verde dentro de la fuente NAT, en cierta medida con la comunicación LAN y la red WAN,

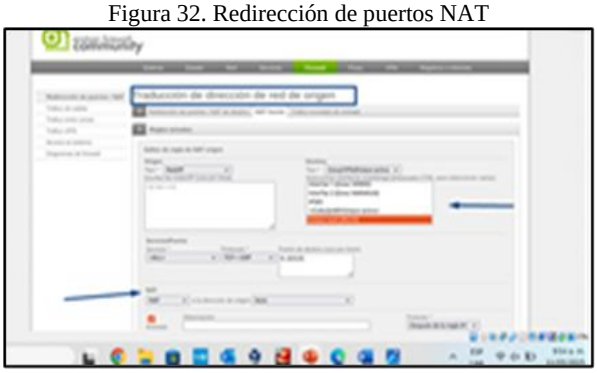
Figura 31. Aplicación de regla NAT



Fuente: Autoría propia

Se verificó la regla NAT, y el establecimiento de comunicación zona DMZ, y el respectivo reenvío de puertos NAT, dentro de la creación de reglas y configuración de NAT – DMZ hacia la internet, por otra parte, comprende el tipo de red, destino y el servicio de puerto.

Figura 32. Redirección de puertos NAT

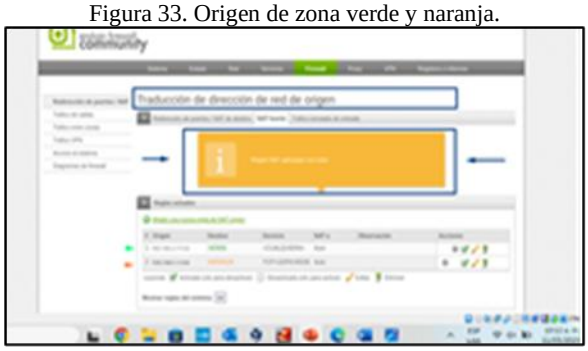


Fuente: Autoría propia

Se verificó las zonas de destino verde y la naranja, con la IP correspondiente 192.168.2.17/24 y 192.168.1/24, cada una con su servicio, dentro de la redirección de puertos /NAT.

Posteriormente se configuró la conexión de salida a internet por el DNS, desde el Ubuntu, con el fin tener las conexiones entre las máquinas y zonas establecidas, con la distribución del ENDIAN de salida, desde LAN y DMZ, en el cual se validó el tráfico entre Zonas, y las reglas de NAT.

Figura 33. Origen de zona verde y naranja.

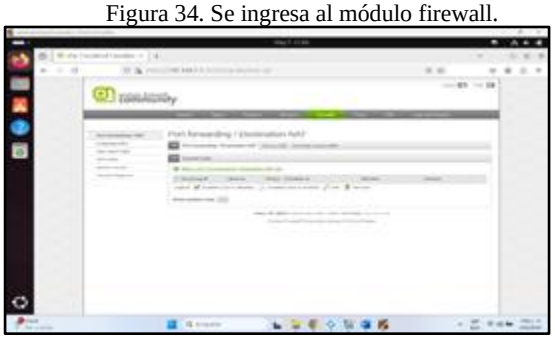


Fuente: Autoría propia

4.3 PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED.

Continuando con el proceso de configuración se accede al Firewall desde el desktop, donde se procede con el inicio de sesión. Este acceso permite gestionar configuraciones y administrar las reglas de seguridad de la red, garantizando un control preciso sobre el tráfico y los servicios habilitados

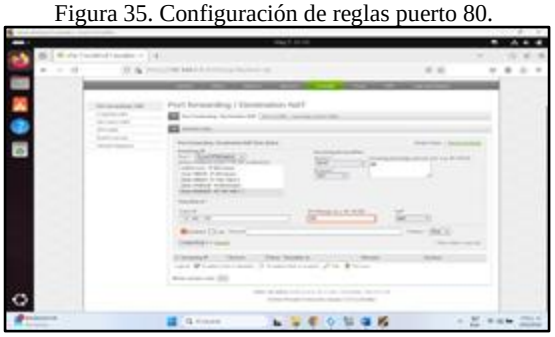
Figura 34. Se ingresa al módulo firewall.



