

INSTALACIÓN Y CONFIGURACIÓN DE ENDIAN COMO FIREWALL PARA LA SEGURIDAD EN GNU/LINUX EN UNA RED SEGMENTADA

Luis Antonio Navarro Cadena
e-mail: lanavarroc@unadvirtual.edu.co

RESUMEN: En este informe detalla el proceso de instalación y configuración de Endian Firewall en un entorno virtual, utilizando el software de virtualización VirtualBox. Se realiza la correcta asignación de tarjetas de red para establecer una red segmentada compuesta por zona Verde (LAN), zona Naranja (DMZ) y zona Roja (WAN), con el fin de proteger los diferentes segmentos de la red y de reforzar la seguridad en sistemas basados en GNU/Linux.

PALABRAS CLAVE: DMZ, Endian Firewall, LAN, WAN.

1 INTRODUCCIÓN

En el contexto actual de la administración de sistemas operativos de código abierto la implementación de medidas de seguridad en sistemas GNU/Linux es una tarea muy importante para los entornos que demandan segmentación de redes. Esta actividad contribuye al desarrollo de competencias prácticas en administración de redes y seguridad sobre sistemas GNU/Linux y tiene como propósito documentar el proceso de instalación e implementación de un entorno de red seguro basado en la distribución GNU/Linux Endian Firewall Community.

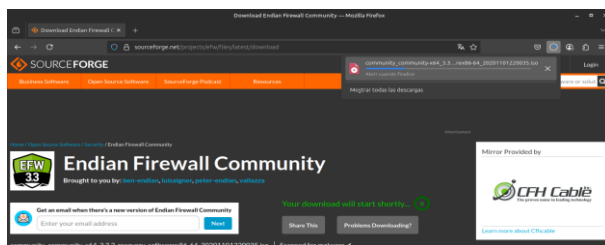
2 DESARROLLO DE LA TEMÁTICA

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

Se descargó la imagen ISO de Endian, en este caso la versión Endian Firewall Community desde su página web oficial <https://sourceforge.net/projects/efw/>.

La Fig. 1 muestra la descarga de Endian Firewall desde su página oficial.

Figura 1. Descarga de Endian

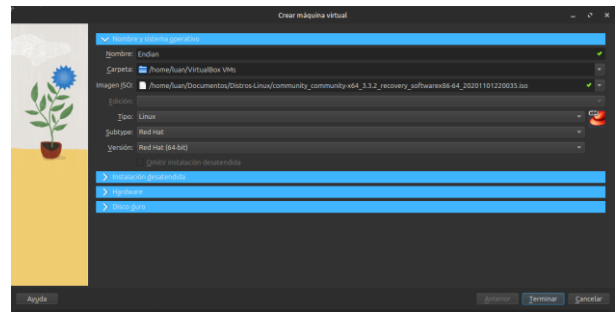


Fuente: Autoría propia

Cuando ha terminado la descarga de la imagen ISO, se realizó la configuración y la instalación de Endian en el software de virtualización VirtualBox.

La Fig. 2 muestra como se asignó nombre de la máquina virtual, se seleccionó la ISO que usará para instalar el sistema, el tipo y la versión.

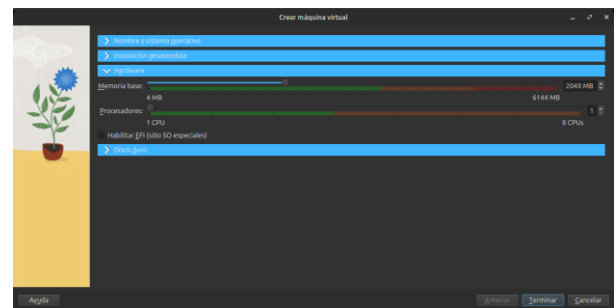
Figura 2. Nombre y sistema operativo de Endian VBox



Fuente: Autoría propia

La Fig. 3 muestra la configuración de hardware donde se asignó 2048 MB de memoria base y 1 CPU de procesador.

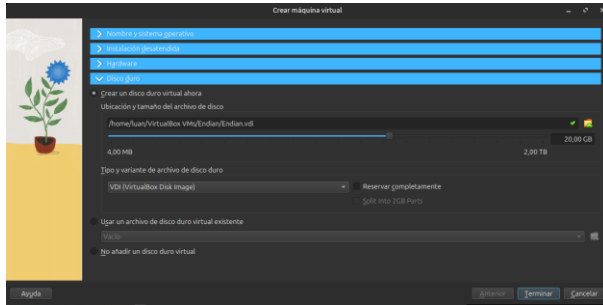
Figura 3. Hardware de Endian VBox



Fuente: Autoría propia

La Fig. 4 muestra como se asignó el espacio de almacenamiento que usará Endian, indicando que es 20 GB.

