# SEGURIDAD EN GNU/LINUX: DE LA TEORÍA A LA PRÁCTICA

Henry Eduardo Curico Saldaña
e-mail: hecuricos@unadvirtual.edu.co
Julián David Delgado Díaz
e-mail: jddelgadodi@unadvirtual.edu.co
Roger Herney Pacheco Rodríguez
e-mail: rhpachecor@unadvirtual.edu.co
Jhon Jairo Carrillo Bonilla
e-mail: jjcarrillob@unadvirtual.edu.co

***Resumen*—Este trabajo presenta la instalación y configuración de una infraestructura de red implementada en el firewall Endian sobre un entorno controlado de virtualización utilizando la herramienta Oracle VirtualBox. En proceso y desarrolló del laboratorio se realiza la preparación del sistema Endian, incluyendo la configuración de los adaptadores de red necesarios para su correcto funcionamiento. Además, se definieron los segmentos de red o zonas y se habilitaron servicios ubicados en la zona DMZ o zona naranja con el fin de permitir su disponibilidad hacia la red interna y externa. Finalmente, se crearon y establecieron reglas de acceso orientadas a permitir o denegar tráfico entre la zona verde, naranja y roja, garantizando así un control adecuado de la seguridad perimetral. Los resultados demostraron el potencial y capacidad del firewall Endian para gestionar de manera eficiente para el control y organización del tráfico en la red bajo un entorno Linux, permitiendo el fortaleciendo de la administración y protección de la infraestructura de red simulada pero muy similar a un entorno productivo.**

**PALABRAS CLAVE**: DMZ, Endian, Firewall, Linux, Oracle, Segmentación de red, VirtualBox.

## 1. INTRODUCCIÓN

En algún momento de nuestras vidas ha surgido la necesidad de protección, ya sea para resguardar nuestros objetos o nuestra integridad. Por ello, buscamos las herramientas que nos puedan brindar esa seguridad.

Un ejemplo claro es cuando una persona desea utilizar una motocicleta: tiene la libertad de usarla, pero surge la necesidad de protegerse frente a caídas o accidentes. La herramienta esencial para un motociclista es el casco de protección, el cual resguarda una parte vital del cuerpo humano. Sin embargo, esta seguridad se puede reforzar con elementos adicionales, tal como el uso de rodilleras o trajes de protección que minimizan los impactos o golpes.

En el mundo de la informática también tenemos riesgos y requerimos herramientas de protección. La parte vital del mundo digital es la información, y este es el tesoro que todo pirata quiere robar.

Una de las herramientas fundamentales en una infraestructura de red y en entornos en los cuales la información es la fuente para el desarrollo cotidiano de las labores o tareas, es el sistema de protección que evita el robo del tesoro informático, pero que también protege las herramientas que lo componen, hablamos específicamente del firewall y si gran capacidad para controlar las conexiones en la infraestructura de red.

En este artículo se presenta un desarrollo de laboratorio en el cual se implementa el sistema de seguridad firewall bajo la distribución Endian de Linux, sistema especializado en seguridad perimetral que integra múltiples herramientas enfocadas en la protección de la red.

El laboratorio está orientado al aprendizaje y fortalecimiento del conocimiento en el uso de sistemas operativos Linux y específicamente en la implementación de seguridad en una infraestructura de red controlada con máquinas virtualizadas que no exponen algún riesgo real que pueda afectar la información o servicios en producción.

Finalmente se mostrarán los resultados de las configuraciones, reglas y servicios que fueron implementados con el objetivo de demostrar la importancia de tener una seguridad de red, un control del tráfico y la capacidad de las herramientas disponibles para administrar entornos empresariales o de infraestructuras de gran escala.

## 2. TEMÁTICAS

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

#### 2.1.1 INSTALACIÓN ENDIAN FIREWALL COMMUNITY EDITION

Como base para el desarrollo de la etapa 7, la cual se centra en la seguridad se trabajará con la distribución Endian

Firewall. Esta distribución italiana se especializa en la seguridad de red que permite montar un sistema de gestión unificada de amenazas, en sus siglas en inglés UTM.

Previa instalación del firewall Endian, se definieron los siguientes segmentos de red.

*Tabla 1.*

| **Zona** | **Segmento de red** |
|---|---|
| Verde | 192.168.56.0/24 |
| Naranja | 172.16.0.0/24 |
| Roja | IP pública definida por el ISP |

Fuente: Autoría Propia

Primero se accede al sitio oficial de Endian www.endian.com/en/community/ y se busca la forma de descargar el ISO de la distribución [1].

Figura 1. Portal Endian para descarga


. Fuente: Autoría Propia

Dentro del sitio se da acceso al sitio de sourceforge que hace la descarga directa de Endian.

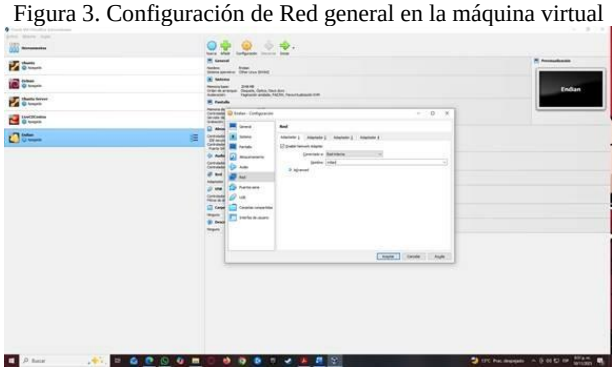
Figura 2. Sitio de descarga en SOURCEFORGE


. Fuente: Autoría Propia

Una vez descargada la ISO, se procede a crear la máquina virtual que va a ejecutar el firewall, para este laboratorio, se usará el gestor de máquinas virtuales VM VirtualBox.

Antes de iniciar la máquina, se deben activar y asignar los adaptadores de red que van a usarse para las Zonas, estas serían Verde, Naranja y Roja.

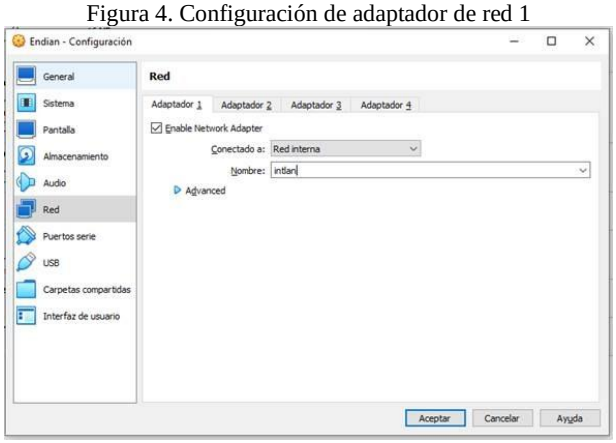
Figura 3. Configuración de Red general en la máquina virtual



. Fuente: Autoría Propia

Cada adaptador se identifica con un nombre de manera opcional para identificar la zona o segmento que se utilizará, en este caso, el adaptador 1 se defina con el nombre “intlan”.

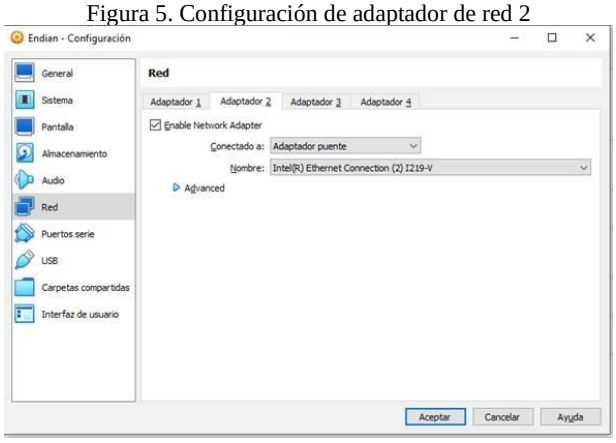
Figura 4. Configuración de adaptador de red 1




. Fuente: Autoría Propia

Para el segundo adaptador de red, se establece como “Adaptador puente”.

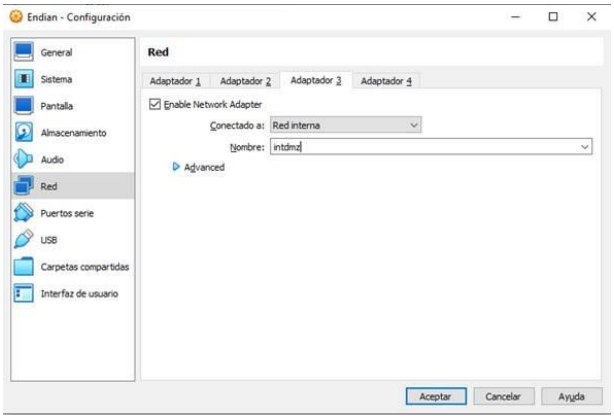
Figura 5. Configuración de adaptador de red 2




. Fuente: Autoría Propia

Para el tercer adaptador de red, se establece como “Red interna” y se define con el nombre “intdmz”.