Fuente: Autoría propia

Se ingresa al módulo de firewall y se selecciona la opción para añadir una nueva regla. En este proceso, se definen los parámetros esenciales, como el tipo de tráfico permitido, las direcciones IP origen y destino, así como los puertos involucrados. Esta configuración permite gestionar el acceso y la seguridad de los servicios dentro de la red.

Figura 35. Configuración de reglas puerto 80.



Fuente: Autoría propia

Se establece la configuración de port forwarding en el Firewall para permitir el tráfico HTTP en el puerto 80 dirigido al servidor Ubuntu ubicado en la zona DMZ con la IP 192.168.1.100. Esta regla de redirección garantiza el acceso al servicio desde redes externas, manteniendo control sobre el tráfico y la seguridad del sistema

Figura 36. Configuración de regla puerto 21.

Fuente: Autoría propia

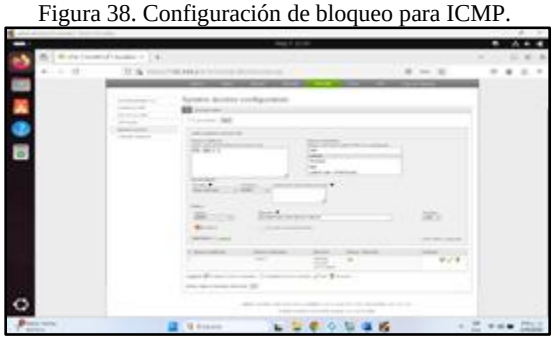
Se ha configurado port forwarding en el firewall para permitir el tráfico FTP (puerto 21) hacia el servidor Ubuntu ubicado en la zona DMZ con la dirección IP 192.168.1.100

Figura 37. Visualización de reglas creadas.

Fuente: Autoría propia

Las reglas creadas se visualizan correctamente en el módulo de firewall, confirmando que la configuración se ha aplicado de manera adecuada. Cada regla refleja los parámetros establecidos, asegurando la correcta gestión del tráfico entre las distintas zonas de la red.

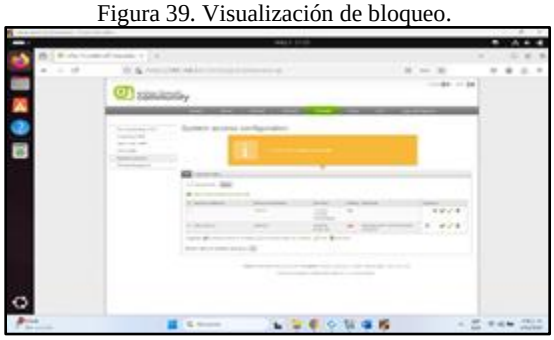
Figura 38. Configuración de bloqueo para ICMP.



Fuente: Autoría propia

Se procede a crear una regla para bloquear el tráfico ICMP desde la dirección IP 192.168.2.1 en la interfaz GREEN (DMZ). La acción de la regla está configurada para denegar el tráfico, asegurando que no se permiten solicitudes ICMP desde esa dirección. La regla ha sido habilitada y aplicada correctamente

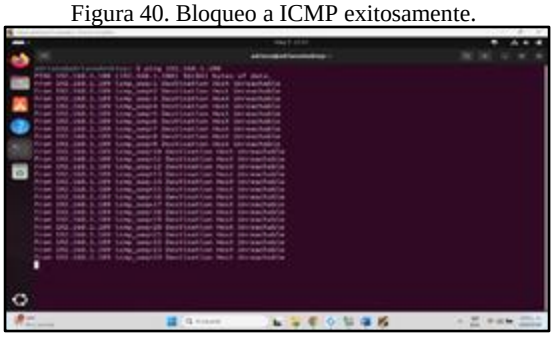
Figura 39. Visualización de bloqueo.



Fuente: Autoría propia

El bloqueo se ha implementado con éxito, asegurando que la regla de firewall restringe el tráfico según la configuración establecida. Con esta medida, se refuerza la seguridad de la red y se gestiona adecuadamente el acceso a los servicios.

Figura 40. Bloqueo a ICMP exitosamente.



Fuente: Autoría propia

Prueba de conexión HTTP desde una máquina cliente en la red WAN: éxito al acceder a la página alojada en el servidor Ubuntu.

