Implementación de Zona Desmilitarizada (DMZ) y Políticas de Acceso en Endian Firewall para Intranets GNU/Linux, con el fin de optimizar la seguridad Perimetral.

Margith Viviana Lemus Castro
mvlemusc@unadvirtual.edu.co
José Luis Gracia Perafan
jlgraciap@unadvirtual.edu.co
Yudy Estefany Sánchez Montes
yesanchezm@unadvirtual.edu.co
Juan Camilo Bustos Silva
jcbustoss@unadvirtual.edu.co

RESUMEN: *Este artículo detalla la implementación de seguridad perimetral mediante la instalación de Endian Firewall (EFW) en un entorno VirtualBox, el desarrollo de cada una de las temáticas se centra en la configuración de tres interfaces de red clave, las cuales son: la zona verde (LAN), la zona roja (WAN) y la zona naranja (DMZ) llevando así a establecer una arquitectura de red segmentada y segura aplicando la funcionalidad de traducción de direcciones de red (NAT) para facilitar la conectividad a Internet desde las zonas LAN y DMZ, tomando en cuenta la seguridad de la red, se crearon reglas de firewall para permitir el tráfico necesario de servicios como HTTP (80) y FTP (21) desde la DMZ , demostrando así el bloqueo de tráfico potencialmente peligroso como el protocolo ICMP (ping). Como resultado se definieron reglas para controlar el flujo de comunicación interzona, demostrando la conectividad requerida entre la LAN, la DMZ y la WAN para los servicios configurados.*

PALABRAS CLAVE: Endian, LAN, Red, WAN, DMZ, HTTP, Firewall, Protocolo, Segmentación.

1 INTRODUCCIÓN

En la actualidad, la seguridad en las redes informáticas se ha convertido en una prioridad esencial, este ya no se trata de un extra, sino de un requisito necesario para proteger la información y mantener la integridad de los sistemas. En este contexto, los *firewalls* cumplen el papel de guardianes digitales los cuales supervisan y controlan el tráfico que entra y sale de la red permitiendo únicamente lo que es seguro y bloqueando posibles amenazas.

Endian Firewall (EFW) aparece como una solución ideal para quienes buscan una herramienta potente, gratuita y basada en GNU/Linux, su gran ventaja es que no necesita hardware especializado ni altas inversiones por lo que resulta perfecto para entornos educativos, laboratorios de prueba o pequeñas implementaciones reales.

Para poner en práctica su funcionamiento, se utilizó VirtualBox como entorno de simulación lo cual permite recrear redes reales sin afectar la infraestructura física. Dentro de este laboratorio virtual se configuraron tres zonas de seguridad, estas son la zona Verde (LAN) destinada a la red interna, la Roja (WAN) conectada a Internet, y la Naranja (DMZ) reservada para servicios públicos como servidores web o FTP. Cada una cumple un rol clave dentro de una arquitectura defensiva moderna.

Durante la instalación de Endian Firewall (EFW) se activan funciones esenciales como el NAT, que permite que los dispositivos internos y los de la DMZ accedan a Internet utilizando la IP pública del firewall. Además, se establecen políticas de filtrado para habilitar únicamente los servicios necesarios y restringir protocolos como ICMP, reduciendo así la superficie de ataque, por otro lado, se crean reglas para controlar qué tipo de tráfico que puede circular entre las diferentes zonas, logrando una red segmentada, segura y funcional.

Este artículo presenta de forma clara y práctica la configuración completa de este entorno de red utilizando Endian Firewall como sistema de seguridad perimetral aplicando buenas prácticas que refuerzan la protección del sistema y permiten comprender los fundamentos de la seguridad en redes modernas.

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

2.1 INSTALACIÓN Y CONFIGURACIÓN

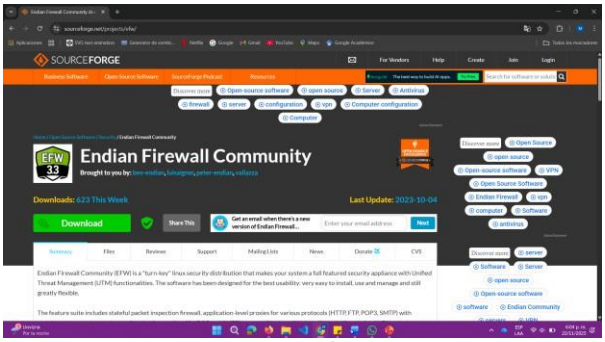
De la presente temática se detalla el proceso de instalación, configuración y verificación de un firewall de código abierto, Endian Firewall Community (EFW), utilizando un entorno virtualizado para crear una arquitectura de red segmentada en tres zonas de seguridad.

2.1.1 CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX

Se realiza la descarga de Endian Firewall directamente desde la página oficial, para posteriormente realizar la creación de la máquina virtual y la respectiva instalación, esto con la finalidad de segmentar efectivamente la red para maximizar la

seguridad y el control de acceso entre los distintos niveles de confianza.

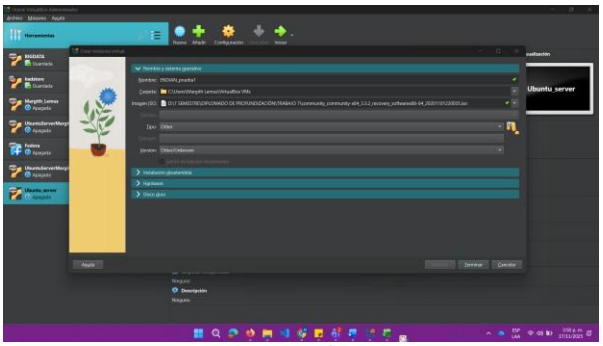
Ilustración 1 Descarga de Endian Firewall



Fuente: Autoría propia

Se debe asignar un nombre para la nueva máquina virtual que crearemos, en este caso con la distribución Endian Firewall que es una distribución GNU/Linux especializada en seguridad de redes.

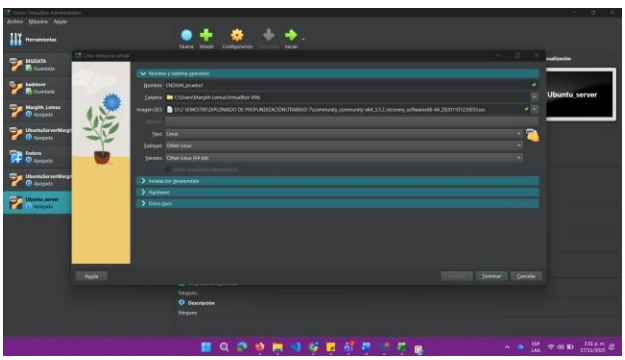
Ilustración 2 Creación de la máquina virtual para Endian, creación de nombre.



Fuente: Autoría propia

Se debe cargar la imagen ISO de la distribución y antes de continuar configuramos para que quede como una distribución de tipo Linux, y con la correspondiente versión de 64 bit.

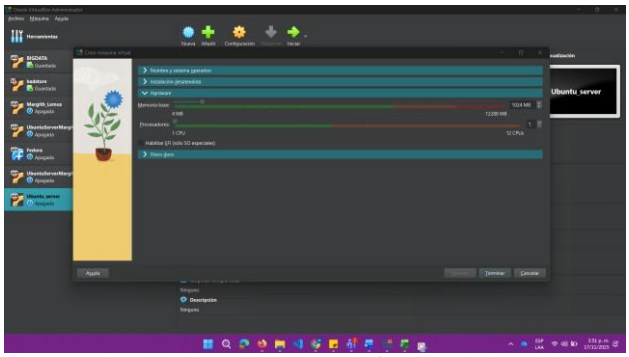
Ilustración 3 Insertar imagen .ISO



Fuente: Autoría propia

Se asigna la capacidad de memoria RAM que utilizará, para este caso 1024 MB y solamente un núcleo del procesador.

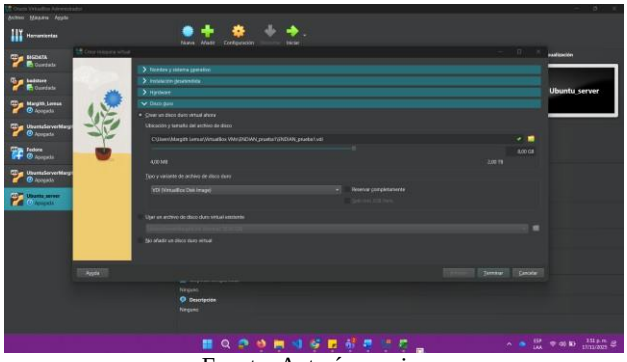
Ilustración 4 Definir capacidad de la memoria base



Fuente: Autoría propia

Para la asignación de la capacidad del disco duro virtual, dejaremos la capacidad que trae por defecto sin realizar ningún cambio.