Figura 6. Configuración de adaptador de red 3




. Fuente: Autoría Propia

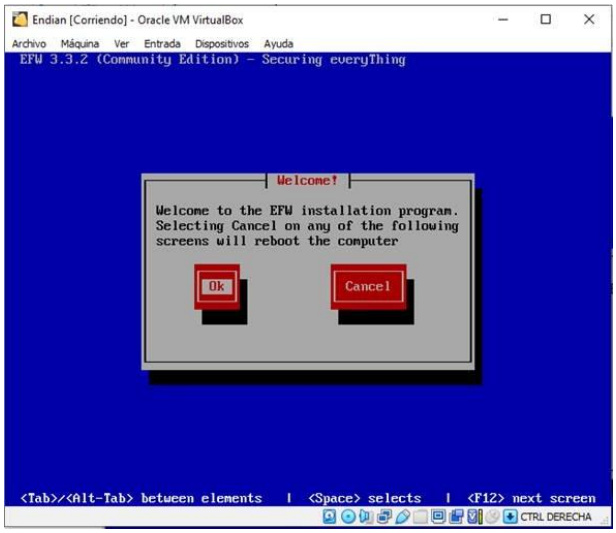
Una vez lista la configuración previa, se puede ejecutar la máquina virtual para la instalación de la distribución Endian. El proceso inicia con la selección del idioma, que por defecto se establece en inglés.

Figura 7. Selección de idioma para instalación


. Fuente: Autoría Propia

Los siguientes pasos de la instalación incluyen una confirmación de la misma. A continuación, la herramienta de instalación solicita preparar el disco duro, indicando que este será particionado y que todo el contenido del disco será eliminado. Se pregunta al usuario si desea continuar. Al confirmar, la instalación se realiza automáticamente.

Figura 8. Confirmación de instalación




. Fuente: Autoría Propia

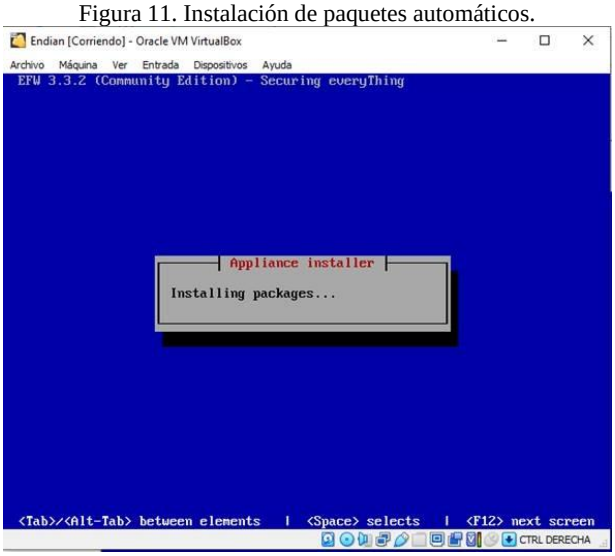
Figura 9. Confirmación eliminación data del disco duro


. Fuente: Autoría Propia

Figura 10. Ejecución de particionado automático


. Fuente: Autoría Propia

Figura 11. Instalación de paquetes automáticos.




. Fuente: Autoría Propia

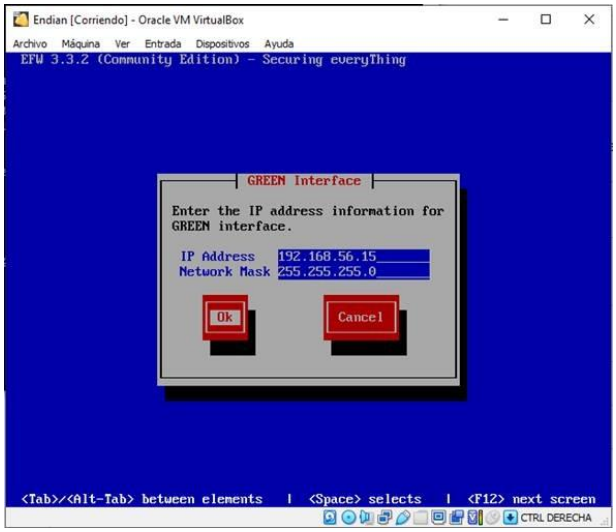
Una vez que el sistema termina de instalar los paquetes básicos, solicita validar si la conexión se realizará a través de un puerto serial, para este laboratorio no se realizará por medio de la conexión serial.

Figura 12. Mensaje de habilitar consola por puerto serial


. Fuente: Autoría Propia

Posteriormente, se debe requiere definir la dirección IP y máscara de red para la zona verde de Endian.

Figura 13. Configuración de IP en Red Verde




. Fuente: Autoría Propia

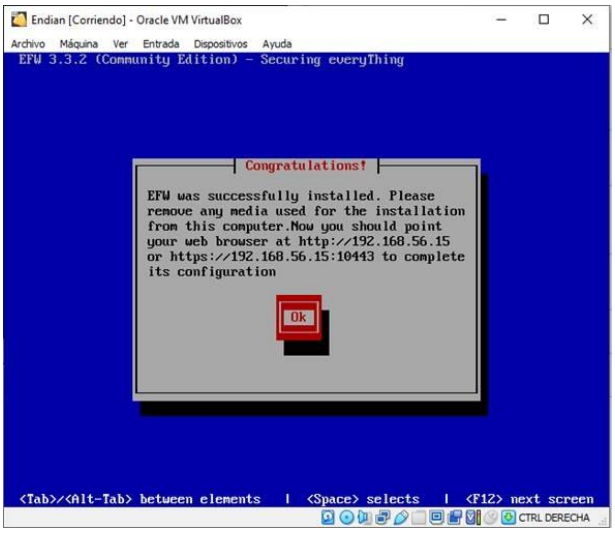
Con esta configuración, finaliza la instalación del sistema, agregando el bootloader para el próximo inicio.

Figura 14. Instalación automática del bootloader


. Fuente: Autoría Propia

Finalizado el proceso anterior, se confirma la instalación a satisfacción y se muestra la información para la conexión web de administración del firewall, generalmente la dirección del panel de administración corresponde a la siguiente ruta: https://<dirección ip inicialmente establecida>:puerto, para este laboratorio, la dirección definida fue 192.168.56.15, siendo la dirección URL de administración: https://192.168.56.15:10443

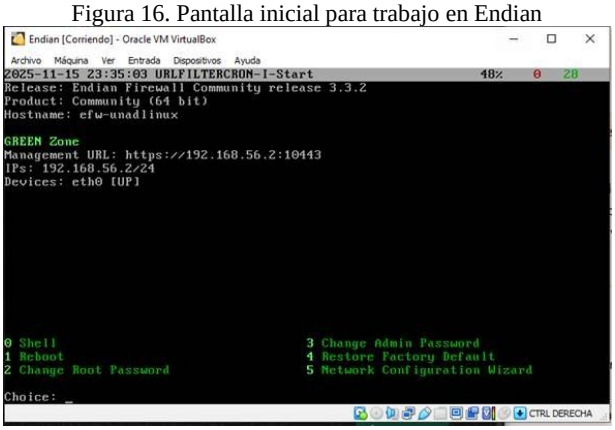
Figura 15. Finalización de la instalación.




. Fuente: Autoría Propia

Una vez finalizado el proceso de instalación de Endian, la máquina virtual se reiniciará automáticamente. Al iniciarse de nuevo, el sistema estará listo para el uso del firewall.

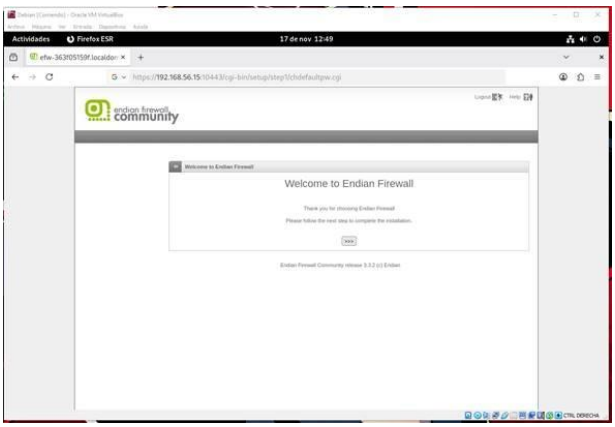
Figura 16. Pantalla inicial para trabajo en Endian




. Fuente: Autoría Propia

Ahora, para la configuración vía web del sistema Endian, se debe conectar una máquina virtual adicional a la misma red y acceder mediante la URL indicada por Endian. Para este ejemplo, utilizaremos el navegador Firefox desde un sistema operativo Debian.