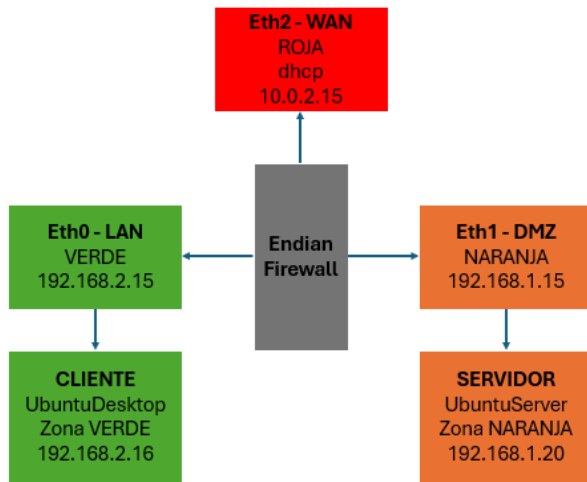
Figura 4. Disco duro de Endian VBox



Fuente: Autoría propia

En este paso se diseñó la siguiente grafica de la red que es la que se implementó para desarrollar la temática 1 como se muestra en la Fig. 5.

Figura 5. Gráfico de la red

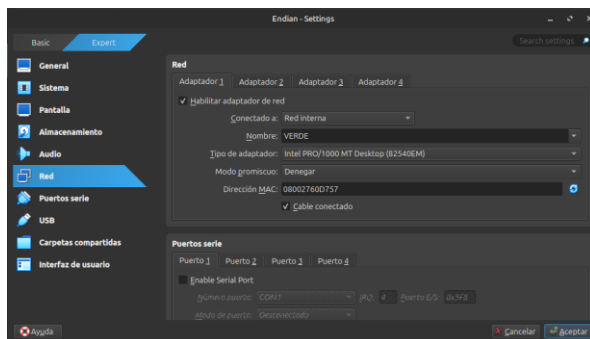


Fuente: Autoría propia

Se configuro tres adaptadores de red, los dos primeros corresponden a una red interna y el tercero fue configurado como un adaptador NAT, que nos permitió tener el acceso a internet.

La Fig. 6 muestra la configuración aplicada al Adaptador 1 Red interna VERDE.

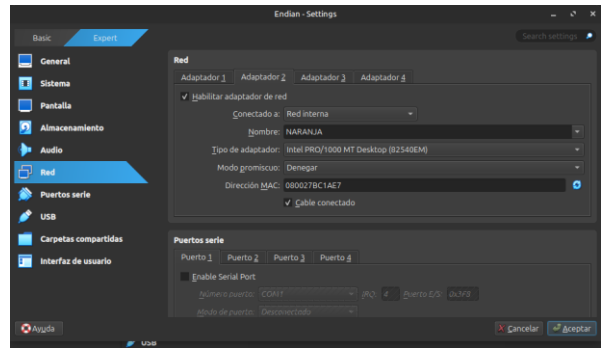
Figura 6. Adaptador 1 Red interna VERDE



Fuente: Autoría propia

La Fig. 7 muestra la configuración aplicada al Adaptador 2 Red interna NARANJA.

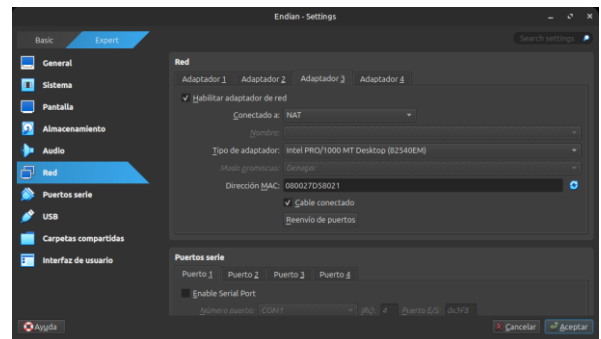
Figura 7. Adaptador 2 Red interna NARANJA



Fuente: Autoría propia

La Fig. 8 muestra la configuración aplicada al Adaptador 3 NAT.

Figura 8. Adaptador 3 NAT

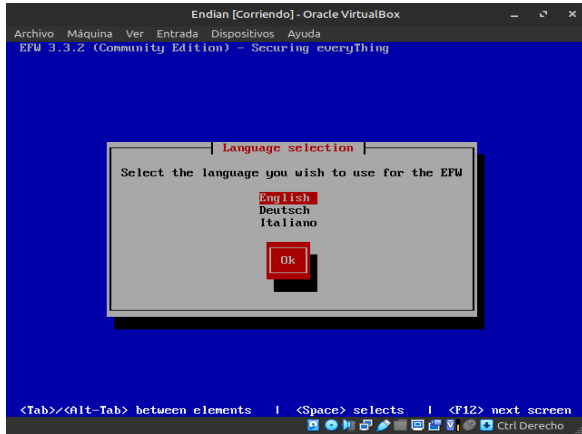


Fuente: Autoría propia

Una vez finalizo las configuraciones de los adaptadores de red se inició la máquina virtual, para comenzar con la instalación de Endian.

Se selecciono el idioma de preferencia, en este caso fue inglés, como se muestra en la Fig. 9.

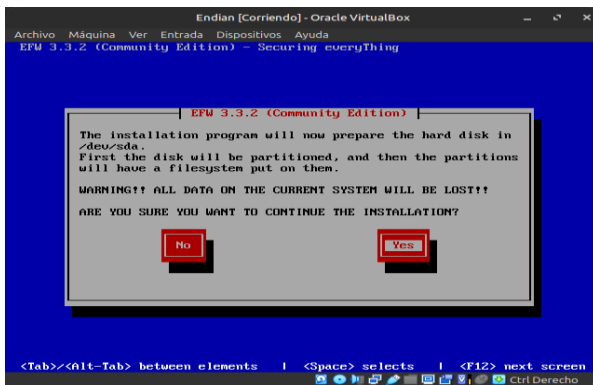
Figura 9. Selección del lenguaje



Fuente: Autoría propia

Se selecciono la opción Yes, para continuar con la instalación, como se muestra en la Fig. 10.

