IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL CON ENDIAN FIREWALL EN ENTORNOS VIRTUALIZADOS

Jhoan Andrés Bastidas Caicedo
jabastidasca@unadvirtual.edu.co
Edwin Esteban Calvache Calvache
eecalvachec@unadvirtual.edu.co
Ingrid Alexandra Muñoz Chicangan
iamunozc@unadvirtual.edu.co
Juan Esteban Oviedo Mora
jeoviedormor@unadvirtual.edu.co
Sofia Catherine Rosero Bolaños
scroserob@unadvirtual.edu.co

RESUMEN: *En este artículo se desarrolla una solución de seguridad perimetral utilizando el sistema operativo GNU/Linux Endian, instalado en una máquina virtual con VirtualBox. Se configuraron las zonas verde (LAN), roja (Internet) y naranja (DMZ), asegurando su correcta comunicación a través de reglas NAT. Además, se habilitaron servicios como HTTP y FTP desde la zona DMZ, y se bloquearon protocolos como ICMP para aumentar la seguridad de la red. Se implementaron reglas de acceso para permitir o denegar el tráfico entre las distintas zonas, y se hicieron pruebas desde navegadores web para validar el funcionamiento. Finalmente, se configuró un proxy HTTP no transparente con autenticación de usuarios y una lista negra de sitios web para controlar el acceso desde la LAN. Todo este trabajo demuestra cómo se puede implementar una red segura y segmentada usando Endian como solución principal.*

PALABRAS CLAVES: Seguridad perimetral, Endian Firewall, VirtualBox, Red DMZ

ABSTRACT: *This article develops a perimeter security solution using the GNU/Linux Endian operating system, installed in a virtual machine with VirtualBox. The green (LAN), red (Internet), and orange (DMZ) zones were configured, ensuring proper communication through NAT rules. Additionally, services such as HTTP and FTP were enabled from the DMZ zone, and protocols such as ICMP were blocked to increase network security. Access rules were implemented to allow or deny traffic between the different zones, and tests were performed from web browsers to validate their operation. Finally, a non-transparent HTTP proxy with user authentication and a website blacklist was configured to control access from the LAN. This work demonstrates how a secure, segmented network can be implemented using Endian as the primary solution.*

KEYWORDS: Perimeter Security, Endian Firewall, VirtualBox, DMZ Network

1 INTRODUCCIÓN

Hoy en día, la seguridad perimetral es clave para proteger redes informáticas frente a posibles amenazas externas e internas. En este trabajo se muestra cómo implementar una solución de seguridad usando GNU/Linux Endian como firewall, todo dentro de una máquina virtual creada en VirtualBox. La idea es lograr una segmentación de red clara y funcional, utilizando las zonas verde (LAN), roja (Internet) y naranja (DMZ), y asegurando una buena comunicación entre ellas.

El artículo se divide en cinco partes. Primero, se hace la instalación y configuración inicial de Endian con sus respectivas tarjetas de red. Luego, se configuran reglas NAT para permitir la salida a Internet desde la LAN y desde la DMZ. En la tercera parte, se habilitan servicios como HTTP y FTP desde un servidor en la DMZ y se bloquean protocolos como ICMP. Después, se crean reglas de acceso entre zonas, probando desde navegadores. Por último, se configura un proxy HTTP con autenticación y bloqueo de sitios web.

2 FUNDAMENTOS TÉCNICOS Y CONTEXTO.

2.1 ENDIAN

Endian es un sistema operativo basado en Linux que funciona como un firewall de código abierto, diseñado para proteger redes mediante la gestión del tráfico entre diferentes zonas. Se utiliza comúnmente para implementar soluciones de seguridad perimetral en pequeñas y medianas empresas. Una de sus principales ventajas es su interfaz web, que facilita la administración incluso a usuarios con poca experiencia. Endian permite configurar zonas de red como LAN, WAN y DMZ, aplicar reglas de acceso, servicios de proxy, filtrado de contenido, y VPN. Gracias a su enfoque práctico y versátil, es ideal para aprender y aplicar conceptos de seguridad en redes reales o simuladas.

2.2 DISEÑO ENDIAN

El diseño de Endian se basa en la segmentación de la red en cuatro zonas: verde (LAN), roja (Internet), naranja (DMZ) y azul (WiFi). Cada zona tiene un propósito específico para mejorar la seguridad y el control del tráfico. El sistema permite definir reglas entre estas zonas, estableciendo qué tipo de comunicación se permite o se bloquea. Esta estructura facilita una administración más clara y segura de los recursos de red.

2.3 CARACTERÍSTICAS ENDIAN

Endian es un sistema operativo basado en Linux que se especializa en funciones de seguridad perimetral. Ofrece una interfaz web intuitiva para la gestión de redes y permite segmentar la red en diferentes zonas como verde (LAN), roja (WAN), naranja (DMZ) y azul (WiFi). Entre sus características principales se incluyen firewall, traducción de direcciones de red (NAT), servidor proxy, VPN, filtrado de contenido, y protección contra intrusos y virus. Además, permite configurar reglas personalizadas de acceso, autenticar usuarios y bloquear sitios web mediante listas negras. Su código abierto lo hace flexible y adecuado para implementaciones en entornos físicos o virtualizados.

2.4 CONFIGURACIÓN NAT

La Traducción de Direcciones de Red (NAT) es una tecnología clave en redes modernas que permite a múltiples dispositivos compartir una misma dirección IP pública al conectarse a Internet [1]. En este proyecto, nos enfocamos en dos tipos de reglas NAT: enmascaramiento (MASQUERADE) para la comunicación LAN-WAN, que oculta las direcciones IP internas, y reenvío de puertos (Port Forwarding) para servicios en la DMZ, que habilita acceso controlado desde Internet [2]. Estas técnicas están estandarizadas en el RFC 3022 y son ampliamente usadas en firewalls como Endian para equilibrar seguridad y funcionalidad [3].

Estudios previos [4] demuestran que una correcta configuración de NAT reduce riesgos como ataques DDoS o escaneo de puertos. Nuestro trabajo aplica estos principios al implementar reglas específicas para LAN y DMZ, verificando su eficacia mediante pruebas de conectividad. A diferencia de configuraciones básicas, nuestro enfoque prioriza el aislamiento de zonas y el filtrado granular, siguiendo mejores prácticas de seguridad perimetral.

3 CONTEXTO DEL PROBLEMA A SOLUCIONAR EN SEGURIDAD PERIMETRAL

Se tiene como prioridad, garantizar la protección de los servidores que conforman la intranet (LAN) / extranet (WAN), para lo cual se requiere delimitarlos a través de una zona DMZ y así garantizar la seguridad e integridad de las bases de datos y aplicaciones bajo plataformas GNU/Linux.

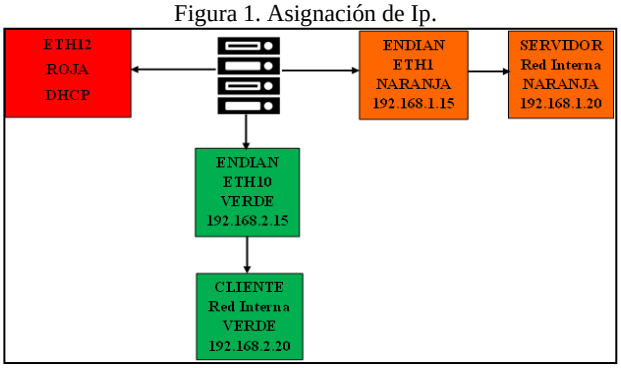
4 TEMÁTICA 1: CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX (TARJETAS DE RED) E INSTALACIÓN EFECTIVA DEL MISMO.

El desarrollo de la temática fue realiza por el estudiante Edwin Esteban Calvache Calvache.

Para realizar la configuración de Endian, en primer lugar, se debe descargar la imagen .iso desde la página oficial https://sourceforge.net/projects/efw/, la cual se utiliza para proceder con la instalación a través de VirtualBox.

Antes de iniciar, es de vital importancia llevar a cabo la distribución y el engranaje de cada uno de los entornos en las zonas roja, verde y naranja, tal como se observa en el gráfico adjunto, donde se asignan las direcciones IP que serán utilizadas en el desarrollo de la temática 1.

Figura 1. Asignación de Ip.

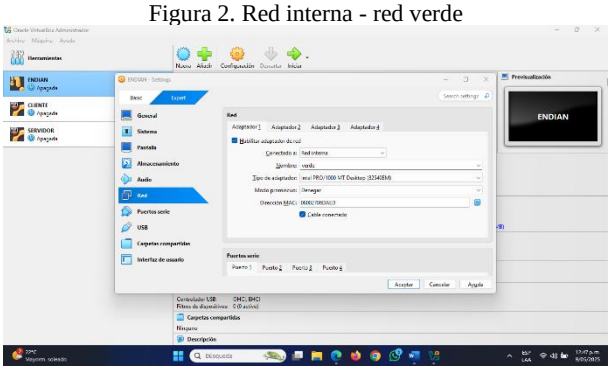


Fuente: Autoría Propia

Una vez plasmado e identificado el direccionamiento ip, se procede a configurar cada una de las maquinas en virtual box. Cargamos la imagen .iso, asignado nombre, tipo, versión, memoria RAM, procesador, almacenamiento y lo más importante en este proceso la red.

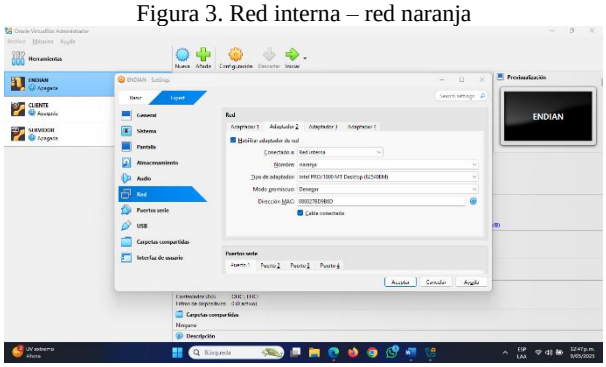
Es por ello que se inicia con la configuración de red en los tres adaptadores de la máquina virtual con Endian,

Figura 2. Red interna - red verde



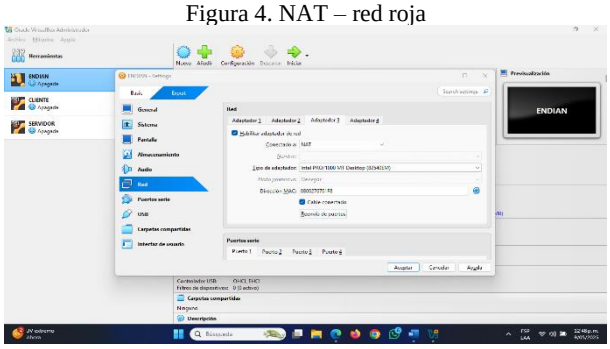
Fuente: Autoría propia

Figura 3. Red interna – red naranja



Fuente: Autoría propia

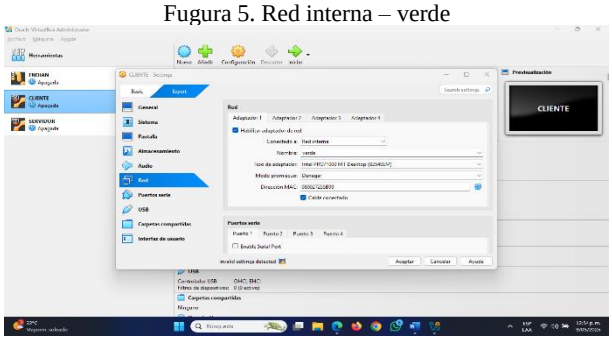
Figura 4. NAT – red roja



Fuente: Autoría propia

Para maquina con Linux desktop, que para este caso es el cliente de la red interna verde, se configura así:

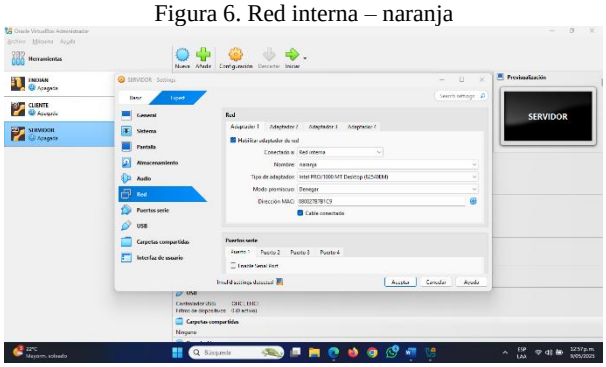
Fugura 5. Red interna – verde



Fuente: Autoría propia

En la máquina virtual con Ubuntu server, se configura así la red naranja que corresponde al servidor en este caso.

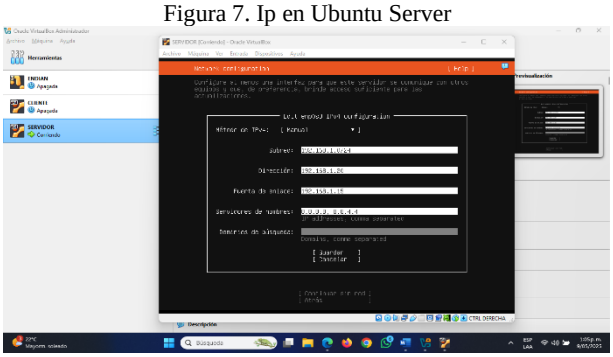
Figura 6. Red interna – naranja



Fuente: Autoría propia

Ya para la instalación es muy importante tener en cuenta la configuración de red, de Ubuntu server el cual tendrá una dirección ip fija 192.168.1.20 dirección de servidor. Y que esta esté en su puerta de enlace para que se comunique a endian con la ip 192.168.1.15.