Figura 17. Inicio de configuración Endian por medio de maquina Debian con interfaz gráfica.

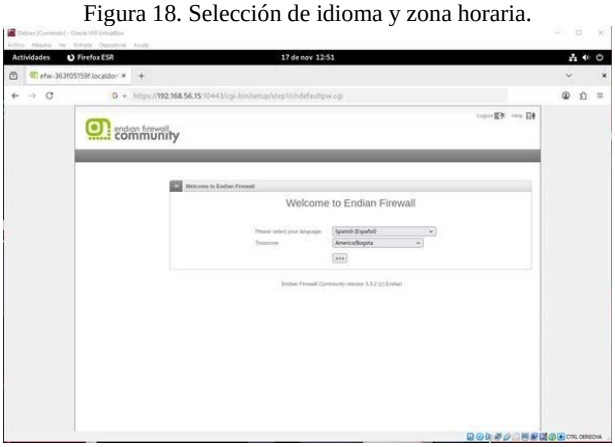



. Fuente: Autoría Propia

Una vez que se ha ingresado al sitio de administración de Endian desde el equipo Debian, se deben seguir los siguientes pasos.

Seleccionar el idioma y zona horaria, para este laboratorio se dio selección al idioma español y zona horaria América/Bogotá

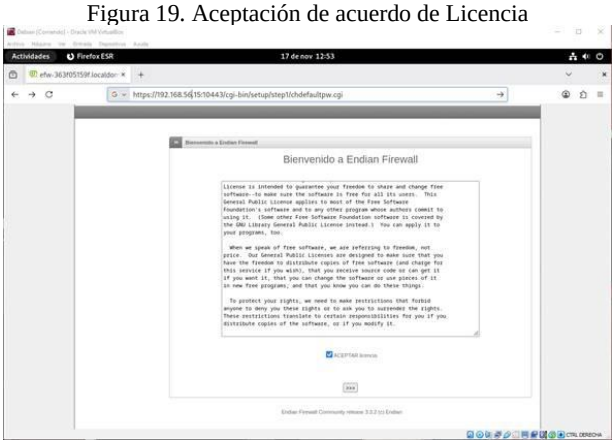
Figura 18. Selección de idioma y zona horaria.




. Fuente: Autoría Propia

Aceptar los acuerdos de licencia definidos para el uso del sistema Endian Firewall.

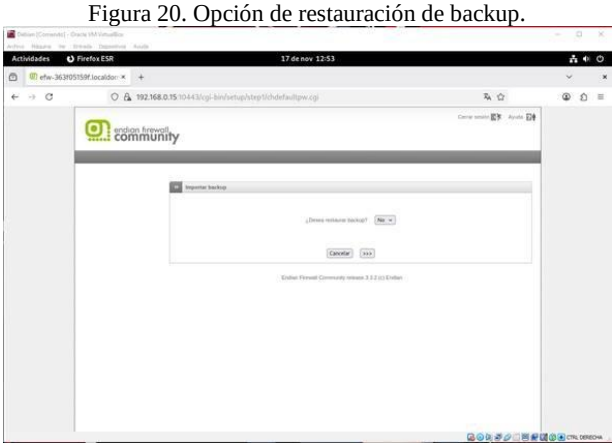
Figura 19. Aceptación de acuerdo de Licencia




. Fuente: Autoría Propia

Preguntará si se requiere restaurar a partir de una copia de seguridad, para este laboratorio no es necesario ya es una instalación de primer uso.

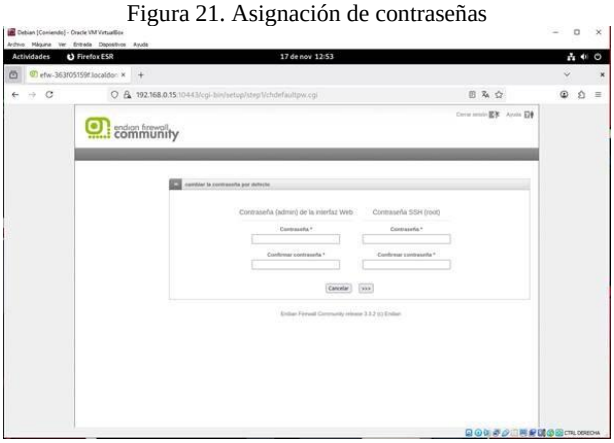
Figura 20. Opción de restauración de backup.



. Fuente: Autoría Propia

Para los usuarios admin y root. Se recomienda usar contraseñas fuertes de un mínimo de 8 caracteres.

Figura 21. Asignación de contraseñas

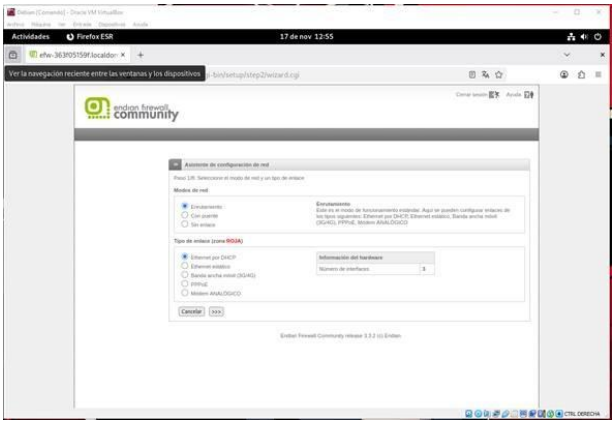


. Fuente: Autoría Propia

Una vez asignadas las contraseñas, se procede a configurar las interfaces de red.

Zona Roja (RED): Esta zona recibirá la conexión a internet. Para este laboratorio se usará el modo de enrutamiento con asignación DHCP para la zona roja.

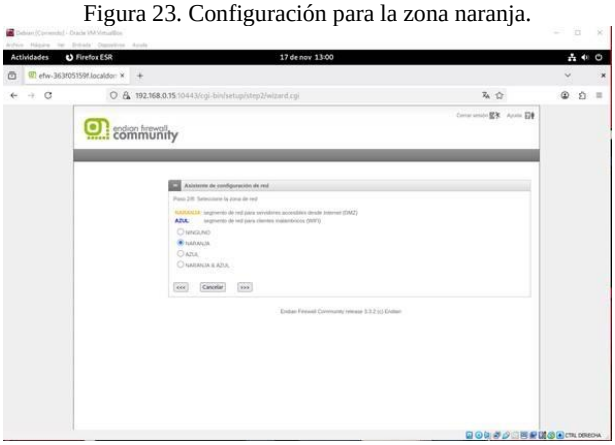
Figura 22. Configuración Zona Roja



. Fuente: Autoría Propia

Zona Naranja (ORANGE): Se selecciona la opción correspondiente para configurar esta zona.

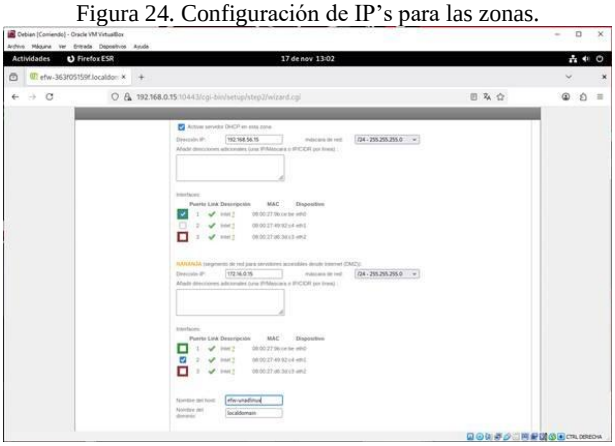
Figura 23. Configuración para la zona naranja.



. Fuente: Autoría Propia

Asignación de Direcciones IP: Se asignan las direcciones IP y máscaras de red necesarias para que ambas zonas se conecten.

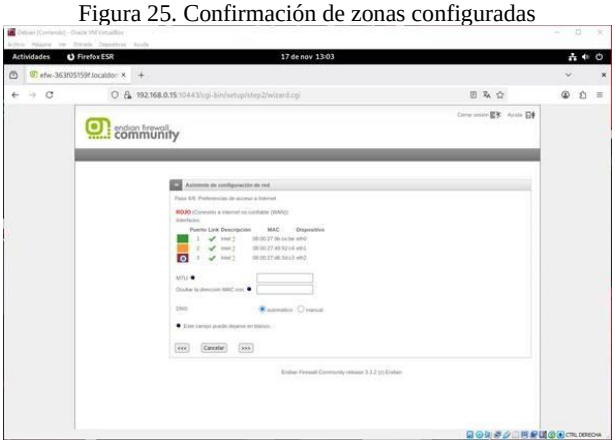
Figura 24. Configuración de IP’s para las zonas.