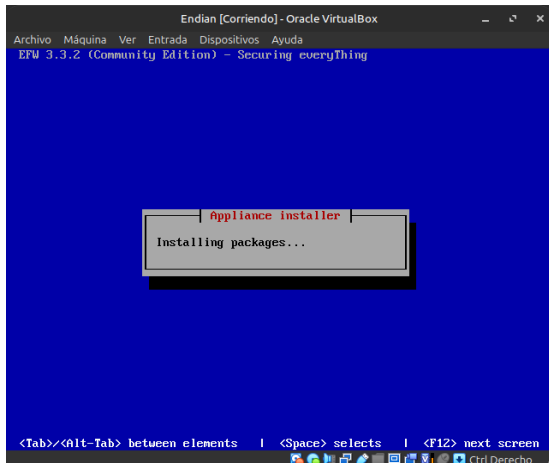
Figura 10. Instalación de Endian



Fuente: Autoría propia

La Fig. 11 muestra la evidencia del proceso de instalación de paquetes para el sistema Endian.

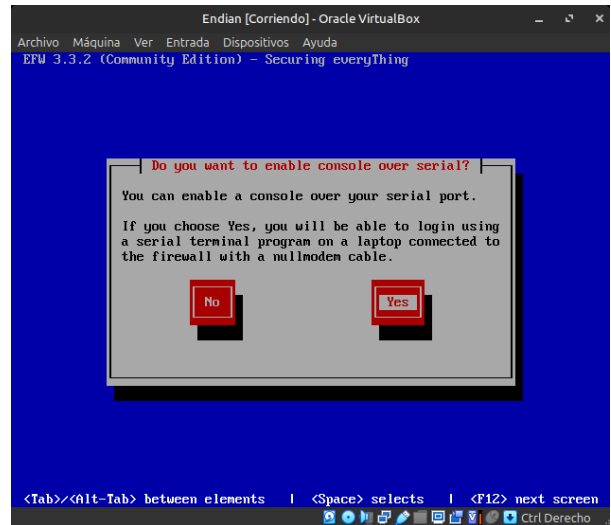
Figura 11. Instalación paquetes de Endian



Fuente: Autoría propia

Se escogió la opción Yes para habilitar consola, como se muestra en la Fig. 12.

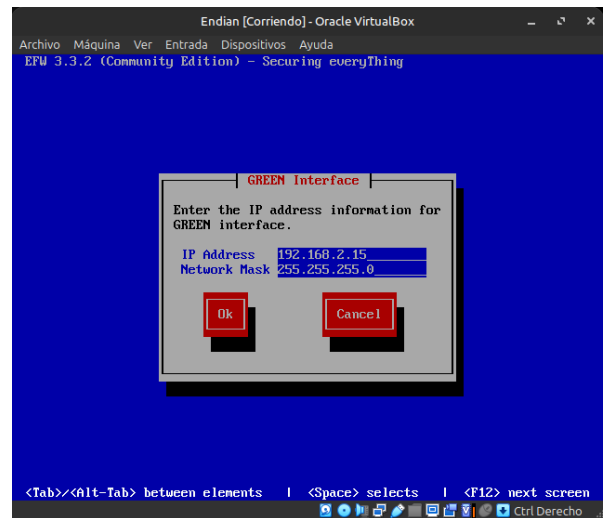
Figura 12. Habilitación de consola



Fuente: Autoría propia

La Fig. 13 muestra cómo se asigno la IP 198.162.2.15 para la zona VERDE.

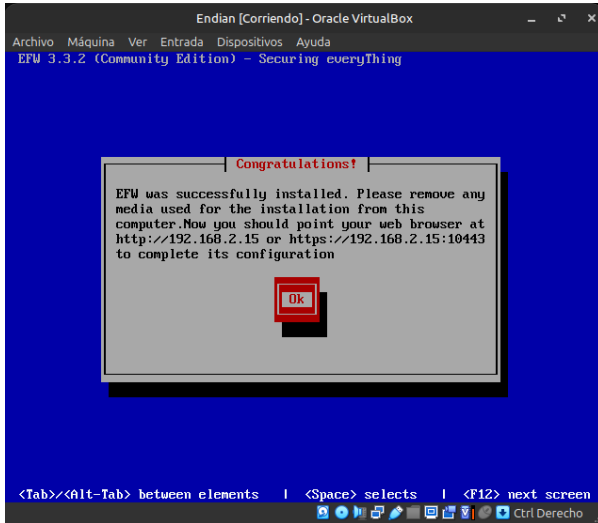
Figura 13. Dirección IP zona VERDE



Fuente: Autoría propia

La Fig. 14 muestra que la instalación de Endian ha sido exitosa. También nos indica que para finalizar la configuración de Endian se abre un navegador web en otro equipo en este caso será UbuntuDesktop y se accede a la dirección <http://192.168.2.15:10443>.