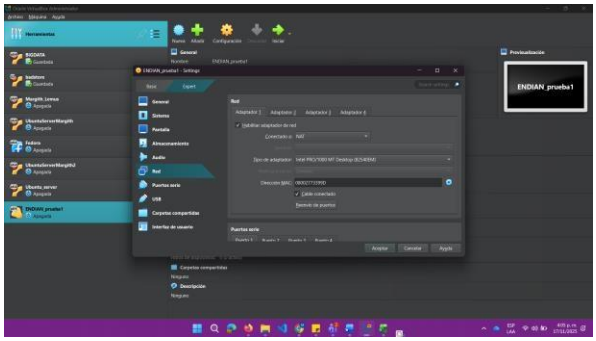
Ilustración 5 Definir capacidad del disco duro virtual.



Fuente: Autoría propia

Previa a la instalación de la distribución se deben configurar los adaptadores para posteriormente realizar la delimitación de las zonas verde, roja y naranja. Para este punto se esta configurando el primer adaptador que será la zona roja conectado como red NAT, en este caso será la zona que permite el acceso a internet (WAN)

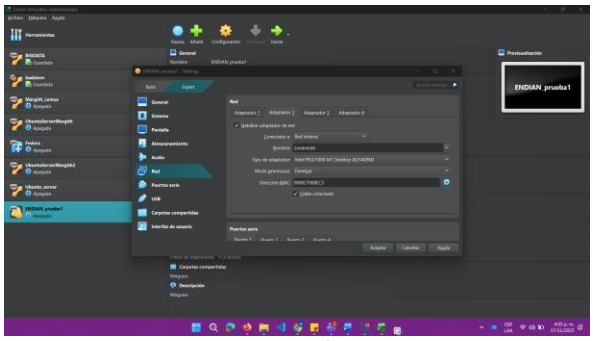
Ilustración 6 Definir adaptador de red para Zona roja



Fuente: Autoría propia

Para este punto se configura el adaptador de la zona verde, indicando que estará conectado a la red interna (LAN) y será el adaptador 2.

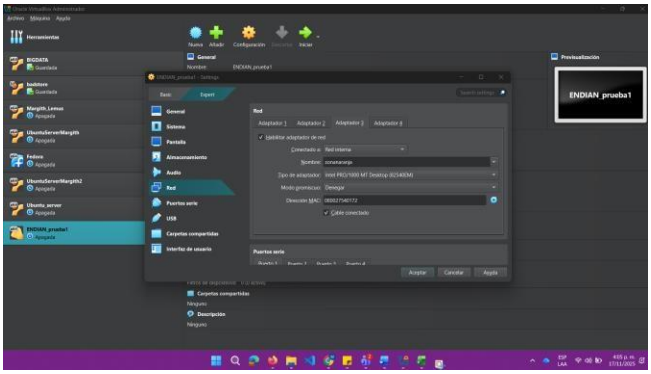
Ilustración 7 Definir adaptador de red para Zona verde



Fuente: Autoría propia

Para este punto se configura el adaptador de la zona naranja, indicando que estará conectado a la red interna, para tener acceso a servidores (DMZ) y será el adaptador 3.

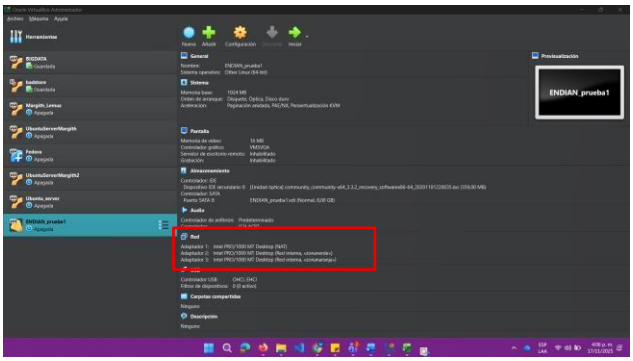
Ilustración 8 Definir adaptador de red para Zona naranja



Fuente: Autoría propia

Por último, antes de iniciar la máquina para la respectiva configuración, verificamos que se han configurado adecuadamente los adaptadores de red para cada una de las zonas.

Ilustración 9 Verificación de configuración de los adaptadores de red

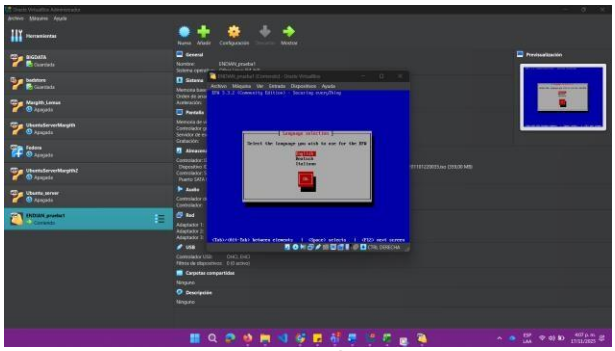


Fuente: Autoría propia

2.1.2 INSTALACIÓN EFECTIVA DE ENDIAN Y CONFIGURACIÓN DE LAS ZONAS DE RED

Iniciamos la máquina eligiendo idioma inglés para el uso de esta distribución y continuamos con el proceso.

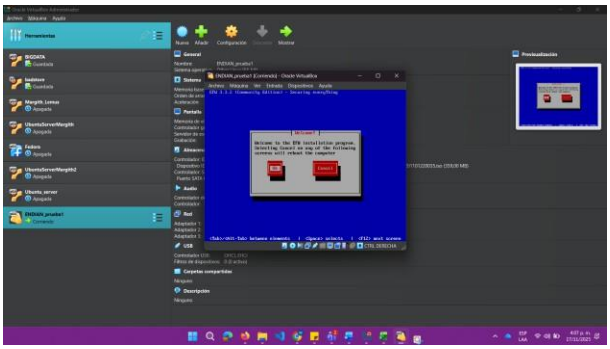
Ilustración 10 Configuración para GNU/Linux Endian



Fuente: Autoría propia

En este punto debemos aceptar, para poder comenzar a realizar la respectiva instalación.

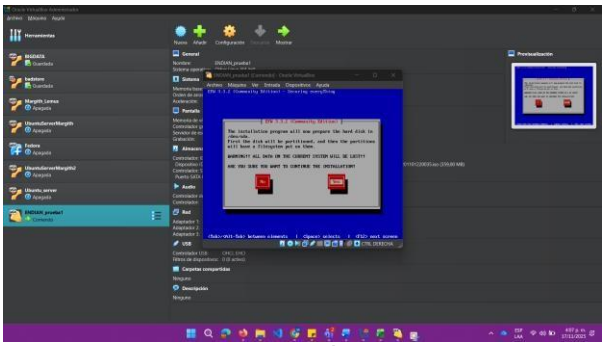
Ilustración 11 Aceptar reinicio de la maquina



Fuente: Autoría propia

Se muestra en pantalla la advertencia que indica que el programa de instalación ahora preparará el disco duro en /dev/sda, indicando como advertencia que toda la información en el sistema actual se perderá.

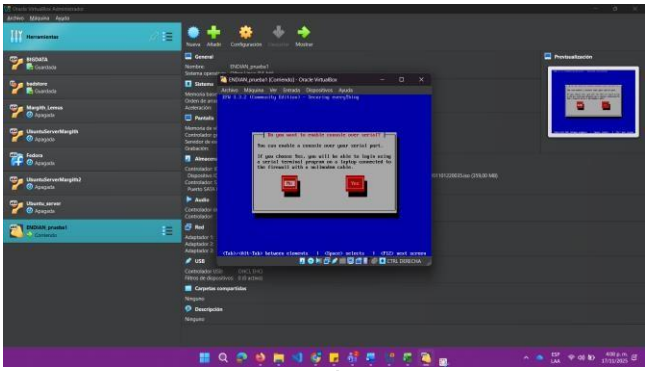
Ilustración 12 Instalar dependencias



Fuente: Autoría propia

Para este punto no aceptaremos que se pueda habilitar una consola a través de su puerto serial.

Ilustración 13 No habilitar una consola a través de tu puerto serial



Fuente: Autoría propia

La tabla define la configuración de tres adaptadores de red distintos, cada uno conectado a una zona de red con reglas y propósitos diferentes, está el adaptador 1 (Zona Roja - Internet/WAN), el adaptador 2 (Zona Verde - Red Local Confiable) y el adaptador 3 (Zona Naranja - DMZ/Red Desmilitarizada). Es una arquitectura de red de firewall de tres patas (Red, Verde, Naranja).