. Fuente: Autoría Propia

El sistema mostrará una confirmación de las zonas activas.

Figura 25. Confirmación de zonas configuradas



. Fuente: Autoría Propia

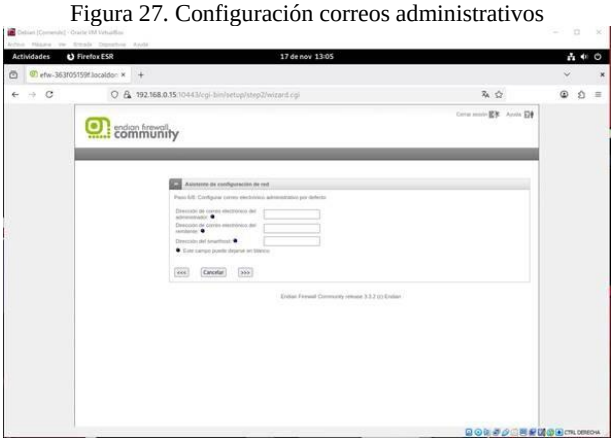
El DNS se mantiene en automático por defecto y se selecciona Siguiente.

Figura 26. Configuración de DNS

. Fuente: Autoría Propia

La configuración de correos administrativos se omite para este ejercicio, dejando los campos vacíos.

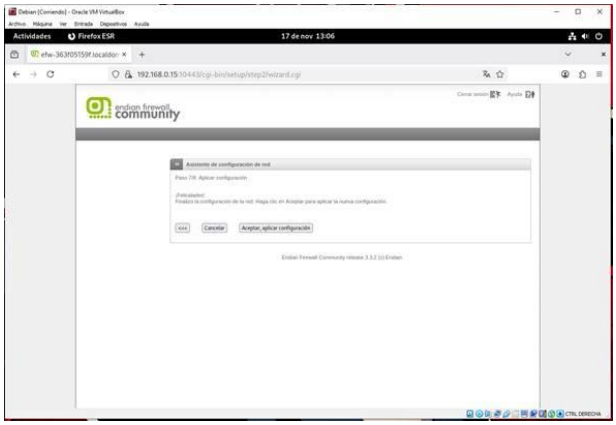
Figura 27. Configuración correos administrativos



. Fuente: Autoría Propia

Se procede a la aplicación de las configuraciones realizadas.

Figura 28. Aplicación de configuraciones.

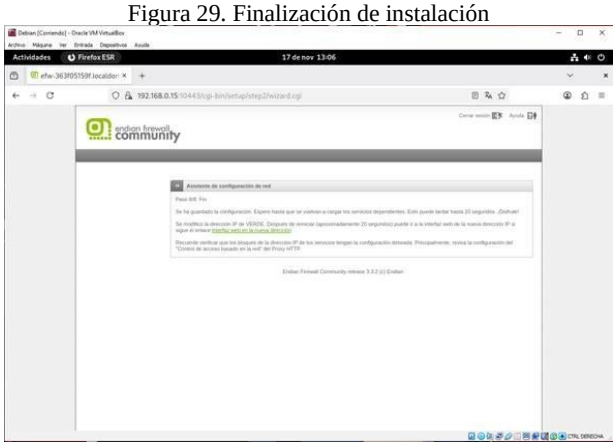


. Fuente: Autoría Propia

El sistema realiza y completa todas las configuraciones correspondientes.

Se omite el registro para actualizaciones, ya que este es un ejercicio de instalación base del sistema Endian.

Figura 29. Finalización de instalación



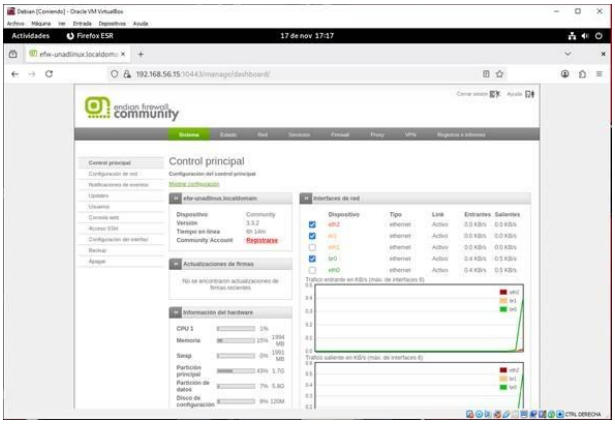
. Fuente: Autoría Propia

Una vez que todas las configuraciones han sido aplicadas, se puede acceder al firewall Endian para su gestión.

Para ello, se debe ingresar a la dirección IP de la Zona Verde e iniciar sesión con el usuario admin y la contraseña previamente configurada. Dentro del panel, es posible visualizar los estados, servicios y realizar los ajustes necesarios para la red.

De este modo, se da por finalizada la instalación base del sistema firewall Endian.

Figura 30. Pantalla inicial de Endian

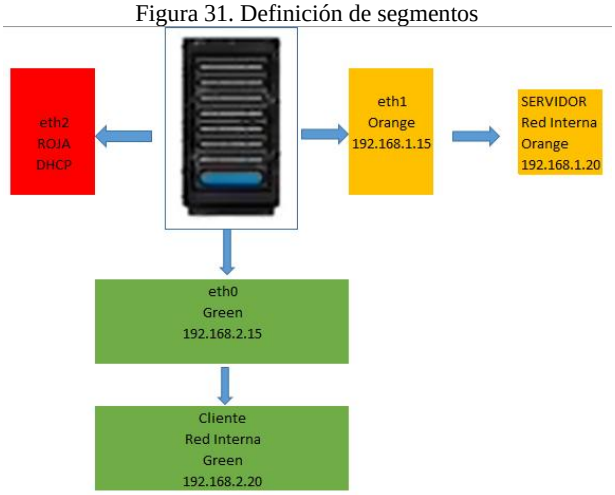


. Fuente: Autoría Propia

## 2.2 TEMÁTICA 2: CONFIGURACIÓN NAT.

Previa instalación del Endian firewall, se definieron los siguientes segmentos de red.

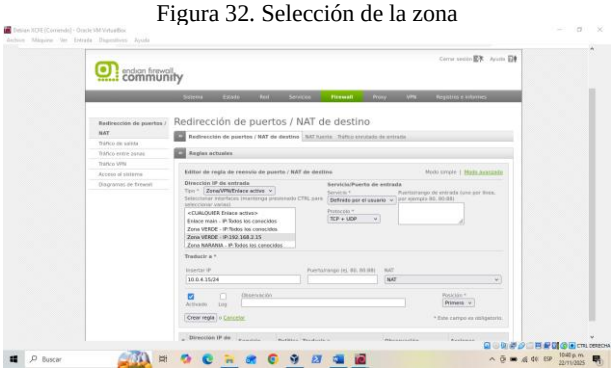
Figura 31. Definición de segmentos




. Fuente: Autoría Propia

Para iniciar, se debe acceder a la red Green, la cual comunica la LAN con la WAN (Internet). Luego, se ingresa a la interfaz de administración y se navega hasta la sección de Firewall.