Figura 14. Instalación exitosa de Endian

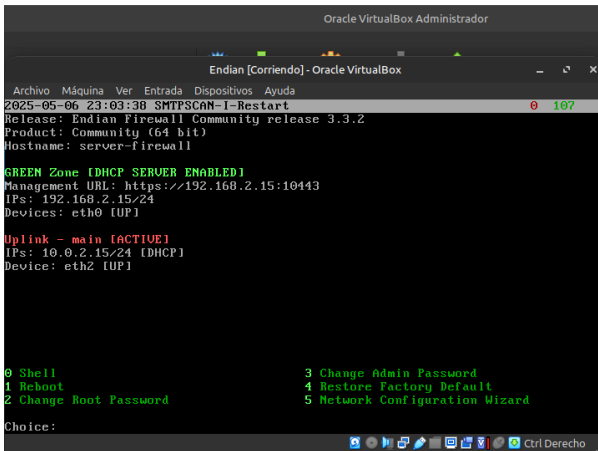


Fuente: Autoría propia

La máquina se ha reiniciado y muestra que Endian Firewall ya está instalado y funcionando correctamente.

También podemos visualizar que en Endian en la Zona ROJA tiene conexión a internet, como se muestra en la Fig. 15.

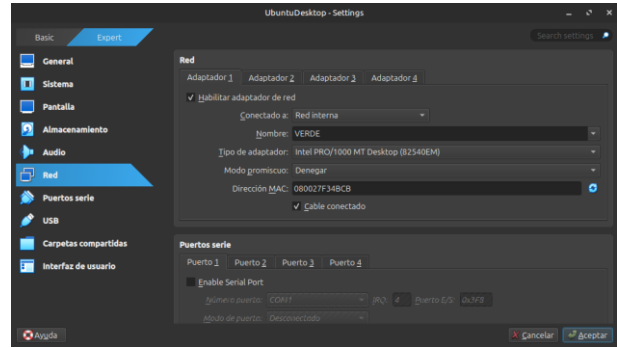
Figura 15. Endian funcionando correctamente



Fuente: Autoría propia

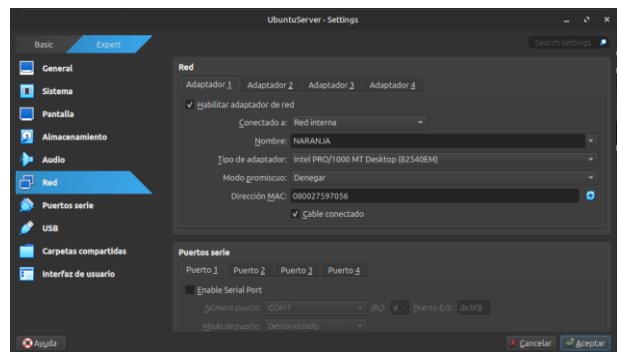
Una vez terminada la instalación de Endian Firewall se configuro de Ubuntu Desktop “cliente” con un adaptador de red conectado a la red interna VERDE como se muestra en la Fig. 16 y Ubuntu Server “servidor” con adaptador conectado a la red interna NARANJA como se muestra en la Fig. 17.

Figura 16. Adaptador de red Ubuntu Desktop



Fuente: Autoría propia

Figura 17. Adaptador de red Ubuntu Server

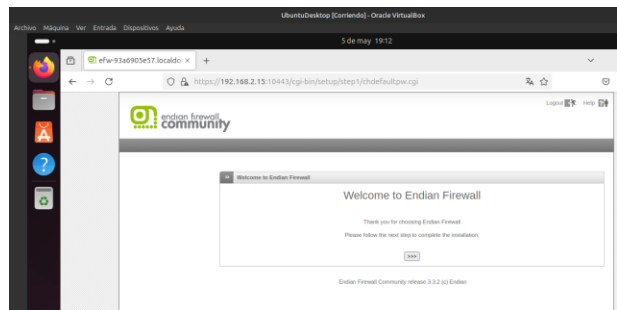


Fuente: Autoría propia

Ya instalados y configurados Endian, Desktop y Server, ahora se inicia la máquina virtual Ubuntu Desktop, la cual se conectará con el sistema de Endian Firewall.

Ahora se accede a la interfaz web de administración de Endian con la dirección IP de la instalación de Endian en este caso <https://192.168.2.15:10443/>, como se muestra en la Fig. 18.

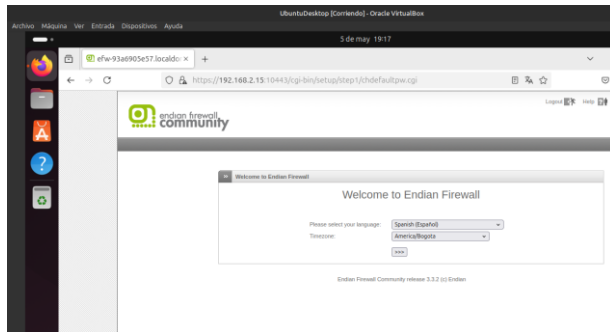
Figura 18. Interfaz web de Endian



Fuente: Autoría propia

La Fig. 19 muestra como se selecciono el idioma deseado y la zona horaria:

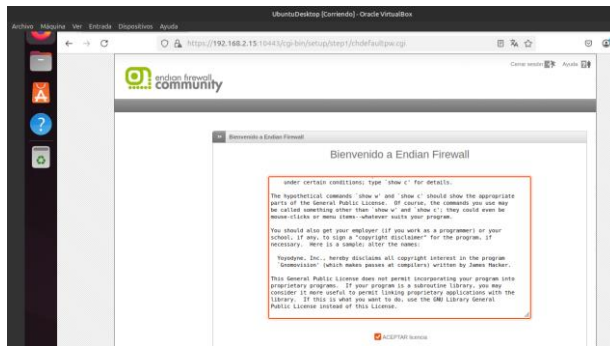
Figura 19. Lenguaje y zona horaria Endian Firewall



Fuente: Autoría propia

Aceptemos términos y condiciones de la licencia de Endian Firewall, como se muestra en la Fig. 20.

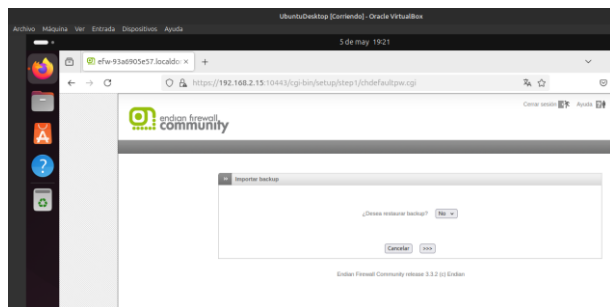
Figura 20. Licencia Endian Firewall



Fuente: Autoría propia

En restaurar una copia de seguridad o backup se dejó la opción por default, como se muestra en la Fig. 21.

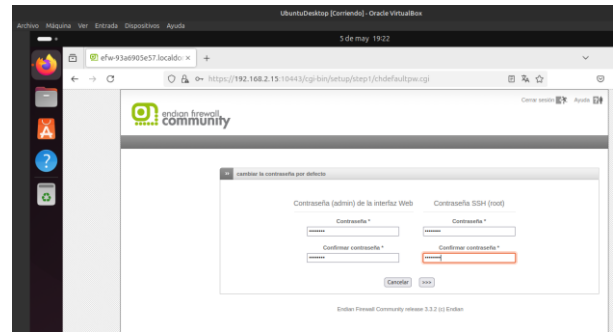
Figura 21. Importar Backup



Fuente: Autoría propia

Se indicaron las contraseñas del administrador de la interfaz web de Endian y la contraseña SSH, como se muestra en la Fig. 22.

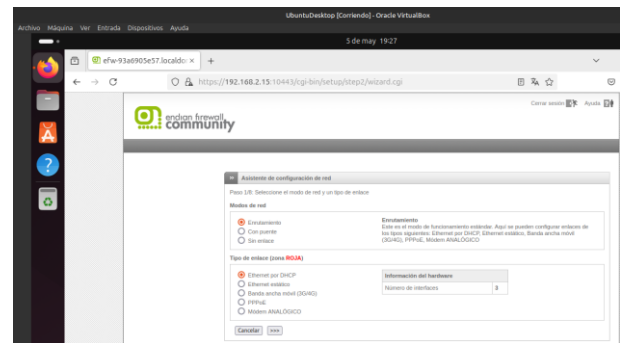
Figura 22. Contraseña admin y SSH



Fuente: Autoría propia

La Fig. 23 muestra como se selecciono el modo de red Enrutamiento y tipo de enlace Ethernet por DHCP a la zona ROJA. También vemos que el servidor de Endian tiene 3 tarjetas configuradas.

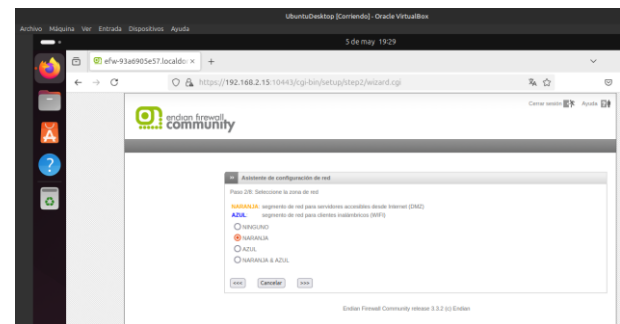
Figura 23. Modos de red y tipo de enlace



Fuente: Autoría propia

La Fig. 24 muestra cómo se seleccionó la zona faltante, por lo que se seleccionó la zona NARANJA para habilitar la segmentación DMZ.

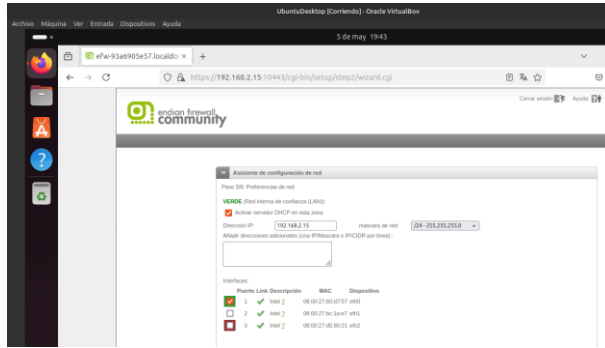
Figura 24. Selección zona DMZ



Fuente: Autoría propia

La Fig. 25 muestra cómo se configuro la zona VERDE (LAN) y zona NARANJA(DMZ). Para ello se asignó la dirección IP 192.168.2.15/24 zona VERDE (LAN), asignado anteriormente en el sistema.