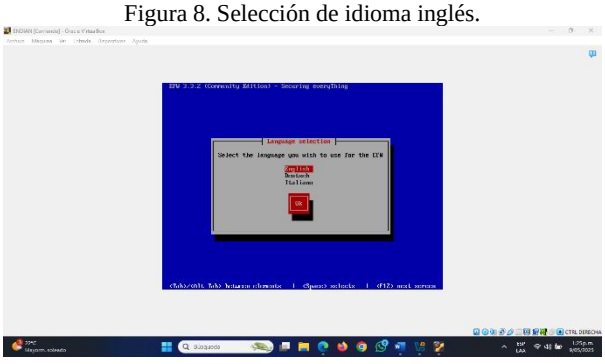
Figura 7. Ip en Ubuntu Server



Fuente: Autoría propia

Ya en la instalación de ENDIAN se siguen los pasos que se relacionan a continuación:

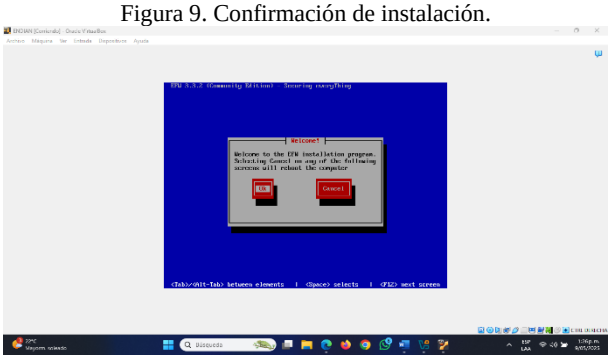
Figura 8. Selección de idioma inglés.



Fuente: Autoría propia

Se realiza el proceso de confirmar la instalación en el asistente Endian Firewall (versión 3.3.2), donde indica que iniciara el proceso.

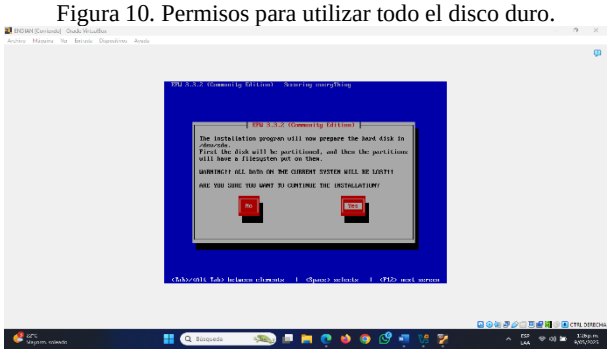
Figura 9. Confirmación de instalación.



Fuente: Autoría propia

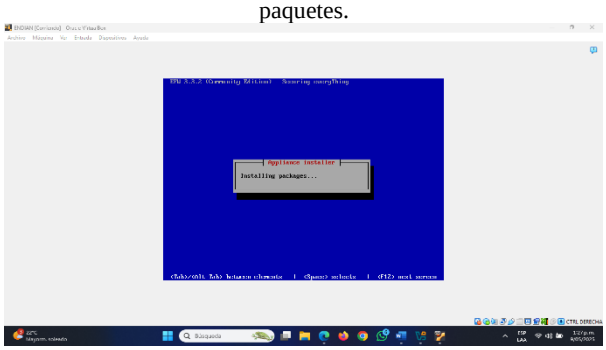
Advierte que para continuar se borrará todos los datos del disco, porque este será particionado y formateado.

Figura 10. Permisos para utilizar todo el disco duro.



Fuente: Autoría propia

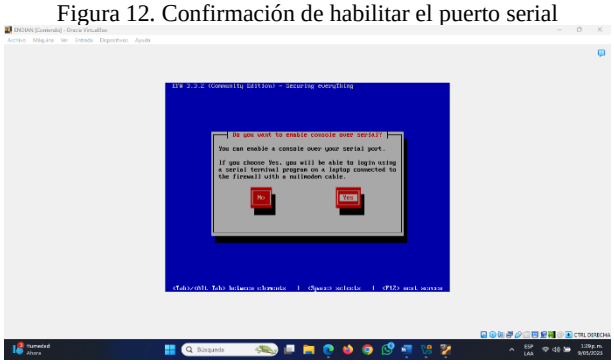
Figura 11. Particionamiento de disco duro e instalación de paquetes.



Fuente: Autoría propia

En este espacio se debe confirmar la administración del firewall desde otro equipo mediante la conexión denominada serial.

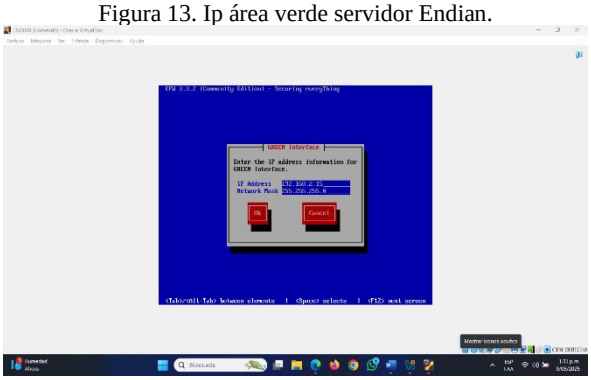
Figura 12. Confirmación de habilitar el puerto serial



Fuente: Autoría propia

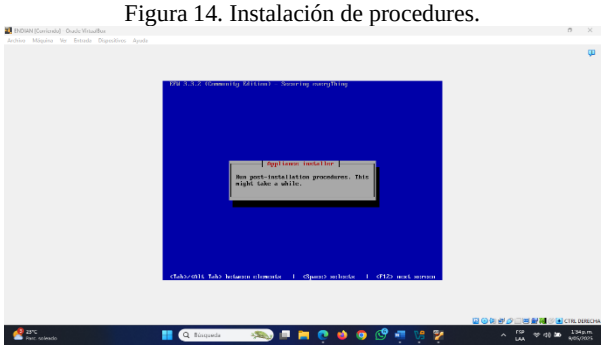
Este espacio es muy importante, ya que solicita la ip de la zona verde, y como al iniciar se plasmó el direccionamiento, procedemos a plasmar la ip designada al área verde que para este caso es: 192.168.2.15, la cual permitirá la comunicación con endian.

Figura 13. Ip área verde servidor Endian.



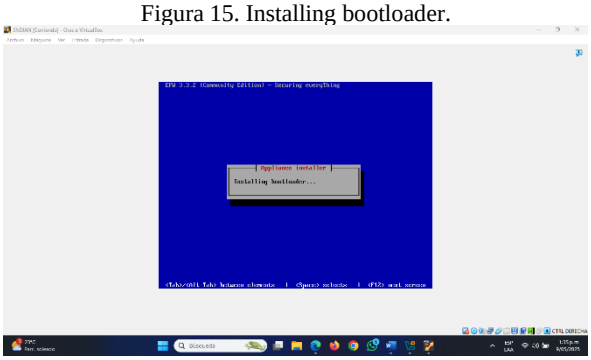
Fuente: Autoría propia

Figura 14. Instalación de procedures.



Fuente: Autoría propia

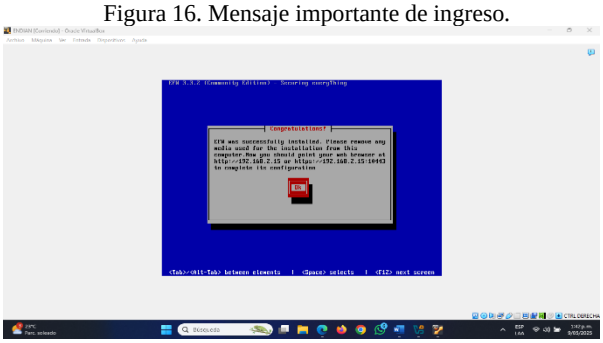
Figura 15. Installing bootloader.



Fuente: Autoría propia

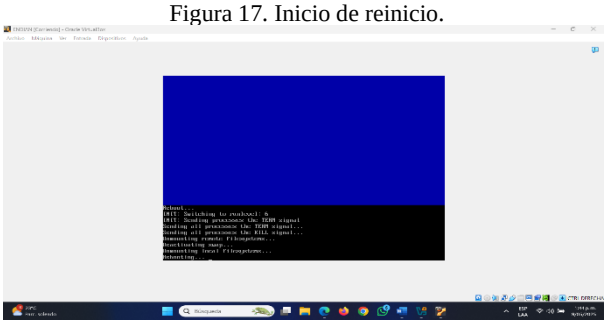
Información para la conexión en la que se debe plasmar la ip 192.168.2.15 en equipo cliente desde el navegador de preferencia. Es decir, desde la red verde.

Figura 16. Mensaje importante de ingreso.



Fuente: Autoría propia

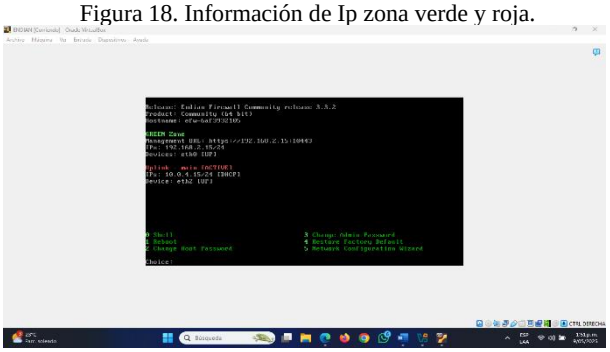
Figura 17. Inicio de reinicio.



Fuente: Autoría propia

Una vez reiniciado se observa que ya inició la zona verde y la roja, cada una con sus respectivas direcciones ip.

Figura 18. Información de Ip zona verde y roja.



Fuente: Autoría propia

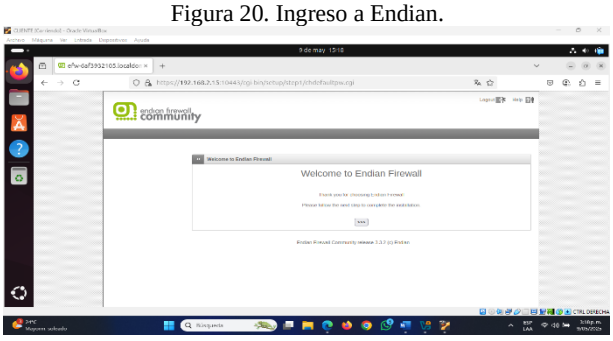
Espacio para verificar la conexión desde el cliente de red verde que sería UBUNTU DESKTOP, hasta el servidor de red verde que para este caso sería ENDIAN. Confirmación con un ping desde Ubuntu desktop hasta Endian.

Figura 19. Ping hasta servidor verde Endian.

Fuente: Autoría propia

Se resalta que, si se hace ping a la otra máquina de red naranja no se va tener respuesta. Por ende, se continua con la configuración desde el navegador del cliente de red verde. Ingresando con la ip sugerida por Endian, la cual corresponde a 192.168.2.15 así:

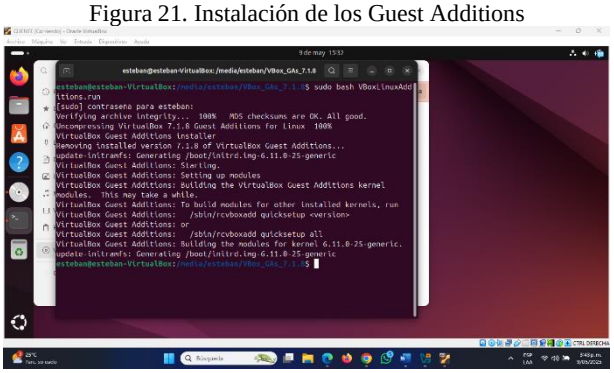
Figura 20. Ingreso a Endian.



Fuente: Autoría propia

Antes de iniciar con la instalación de Endian, se realiza la instalación de los Guest Additions desde el terminar, esto con la finalidad de instalar las mejoras entorno a el rendimiento, la usabilidad y la compatibilidad.

Figura 21. Instalación de los Guest Additions

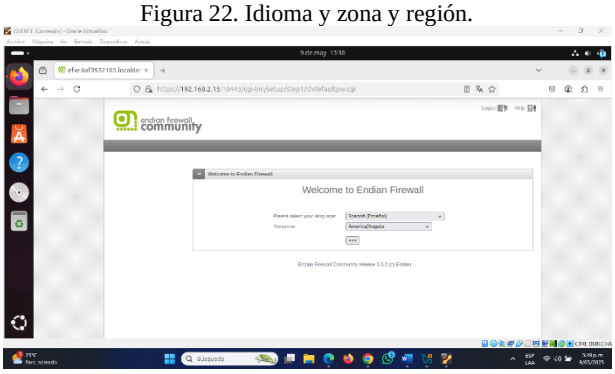


Fuente: Autoría propia

Realizado el proceso de instalación de Guest Additions, se continua con la instalación de endian así:

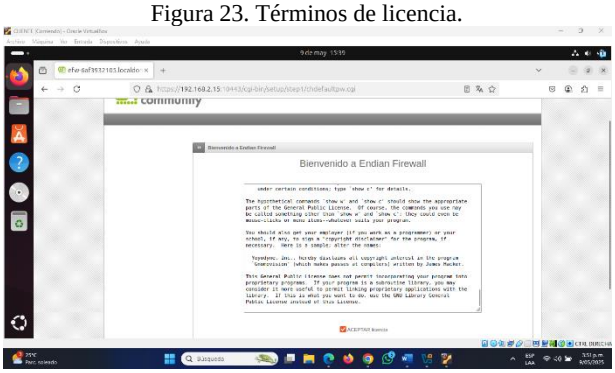
Selección de idioma y lugar de ubicación, que para el caso es Español y América - Bogotá.

Figura 22. Idioma y zona y región.