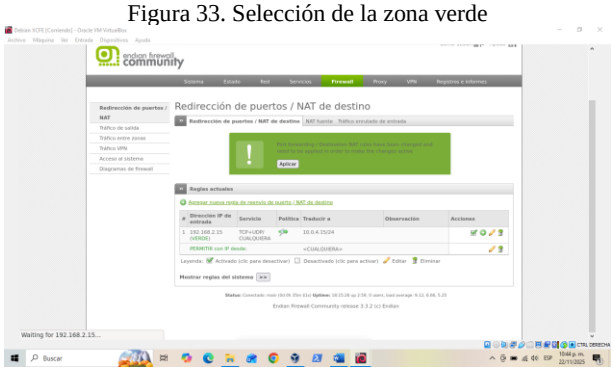
Figura 32. Selección de la zona



. Fuente: Autoría Propia

Crear la regla y aplicar los cambios

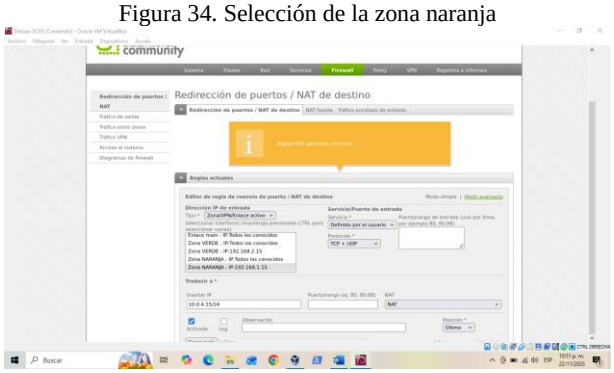
Figura 33. Selección de la zona verde



. Fuente: Autoría Propia

A continuación, se crea la red Orange, la cual va desde la DMZ hacia Internet. Se siguen los mismos pasos anteriores, pero utilizando una dirección IP diferente

Figura 34. Selección de la zona naranja

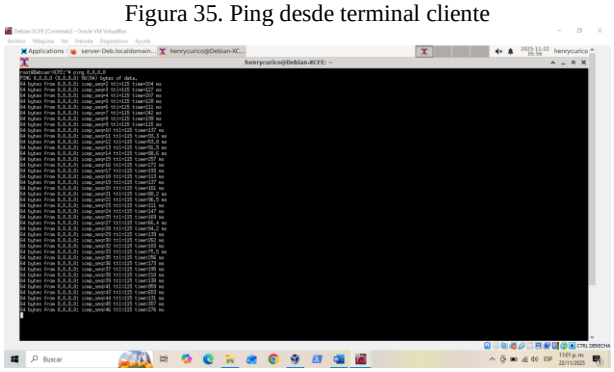


. Fuente: Autoría Propia

A continuación, se verifica la funcionalidad del acceso a Internet tanto del servidor como del cliente.

Desde el terminal del cliente Debian Xfce, se ejecuta un ping a la dirección 8.8.8.8, confirmando que la conexión es exitosa.

Figura 35. Ping desde terminal cliente

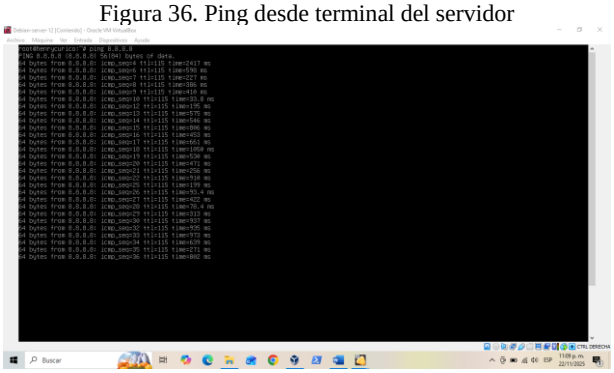


. Fuente: Autoría Propia

Ahora se accede al servidor Debian y se realiza un ping a la dirección 8.8.8.8.

La conexión a Internet del cliente se verifica como exitosa.

Figura 36. Ping desde terminal del servidor



. Fuente: Autoría Propia

El laboratorio demostró exitosamente la correcta implementación y funcionamiento de las reglas de NAT dentro de la infraestructura configurada. En primer lugar, se estableció la comunicación desde la LAN hacia la WAN mediante la creación y validación de la regla de NAT correspondiente, evidenciando que los equipos internos pueden acceder a la red simulada de Internet sin inconvenientes. Del mismo modo, se configuró y comprobó la comunicación desde la Zona DMZ hacia Internet, garantizando que los servicios ubicados en esta zona intermedia operen con el nivel de acceso previsto.

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

### 2.3.1 PERMITIR LOS SERVICIOS HTTP (PUERTO 80) Y FTP (PUERTO 21) DESDE EL SERVIDOR WEB BAJO UBUNTU SERVER.

Configuración de red de la zona verde y zona naranja.

*Tabla 2.*

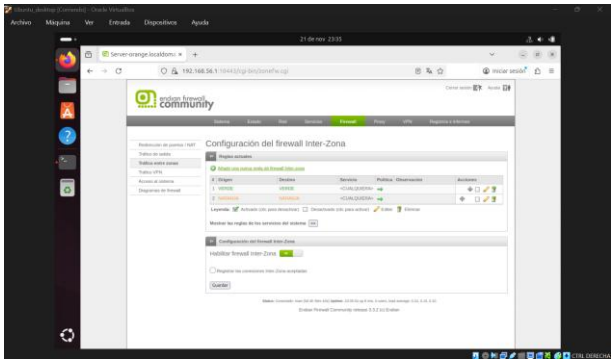
| Zona | Ip definida | Sistema |
|---|---|---|
| Verde | 192.168.56.3 | Ubuntu Desktop |
| Naranja | 172.16.0.5 | Ubuntu Server |

Fuente: Autoría Propia

El tráfico de la zona naranja hacia la zona verde está bloqueado por defecto, lo cual, se crearán las reglas explícitas.

Inicialmente se procede a agregar la regla para la conexión por el puerto 80 (HTTP), este proceso se realiza desde el panel de administración de Endian en la pestaña Firewall y la opción “Tráfico entre zonas”

Figura 37. Tráfico entre zonas




. Fuente: Autoría Propia

La creación de la primera regla se establecerá para que la el equipo cliente (zona verde) tenga respuesta desde el servidor web (zona naranja) por medio del servicio HTTP, inicialmente este servicio no está definido lo cual se interpreta como una negación del protocolo HTTP.

La primera validación se realizará ingresando a la tienda virtual expuesta por el servidor web en la url http://172.16.0.5

Figura 38. Validación del servicio HTTP desde el cliente


. Fuente: Autoría Propia

La regla se define seleccionando la zona verde como origen y seleccionando la zona naranja como destino; el servicio a seleccionar es HTTP, el protocolo TCP y el puerto 80, la acción requerida para permitir el servicio es “PERMITIR”

Figura 39. Creación de la regla para permitir HTTP


. Fuente: Autoría Propia

Se realiza la creación de la regla y se aplican los cambios.

Una vez activa la regla, se procede a validar nuevamente la petición del servicio web desde el navegador del cliente hacia el sitio web expuesto por el servidor, para este caso es http://172.16.0.5

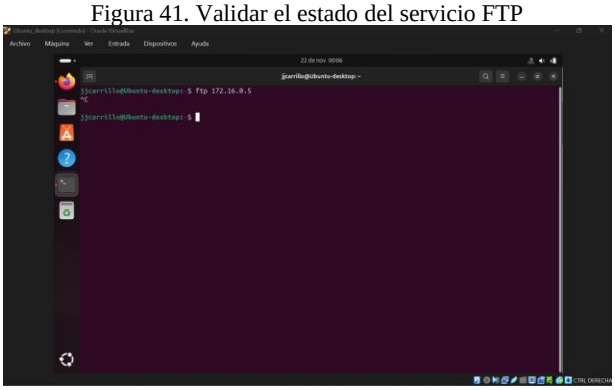
Figura 40. Validar el servicio web


. Fuente: Autoría Propia

Definida la regla para permitir el servicio HTTP, se procede con la creación de la regla para permitir el servicio FTP correspondiente al puerto 21.

Se valida el estado del servicio FTP antes de la creación de la regla.

Figura 41. Validar el estado del servicio FTP

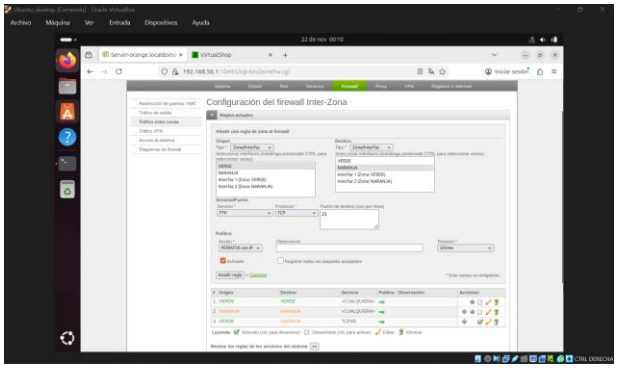


. Fuente: Autoría Propia

Se comprueba que no se tiene respuesta a la petición de conexión FTP.

Se procede con la creación de la regla para permitir el servicio, para este paso, se requiere crear la regla desde el tráfico entre zonas y agregar la regla en la cual se define la zona verde como origen y la zona naranja como destina, seleccionando el servicio FTP, protocolo TCP, puerto 21 y seleccionando la acción “PERMITIR”.

Figura 42. Creación de la regla para permitir FTP




Creada la regla y aplicados los cambios, se realiza nuevamente la validación para realizar la conexión al servidor web por medio del servicio FTP.