Figura 25. Configuración zona VERDE (LAN)



Fuente: Autoría propia

La Fig. 26 muestra cómo se asignó la dirección IP 192.168.1.15/24 zona NARANJA (LAN) y se estableció el nombre del host como server-firewall.

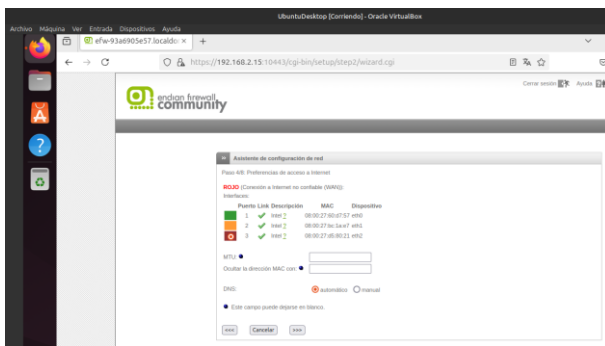
Figura 26. Configuración zona NARANJA (DMZ)



Fuente: Autoría propia

Se define la zona ROJA (WAN), para el acceso a la conexión de internet, como se muestra en la Fig. 27.

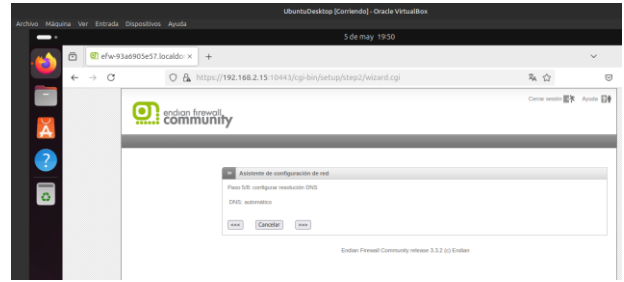
Figura 27. Conexión a internet zona ROJA (WAN)



Fuente: Autoría propia

Se dejó como automático en configuración de la resolución DNS, como se muestra en la Fig. 28.

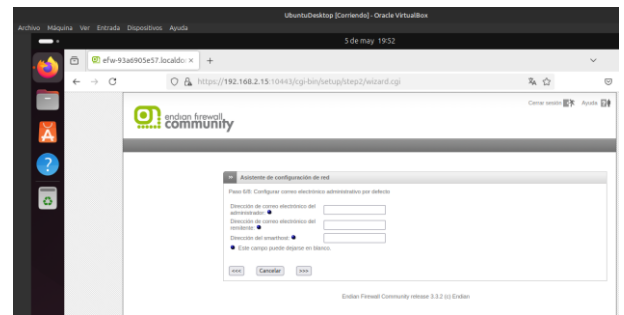
Figura 28. Resolución DNS



Fuente: Autoría propia

En la configuración de correo electrónico administrativo se dejó en blanco y se continuó con la configuración, como se muestra en la Fig. 29.

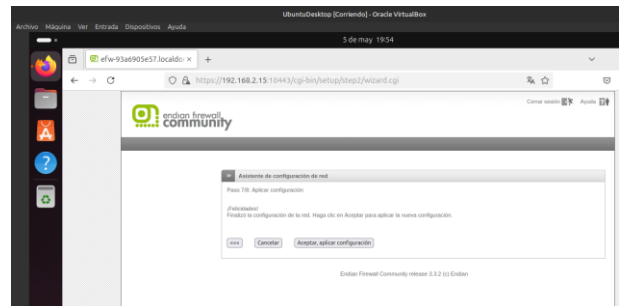
Figura 29. Correo electrónico administrativo por defecto



Fuente: Autoría propia

Hemos finalizado la configuración de la red y se procede a aplicar las configuraciones realizadas, como se muestra en la Fig. 30.

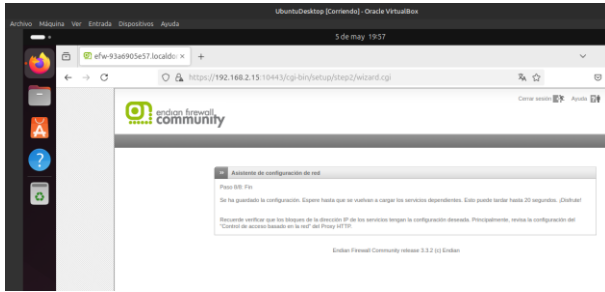
Figura 30. Aplicar la configuración



Fuente: Autoría propia

En la Fig. 31 muestra cómo se evidencia la finalización de la configuración mediante la interfaz web de Endian, lo que indica que la configuración ha sido guardada correctamente.