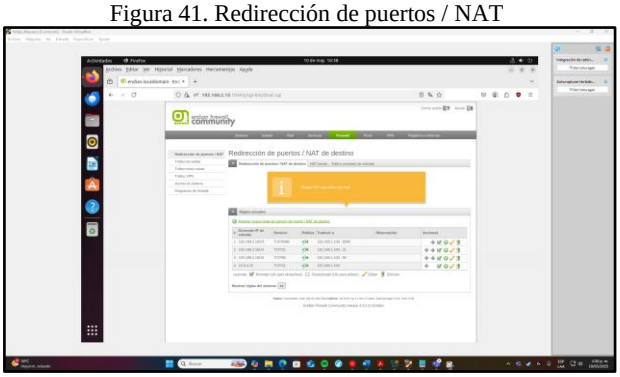
Prueba de conexión FTP: establecimiento de sesión exitosa desde cliente remoto.

Bloqueo de ICMP verificado: intento de ping al servidor DMZ resultó en mensaje "Destination Host Unreachable".

4.4 REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO

Diseñar y configurar reglas de acceso entre distintas zonas de una infraestructura, asegurando una comunicación efectiva y segura mediante los protocolos HTTP y FTP. Además, se pretende verificar la correcta aplicación de dichas reglas y su funcionalidad mediante pruebas de acceso desde un navegador web y otras herramientas de red.

Figura 41. Redirección de puertos / NAT



Fuente: Autoría propia

Se han configurado reglas de NAT en el módulo de reglas para permitir la redirección de puertos HTTP y FTP, estableciendo la conexión entre la zona de internet y la DMZ. Estas reglas garantizan el acceso controlado desde el exterior a servicios internos, optimizando la seguridad y gestión del tráfico de red

Regla 1, conexión zona internet con DMZ

Dirección IP origen: 192.168.2.16/24
Servicio: TCP/8080
IP destino traducido: 192.168.1.130:8080

Regla 2, FTP puerto 21

Dirección IP origen: 192.168.2.16/24
Servicio: TCP/21
IP destino traducido: 192.168.1.100:21

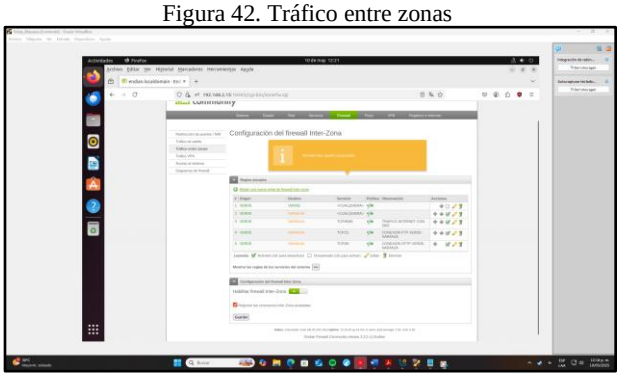
Regla 3, HTTP Puerto 80

Dirección IP origen: 192.168.2.16/24
Servicio: TCP/80
IP destino traducido: 192.168.1.100:21

Regla 4, WAN - FTP Puerto 21

Dirección IP origen: 10.0.4.15
Servicio: TCP/21
IP destino traducido: 192.168.1.100:21

Figura 42. Tráfico entre zonas



Fuente: Autoría propia

Se implementó una configuración de firewall Interzona con el fin de controlar y segmentar el tráfico entre la red interna (zona VERDE) y la zona desmilitarizada (DMZ, zona NARANJA). Esta segmentación permitió aplicar políticas específicas para habilitar solo los servicios estrictamente necesarios

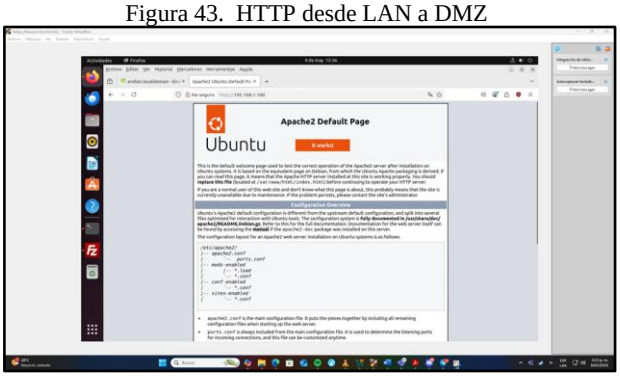
Las siguientes reglas fueron establecidas:

Regla 3: Se permitió el tráfico desde la zona VERDE hacia la zona NARANJA mediante el puerto TCP/8080, utilizado para servicios web alternativos.