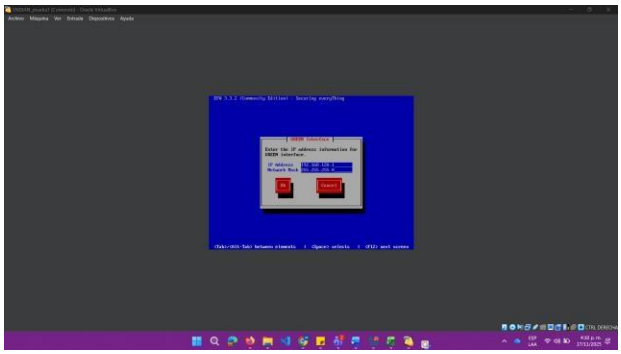
Ilustración 14 Definición de IP

	Adaptador1	Adaptador2:zona verde	Adaptador3: zona naranja
IP	NAT	192.168.120.0/24	192.168.150.0/24
DHCP	DHCP activado	DHCP desactivado	DHCP desactivado
Puerta de enlace	N/A	192.168.120.1	192.168.150.1
Mascara de red		255.255.255.0	255.255.255.0
Rango de ip		192.168.120.2 - 192.168.120.253	192.168.150.2 - 192.168.150.253

Fuente: Autoría propia

Desde la interfaz de instalación para Endian, se ingresa la IP de la zona verde, con la respectiva máscara de red y continuamos con la instalación.

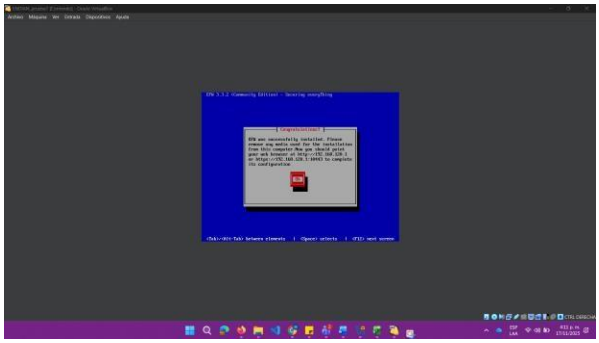
Ilustración 15 Asignación de IP para la zona verde



Fuente: Autoría propia

Para este punto el firewall ya está en funcionamiento, y la dirección 192.168.120.1 es la IP de la interfaz de administración.

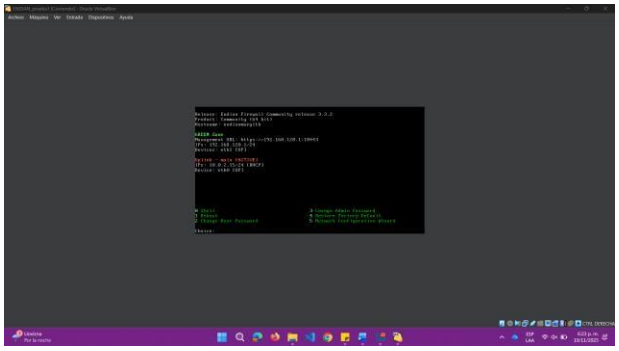
Ilustración 16 Indicación para utilizar navegador web https://192.168.120.1:10443



Fuente: Autoría propia

La interfaz esta lista para comenzar a establecer las reglas, usuarios, y servicios.

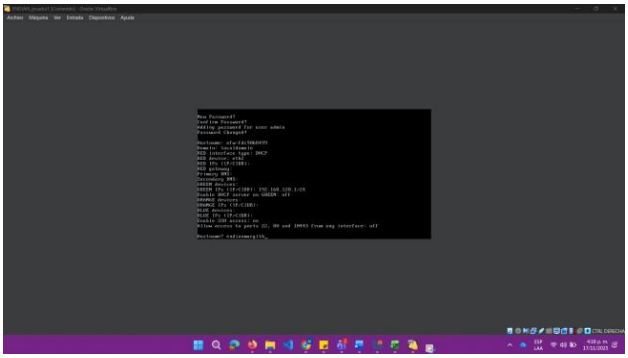
Ilustración 17 Comprobante de implementación de GNU/Linux Endian con las zonas verde, roja y naranja.



Fuente: Autoría propia

El sistema ya instaló el firewall, cambió la contraseña del administrador y configuró la interfaz de Internet (Roja) para usar DHCP y la interfaz interna (Verde) con una IP estática (192.168.120.1). El paso siguiente es la asignación de un nuevo nombre del host, y continua la configuración.

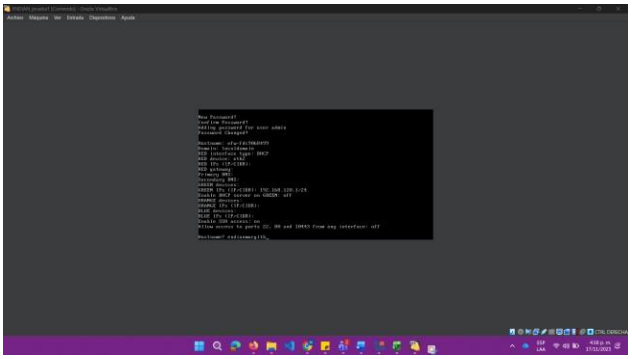
Ilustración 18 Configuración para delimitar las zonas verde, roja y naranja.



Fuente: Autoría propia

Para este punto ha finalizado la asignación física de las tres tarjetas de red (eth0, eth1, eth2) a las tres zonas lógicas (Roja, Verde, Naranja) del firewall, y ha confirmado los parámetros de IP y DNS.

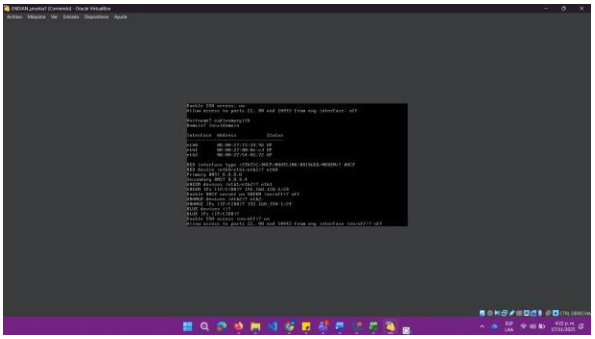
Ilustración 19 Configuración para delimitar las zonas verde, roja y naranja.



Fuente: Autoría propia

Para este punto ha finalizado la asignación física de las tres tarjetas de red (eth0, eth1, eth2) a las tres zonas lógicas (Roja, Verde, Naranja) del firewall, y ha confirmado los parámetros de IP y DNS.

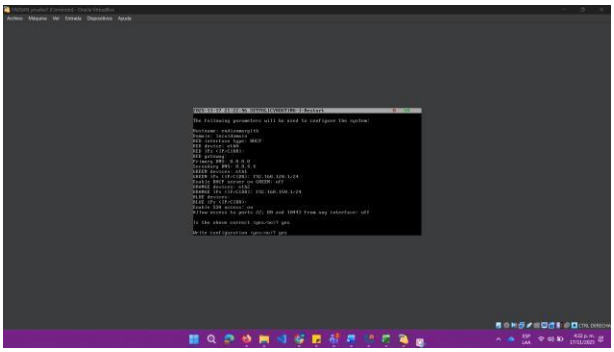
Ilustración 20 Configuración para delimitar las zonas verde, roja y naranja.



Fuente: Autoría propia

En este momento se ha finalizado la configuración de red en la consola. Después de responder "yes" a ambas preguntas, el firewall aplicará la segmentación de red (eth0 = Internet, eth1 = LAN, eth2 = DMZ) y estará listo para ser administrado a través de su interfaz web en la IP 192.168.120.1

Ilustración 21 Configuración para delimitar las zonas verde, roja y naranja.

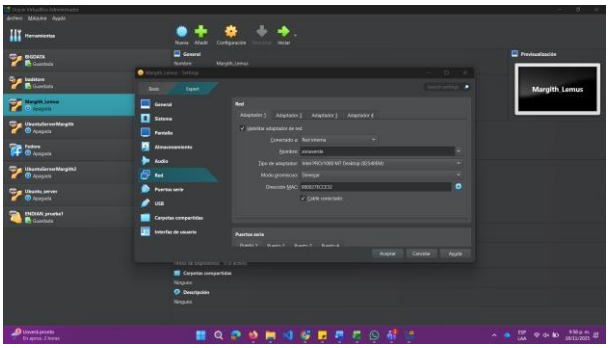


Fuente: Autoría propia

2.1.3 CONFIGURACIÓN MANUAL DE UNA DIRECCIÓN IP ESTÁTICA EN UN SISTEMA UBUNTU DESKTOP

Para realizar la asignación de la IP fija en Ubuntu desktop, primero seleccionamos como adaptador principal, la red interna que en este caso es la zona verde.