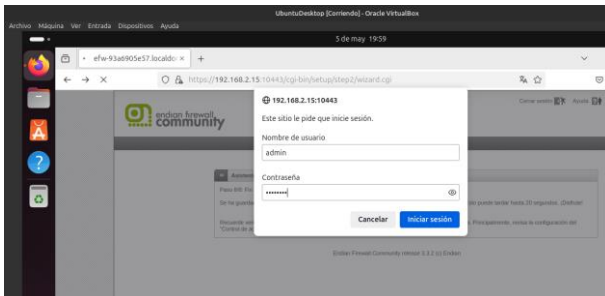
Figura 31. Finalización de la configuración de red



Fuente: Autoría propia

La Fig. 32 muestra el inicio sesión luego de la configuración, con el nombre de usuario y la contraseña que ha sido previamente configurada.

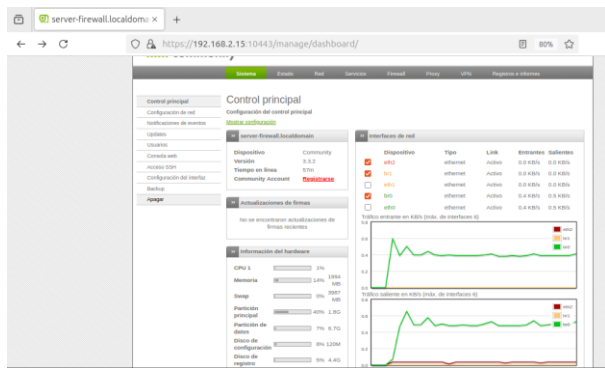
Figura 32. Inicio de cesión Endian Firewall



Fuente: Autoría propia

Hemos llegado al panel de control principal de Endian Firewall. Esta interfaz ofrece una visión general del sistema mostrando el estado de las interfaces de red, como se muestra en la Fig. 33.

Figura 33. Panel de control principal de Endian Firewall

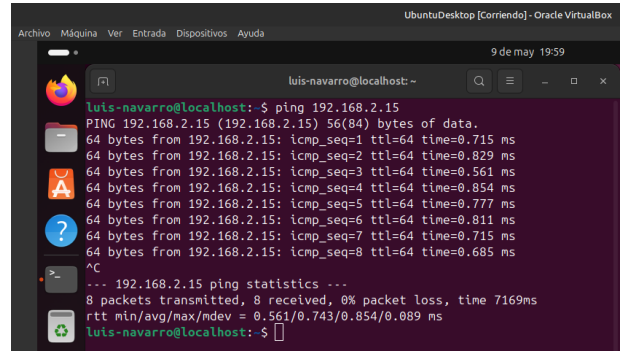


Fuente: Autoría propia

Validamos la conectividad de la configuración de red realizada:

Validación desde el Cliente UbuntuDesktop hacia Zona VERDE (LAN - Eth0), como se muestra en la Fig. 34.

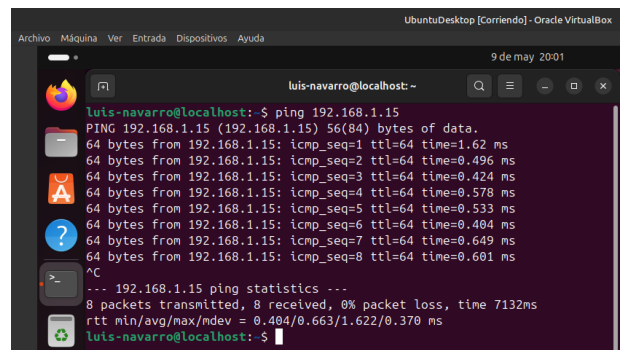
Figura 34. Conectividad del cliente hacia zona Verde



Fuente: Autoría propia

Validación desde el Cliente UbuntuDesktop hacia Zona NARANJA (DMZ – Eth1), como se muestra en la Fig. 35

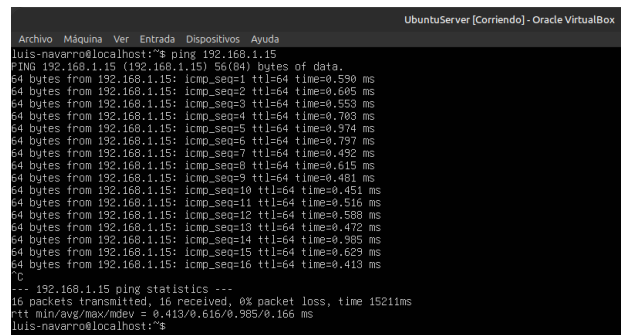
Figura 35. Conectividad del cliente hacia zona NARANJA



Fuente: Autoría propia

Validación desde el Servidor UbuntuServer hacia Zona NARANJA (DMZ – Eth1), como se muestra en la Fig. 36.

Figura 36. Conectividad del servidor hacia zona NARANJA



Fuente: Autoría propia

Validación desde el Servidor UbuntuServer hacia Zona VERDE (LAN - Eth0), como se muestra en la Fig. 37.