Figura 43. Validar el servicio FTP

. Fuente: Autoría Propia

Se comprueba que la conexión al servicio FTP es exitosa, esto se puede confirmar al tener respuesta de parte del servidor el cual solicita la autenticación para establecer la conexión (usuario y contraseña)

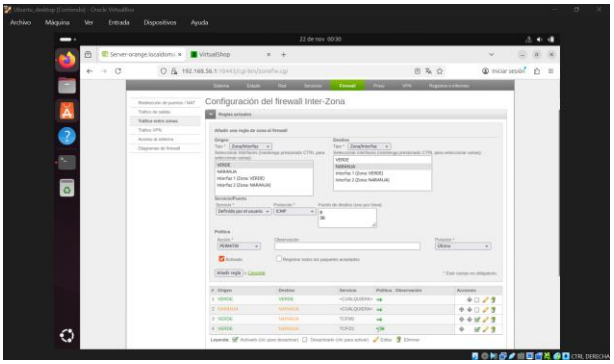
### 2.3.2 DENEGAR EL PROTOCOLO ICMP (PUERTO 8 Y PUERTO 30) PARA NO PERMITIR HACER PING EN LA RED. PROBAR A TRAVÉS DE UNA CONSOLA O TERMINAL LA NO RESPUESTA DEL COMANDO PING HACIA UNA IP DE LA RED.

En el tráfico entre zonas, en la cual se crearon las reglas anteriores, se realiza la negación del servicio ICMP, este servicio permite realizar peticiones por medio de la herramienta “ping” que permite comprobar la accesibilidad de un host.

Para este caso, se realizará la creación de dos reglas definidas para denegar las peticiones ping desde cualquier host de la red y hacia internet.

Inicialmente se realiza la creación de la regla que permitirá la petición ping desde el equipo cliente (zona verde) hacia el servidor web (zona naranja) y hacia internet (zona roja) para realizar la validación de respuesta.

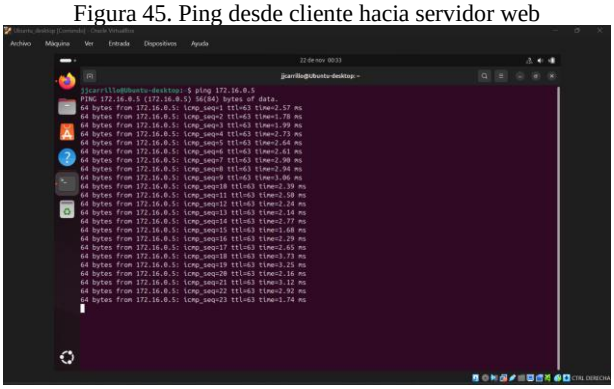
Figura 44. Creación de la regla 1 para permitir ICMP



. Fuente: Autoría Propia

Creada la regla y aplicados los cambios, se realiza la validación del servicio ICMP realizando la petición ping desde la terminal del cliente (zona verde) hacia el servidor web (zona naranja).

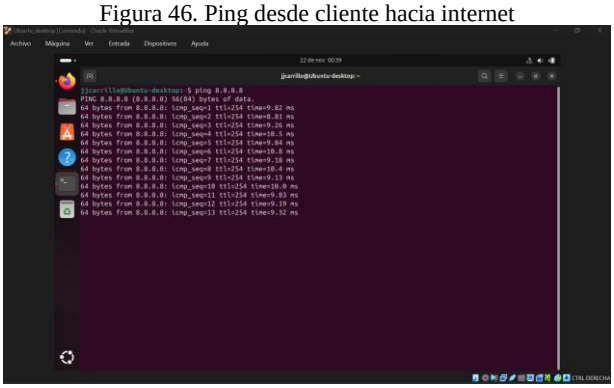
Figura 45. Ping desde cliente hacia servidor web



. Fuente: Autoría Propia

Se realiza la petición desde el cliente (zona verde) hacia internet (zona roja) para este caso usaremos la dirección IP de los DNS públicos de Google (8.8.8.8)

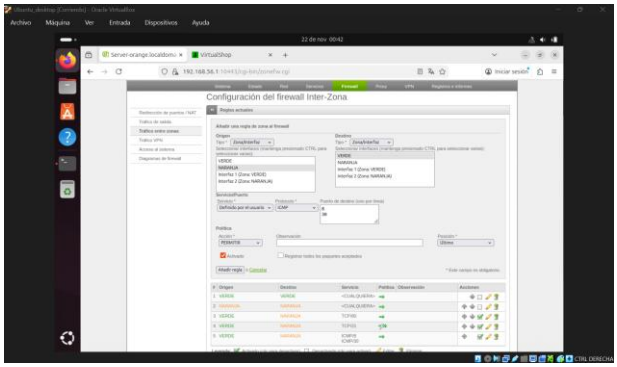
Figura 46. Ping desde cliente hacia internet



. Fuente: Autoría Propia

Ahora se realiza la creación de la regla que permitirá la petición ping desde el servidor web (zona naranja) hacia el cliente (zona verde) y hacia internet (zona roja) para realizar la validación de respuesta.

Figura 47. Creación de la regla 2 para permitir ICMP



. Fuente: Autoría Propia

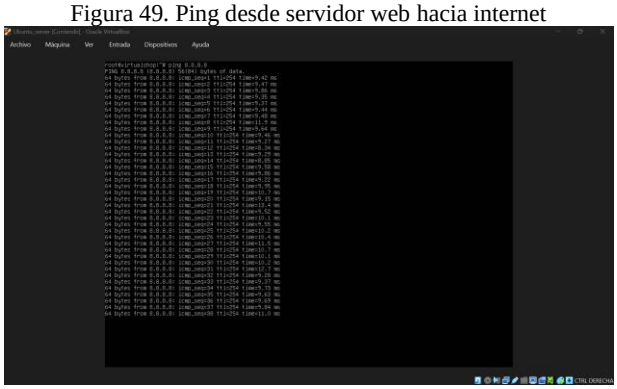
Creada la regla 2 y aplicados los cambios, se realiza la validación del servicio ICMP realizando la petición ping desde la terminal del servidor web (zona naranja) hacia el cliente (zona verde).

Figura 48. Ping desde servidor web hacia el cliente

. Fuente: Autoría Propia

Se realiza la petición desde el servidor web (zona naranja) hacia internet (zona roja) para este caso usaremos la dirección IP de los DNS públicos de Google (8.8.8.8)

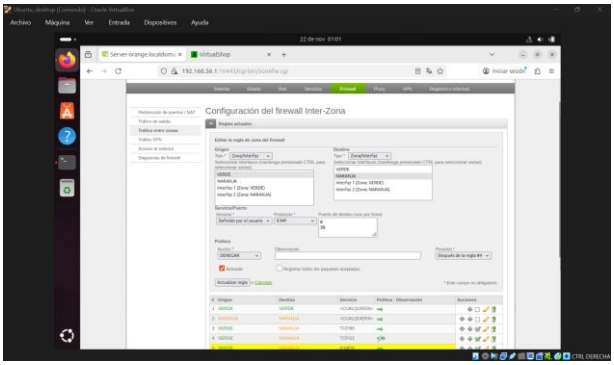
Figura 49. Ping desde servidor web hacia internet



. Fuente: Autoría Propia

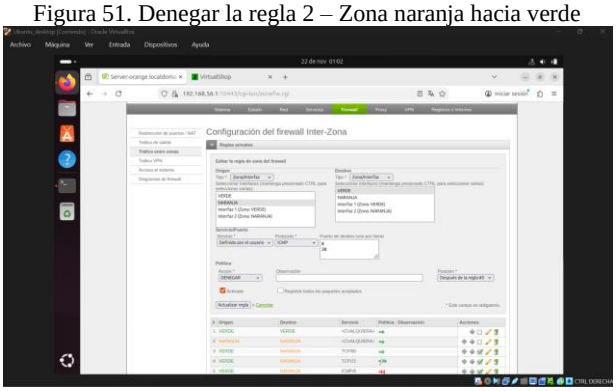
Se procede con la negación del servicio ICMP, este proceso se realiza sobre las reglas ya creadas en donde se modificará la acción estableciéndose en estado “DENEGAR”.