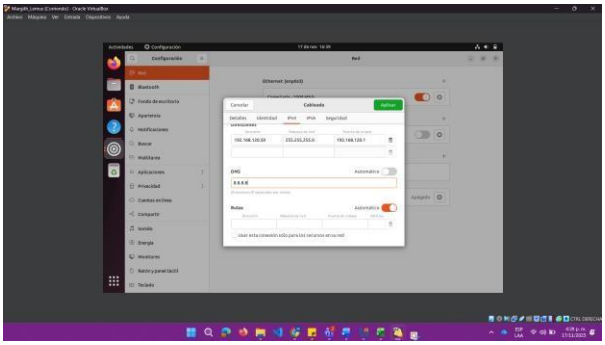
Ilustración 22 Configuración de Adaptador de red, para red interna- zona verde (LAN)



Fuente: Autoría propia

Se asigna una identidad IP válida y la ruta de salida (Puerta de enlace) al cliente para que sea parte de la red local segura (Zona Verde), cumpliendo con la configuración estricta definida en el firewall.

Ilustración 23 Asignación de IP para Ubuntu Desktop - Zona Verde



Fuente: Autoría propia

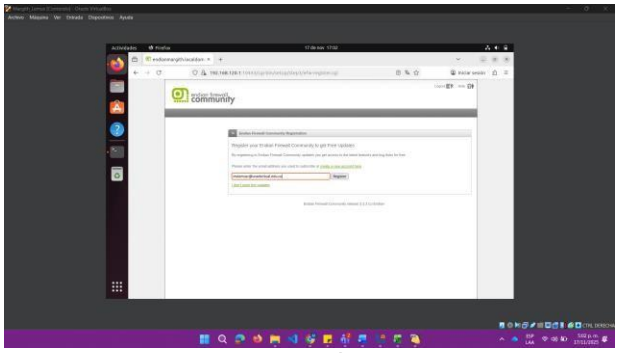
Esta es la verificación final de la conectividad de Ubuntu Desktop (cliente de la Zona Verde) con el firewall EFW (la Puerta de Enlace). Mostrando la configuración de las interfaces de red y la tabla de enrutamiento, confirmando cómo el tráfico saldrá de la red local.

Ilustración 24 Validación de funcionalidad de red, y correcta asignación de IP

Fuente: Autoría propia

El sistema ha completado la instalación de consola, la red de la Zona Verde está operativa, y ahora comienza la fase de configuración final y registro del firewall a través de la interfaz gráfica web.

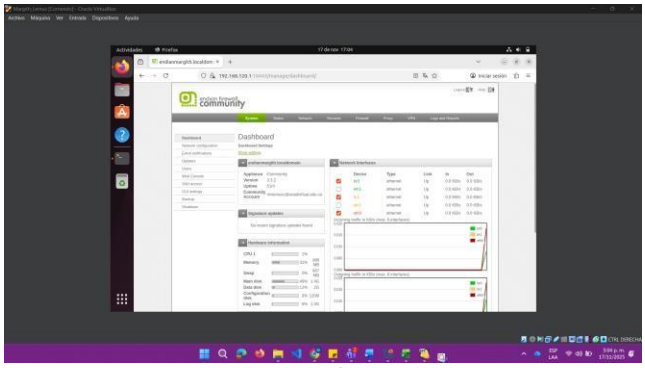
Ilustración 25 Confirmación del correo en la comunidad firewall endian



Fuente: Autoría propia

Endian Firewall está operacional, sus interfaces de red están activas y mapeadas según la configuración de zonas (Roja/Verde/Naranja), y su hardware está estable (uso bajo de CPU/Memoria).

Ilustración 26 Vista de configuración correcta en la delimitación de las zonas verde, roja y naranja.

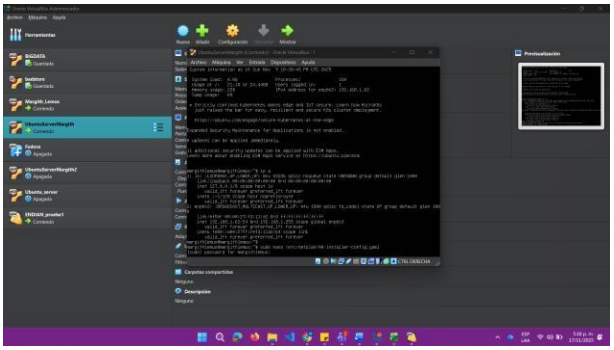


Fuente: Autoría propia

2.1.4 CONFIGURACIÓN MANUAL DE UNA DIRECCIÓN IP ESTÁTICA EN UN SISTEMA UBUNTU SERVER

Para poder iniciar la configuración de red para tu Ubuntu Server, que está destinado a ser un servidor en la Zona Naranja (DMZ), editaremos el archivo Netplan para cambiar la configuración de la interfaz enp0s3 de la IP dinámica actual (192.168.1.62) a una IP estática válida dentro de la Zona Naranja (192.168.150.x), usando la Puerta de Enlace 192.168.150.1 (el firewall EFW).

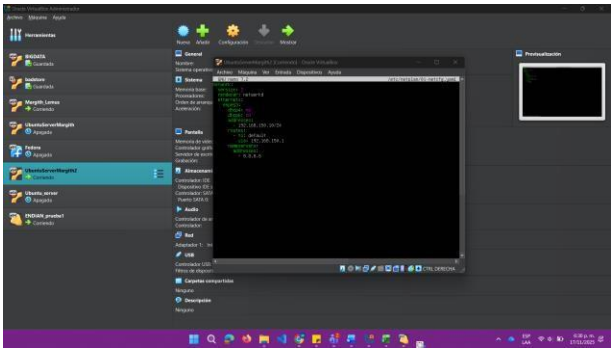
Ilustración 27 Configuración para asignación de IP fija en Ubuntu server - Zona Naranja



Fuente: Autoría propia

Se configura de forma estricta la IP estática 192.168.150.10, asegurando que utilice el firewall EFW (192.168.150.1) como su única ruta para acceder a otras redes, cumpliendo así con la definición de un servidor en la Zona Naranja (DMZ).

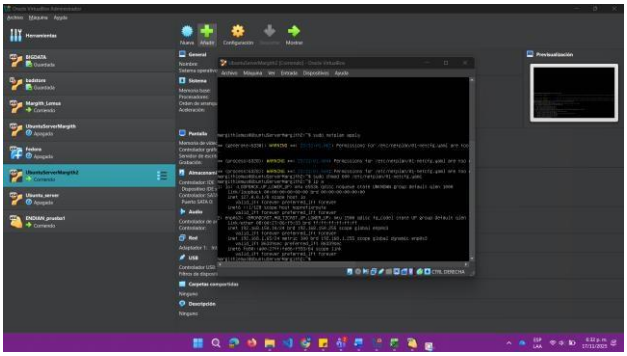
Ilustración 28 Asignación de IP fija mediante edición de archivo nano



Fuente: Autoría propia

Se ha logrado configurar la IP estática en el servidor de la Zona Naranja, resolviste un error común de permisos de Linux, y verificando que la dirección IP 192.168.150.10 ya está asignada al servidor, completando su preparación para la DMZ.

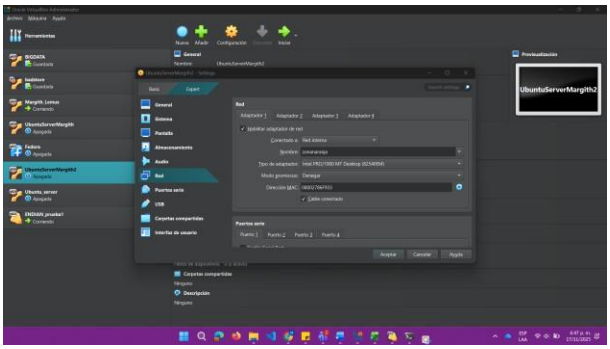
Ilustración 29 Aplicación de cambios y confirmación de IP fija correctamente asignada.



Fuente: Autoría propia

Como configuración de VirtualBox para conectar tu Ubuntu Server (el servidor de la Zona Naranja) al firewall EFW escogemos el adaptador 1 del servidor DMZ para que se conecte a un segmento de red virtual aislado llamado zona naranja.