Fuente: Autoría propia

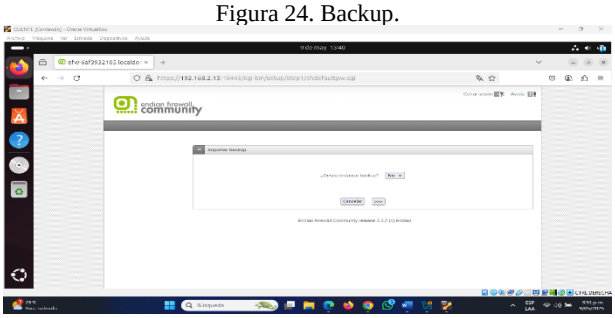
Figura 23. Términos de licencia.



Fuente: Autoría propia

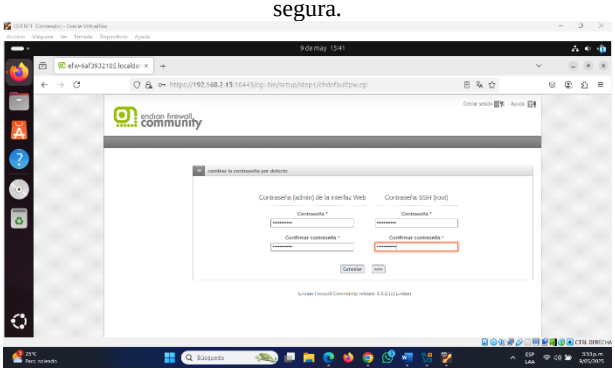
Se permite realizar el restablecimiento de Backup, pero en este caso se realiza una instalación nueva y por primera vez, ante lo cual se selecciona no.

Figura 24. Backup.



Fuente: Autoría propia

Figura 25. Cambio de contraseña por defecto, por una más segura.

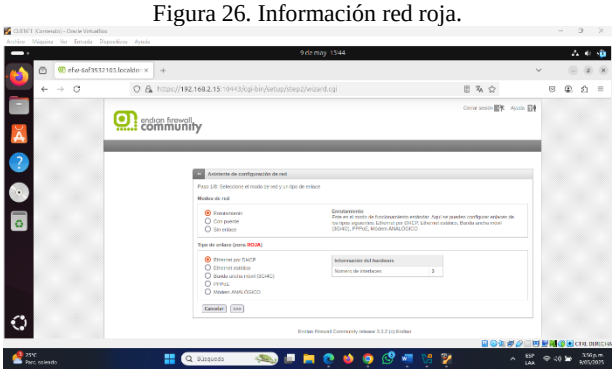


Fuente: Autoría propia

En este espacio se inicia la configuración de red, y se deja el modo de enrutamiento, el cual permite tener acceso a internet. Y en la zona roja se deja en DCHP tal como lo plasma el grafico inicial.

Además, se informa que hay configuradas 3 tarjetas de red en el servidor de endian, confirmando que las 3 fueron configuradas al iniciar el proceso de instalación desde VirtualBox.

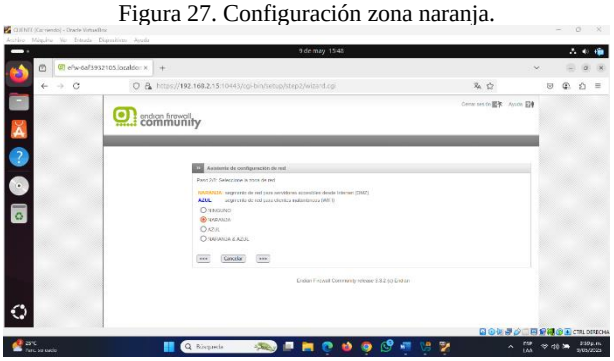
Figura 26. Información red roja.



Fuente: Autoría propia

En este punto como ya se cuenta configurada la red roja y verde, se debe proceder a configurar una zona adicional que es la naranja.

Figura 27. Configuración zona naranja.

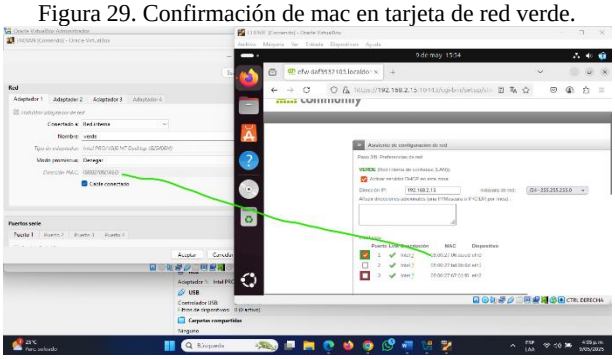


Fuente: Autoría propia

Figura 28. Verificación de configuración de la red verde.

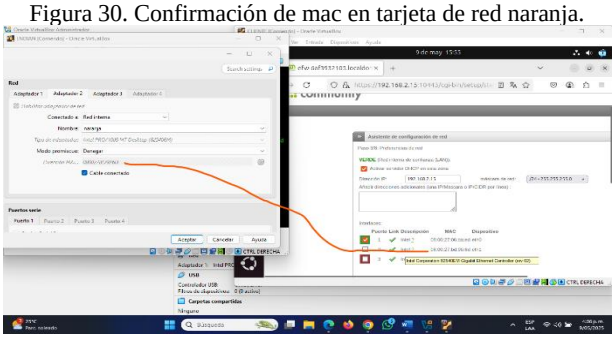
Fuente: Autoría propia

Figura 29. Confirmación de mac en tarjeta de red verde.



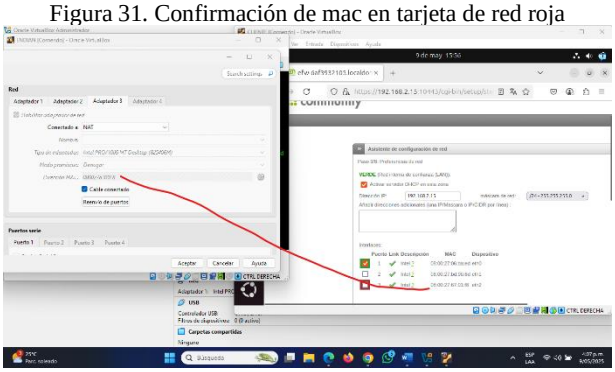
Fuente: Autoría propia

Figura 30. Confirmación de mac en tarjeta de red naranja.



Fuente: Autoría propia

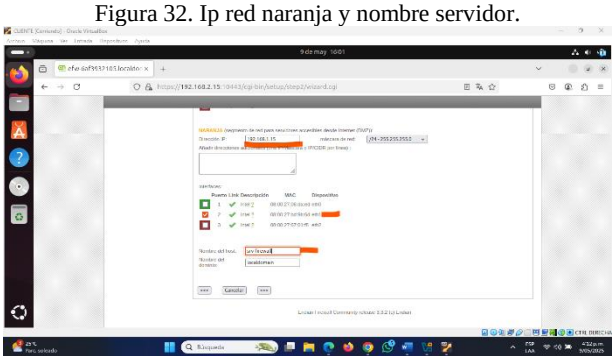
Figura 31. Confirmación de mac en tarjeta de red roja



Fuente: Autoría propia

Una vez verificada la conexión ya realizada y las mac de las tarjetas de red. Se Procede a la configuración de la red naranja la cual es la faltante, asignando la ip 192.168.1.15, ip plasmada en el diseño inicial. También, se asigna un nuevo nombre al servidor denominándose srv-firewall.

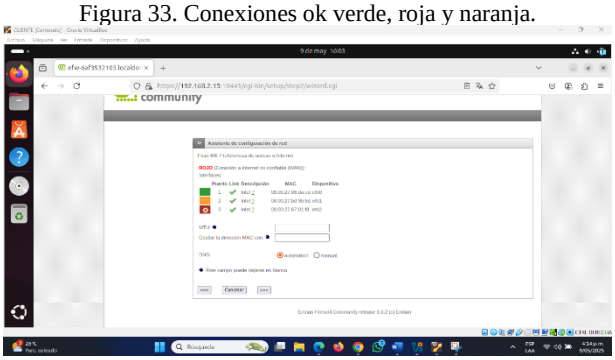
Figura 32. Ip red naranja y nombre servidor.



Fuente: Autoría propia

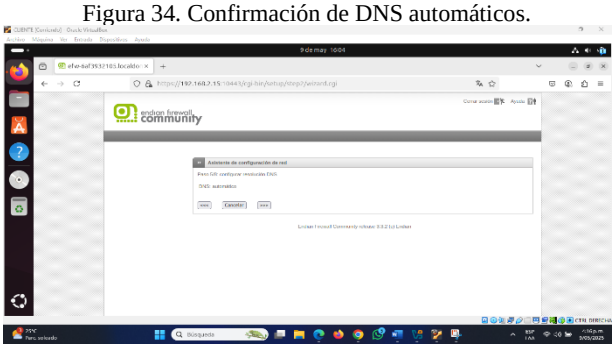
Ya en esta instancia se muestra que ya está configurada la red verde, la naranja y que la roja, es la que brinda conexión a internet.

Figura 33. Conexiones ok verde, roja y naranja.



Fuente: Autoría propia

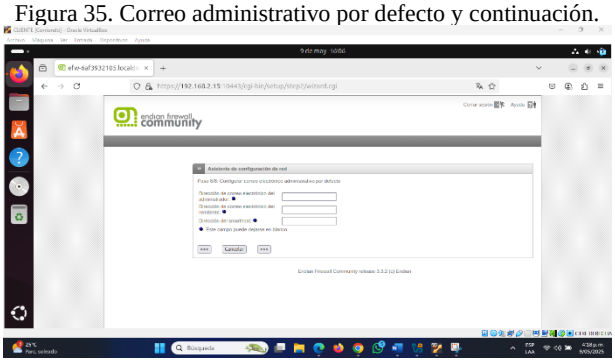
Figura 34. Confirmación de DNS automáticos.



Fuente: Autoría propia

El asistente de red solicita el cambio de la dirección de correo del administrador, el cual se deja por defecto. Al igual que el nombre del firewall.

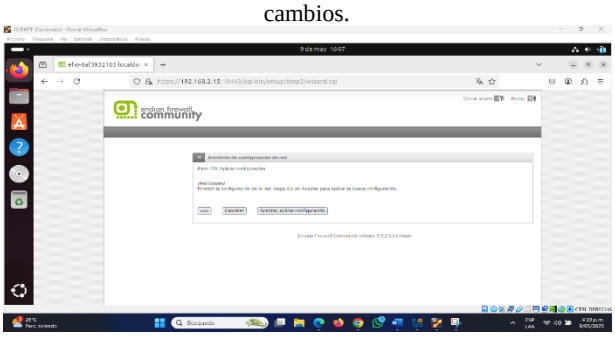
Figura 35. Correo administrativo por defecto y continuación.



Fuente: Autoría propia

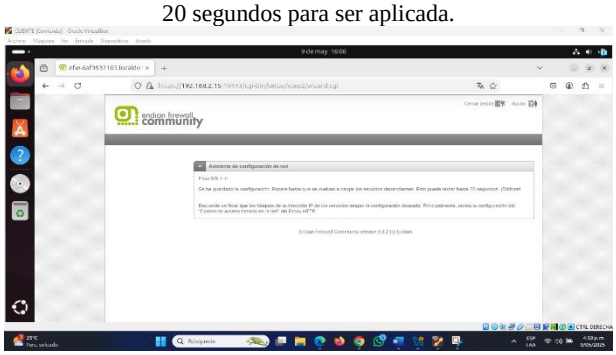
Ya en este punto indica que la configuración básica ha sido aplicada correctamente y que está listo para reiniciar el firewall y aplicar los cambios.

Figura 36. Confirmación de terminación y aplicación de cambios.



Fuente: Autoría propia

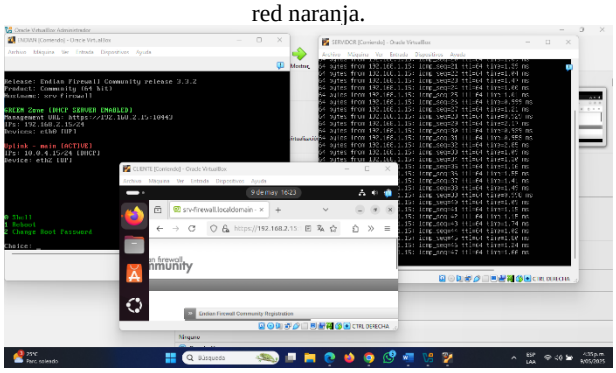
Figura 37. Notificación de configuración guardada con éxito y 20 segundos para ser aplicada.



Fuente: Autoría propia

Finalizado el proceso anterior, se logra verificar que Ubuntu server, es el que está en la red naranja dando respuesta a través de ping al servidor de endian en la red naranja.

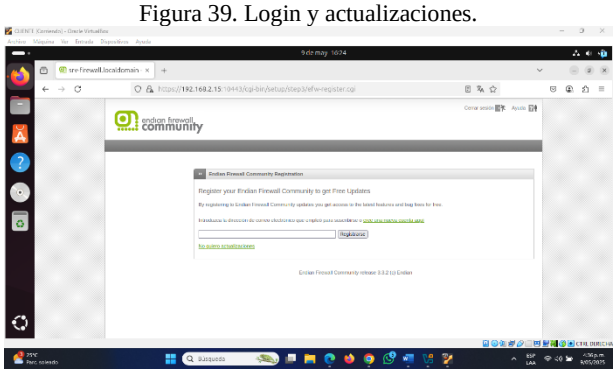
Figura 38. Ping Ubuntu Server a servidor Endian, ambos en red naranja.