Figura 50. Denegar la regla 1 – Zona verde hacia Naranja



. Fuente: Autoría Propia

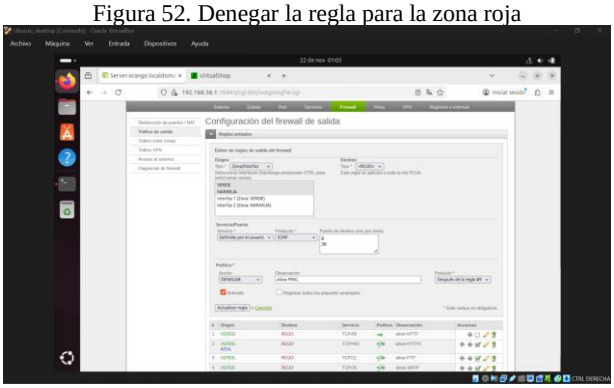
Figura 51. Denegar la regla 2 – Zona naranja hacia verde



. Fuente: Autoría Propia

Es necesario modificar la regla de la opción “Tráfico de salida” ya que es la regla que restringe la petición ping hacia internet, si la regla no existe, es necesario crearla para definir la denegación del servicio.

Figura 52. Denegar la regla para la zona roja

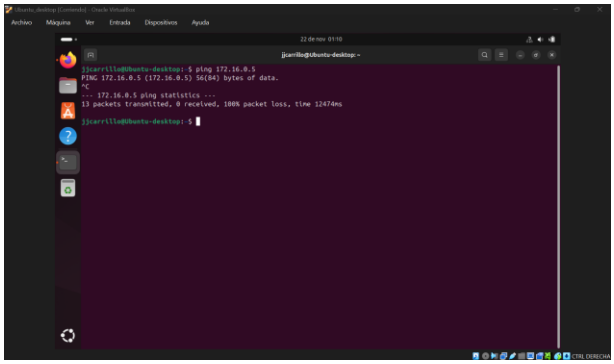


. Fuente: Autoría Propia

Posterior a la denegación de todas las reglas, se procede con la validación del servicio ICMP, el cual no debe responder a ping desde ninguna de las zonas.

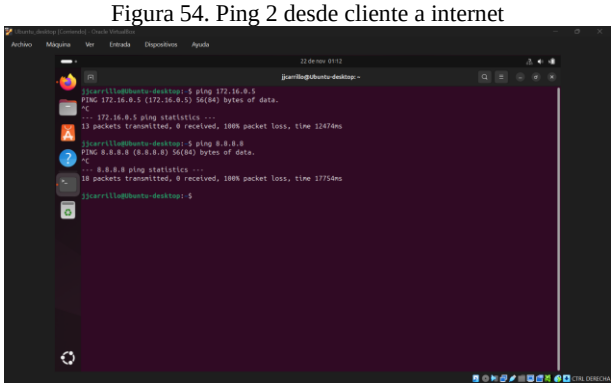
La primera validación se realiza desde el equipo cliente (zona verde) hacia el servidor web (zona naranja) y hacia internet (zona roja).

Figura 53. Ping 2 desde cliente a servidor web



. Fuente: Autoría Propia

Figura 54. Ping 2 desde cliente a internet



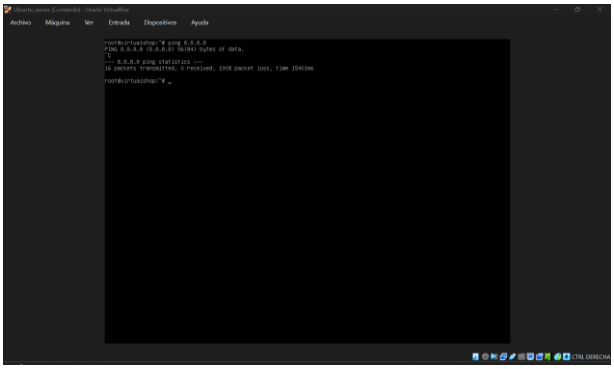
. Fuente: Autoría Propia

La segunda validación se realiza desde el servidor web (zona naranja) hacia el cliente (zona verde) y hacia internet (zona roja).

Figura 55. Ping 2 desde servidor web a cliente

. Fuente: Autoría Propia

Figura 56. Ping 2 desde servidor web a internet



. Fuente: Autoría Propia

Posterior a las validaciones, se puede comprobar que las reglas se implementaron de forma correcta denegando el servicio ICMP y permitiendo los servicios HTTP y FTP.

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

Previa configuración del Endian Firewall, se definió la siguiente segmentación de red.

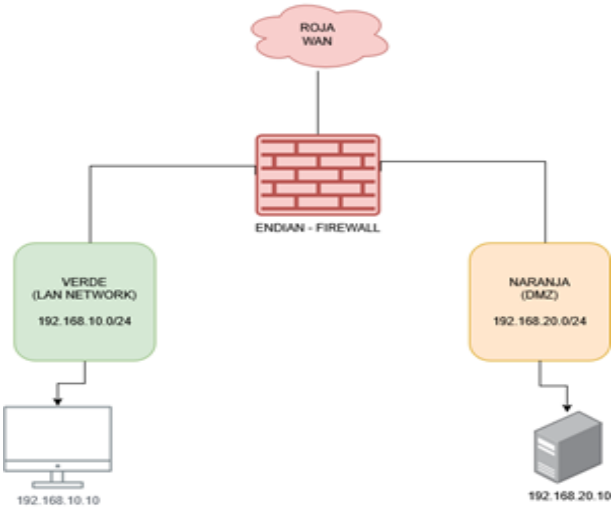
*Tabla 3.*

| | **Zona verde** | **Zona naranja** |
|---|---|---|
| Nat | 192.168.10.0/24 | 192.168.20.0/24 |
| Tipo de asignación | DHCP | DHCP |
| Puerta de enlace | 192.168.10.1 | 192.168.20.1 |
| Máscara de red | 255.255.255.0 | 255.255.255.0 |
| Rango de Ip´s | 192.168.10.2-253 | 192.168.20.2-253 |

Fuente: Autoría Propia

Y se diagrama la estructura de configuración del laboratorio para esta temática.

Figura 57. Diagrama de red




. Fuente: Autoría Propia

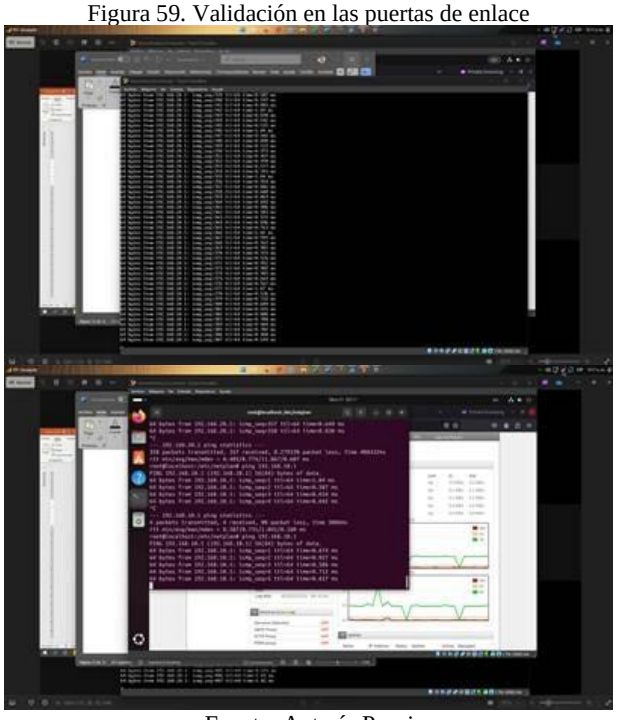
Se procede a ingresar a la administración del firewall, para este caso el acceso se realiza desde la dirección ip: 192.168.10.1:10443.

Figura 58. Administración Endian

. Fuente: Autoría Propia

Se verifica el alcance a las puertas de enlace 192.168.10.1 y 192.168.20.1 tanto desde Ubuntu Desktop como desde Ubuntu Server, confirmando así la correcta conectividad en los dos entornos.

Figura 59. Validación en las puertas de enlace



. Fuente: Autoría Propia

En el servidor se realiza la instalación del servicio Apache y se habilita el servicio FTP. Posteriormente, se configura un sitio sencillo con el fin de realizar pruebas de acceso a través del servicio FTP.

Figura 60. Instalación de servicios

```
listen=YES
anonymous_enable=NO
local_enable=YES
write_enable=YES
chroot_local_user=YES
pasv_enable=YES
pasv_min_port=20000
pasv_max_port=21010
```

. Fuente: Autoría Propia

Se establece la comunicación entre la zona Verde y la zona Naranja mediante los protocolos HTTP y FTP, utilizando sus respectivos puertos. De acuerdo a los requerimientos, la red Naranja debe tener acceso tanto a la red Roja como a la red Verde. Para ello, se habilitan los permisos correspondientes en el firewall, permitiendo también la salida a Internet, y se crean dos nuevas reglas específicas para la red Naranja.