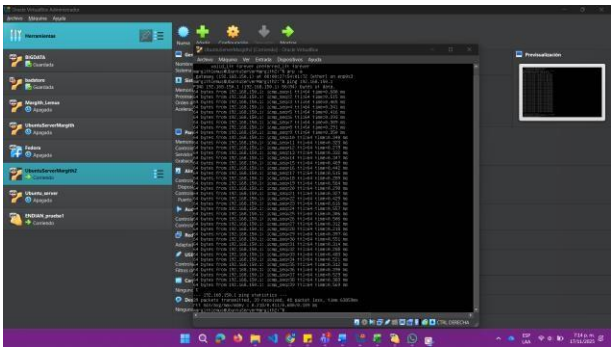
Ilustración 30 Activar el adaptador para red interna - Zona naranja



Fuente: Autoría propia

Esta es la prueba que confirma que Ubuntu Server de la Zona Naranja (192.168.150.10) está perfectamente conectado y comunicado con la interfaz de la Zona Naranja del firewall EFW (192.168.150.1).

Ilustración 31 Ping para validar conexión de la zona naranja.



Fuente: Autoría propia

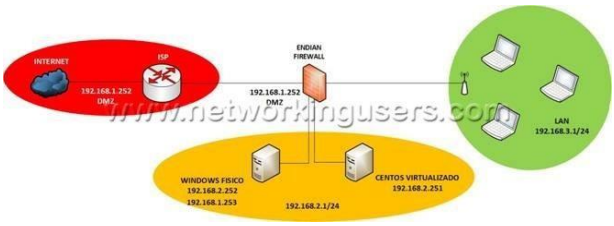
3 TEMÁTICA 2: CONFIGURACIÓN NAT.

La configuración de NAT es muy clave para la seguridad y eficiencia de las redes ya que esta nos permite ocultar las direcciones IP internas, controlar el tráfico entre la LAN (nuestra IP personal), la DMZ y la Internet, y optimizar el uso de direcciones IP públicas con esto nos facilita el acceso seguro a servicios expuestos al exterior y mantiene encerradas diferentes zonas de la red para

garantizar la conectividad como protección de nuestros recursos internos.
Se realizará reglas de NAT por medio de firewall ENDIAN para permitir la comunicación

3.1 TOPOLOGÍA DE RED

Ilustración 32 Topología de red



Fuente: Fig. 1. Topología de red. Adaptado de "Parte 1: Instalación y configuración de Endian Firewall Community" por A. Granada, 2014, *Blog para admins de redes y webmasters*. Recuperado de https://networkingusers.blogspot.com/2014

3.1.1 ARQUITECTURA

Se procedió a la implementación de las zonas de red dentro del firewall, clasificándolas según su nivel de seguridad y funcionalidad:

1. **Zona verde (LAN)**: Corresponde a la red interna de la organización, donde se ubican los dispositivos de los usuarios finales. Esta zona se configura como **Red Interna**, asignándole un rango de direcciones IP privadas para garantizar la comunicación segura y eficiente entre los equipos internos.

2. **Zona naranja (DMZ)**: Destinada a alojar los servidores que requieren acceso tanto desde la red interna como desde Internet, como servidores web, correo o FTP. También se configura como **Red Interna**, pero con políticas de acceso más estrictas para limitar la exposición de los servicios a posibles amenazas externas.

3. **Zona roja (WAN)**: Representa la conexión hacia Internet, la cual es una red de alta concurrencia y exposición. Esta zona se configura como **Red NAT**, permitiendo que los dispositivos internos accedan a Internet mediante traducción de direcciones, mientras se protege la identidad de las direcciones privadas internas y se controla el tráfico entrante y saliente mediante reglas de firewall.

Cada zona se configura con su respectivo rango de IP, máscara de subred y políticas de seguridad, asegurando así una segmentación adecuada y un control granular del tráfico dentro de la infraestructura de red.

Tabla 1 NAT e IP

Zona	Interfaz VirtualBox	Tipo de Red	IP
Roja (WAN)	Adaptador 1	NAT	10.0.2.15/24
Verde (LAN)	Adaptador 2	Red Interna	192.168.120.1
Naranja(DMZ)	Adaptador 3	Red Interna	192.168.150.1

Fuente: Autoría propia

3.1.2 PUERTOS Y TIPOS DE NAT

NAT es como un portero que traduce los nombres de tus dispositivos dentro de casa a un solo nombre público cuando salen a Internet, y viceversa.

- SNAT (salida a Internet): Cambia tu IP interna a la IP pública para que todos tus dispositivos puedan usar Internet con una sola dirección.

- DNAT (llegada desde Internet): Recibe los datos que vienen de afuera y los manda al dispositivo correcto dentro de tu red.

- Port Forwarding: Igual que DNAT, pero redirige a un puerto específico para que llegue al servicio exacto.

3.2 COMUNICACIÓN DESDE LA LAN HACIA LA WAN

Durante la práctica usamos Endian como un "puente de seguridad" entre la computadora de la LAN (Ubuntu Desktop) y la red externa que simula Internet, gracias a este se permitió que la máquina accediera a Internet usando NAT, traduciendo la dirección interna a una sola dirección visible hacia afuera, con

esto protegemos la red y permite que varias computadoras compartan la misma conexión.

Para corroborar la comunicación la realizamos con una navegación funcionando correctamente, lo que confirma que la salida de la LAN hacia la WAN está bien configurada.

Ilustración 33 Enlace LAN a WAN mediante red simulada (HTTP)

Fuente: Autoría propia

3.2.1 ACCESO A INTERNET EN UBUNTU DESKTOP

1. Acceso a la máquina virtual: Se ingresa a la máquina virtual que ejecuta Ubuntu Desktop. Inicialmente, se verifica la conectividad de red, observándose que no hay acceso a Internet.

2. Acceso a la configuración de red: Se abre el menú Inicio → Configuración → Red, donde se presentan las opciones de conexión cableada o inalámbrica.

3. Configuración de IPv4:

- Se selecciona la pestaña IPv4 y se establece el método manual.
- Se ingresan los parámetros de red requeridos:
- Dirección IP de la máquina.
- Máscara de subred correspondiente a la red interna.
- Puerta de enlace (Gateway), que conecta la red interna con la WAN.
- Servidor DNS, en este caso se utiliza el DNS público de Google (8.8.8.8).

4. Aplicación de la configuración: Se guardan los cambios y se activa la conexión de red.

5. Verificación de conectividad: Se realiza una prueba de conexión a Internet mediante ping a una dirección externa o navegación web, confirmando que Ubuntu Desktop tiene acceso correcto a la WAN

3.3 Comunicación desde la DMZ (Zona Naranja) hacia Internet mediante DNAT

Para que los servidores de la DMZ puedan ser accesibles desde Internet, se usa DNAT. Esta opción en Endian permite que cuando alguien desde afuera quiera entrar a un servicio (por ejemplo, un servidor web), el firewall redirija ese tráfico a la IP privada del servidor en la DMZ. Así, se puede acceder desde Internet sin exponer directamente la red interna, manteniendo la conexión segura y controlada.

3.3.1 Configuración de Internet en el Servidor de la DMZ

Para establecer la conexión a Internet desde el servidor ubicado en la DMZ, primero se comprobó la conectividad utilizando un comando ping, el cual arrojó el error: "Temporary failure in name resolution". Este mensaje indica que no hay acceso a Internet ni resolución DNS.

Pasos realizados para la configuración:

Acceder como usuario root:
sudo -i

Editar el archivo de configuración de red:

sudo nano /etc/netplan/01-netcfg.yaml
En este archivo se asignaron manualmente los siguientes parámetros:

Dirección IP del servidor.

Máscara de subred.

Puerta de enlace (gateway).

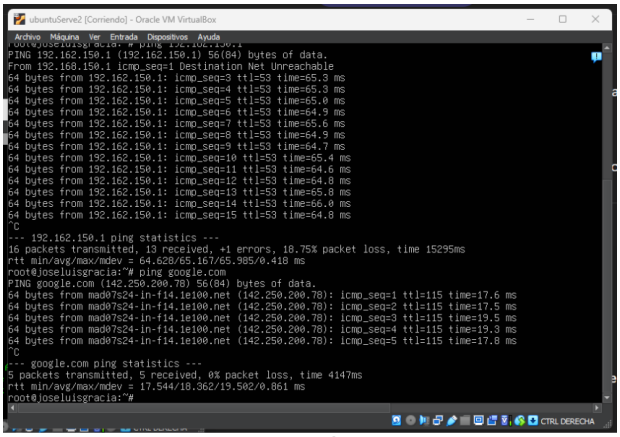
Servidores DNS, en este caso se utilizaron los de Google: **8.8.8.8**.

Aplicar la configuración:

sudo netplan apply
Es posible que aparezca algún mensaje de advertencia, pero mientras no impida la ejecución, la configuración será aplicada correctamente.
Verificación de conectividad:

ping google.com
Si el ping responde, se confirma que el servidor ya cuenta con conexión a Internet y resolución DNS funcional.