Fuente: Autoría propia

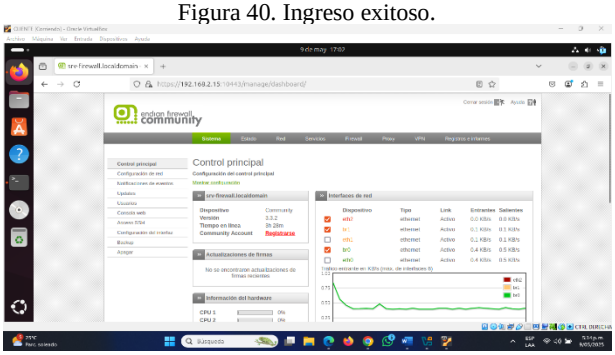
Continuando con el proceso, una vez se realiza el login con la ip 192.168.2.15, se rechazan las actualizaciones por el momento

Figura 39. Login y actualizaciones.



Fuente: Autoría propia

Figura 40. Ingreso exitoso.



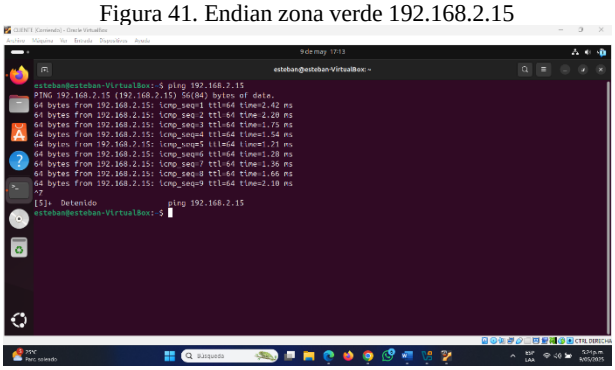
Fuente: Autoría propia

Una vez terminado todo el proceso, se hace verificación del funcionamiento desde las diferentes zonas con ping:

Desde la maquina Cliente Ubuntu Desktop con ip 192.168.2.20 a:

Verificación de la conexión desde el cliente de la zona verde con Ubuntu desktop, hasta servidor Endian en la misma zona verde.

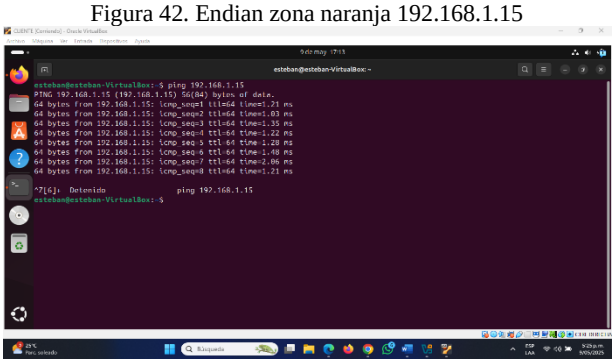
Figura 41. Endian zona verde 192.168.2.15



Fuente: Autoría propia

Verificación de la conexión desde el cliente de la zona verde con Ubuntu desktop, hasta servidor Endian en la zona naranja.

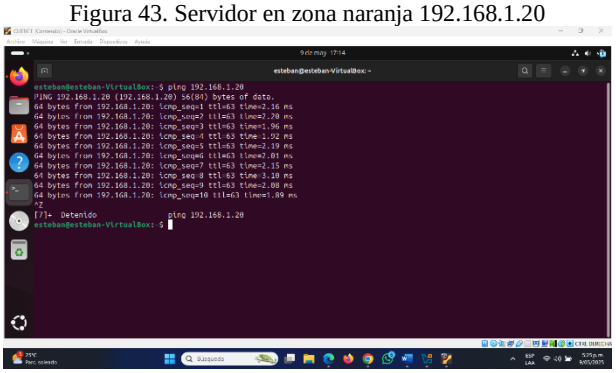
Figura 42. Endian zona naranja 192.168.1.15



Fuente: Autoría propia

Verificación de la conexión desde el cliente de la zona verde con Ubuntu desktop, hasta cliente en zona naranja.

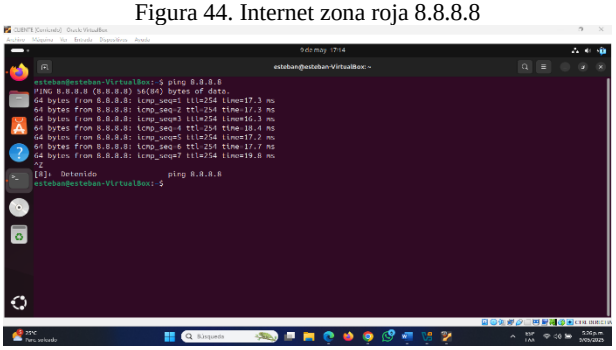
Figura 43. Servidor en zona naranja 192.168.1.20



Fuente: Autoría propia

Verificación de que la zona roja está con acceso a internet y que cuya verificación se realiza desde cliente zona verde con Ubuntu desktop.

Figura 44. Internet zona roja 8.8.8.8

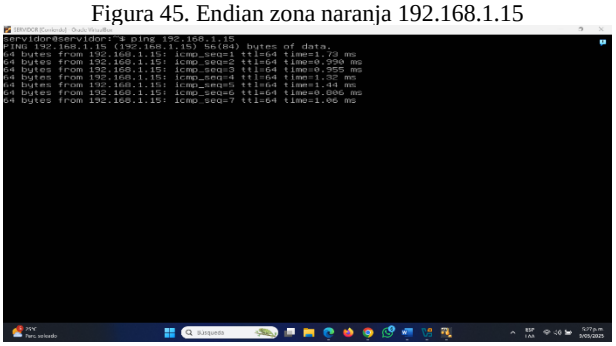


Fuente: Autoría propia

Por otro lado, se verifica desde el cliente Ubuntu Server con ip 192.168.1.20 a:

Verificación de la conexión desde el cliente de la zona naranja con Ubuntu server, hasta servidor Endian en la zona naranja.

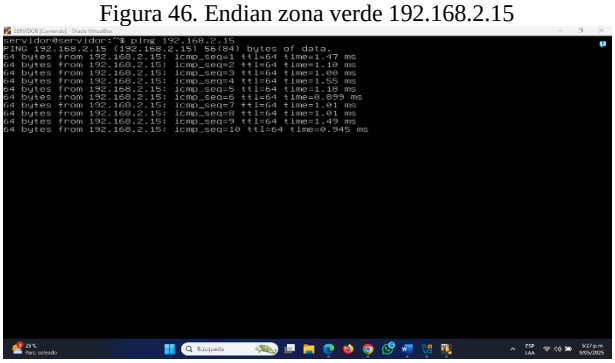
Figura 45. Endian zona naranja 192.168.1.15



Fuente: Autoría propia

Verificación de la conexión desde el cliente de la zona naranja con Ubuntu server, hasta servidor Endian en la zona verde.

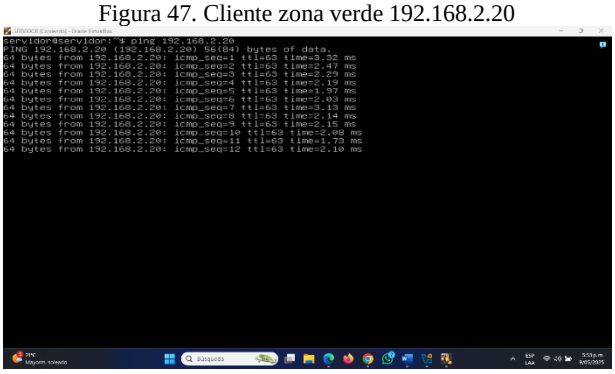
Figura 46. Endian zona verde 192.168.2.15



Fuente: Autoría propia

Verificación de la conexión desde el cliente de la zona naranja con Ubuntu server, hasta cliente en la zona verde.

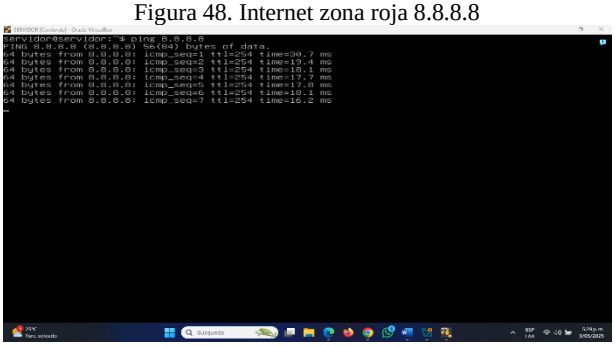
Figura 47. Cliente zona verde 192.168.2.20



Fuente: Autoría propia

Verificación del acceso a internet en la zona roja, desde el cliente de la zona naranja con Ubuntu server.

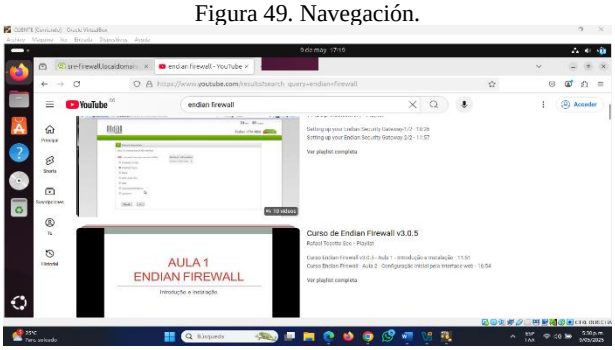
Figura 48. Internet zona roja 8.8.8.8



Fuente: Autoría propia

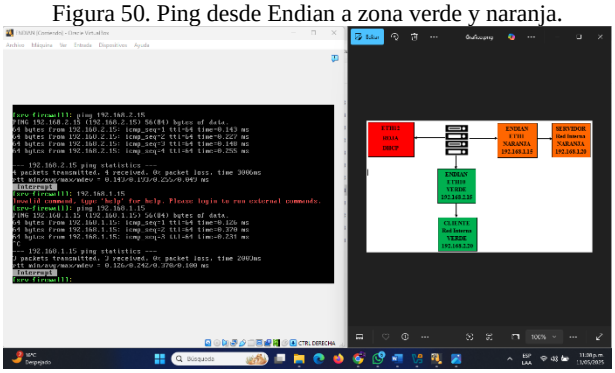
Por último, se comprueba la navegación desde el cliente, que en este caso es Ubuntu Desktop en zona verde.

Figura 49. Navegación.



Fuente: Autoría propia

Figura 50. Ping desde Endian a zona verde y naranja.



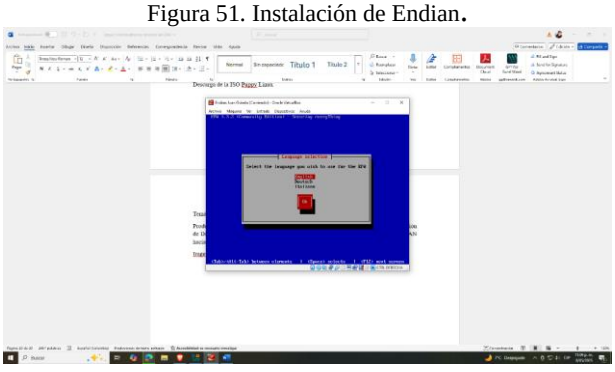
Fuente: Autoría propia

5 TEMÁTICA 2: CONFIGURACIÓN NAT.

Esta temática fue desarrollada por el estudiante Juan Esteban Oviedo Mora

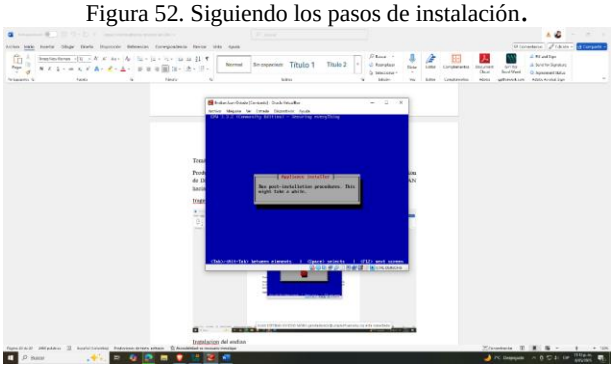
Desarrollo de la temática

Figura 51. Instalación de Endian.



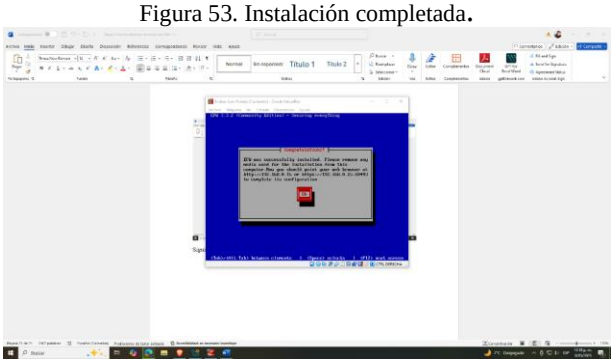
Fuente: Autoría propia.

Figura 52. Siguiendo los pasos de instalación.



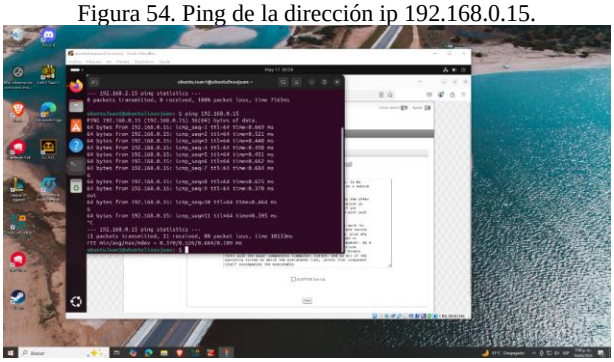
Fuente: Autoría propia.

Figura 53. Instalación completada.