Regla 4: Se habilitó el acceso por medio del protocolo FTP (TCP/21), permitiendo transferencias de archivos entre cliente interno y servidor alojado en la DMZ.

Regla 5: Se autorizó el tráfico HTTP (TCP/80) para el acceso a aplicaciones web públicas alojadas en la zona intermedia.

Figura 43. HTTP desde LAN a DMZ



Fuente: Autoría propia

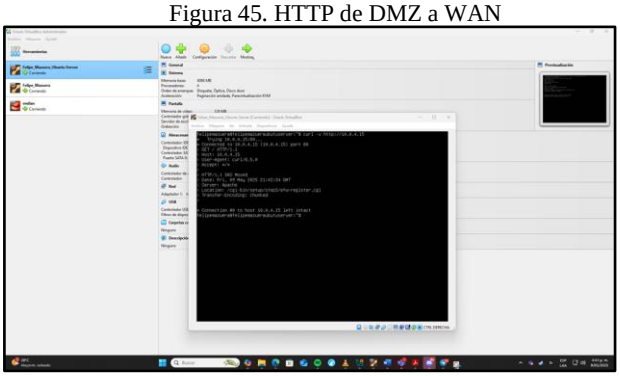
Se verificó el acceso al servidor ubicado en la zona DMZ utilizando el navegador y la dirección IP http://192.168.1.100:80. La conexión se estableció correctamente, confirmando que el servicio HTTP está operando como se esperaba y es accesible desde la red configurada (ver Figura 43).

Figura 44. HTTP de LAN a WAN

Fuente: Autoría propia

Se llevaron a cabo pruebas tras la configuración del tráfico entre zonas. Para verificar la conectividad, se accedió al servidor en la zona DMZ a través del navegador utilizando la dirección IP http://10.0.4.15:80. La conexión se estableció correctamente, confirmando el acceso al servicio HTTP desde la WAN. (ver Figura 44).

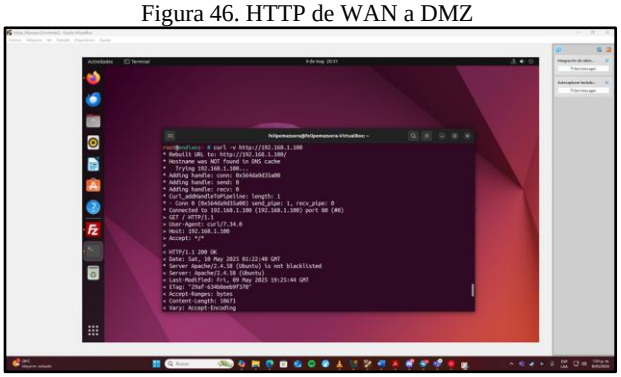
Figura 45. HTTP de DMZ a WAN



Fuente: Autoría propia

Se ejecuta la prueba utilizando el comando curl -v http://10.0.4.15, lo que permite verificar la conexión al servicio HTTP desde la zona DMZ hacia la WAN. Mediante esta acción, se observa el comportamiento de la comunicación y la respuesta del servidor en la dirección especificada (ver Figura 45).

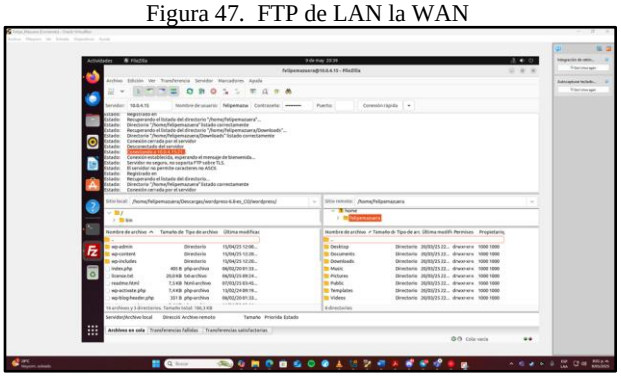
Figura 46. HTTP de WAN a DMZ



Fuente: Autoría propia

Se establece la conexión mediante SSH desde Ubuntu Desktop a través del terminal, accediendo al servidor de firewall en Endian. A continuación, se procede a realizar la prueba de HTTP desde la WAN hacia la zona DMZ, verificando la correcta comunicación y acceso al servidor web ubicado en la DMZ. (ver Figura 46).