Ilustración 34 Comprobación Internet DMZ a WAN mediante Ping



Fuente: Autoría propia.

El título principal debe empezar en el margen superior de la primera página, en mayúsculas, centrado, Times News Roman de 14 Pts, negrita. Deje un espacio en blanco después del título.

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

4.1.1 CREACIÓN DE LA MÁQUINA VIRTUAL ENDIAN

Como parte del proceso práctico del curso de Administración de Servicios en Red, se realizó un conjunto de actividades orientadas a comprender cómo funcionan las redes segmentadas y cómo aplicar medidas de seguridad utilizando herramientas basadas en GNU/Linux. Durante el ejercicio, se configuró una red dividida en distintas zonas a través del firewall Endian, comenzando desde su instalación inicial hasta la comprobación final de los servicios que debían permitirse o bloquearse entre cada segmento.

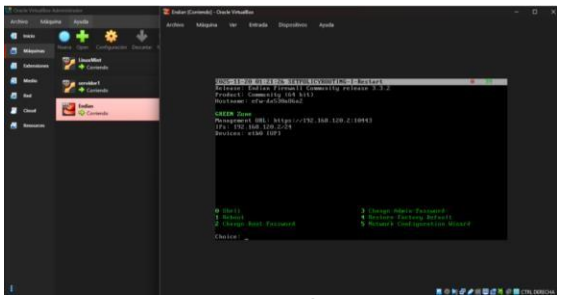
Se utilizó VirtualBox para crear la máquina virtual Endian, configurada con sistema operativo Linux (64-bit), 2048 MB de RAM y disco duro VDI de 4 GB. Se asignaron tres adaptadores de red:

1. Adaptador 1: red interna llamada LAN
2. Adaptador 2: red interna llamada DMZ
3. Adaptador 3: modo NAT para salida a Internet

4.1.2 INSTALACIÓN DEL SISTEMA ENDIAN FIREWALL

Se montó la ISO EFW-COMMUNITY-3.3.2.iso en la VM y se procedió con la instalación. Durante la configuración inicial, se asignó la zona verde con IP estática 192.168.120.2/24. Luego se accedió a la interfaz gráfica desde un navegador en una máquina cliente LAN.

Ilustración 35 Endian Firewall instalado.

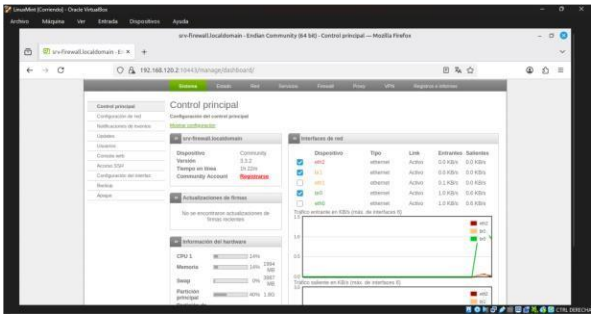


Fuente: Autoría propia

4.1.3 ACCESO AL DASHBOARD Y CONFIGURACIÓN BÁSICA

Desde el navegador de una de las máquinas "cliente" (configurada con la IP 192.168.120.2), se ingresó a la dirección https://192.168.120.2 con el fin de acceder al panel de administración de Endian. Una vez dentro, se completó el asistente de configuración inicial. Posteriormente, se procedió a configurar las direcciones IP de cada interfaz según la estructura de red definida. Para la zona verde, asociada al segmento 192.168.120.0/24, se asignó como puerta de enlace la dirección 192.168.120.1, manteniendo el rango disponible entre 192.168.120.2 y 192.168.120.253. De forma similar, en la zona naranja, correspondiente a la red 192.168.150.0/24, se configuró la interfaz con la puerta de enlace 192.168.150.1, dejando habilitado el rango 192.168.150.2 a 192.168.150.253.

Ilustración 36 Acceso a dashboard

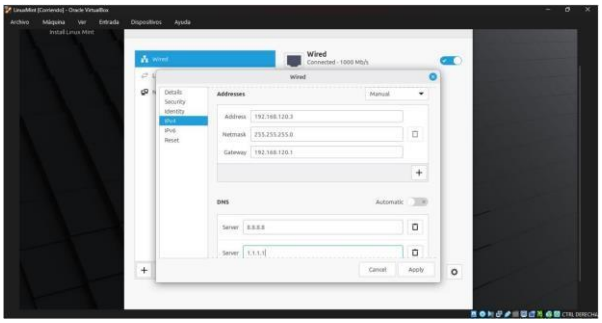


Fuente: Autoría propia.

4.1.4 CREACIÓN DE "CLIENTES" LAN Y DMZ

1. cliente_lan con IP 192.168.120.3 red interna LAN

Ilustración 37 Creación de "clientes" LAN Y DMZ

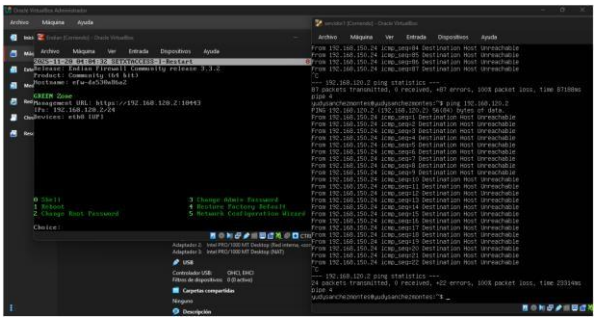


Fuente: Autoría propia.

4.1.5 PRUEBAS DE CONECTIVIDAD

Se realizaron pings exitosos:
Desde Endian:
ping 192.168.120.2

Ilustración 38 Máquina configurada en LAN.

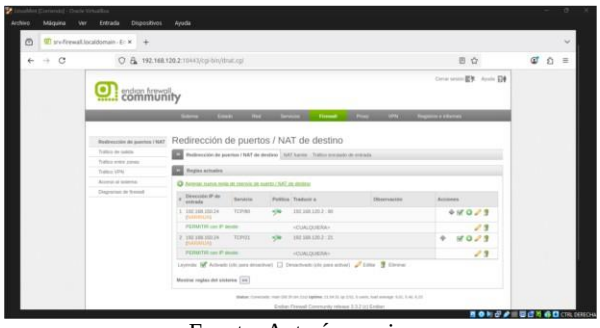


Fuente: Autoría Porpia.

4.1.6 REGLAS DE FIREWALL Y FILTRADO DE SERVICIOS

Se configuraron diferentes reglas para permitir o bloquear servicios como HTTP, FTP e ICMP según la zona de la red. Después de aplicar estos ajustes, se realizaron pruebas de conexión y acceso para comprobar que cada servicio funcionara —o se bloqueara— exactamente como estaba definido en la configuración.

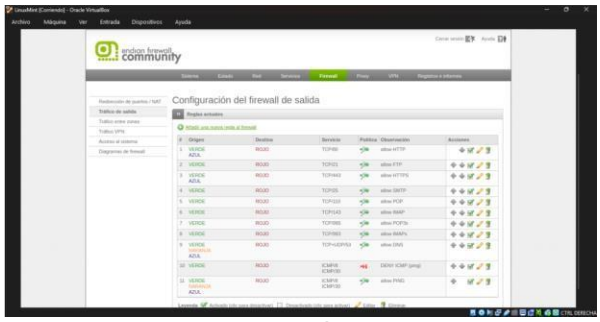
Ilustración 39 Máquina configurada en LAN.



Fuente: Autoría propia.

Regla 1: HTTP desde DMZ a LAN
Regla 2: FTP desde DMZ a LAN

Ilustración 40 Configuración de Firewall de salida.



Fuente: Autoría propia.

4.1.7 RESULTADOS TEMÁTICA 3

La implementación permitió comprobar de manera práctica cómo el firewall garantiza el aislamiento entre las distintas zonas de la red. Durante las pruebas, se confirmó que el acceso al panel de administración sólo era posible desde la red interna (LAN), lo que refuerza la seguridad del sistema. Además, se logró definir y controlar con precisión qué servicios podrían comunicarse entre cada zona, reproduciendo así el comportamiento de un entorno real con una DMZ y redes internas protegidas. Esta validación demuestra la importancia de segmentar la red y aplicar políticas claras para asegurar su correcto funcionamiento y proteger los recursos más críticos.