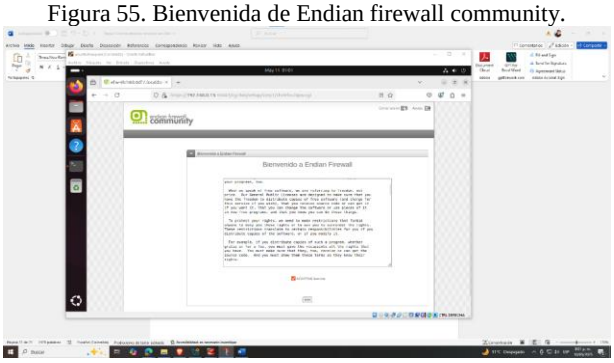
Fuente: Autoría propia.

Figura 54. Ping de la dirección ip 192.168.0.15.



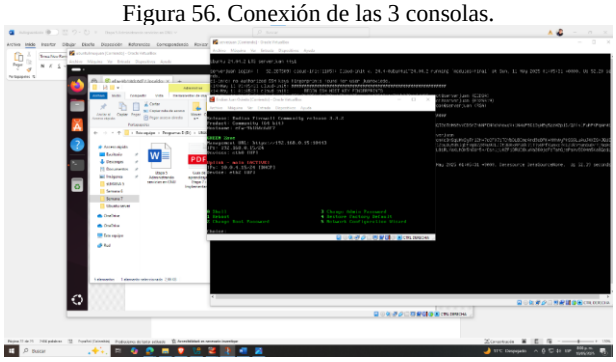
Fuente: Autoría propia.

Figura 55. Bienvenida de Endian firewall community.



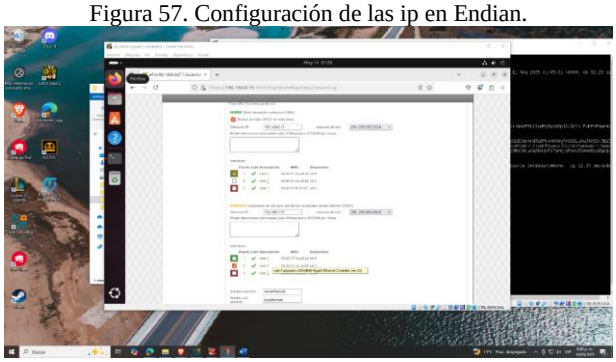
Fuente: Autoría propia.

Figura 56. Conexión de las 3 consolas.



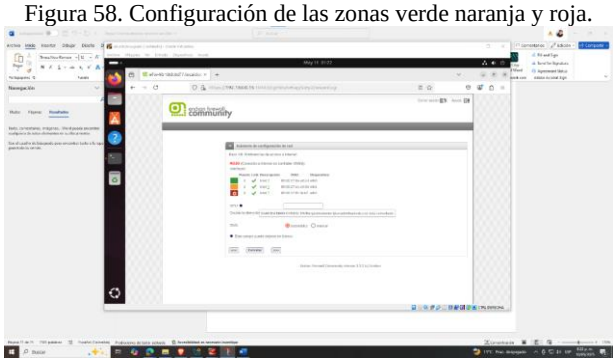
Fuente: Autoría propia.

Figura 57. Configuración de las ip en Endian.



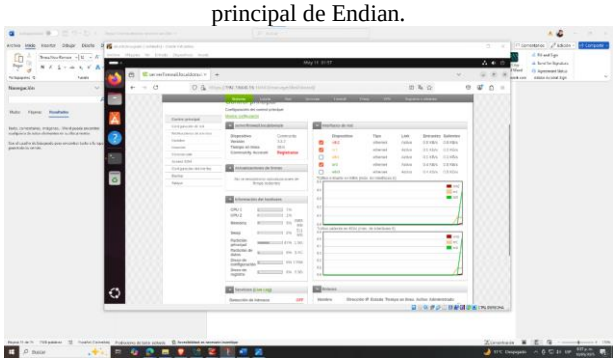
Fuente: Autoría propia.

Figura 58. Configuración de las zonas verde naranja y roja.



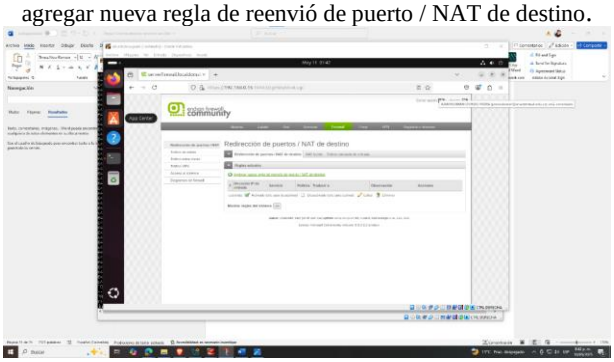
Fuente: Autoría propia.

Figura 59. Conexión de las 3 máquinas además de la página principal de Endian.



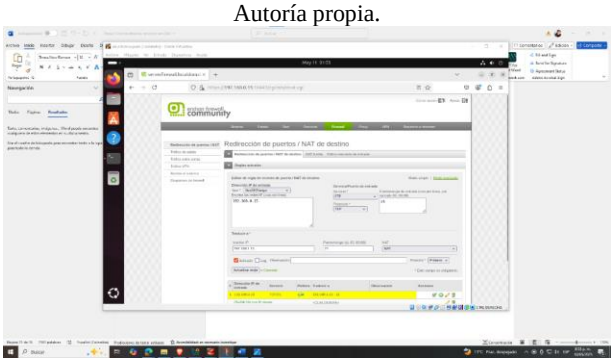
Fuente: Autoría propia.

Figura 60. Se va a la pestaña Firewall y se le da al botón agregar nueva regla de reenvió de puerto / NAT de destino.



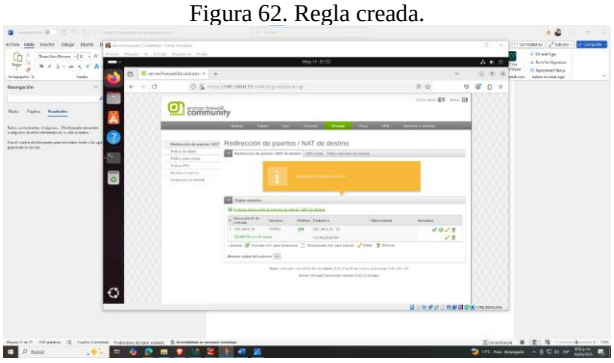
Fuente: Autoría propia.

Figura 61. Se accede al formulario nuevo donde se agrega los datos para acceder al servicio HTTP, FTP y SSH desde la WAN que es la red roja a la DMZ (la red naranja). En el espacio que dice escriba las redes/IP (la red WAN). Fuente: Autoría propia.



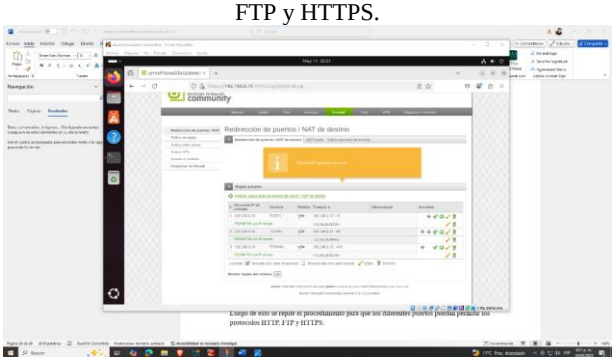
Fuente: Autoría propia.

Figura 62. Regla creada.



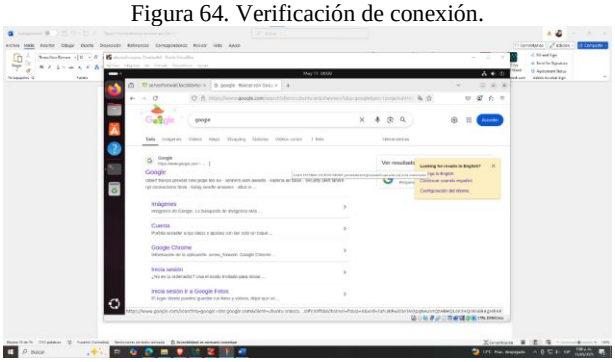
Fuente: Autoría propia.

Figura 63. Luego de esto se repite el procedimiento para que los diferentes puertos puedan permitir los protocolos HTTP, FTP y HTTPS.



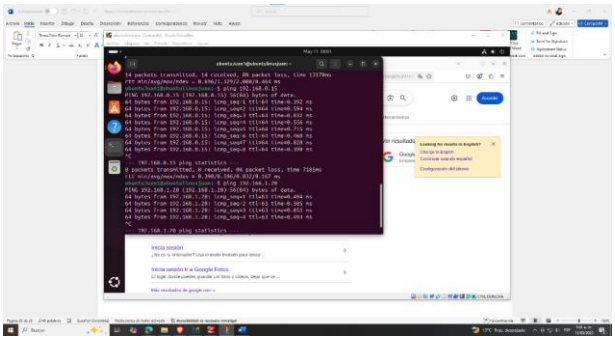
Fuente: Autoría propia.

Figura 64. Verificación de conexión.



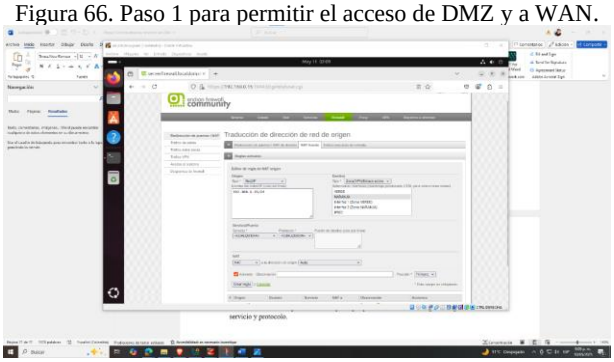
Fuente: Autoría propia.

Figura 65. Verificación de paquetes enviados y recibidos del Ubuntu server.



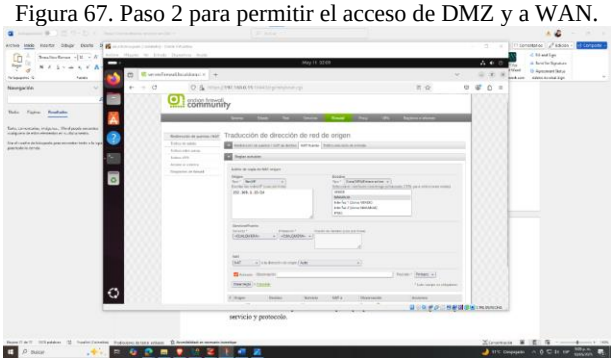
Fuente: Autoría propia.

Figura 66. Paso 1 para permitir el acceso de DMZ y a WAN.



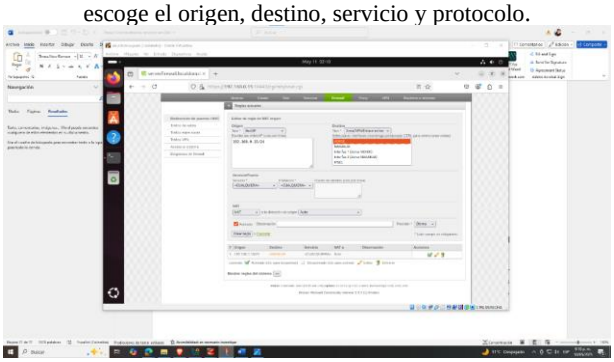
Fuente: Autoría propia.

Figura 67. Paso 2 para permitir el acceso de DMZ y a WAN.



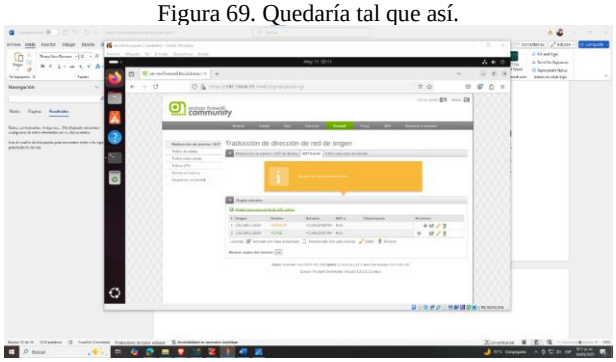
Fuente: Autoría propia.

Figura 68. Se procede permitiendo que LAN acceda a DMZ y a WAN, por lo cual se puede permitir cualquier servicio. En el botón Fuente NAT se agrega una regla con la dirección y la indicación de la red que se necesite para que pueda acceder, se escoge el origen, destino, servicio y protocolo.



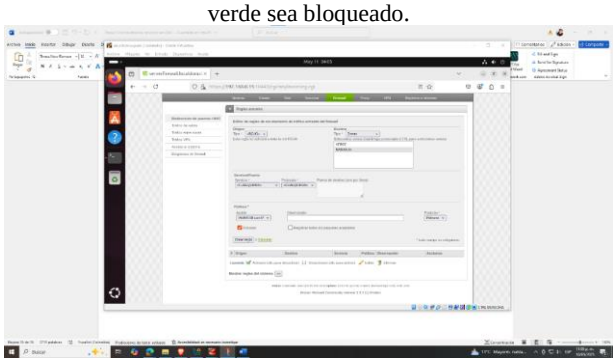
Fuente: Autoría propia.

Figura 69. Quedaría tal que así.



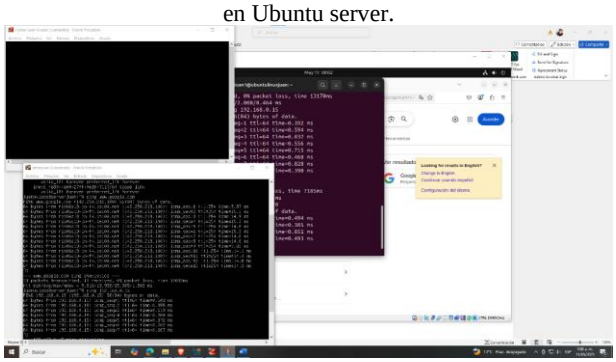
Fuente: Autoría propia.