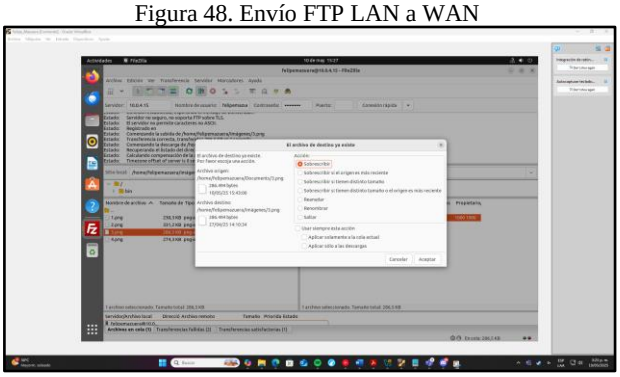
Figura 47. FTP de LAN la WAN



Fuente: Autoría propia

Se estableció la conexión al servicio FTP utilizando la herramienta FileZilla. Para ello, se emplea la dirección de la WAN 10.0.4.15 y el puerto 21, ingresando las credenciales correspondientes. La conexión se realiza de manera exitosa, permitiendo el acceso al servidor y la gestión de archivos de forma remota.

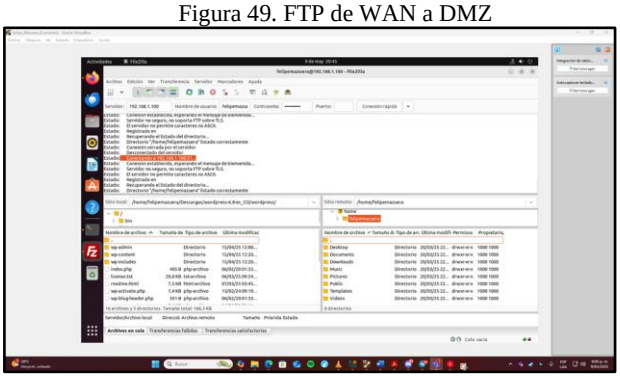
Figura 48. Envío FTP LAN a WAN



Fuente: Autoría propia

El envío de archivos se efectúa desde Ubuntu Desktop a través del servicio FTP, el cual está conectado a la WAN con la dirección 10.0.4.15 y el puerto 21. Para el acceso, se utilizan las credenciales correspondientes, garantizando una conexión adecuada al servidor.

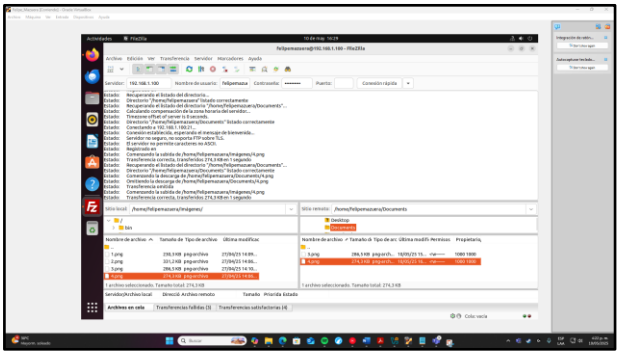
Figura 49. FTP de WAN a DMZ



Fuente: Autoría propia

Se estableció la conexión al servicio FTP a través de FileZilla, utilizando la dirección IP del servidor 192.168.1.100 en la zona DMZ y el puerto 21. La autenticación se realiza con éxito, permitiendo el acceso al servidor y la gestión de archivos de manera remota.