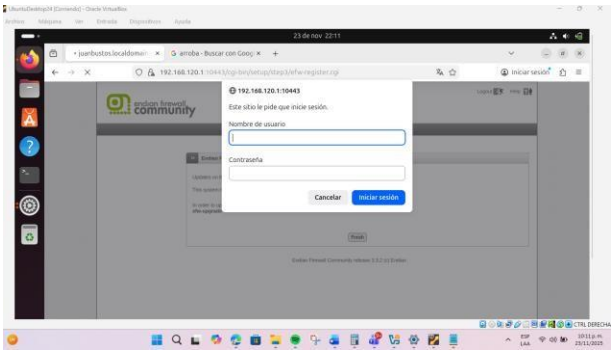
5 TEMÁTICA 4: REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO.

El control del tráfico de red mediante reglas de acceso es un aspecto fundamental en la administración de infraestructuras seguras y eficientes. En este trabajo se abordan distintos escenarios de comunicación entre zonas segmentadas —como la Zona Verde, Zona Naranja, DMZ e Internet— con el fin de configurar y verificar políticas que permitan o restrinjan el flujo de información según los servicios requeridos. En los pasos previos (1, 2 y 3), se llevaron a cabo las configuraciones necesarias tanto en **Endian Firewall**, **Ubuntu Desktop** y **Ubuntu Server**, estableciendo así la base para la correcta

implementación del enrutamiento y la gestión del tráfico. A través de pruebas prácticas, se evalúa el funcionamiento de protocolos como HTTP y FTP en sus puertos correspondientes, garantizando una comunicación adecuada entre zonas internas y externas. Asimismo, se revisa la correcta aplicación de las reglas de tráfico inter-zona y se validan las directivas de acceso desde navegadores web para asegurar un comportamiento coherente con los lineamientos de seguridad establecidos.

Pantalla de inicio de sesión del sistema Endian Firewall Community en la IP 192.168.120.1:10443 desde máquina virtual Ubuntu desktop

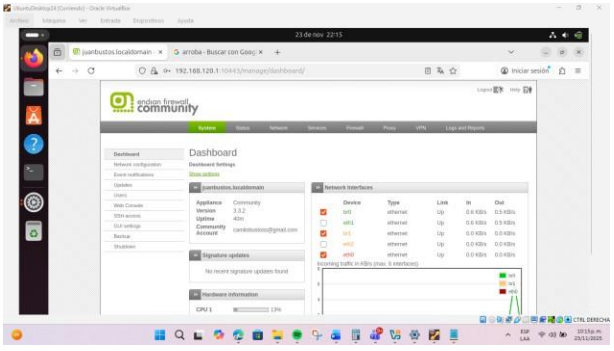
Ilustración 41 Inicio de sesión del sistema Endian Firewall



Fuente: Autoría propia

Endian Firewall Community abierta en un navegador dentro de una máquina virtual Ubuntu. Dashboard con información del sistema, versión (Community 3.3.2).
URL https://192.168.120.1:10443/manage/dashboard.

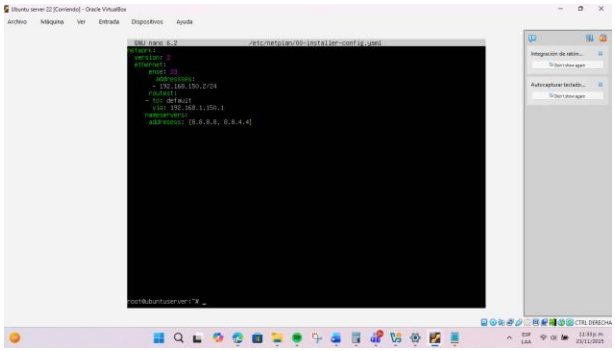
Ilustración 42 Endian Firewall Community abierta en un navegador



Fuente: Autoría propia

Edición del archivo /etc/netplan/00-installer-config.yaml en Ubuntu Server, configurando la red con dirección IP, puerta de enlace y servidores DNS.

Ilustración 43 Edición de archivo nano

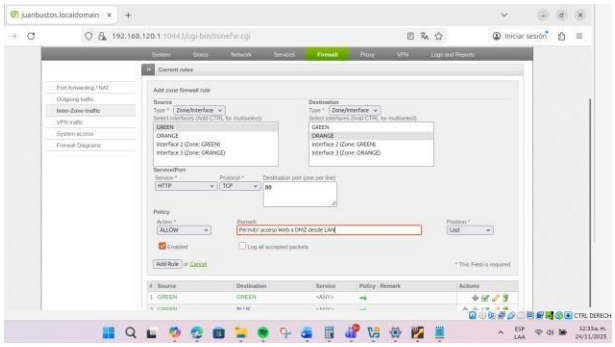


Fuente: Autoría propia

5.1.1 COMUNICAR LA ZONA VERDE CON LA ZONA NARANJA CON EL PROTOCOLO HTTP Y FTP CON SUS RESPECTIVOS PUERTOS.

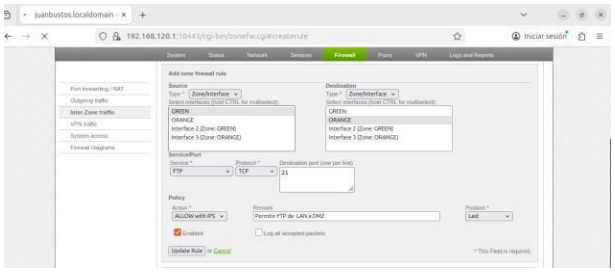
Se configuran en Endian Firewall dos reglas para permitir la comunicación entre la zona GREEN y la zona ORANGE: una para tráfico HTTP en el puerto 80 y otra para tráfico FTP en el puerto 21.

Ilustración 44 Configuración de puertos en Endian Firewall



Fuente: Autoría propia

Ilustración 45 Configuración de puertos en Endian Firewall

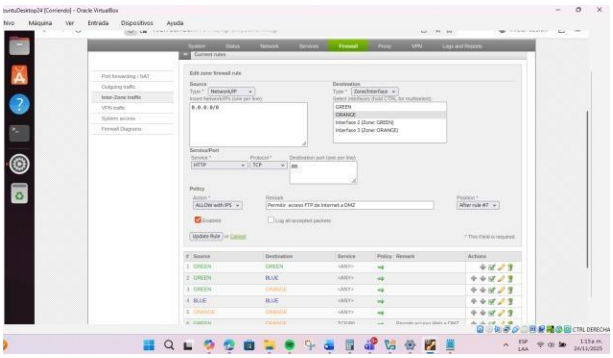


Fuente: Autoría propia

5.1.2 COMUNICAR LA ZONA INTERNET CON LA ZONA DMZ.

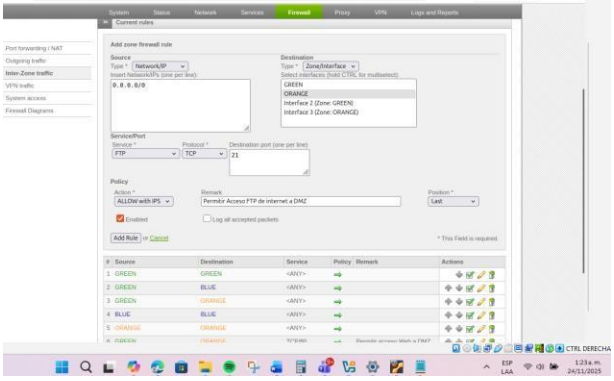
Se configuran en Endian Firewall dos reglas para permitir acceso desde Internet a la zona DMZ: una para HTTP (puerto 80) y otra para FTP (puerto 21)

Ilustración 46 Regla de acceso para la zona DMZ



Fuente: Autoría propia

Ilustración 47 Regla de acceso para la zona DMZ

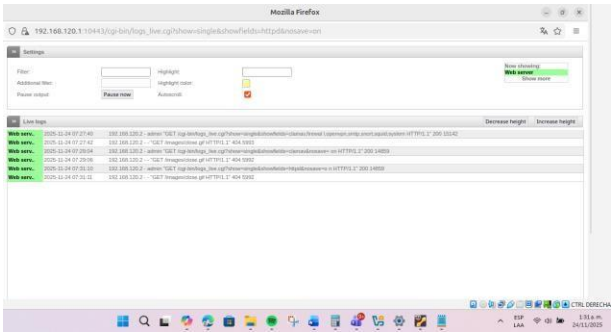


Fuente: Autoría propia

5.1.3 VERIFICAR EN EL TRÁFICO INTER - ZONA, LA CREACIÓN DE LAS REGLAS.

Se verifica en los registros en vivo del Endian Firewall el tráfico HTTP permitido entre zonas, mostrando solicitudes GET y respuestas del servidor.

Ilustración 48 Respuestas del servidor, tráfico HTTP



Fuente: Autoría propia

5.1.4 PROBAR DESDE UN NAVEGADOR WEB, LAS SIGUIENTES DIRECTIVAS:

- El Ingreso Del Servicio Http Desde La Lan Hacia La Zona Dmz.