Figura 70. Se hace una configuración en la sección tráfico que se puede ingresar para que la conexión llegue al servidor. En la pestaña Trafico enrutado de entrada, se establece la fuente (red WAN roja) y destino (red naranja WDZ). Ya con esta configuración se hace un permiso que consiste que cualquier servicio con protocolo de tráfico que quiera entrar a la red verde sea bloqueado.



Fuente: Autoría propia.

Figura 71. Verificación de paquetes enviados de Google.com en Ubuntu server.



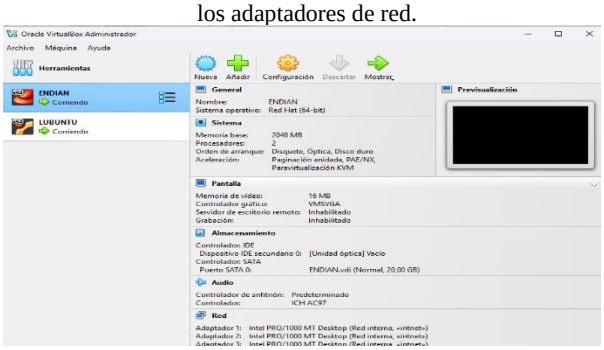
Fuente: Autoría propia.

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

Desarrollada por Sofia Catherine Rosero Bolaños

Se asignaron tres adapatadores en modo red interna cada uno con su respectiva interfaz,esta configuracion permite segmentar correctamente las redes y garantizar la comunicación entre la zonas atraves del firewall Endian.

Figura 72. Creamos la maquina virtual Endian y configuramos los adaptadores de red.



Fuente: Autoría propia

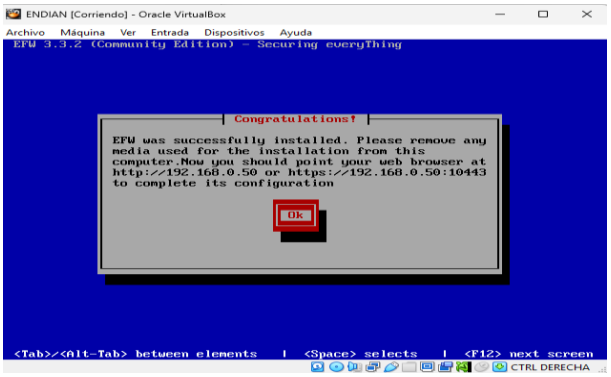
Figura 73. Creamos la máquina virtual Lubuntu y configuramos los adaptadores de red.

Fuente: Autoría propia

Figura 74. Instalamos Endian

Fuente: Autoría propia

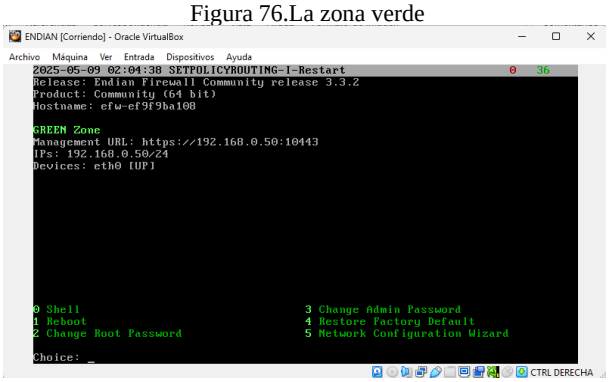
Figura 75. Se asigna la ip 192.168.0.50



Fuente: Autoría propia

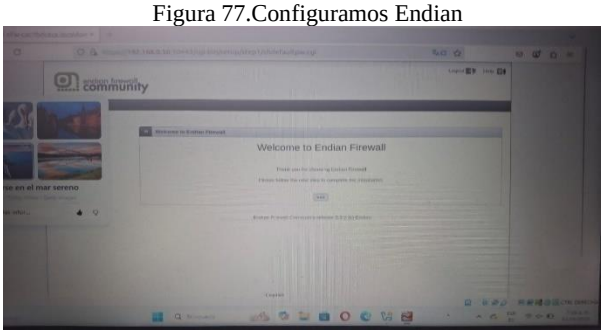
Una vez finalizada la configuracion de Endian y aasignada la direccion IP corespondiente,se muestra la zona verde ,con la Ip previamente definida

Figura 76.La zona verde



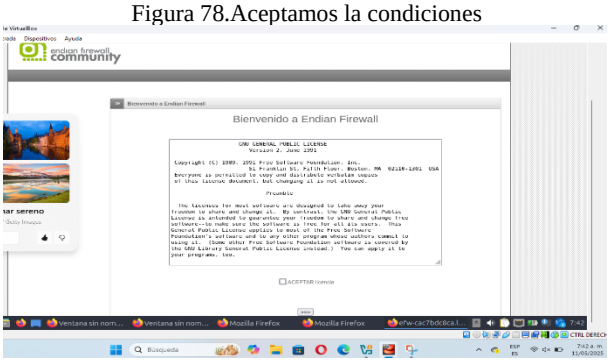
Fuente: Autoría propia

Figura 77.Configuramos Endian



Fuente: Autoría propia

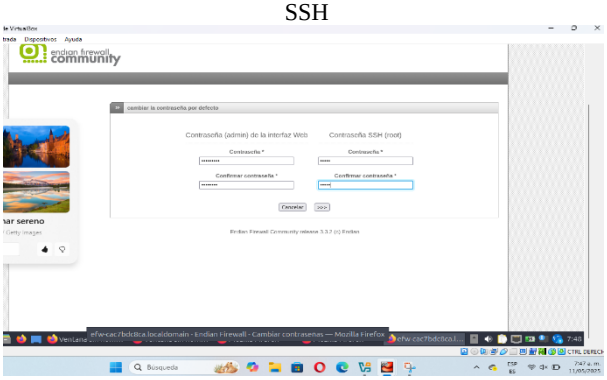
Figura 78.Aceptamos la condiciones



Fuente: Autoría propia

Una vez que aceptamos la condiciones procedemos a ingresar las contraseñas tanto para el acceso ala interfaz web,la cual facilita la administracion mediante un entorno grafico,como para la conexión remota a tarves del protocolo SSH

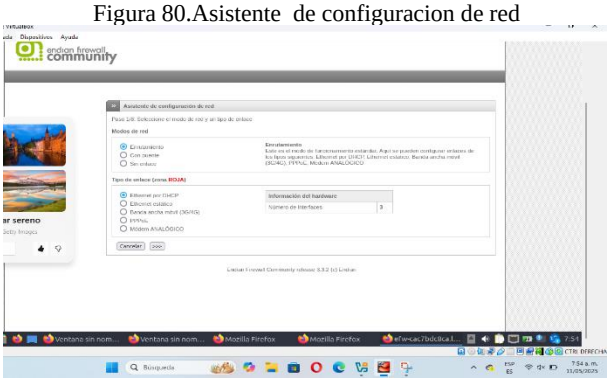
Figura 79.Digitamos las contraseñas de la interfaz web y el SSH



Fuente: Autoría propia

Seleccionamos el modo de red y un tipo de enlace el cual estamos en la zona roja

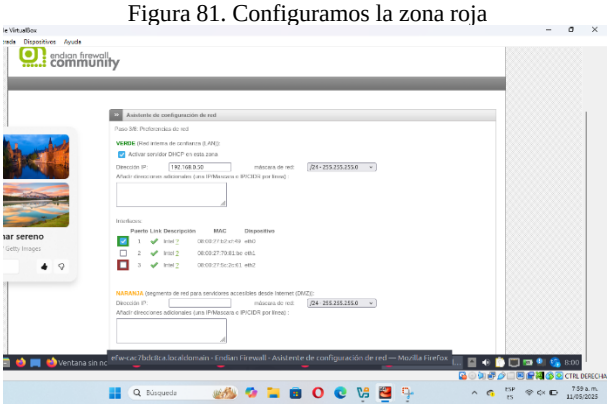
Figura 80.Asistente de configuracion de red



Fuente: Autoría propia

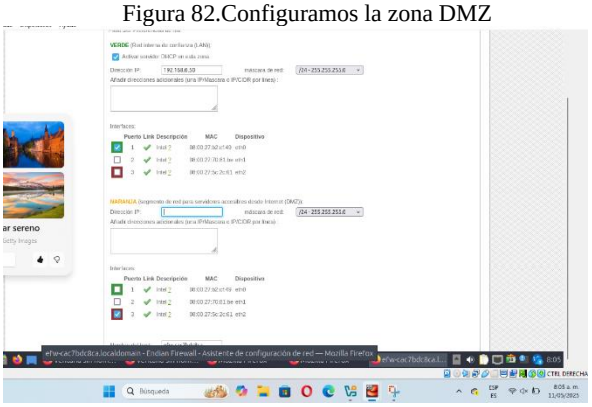
Le asignamos una direecion ip fija la cual es la zona desmilitirazada designamos el puerto numero 3 la cual vendria siendo la zona naraja

Figura 81. Configuramos la zona roja



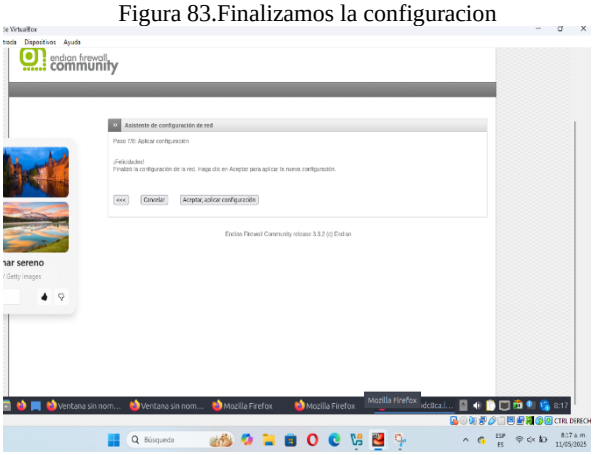
Fuente: Autoría propia

Figura 82.Configuramos la zona DMZ



Fuente: Autoría propia

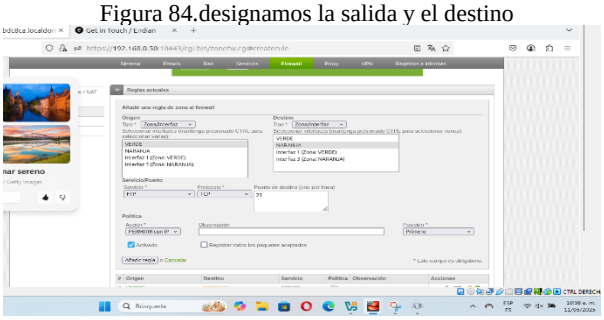
Figura 83.Finalizamos la configuracion



Fuente: Autoría propia

1.Producto esperado:permitir los servicios HTTP Puerto 80 y FTP 21 desde el servidor web Lubuntu *Se crean las reglas de permiso para los servicios HTTP con puerto 80 y FTP con puerto 21.

Figura 84.designamos la salida y el destino



Fuente :Autoria propia

Figura85.Configuramos la salida de la zona roja

Fuente: Autoría propia

Figura86.verificamos la regla

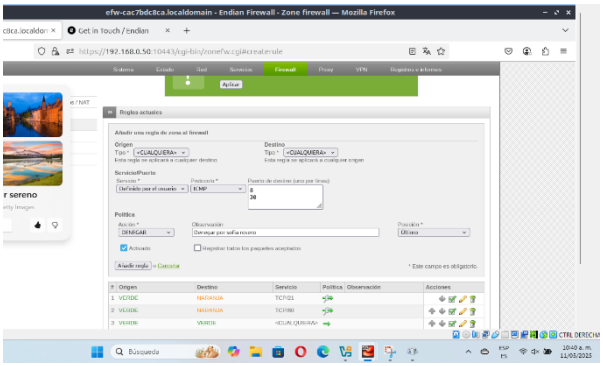
Fuente: Autoría propia

Figura87.Verificamos la salida

Fuente: Autoría propia

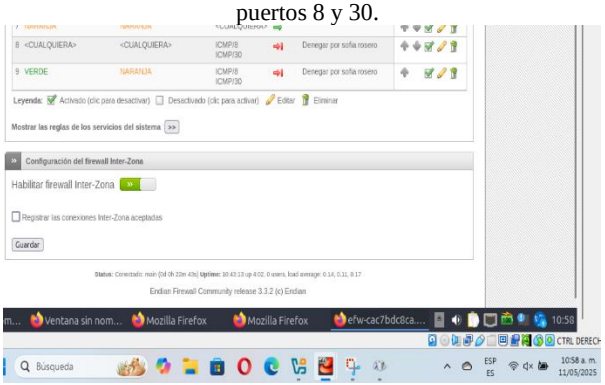
2. Denegar el protocolo ICMP (Puerto 8 y puerto 30) para no permitir hacer ping en la red. Probar a través de una consola o terminal la no respuesta del comando ping hacia una IP de la red. Verificar en el tráfico de salida, la creación de las reglas

Figura88. Denegar ping configuración en las reglas de salida zona interna



Fuente: Autoría propia

Figura 89. Se impide el tráfico en el protocolo ICMP en los puertos 8 y 30.



Fuente:Autoria Propia.

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

Con el desarrollo de las temáticas anteriores tenemos la configuración necesaria para el desarrollo de este punto.

1.Comunicar la zona Verde con la zona Naranja con el protocolo HTTP y FTP con sus respectivos puertos.

Para realizar la comunicación de la Zona verde y naranja con el protocolo http y ftp, se deben crear reglas en la configuración web de Endian, para ello nos dirigimos a la pestaña *Firewall* y en la pestaña de *Tráfico entre zonas* elegimos la opción de añadir una nueva regla, seleccionamos las zonas y el protocolo requerido y damos clic en Añadir regla.