Figura 37. Conectividad del servidor hacia zona Verde

```

UbuntuServer [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
luis-navarro@localhost:~$ ping 192.168.2.15
PING 192.168.2.15 (192.168.2.15) 56(84) bytes of data.
64 bytes from 192.168.2.15: icmp_seq=1 ttl=64 time=0.913 ms
64 bytes from 192.168.2.15: icmp_seq=2 ttl=64 time=0.557 ms
64 bytes from 192.168.2.15: icmp_seq=3 ttl=64 time=0.766 ms
64 bytes from 192.168.2.15: icmp_seq=4 ttl=64 time=0.548 ms
64 bytes from 192.168.2.15: icmp_seq=5 ttl=64 time=0.820 ms
64 bytes from 192.168.2.15: icmp_seq=6 ttl=64 time=0.609 ms
64 bytes from 192.168.2.15: icmp_seq=7 ttl=64 time=0.512 ms
64 bytes from 192.168.2.15: icmp_seq=8 ttl=64 time=0.791 ms
64 bytes from 192.168.2.15: icmp_seq=9 ttl=64 time=0.730 ms
64 bytes from 192.168.2.15: icmp_seq=10 ttl=64 time=0.742 ms
64 bytes from 192.168.2.15: icmp_seq=11 ttl=64 time=0.533 ms
64 bytes from 192.168.2.15: icmp_seq=12 ttl=64 time=0.594 ms
64 bytes from 192.168.2.15: icmp_seq=13 ttl=64 time=0.543 ms
64 bytes from 192.168.2.15: icmp_seq=14 ttl=64 time=0.495 ms
64 bytes from 192.168.2.15: icmp_seq=15 ttl=64 time=0.529 ms
^C
--- 192.168.2.15 ping statistics ---
15 packets transmitted, 15 received, 0% packet loss, time 14235ms
rtt min/avg/max/mdev = 0.495/0.645/0.913/0.129 ms
luis-navarro@localhost:~$

```

Fuente: Autoría propia

Las pruebas de conectividad con ping desde diferentes zonas demostraron que la configuración de Endian Firewall y la segmentación de red (zonas VERDE LAN, NARANJA DMZ y ROJA WAN) fueron implementadas correctamente.

3 TÍTULO PRINCIPAL

La correcta implementación de Endian Firewall para la temática 1 permite establecer un entorno de red segmentado y seguro, fortaleciendo la seguridad perimetral al controlar el tráfico de forma eficiente entre las diferentes zonas LAN, DMZ y WAN. Estas competencias adquiridas son esenciales para garantizar seguridad de las redes en entornos corporativos o empresariales.

Las pruebas de conectividad que se realizaron entre las diferentes zonas de la red confirman que pueden comunicarse según lo previsto, asegurando la correcta segmentación de red y correcta implementación del firewall Endian.

Aprender a realizar configuraciones de interfaces de red dentro Endian Firewall, es muy importante para los Ingenieros de Sistemas, porque durante todo el proceso de aprendizaje con el conocimiento que adquieren pueden dedicarse a la administración de sistemas con GNU/Linux.

Verificar la conectividad con comandos como ping entre los distintos segmentos de red garantizo que las configuraciones realizadas son correctas y funcionales, garantizando la importancia de la validación en cualquier despliegue de infraestructura de red.

El uso de herramientas de virtualización como el software VirtualBox es muy importante porque facilita el diseño, las pruebas y validación de infraestructuras de red complejas como la que se implementó, permitiendo experimentar configuraciones reales sin comprometer entornos de producción.

4 REFERENCIAS

[1] Endian (2016), Endian UTM 3.2 Manual referencia. Endian. <http://docs.endian.com/3.2/utm/index.html>. [Accessed May 2025].
 [2] Canonical (2023). Guía del Ubuntu desktop 20.04 LTS . Help Ubuntu. <https://help.ubuntu.com/20.04/ubuntu-help/index.html>. [Accessed May 2025].

[3] 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>. [Accessed May 2025].
 [4] Oracle (2020), Manual de usuario VirtualBox . VirtualBox. <https://www.virtualbox.org/manual/>. [Accessed May 2025].
 [5] Free Software Foundation (2016). Software Libre y educación . El sistema operativo GNU. <http://www.gnu.org/education/education.html>. [Accessed May 2025].
 [6] Debian (2023). El manual del administrador de Debian 12.5.0 . Debian. <https://www.debian.org/releases/stable/amd64/index.es.html>. [Accessed May 2025].
 [7] Cerveli3n, . J. (2023). Instalaci3n de Nagios Core 4.4 en Ubuntu 22.04 . [Objeto_virtual_de_informaci3n_OVI]. Repositorio Institucional UNAD. <https://repository.unad.edu.co/handle/10596/54230>. [Accessed May 2025].
 [8] Hernandez, P. F., & Snchez, J. (2022). Monitoreo y administraci3n de sistemas Linux . [Objeto_virtual_de_informaci3n_OVI]. Repositorio Institucional UNAD. <https://repository.unad.edu.co/handle/10596/53211>. [Accessed May 2025].
 [9] Hernndez, P. F., & Snchez, J. (2022). Servidores para administraci3n remota y compartir recursos . [Objeto_virtual_de_informaci3n_OVI]. Repositorio Institucional UNAD. <https://repository.unad.edu.co/handle/10596/53212>. [Accessed May 2025].
 [10] LPI LPIC-1 Exam 101. (2022). Tema 102: Comandos GNU y Unix. <https://learning.lpi.org/es/learning-materials/101-500/102/>. [Accessed May 2025].

Notas:

1. Las configuraciones descritas en este documento fueron realizadas en un entorno virtualizado con la herramienta de virtualizaci3n Oracle VirtualBox con fines didcticos y educativos.