Endian Firewall Community mediante la URL http://192.168.150.1:10443/manage/dashboard. Esto indica que se ha permitido el tráfico HTTP desde la zona LAN (GREEN) hacia la zona DMZ (ORANGE)

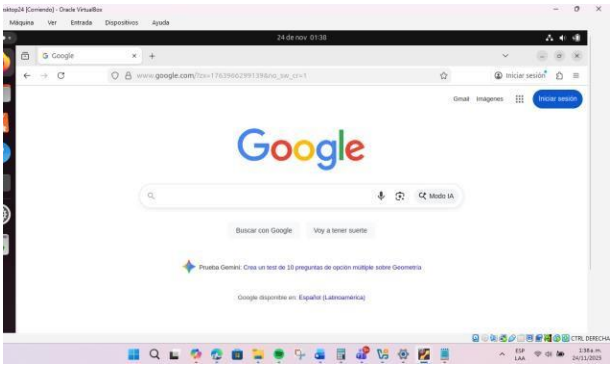
Ilustración 49 Respuesta desde zona LAN a DMZ

Fuente: Autoría propia

- El Ingreso Del Servicio Http Desde La Lan Hacia La Wan.

Se verifica el acceso HTTP desde la zona LAN hacia la WAN mediante la apertura del sitio web externo Google en el navegador.

Ilustración 50 Respuesta desde zona LAN a Wan desde web



Fuente: Autoría propia

- El Ingreso Del Servicio Http Desde La Zona Dmz Hacia La Wan.

Acceso HTTP desde la zona DMZ hacia la WAN mediante la apertura del sitio web externo.

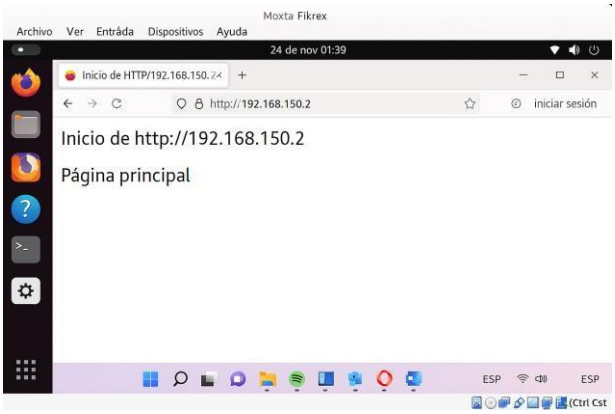
Ilustración 51 Respuesta desde DMZ a WAN

Fuente: Autoría propia

- El Ingreso Del Servicio Http Desde La Wan Hacia La Zona Dmz.

Ingreso del servicio HTTP desde la WAN hacia la zona DMZ. Se muestra un navegador accediendo a la URL http://192.168.150.2, con una página simple que indica “Inicio de http://192.168.150.2” y “Página principal”

Ilustración 52 Respuesta desde Wan a DMZ

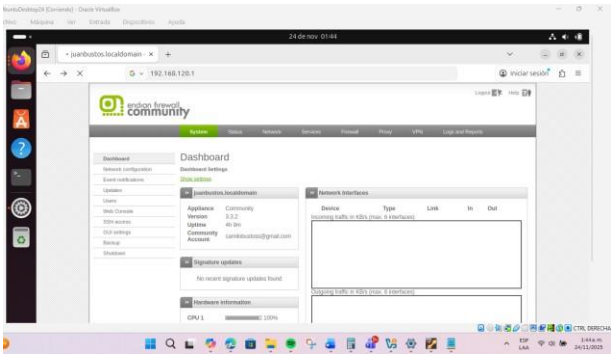


Fuente: Autoría propia

- El Ingreso Del Servicio Ftp Desde La Lan Hacia La Wan.

Conectividad FTP desde la zona LAN hacia la WAN, permitiendo que el cliente LAN acceda a un servidor FTP externo

Ilustración 53 Respuesta FTP desde LAN a WAN

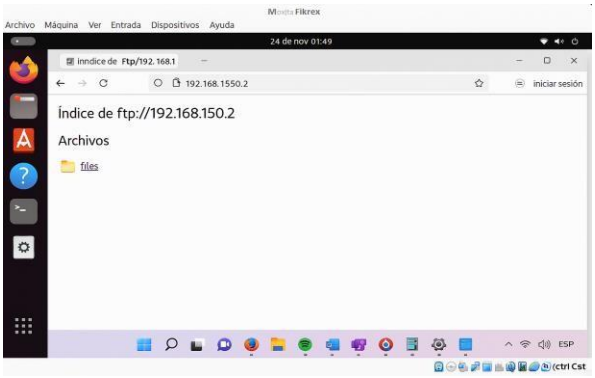


Fuente: Autoría propia

- El Ingreso Del Servicio Ftp Desde La Wan Hacia La Zona Dmz.

Acceso FTP desde la WAN hacia la zona DMZ, mostrando en el navegador el índice de archivos del servidor FTP.

Ilustración 54 Respuesta FTP desde WAN a DMZ



Fuente: Autoría propia

6 CONCLUSIONES

6.1 TEMÁTICA 1

Se ha implementado una arquitectura de seguridad de red segmentada, utilizando Endian Firewall (EFW) en un entorno virtualizado, Se validó la correcta asignación de interfaces a las zonas Lógica (Roja, Verde, Naranja) y Física (eth0, eth1, eth2), así mismo la configuración estática y el enrutamiento (Netplan) de los clientes y servidores en la zona verde (192.168.120.x) y la zona naranja (192.168.150.x) realizando las pruebas de conectividad que incluyen realizar el ping exitoso de la LAN (Verde) a la DMZ (Naranja) para confirmar la funcionalidad del sistema y la preparación de la infraestructura para aplicar políticas de seguridad estrictas.

6.2 TEMÁTICA 2

Con esta configuración de NAT en Endian aprendí lo importante que es organizar bien la red para que todo funcione seguro y sin problemas. Al separar las zonas (LAN, DMZ y WAN), pude controlar mejor quién entra, quién sale y qué servicios se pueden usar.

El NAT permitió que los equipos internos se conectaran a Internet sin mostrar sus IP reales, lo que mejora la seguridad. También pude comprobar que desde la LAN y la DMZ sí se puede acceder a Internet usando SNAT y DNAT correctamente.

En resumen, la práctica me mostró que un buen firewall y una buena configuración de NAT son esenciales para proteger la red, permitir la comunicación y mantener todo funcionando de forma ordenada y segura

6.3 TEMÁTICA 3

La configuración realizada permitió establecer adecuadamente los servicios expuestos en la zona DMZ, asegurando que solo los protocolos requeridos — HTTP (80) y FTP (21)— estuvieran disponibles desde el servidor web en Ubuntu Server. De igual manera, la restricción del protocolo ICMP (puertos 8 y 30) evidenció el control efectivo del firewall al impedir respuestas a solicitudes ping, cumpliendo con los criterios de seguridad establecidos. Las pruebas de conectividad, junto con la verificación del tráfico saliente y la Confirmación de las reglas generadas en el firewall, validaron de forma técnica la correcta segmentación y protección entre la DMZ y la red interna. En conjunto, estos resultados demuestran una gestión segura y funcional de los servicios en un entorno segmentado.

6.4 TEMÁTICA 4

La configuración y verificación de reglas en el Endian Firewall Community permitió cumplir con los objetivos planteados, garantizando la correcta segmentación y comunicación entre las diferentes zonas de la red. Se estableció la conectividad entre la zona GREEN (LAN) y la zona ORANGE (DMZ) mediante los protocolos HTTP (puerto 80) y FTP (puerto 21), así como la comunicación entre la zona WAN (Internet) y la DMZ, asegurando el acceso controlado a servicios web y transferencia de archivos.

La revisión del tráfico Inter-Zona confirmó la aplicación efectiva de las políticas configuradas, y las pruebas funcionales realizadas desde navegadores y clientes FTP validaron el acceso en todos los escenarios definidos: HTTP y FTP desde LAN hacia DMZ y WAN, desde DMZ hacia WAN, y desde WAN hacia DMZ.

Este ejercicio demuestra la importancia de aplicar reglas específicas en un firewall para mantener la seguridad, controlar el flujo de datos y garantizar la disponibilidad de los servicios, logrando un equilibrio entre conectividad y protección frente a amenazas externas.

7 REFERENCIAS

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

[2] Cervelión, Á. J. (2023). Instalación de Nagios Core 4.4 en Ubuntu 22.04 . [Objeto_virtual_de_información_OVI]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/54230

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

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

[5] Jay LaCroix. (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

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

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