Figura 90. Comunicación FTP Verde a Naranja

Fuente: Autoría propia

Figura 91. Comunicación HTTP Verde a Naranja.

Fuente: Autoría propia

2. Comunicar la zona Internet con la zona DMZ: Para comunicar la zona internet (Endian) con la Zona DMZ (Ubuntu Server) hay que crear un Gateway para establecer un enlace. Primero se asigna una ip que permita relacionar Endian con Ubuntu server, después se configura el Gateway de enlace.

Figura 92. Comunicación zona internet con zona DMZ.

```
Andres_Bastidas@Server:~$ sudo ip addr add 192.168.1.21/24 dev enp0s3
[sudo] password for Andres_Bastidas:
Sorry, try again.
[sudo] password for Andres_Bastidas:
Andres_Bastidas@Server:~$ sudo ip route add default via 192.168.1.16
Andres_Bastidas@Server:~$ ip r
default via 192.168.1.16 dev enp0s3
192.168.1.0/24 dev enp0s3 proto kernel scope link src 192.168.1.21
Andres_Bastidas@Server:~$ ping google.com
PING google.com (142.251.132.110) 56(84) bytes of data.
64 bytes from bog03s04-in-f14.1e100.net (142.251.132.110): icmp_seq=1 ttl=117 time=17.2 ms
64 bytes from bog03s04-in-f14.1e100.net (142.251.132.110): icmp_seq=2 ttl=117 time=18.0 ms
64 bytes from bog03s04-in-f14.1e100.net (142.251.132.110): icmp_seq=3 ttl=117 time=18.6 ms
64 bytes from bog03s04-in-f14.1e100.net (142.251.132.110): icmp_seq=4 ttl=117 time=18.6 ms
64 bytes from bog03s04-in-f14.1e100.net (142.251.132.110): icmp_seq=5 ttl=117 time=18.8 ms
64 bytes from bog03s04-in-f14.1e100.net (142.251.132.110): icmp_seq=6 ttl=117 time=18.8 ms
64 bytes from bog03s04-in-f14.1e100.net (142.251.132.110): icmp_seq=7 ttl=117 time=17.4 ms
^C
--- google.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6088ms
rtt min/avg/max/mdev = 17.164/18.189/18.847/0.650 ms
Andres_Bastidas@Server:~$ _
```

Fuente: Autoría propia

3.Verificar en el tráfico Inter - Zona, la creación de las reglas: En la pestaña *Firewall* tenemos la opción de *Tráfico entre zonas* donde se encuentran las respectivas reglas creadas.

Figura 93. Trafico entre zonas.

Fuente: Autoría propia

4.Probar desde un navegador Web, las siguientes directivas:

El ingreso del servicio HTTP desde la LAN hacia la zona DMZ.

El ingreso del servicio HTTP desde la LAN hacia la WAN.

El ingreso del servicio HTTP desde la zona DMZ hacia la WAN.

El ingreso del servicio HTTP desde la WAN hacia la zona DMZ.

El ingreso del servicio FTP desde la LAN hacia la WAN.

El ingreso del servicio FTP desde la WAN hacia la zona DMZ.

Ya hemos conectado la zona verde y naranja con protocolo http y ftp, pero además de ello debemos configurar la zona internet (Endian) con la zona naranja por los mismos protocolos, para ello añadimos estas reglas en la configuración web de Endian.

Nos dirigimos a la pestaña *Firewall* y añadimos las reglas en la opción *Tráfico de salida.*

Figura 94. Reglas creadas en Tráfico de salida.

Fuente: Autoría propia

Para establecer una conexión http y ftp con el servidor, primero se hace la instalación de Apache2 y de un servicio ftp en Ubuntu server.

La forma más fácil de verificar que las reglas de protocolo http funcionan es ingresar a la dirección de Ubuntu server desde el servidor web en Ubuntu Desktop, como se muestra en la Figura 5.

Figura 95. Ingreso http zona naranja desde la zona verde.

Fuente: Autoría propia

Lo que se observa en la figura 5 es la página por defecto de apache2 que se instaló previamente en Ubuntu server. Esto dado que no se ha realizado ninguna configuración en el servicio de Apache.

De la misma forma, para evidenciar el protocolo ftp en la zona naranja desde la zona verde, lo que haremos es hacer in "ping ftp" desde la consola de Ubuntu Desktop y verificar que haya una respuesta.

Figura 96. Ingreso FTP zona naranja desde la zona verde.

Fuente: Autoría propia

Con esto se ha verificado que la conexión existe e incluso se puede observar la versión FTP instalada en Ubuntu Server.

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

La temática fue elaborada por la estudiante Ingrid Alexandra Muñoz.

1. Crear un perfil y establecer una lista negra bloqueando los siguientes sitios:

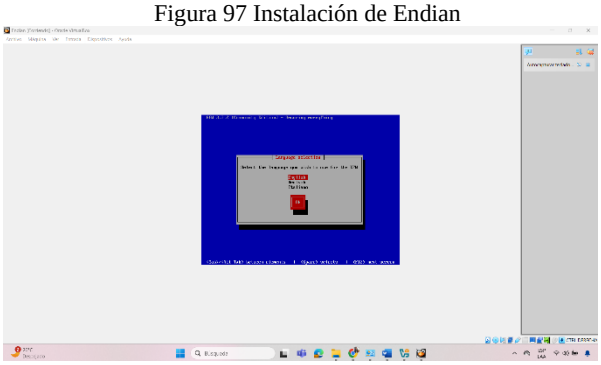
www.hotmail.com
www.youtube.com
www.elnuevodia.com.co

2. Autenticación por usuario: A través de la opción proxy cree un usuario y asócielo a un grupo. Establezca una política de acceso y vincule el perfil creado en el punto anterior y relaciónelo también con la política de autenticación.

3. Probar desde la LAN a través de un navegador Web, el acceso a los portales referenciados en la lista negra.

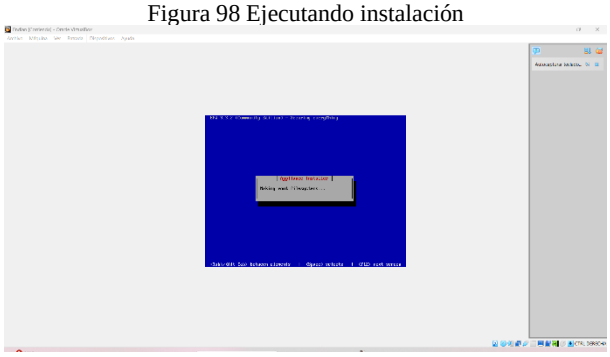
Esta figura muestra el proceso de instalación del firewall y gateway de seguridad Endian en el sistema

Figura 97 Instalación de Endian



Fuente: autoria propia

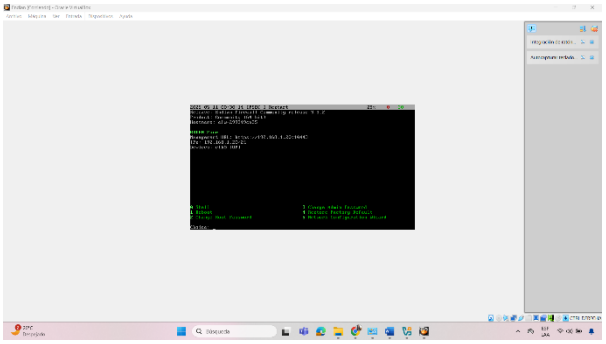
Figura 98 Ejecutando instalación



Fuente: autoria propia

Endian instalado correctamente y configurado la ip en zona verde. La pantalla final del proceso de instalación de Endian, indicando que el sistema se instaló exitosamente. Además, se observa la configuración de la dirección IP asignada a la zona verde, que corresponde a la red interna o confiable dentro del esquema de seguridad.

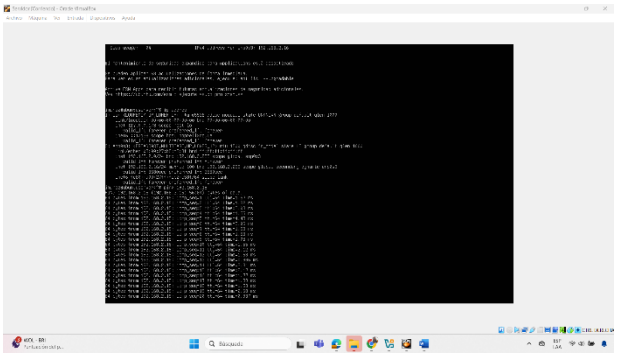
Figura 99 Endian instalado correctamente y configurado la ip en zona verde



Fuente: autoria propia

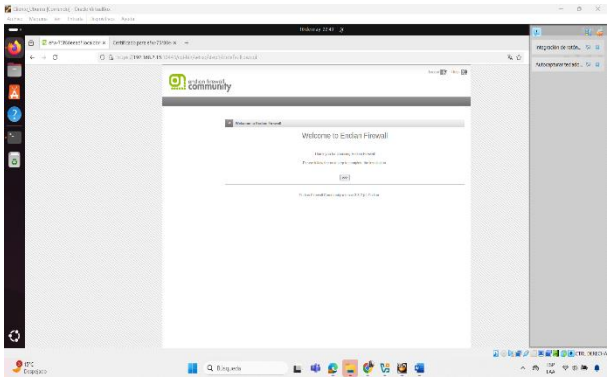
Se muestra la ejecución del comando ping desde el servidor con sistema operativo Ubuntu hacia la dirección IP 192.168.2.16, correspondiente al firewall de la red. Esta prueba permite verificar la conectividad entre ambos dispositivos y confirmar que no existen bloqueos a nivel de red ni fallos de configuración en las interfaces involucradas.

Figura 100 Ping al firewall (192.168.2.16) desde el servidor ubunutu



Fuente: autoria propia

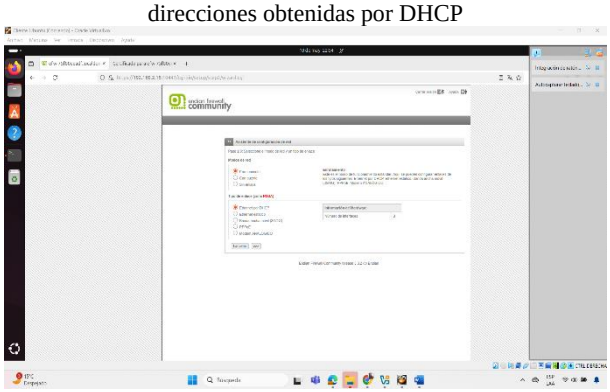
Figura 101 Ingreso a firewall dedes la computadora cliente



Fuente: autoria propia

Se observa la tabla de enrutamiento generada automáticamente en un equipo que recibe su configuración de red a través del protocolo DHCP (Protocolo de Configuración Dinámica de Host).

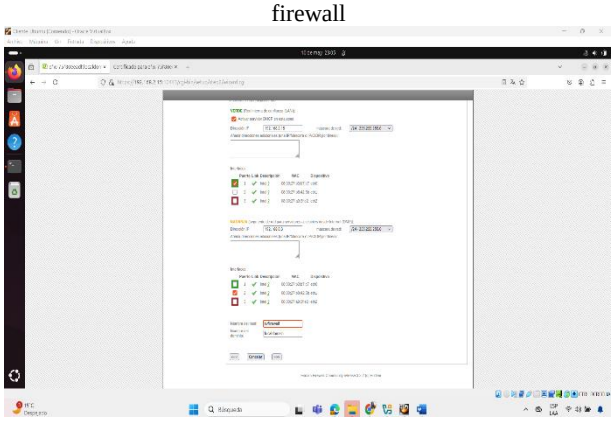
Figura 102 Configuración de rutas basada en enrutamiento y direcciones obtenidas por DHCP



Fuente autoria propia

Proceso de verificación de la correcta configuración y funcionamiento de las zonas de seguridad verde (LAN confiable) y naranja (zona DMZ o desmilitarizada) dentro del firewall.

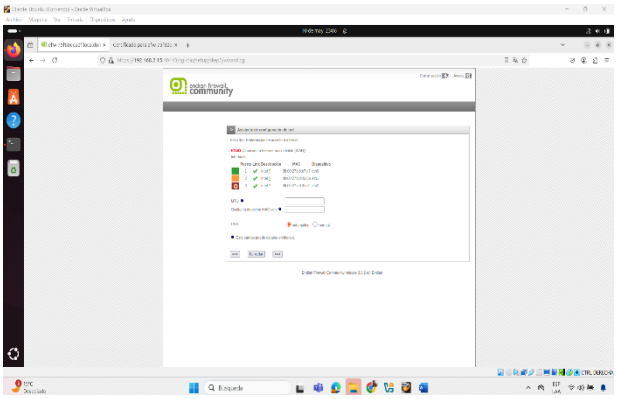
Figura 103 Validacion de las zonas verdes y naranja dentro del firewall



Fuente: autoria propia

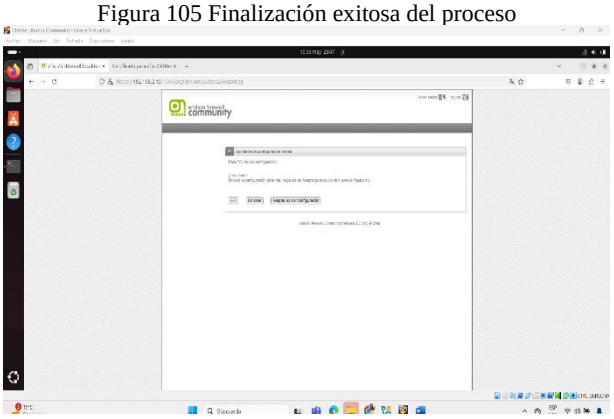
Evidencia la verificación de la configuración del servidor DNS en modo automático, a través del uso de DHCP (Protocolo de Configuración Dinámica de Host). Este proceso permite que el equipo obtenga de forma dinámica la dirección IP del servidor DNS, sin necesidad de realizar una configuración manual.