Figura 61. Red Naranja, servicio de HTTP puerto 80

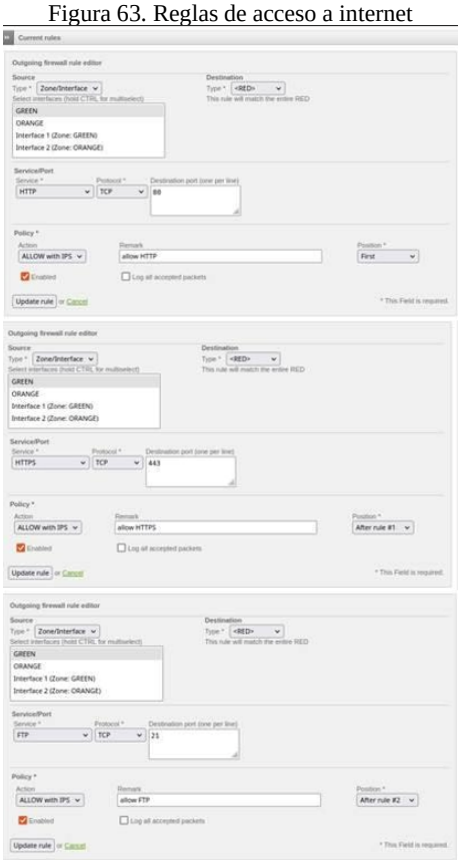

. Fuente: Autoría Propia

Figura 62. Red Naranja, servicio HTTPS puerto 443


. Fuente: Autoría Propia

Para el tráfico saliente de la LAN se crean las reglas necesarias que permitirán el acceso a Internet. Se selecciona la zona Naranja, el servicio HTTP, el protocolo TCP y el puerto 80, con el fin de habilitar correctamente dicho servicio.

Figura 63. Reglas de acceso a internet



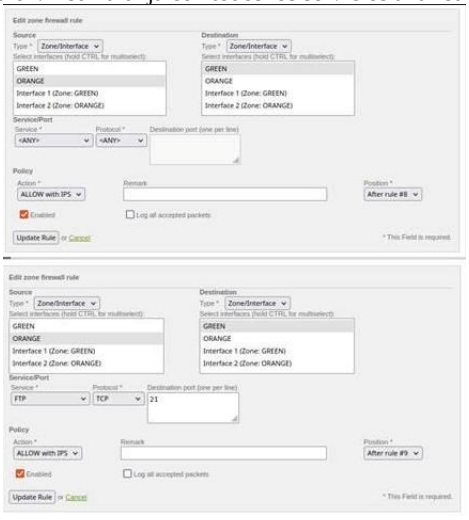
. Fuente: Autoría Propia

Con estas mismas reglas creadas en esta zona, se permite que pueda comunicar la zona con internet. Lo cual confirma la aplicación de la regla.

Ahora se validan las reglas del tráfico entre zonas.

El enfoque principal se centrará en la red naranja, ya que es la que presenta mayores restricciones. Para ello, se crean tres reglas que permiten el tráfico HTTP, HTTPS y FTP hacia la red verde.

Figura 64. Red naranja con todos los servicios a la red verde



. Fuente: Autoría Propia

Para la zona naranja se implementa un sitio web HTTP que podrá ser accedido desde la red LAN.

Figura 65. Sitio test en DMZ

. Fuente: Autoría Propia

Desde la red LAN se accede y se verifica el alcance al sitio web HTML mediante el protocolo HTTP.

Figura 66. Validación desde LAN hacia el sitio HTTP


. Fuente: Autoría Propia

Se realiza el ingreso del servicio HTTP desde la LAN hacia la WAN.

Figura 67. Validación desde LAN a WAN

. Fuente: Autoría Propia

Se valida el servicio HTTP desde la zona DMZ (zona naranja) hacia la red WAN

Figura 68. Validación del servicio HTTP en DMZ

. Fuente: Autoría Propia

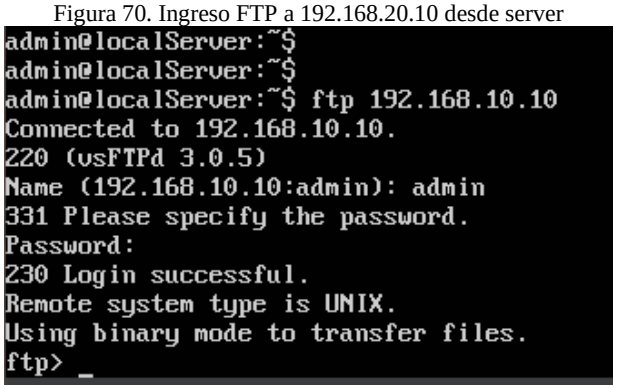
Se valida el ingreso del servicio FTP desde la LAN hacia la WAN.

Figura 69. Ingreso FTP a 192.168.20.10 desde cliente


. Fuente: Autoría Propia

Validación de ingreso del servicio FTP desde la WAN hacia la zona DMZ.

Figura 70. Ingreso FTP a 192.168.20.10 desde server




. Fuente: Autoría Propia

El laboratorio permitió validar de manera exitosa la configuración y funcionamiento de las reglas de comunicación entre las distintas zonas de la infraestructura. Se logró establecer correctamente la conexión entre la zona verde y la zona naranja mediante los protocolos HTTP, FTP y la comunicación entre la zona roja (WAN) y la zona naranja (DMZ).

## 3. CONCLUSIONES

La implementación de un sistema firewall otorga al administrador de sistemas el control total sobre el tráfico de la red, permitiéndole gestionar el uso de los recursos internos. La destreza para instalar y configurar herramientas de código abierto como Endian es una gran alternativa empresas, ya que proporciona una solución de seguridad robusta y de alta calidad con inversiones de bajo costos. El conocimiento en estas herramientas open source se posiciona como un activo indispensable para el control y la eficiencia operativa.

La ejecución individual de cada temática propuesta ha sido fundamental para el desarrollo de competencias prácticas y sólidas en el manejo de Endian Firewall como plataforma de seguridad perimetral.

A través de la instalación, configuración inicial y administración de sus servicios clave, se adquirido un entendimiento profundo de conceptos esenciales como el control de tráfico, la Traducción de Direcciones de Red (NAT) y la Zona Desmilitarizada (DMZ)

Habilitar los servicios HTTP (puerto 80) y FTP (puerto 21) desde el servidor web y con una configuración correcta en el firewall Endian, permitió el acceso controlado a los servicios esenciales de publicación web y transferencia de archivos. Mediante la creación de reglas de tráfico, se logró definir las conexiones necesarias hacia el servidor, manteniendo la arquitectura de red organizada por zonas (verde, naranja y roja) que brinda la seguridad del entorno.

La configuración de reglas para denegar el protocolo ICMP en los puertos 8 y 30 permitió bloquear eficazmente las peticiones ping dentro de la red. Estas reglas fortalecieron la seguridad del entorno, impidiendo que los equipos utilicen el ICMP como mecanismo de reconocimiento de terminales o equipos, ataques de denegación de servicios, falsificación de paquetes u otras actividades maliciosas que vulneren la integridad de la red y la información.

## 4. CITAS Y/O REFERENCIAS


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

[2] Install and configure Endian Firewall on VirtualBox. (2019, May 21). Kifarunix.com. https://kifarunix.com/install-and-configure-endian-firewall-on-virtualbox

[3] Guía Debian GNU/Linux de instalación. (n.d.). Debian.org. Retrieved November 22, 2025, from https://www.debian.org/releases/stable/amd64/index.es.html

[4] User guide for release 7.2. (n.d.). Virtualbox.org. Retrieved November 22, 2025, from https://www.virtualbox.org/manual/

[5] Endian UTM 3.2 Reference Manual — Endian UTM 3.2 Reference Manual. (n.d.). Endian.com. Retrieved November 22, 2025, from https://docs.endian.com/3.2/utm/index.html

[6] The vsftpd Project, "vsftpd — Very Secure FTP Daemon," Documentación oficial, 2023. [En línea]. Disponible: http://vsftpd.beasts.org

[7] J. Postel y J. Reynolds, "File Transfer Protocol (FTP)," RFC 959, Internet Engineering Task Force (IETF), Oct. 1985. [En línea]. Disponible: https://www.rfc-editor.org/rfc/rfc959

[8] Á. J. Cervelión, "Instalación de Nagios Core 4.4 en Ubuntu 22.04," Repositorio Institucional UNAD, 2023. [En línea]. Disponible: https://repository.unad.edu.co/handle/10596/54230

[9] The Linux Documentation Project, Linux Networking-HOWTO, 2008. [En línea]. Disponible: https://tldp.org/HOWTO/NET3-4-HOWTO.html

[10] (N.d.). Endian.com. Retrieved November 25, 2025, from https://help.endian.com/hc/en-us/articles/218144668-Basic-Network-Commands