Figura 50. Envío de ftp WAN a DMZ



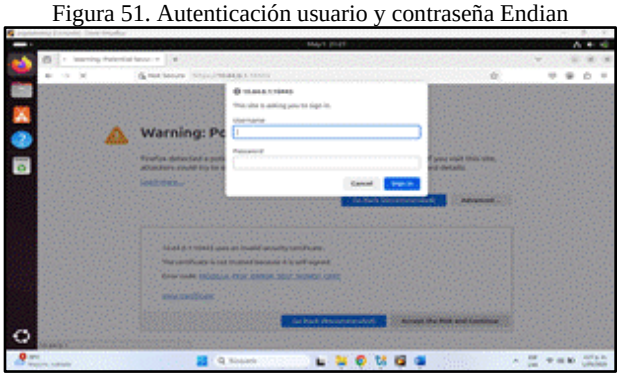
Fuente: Autoría propia

Se efectúa el envío de un archivo desde Ubuntu Desktop utilizando el servicio FTP, el cual está conectado al servidor en la zona DMZ. La transferencia se realiza correctamente tras la autenticación con las credenciales correspondientes, permitiendo la gestión de archivos en el servidor destino

4.5 IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE) CON POLÍTICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET.

Crear un perfil y establecer una lista negra que bloquee los sitios www.hotmail.com, www.youtube.com y www.elnuevodia.com.co. Además, se debe implementar la autenticación por usuario, creando un usuario y asignándole a un grupo, estableciendo una política de acceso y vinculando esta política con el perfil creado. Finalmente, se debe probar el acceso a los sitios bloqueados desde la LAN utilizando un navegador web.

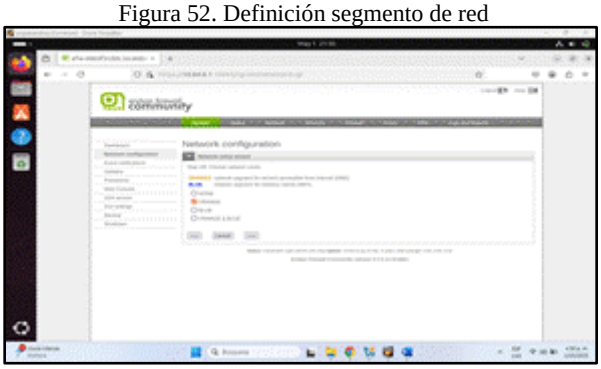
Figura 51. Autenticación usuario y contraseña Endian



Fuente: Autoría propia

Se ingresa usuario y contraseña y le da click en sing in, se dirige al módulo de Network configuración y se procedemos a configurar RED de manera DHCP

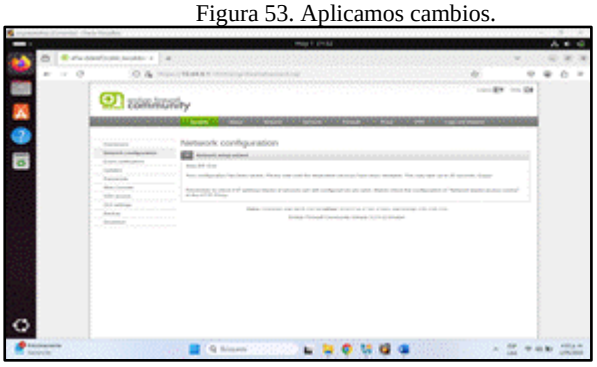
Figura 52. Definición segmento de red



Fuente: Autoría propia

Se configura el tipo de red para las zonas del firewall. Se selecciona ORANGE para definir el segmento de red que será accesible desde Internet (DMZ). Se confirman las ip de GREEN 10.64.0.1 y ORANGE 10.128.0.1. De igual forma se confirma RED DHCP.

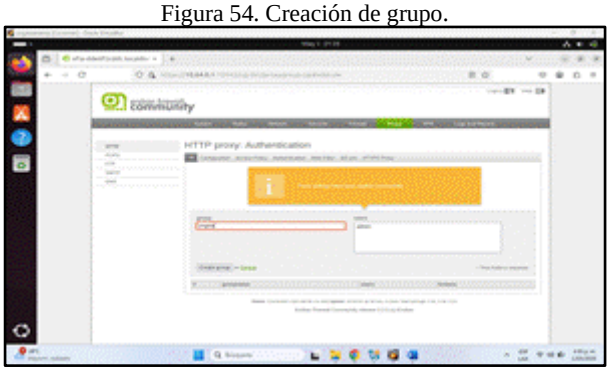
Figura 53. Aplicamos cambios.



Fuente: Autoría propia

Se crea el usuario en el módulo de autenticación. Además, se crea el grupo llamado angela y se asocia el usuario admin a dicho grupo.

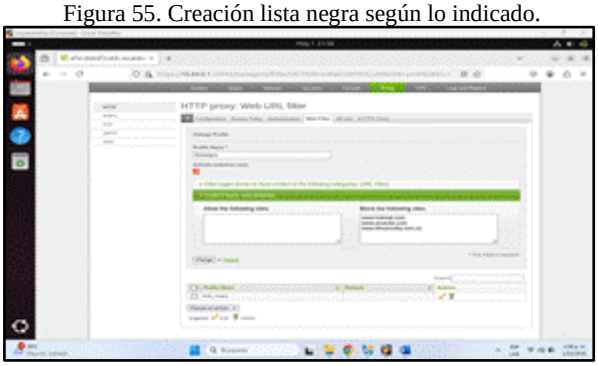
Figura 54. Creación de grupo.



Fuente: Autoría propia

Se dirige al módulo Configuración y se habilita el servicio de Proxy por medio de Enable HTTP Proxy y se configura con el puerto 8080. Se crea un nuevo filtro con el nombre listanegra, donde se bloquean 3 páginas, www.hotmail.com, www.youtube.com, www.elnuevodia.com.co se aplica y se guarda los cambios.

Figura 55. Creación lista negra según lo indicado.



Fuente: Autoría propia

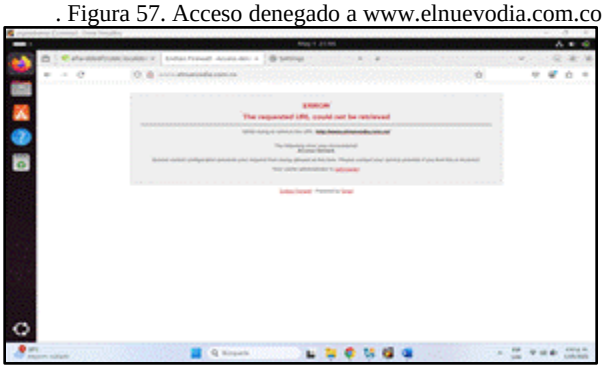
Se crea una política de acceso donde se asocia el usuario admin, le da que apruebe la regla que se creó llamada listanegra y se llena la demás configuración. Se va a la configuración de proxy en el buscador Firefox y manualmente se configura el Proxy donde se coloca 10.64.0.1 y se le indica usar el mismo proxy en HTTPS.

Figura 56. Configuración de proxy en Firefox.

Fuente: Autoría propia

Se hace la prueba ingresando a la página www.hotmail.com y esta pide autenticación de usuario y contraseña, después de colocar la autenticación muestra el siguiente mensaje de Acceso denegado de www.hotmail.com, De igual forma se prueba entrar a www.youtube.com y muestra el siguiente mensaje, por último, se prueba entrar a www.elnuevodia.com.co, verificando que no se puede ingresar.

. Figura 57. Acceso denegado a www.elnuevodia.com.co



Fuente: Autoría propia

4 CONCLUSIONES

La implementación de GNU/Linux Endian Firewall permite establecer una arquitectura de seguridad robusta mediante la segmentación efectiva en tres zonas (verde, roja y naranja), lo que facilita el control del tráfico de red y minimiza los riesgos de seguridad.

La configuración de reglas NAT demostró ser fundamental para permitir la comunicación controlada entre las diferentes zonas de red, habilitando el acceso a Internet desde la LAN y la DMZ mientras se mantiene un nivel adecuado de seguridad.

El filtrado de servicios específicos (HTTP y FTP) y el bloqueo del protocolo ICMP permitieron establecer un control granular sobre las comunicaciones, lo que resulta esencial para reducir la superficie de ataque y proteger los recursos críticos.

La implementación del proxy HTTP no transparente con autenticación y listas negras proporciona un mecanismo efectivo para controlar el acceso a Internet de los usuarios internos, permitiendo aplicar políticas de uso aceptable y

restringir el acceso a sitios no autorizados.

Las pruebas realizadas confirmaron la efectividad del sistema para aplicar las políticas de seguridad configuradas, demostrando que un firewall basado en GNU/Linux puede ofrecer una solución de seguridad completa y adaptable a diferentes necesidades organizacionales.

5 REFERENCIAS

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

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

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

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

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

[6]Oracle (2020). Manual de usuario VirtualBox . Disponible en: https://www.virtualbox.org/manual/
.