Figura 104 Confirmación y configuración de DNS en modo automático



Fuente autoria propia

Figura 105 Finalización exitosa del proceso



Fuente autoria propia

Figura 106 cambios aplicados para finalizar el proceso de instalación

Fuente autoria propia

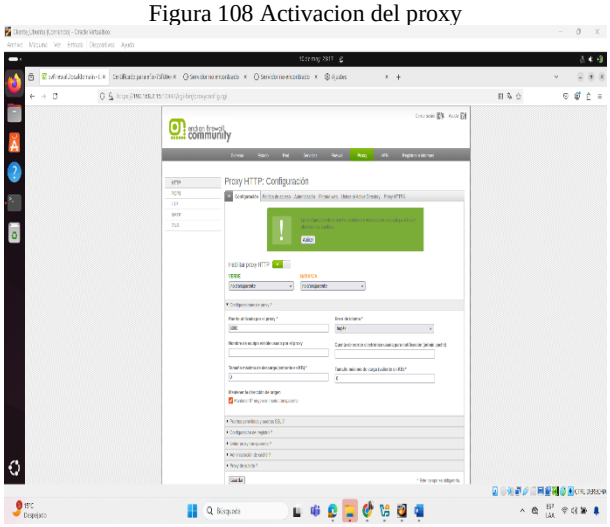
La consola de administración web del firewall Endian Community, accesible a través de una conexión HTTPS desde un navegador en un entorno Ubuntu (VirtualBox). Esta consola permite gestionar y supervisar de forma centralizada la configuración de red, políticas de seguridad, servicios activos y estado general del sistema.

Figura 107 Interface del firewall y su menu de funciones

Fuente autoria propia

El proxy HTTP ha sido habilitado, tanto para la zona VERDE (LAN) como para la zona NARANJA (DMZ). Se puede seleccionar el tipo de funcionamiento del proxy, en este caso configurado como "no transparente", lo que implica que los dispositivos deben ser configurados explícitamente para utilizar el proxy, ya sea manualmente o a través de un archivo de configuración automática.

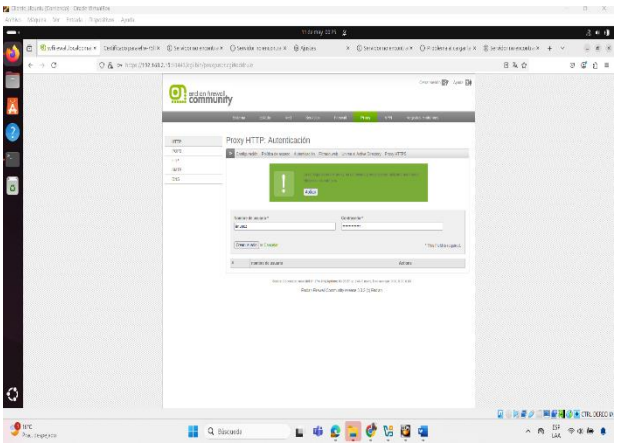
Figura 108 Activacion del proxy



Fuente de autoria propia

En este módulo de autenticación se realiza la creación del usuario que permitirá el acceso al navegador web. Esta autenticación es necesaria para validar si la política de navegación, específicamente el bloqueo de páginas incluidas en la lista.

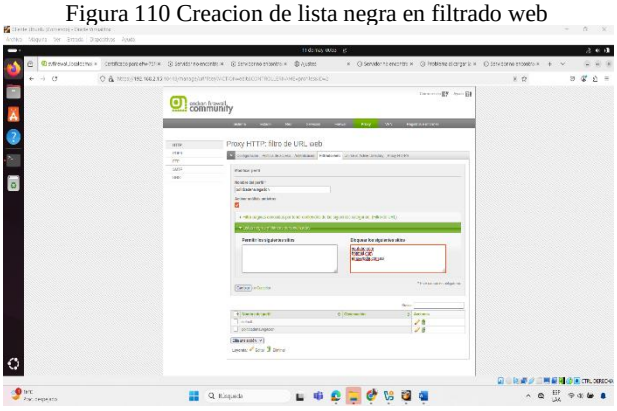
Figura 109 Autentificacion del usuario



Fuente de autoria propia

La imagen muestra la interfaz del módulo de filtrado web en la plataforma Endian Firewall Community, específicamente en la pestaña “Filtrado web” del proxy HTTP. En esta sección se está configurando un perfil personalizado de filtrado que permite bloquear el acceso a ciertos sitios web mediante una lista negra.

Figura 110 Creacion de lista negra en filtrado web



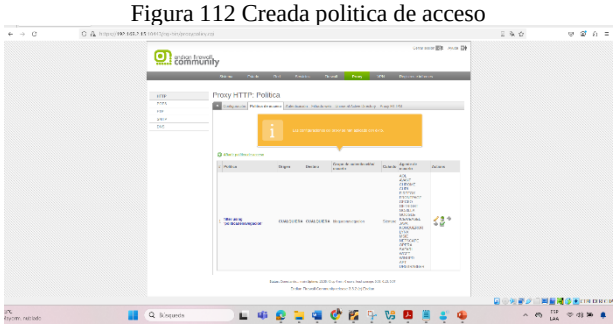
Fuente autoria propia

Figura 111 Se establece una política de acceso y autenticación asociada al grupo, enlazada con el usuario previamente configurado en el módulo de autenticación.

Fuente auotria propia

La imagen muestra la interfaz de configuración de políticas de acceso dentro del módulo Proxy HTTP de Endian Firewall Community, en la pestaña "Política de acceso". Esta funcionalidad permite controlar cómo y cuándo los usuarios o grupos pueden acceder a internet, mediante reglas definidas por el administrador.

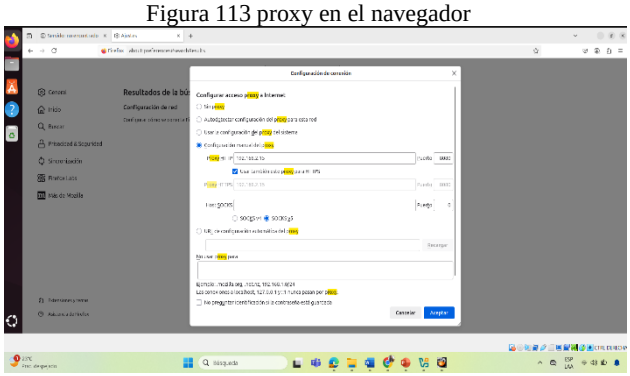
Figura 112 Creada politica de acceso



Fuente: autoria propia

Ingresamos a la configuración del navegador Firefox y, de forma manual, configuramos el proxy estableciendo la dirección 192.168.2.15 Además, seleccionamos la opción para utilizar el mismo proxy también para las conexiones HTTPS.

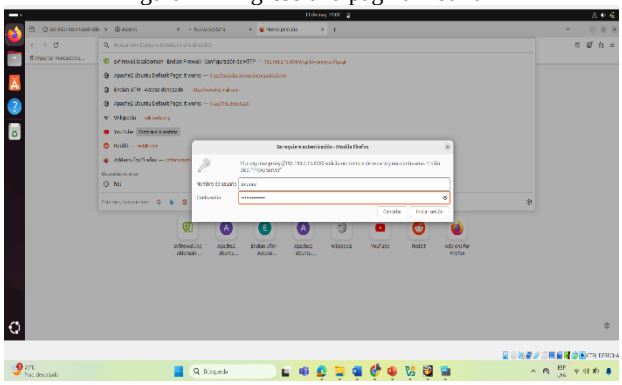
Figura 113 proxy en el navegador



Fuente: autoria propia

Al intentar acceder al sitio web, se nos solicita autenticación. Ingresamos las credenciales del usuario con los permisos correspondientes.

Figura 114 Ingreso a la pagina Hotmail



Fuente: autoria propia

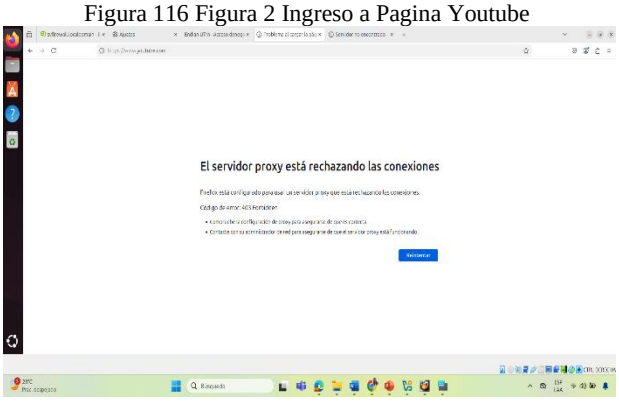
El acceso ha sido bloqueado por la política de navegación definida en el firewall esta advertencia es generada por el proxy HTTP, informando al usuario que se ha denegado el acceso

Figura 115 Error: el acceso ha sido bloqueado por la política de navegación definida en el firewall.

Fuente: autoria propia

De igual forma, al intentar acceder a **www.youtube.com**, se muestra el siguiente mensaje: *"Acceso denegado. Este sitio ha sido bloqueado por la política de navegación del firewall.*

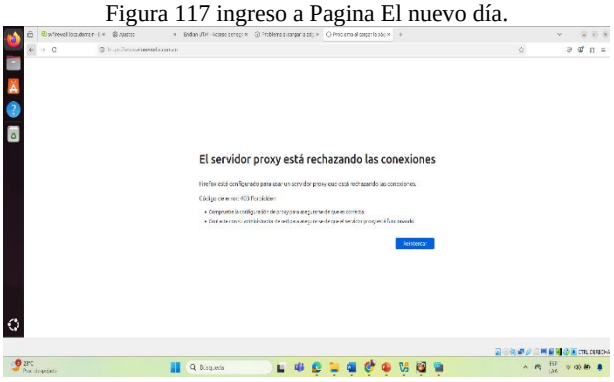
Figura 116 Figura 2 Ingreso a Pagina Youtube



Fuente: autoria propia

De igual forma, al intentar acceder, se muestra el siguiente mensaje: *"Acceso denegado. Este sitio ha sido bloqueado por la política de navegación del firewall.*

Figura 117 ingreso a Pagina El nuevo día.



Fuente: autoria propia

9 CONCLUSIONES.

- Temática 1: La configuración de GNU/Linux Endian en VirtualBox permitió entender de forma práctica cómo se estructura un firewall perimetral con zonas bien definidas. Al implementar las interfaces de red y asignar las zonas verde, roja y naranja, se logró segmentar correctamente la red, lo cual es clave para mejorar la seguridad y el control del tráfico. Esta primera etapa es fundamental, ya que sienta las bases para aplicar reglas y políticas de acceso en las siguientes configuraciones. Además, trabajar en un entorno virtual facilitó el aprendizaje sin afectar redes reales, lo que hace más accesible la práctica de conceptos avanzados de seguridad de red.

- Temática 2: Se conoce la configuración Endian Firewall con las zonas verde (LAN), roja (WAN) y naranja (DMZ), lo que me permitió ver cómo se protege una red real. Al aplicar las reglas de NAT, pude hacer que los dispositivos de la LAN salieran a Internet de forma segura y también expuse servicios en la DMZ sin comprometer la red interna.

- Temática 3: La práctica de implementar servicios dentro de una zona DMZ utilizando herramientas como Endian y Ubuntu Server refuerza la comprensión del diseño de redes seguras y funcionales. Como también la correcta configuración de reglas de firewall es fundamental para permitir únicamente el tráfico necesario, evitando vulnerabilidades que puedan comprometer la integridad del sistema.

- Temática 4: La configuración inicial de Endian en VirtualBox permitió establecer correctamente las zonas de red y preparar el entorno para aplicar reglas de seguridad. Esta base es esencial para gestionar el tráfico entre LAN, WAN y DMZ de forma controlada.

- Temática 5: La implementación de un proxy HTTP no transparente con autenticación representa una solución efectiva para gestionar el uso de Internet en redes organizacionales. Permite identificar a los usuarios que acceden a la red, aplicar políticas diferenciadas según su perfil y mejorar la seguridad informática al restringir el acceso a contenidos no autorizados. Además, proporciona una herramienta poderosa de auditoría y control que fortalece la administración de los recursos tecnológicos. Con esta solución, se contribuye significativamente a una gestión responsable, eficiente y segura del entorno digital institucional.

10 REFERENCIAS

Aplicar las normas APA V7 ed

[1] w. Stallings, Network security essentials (6a ed.)., Boston, MA.: Pearson Education., 2020.

[2] P. &. E. K. Srisuresh, «Traditional IP network address translator (NAT) (RFC 3022),» 2001. [En línea]. Available: https://tools.ietf.org/html/rfc3022.

[3] L. L. X. &. W. Y. Zhang, Network segmentation strategies for modern data centers. IEEE Transactions on Network and Service Management, Nueva York, NY: IEEE, 2018.

[4] Cisco Systems, Network Address Translation (NAT) best practices., San José, CA.: Cisco Systems Inc., 2022.

[5] LPI, LPIC-1 Exam 101. Tema 102: Comandos GNU y Unix, 2022. [En línea]. Disponible en: https://learning.lpi.org/es/learning-materials/101-500/102/
[6] Canonical, Guía del Ubuntu desktop 20.04 LTS, Help Ubuntu, 2023. [En línea]. Disponible en: https://help.ubuntu.com/20.04/ubuntu-help/index.html
[7] Debian, El manual del administrador de Debian 12.5.0, 2023. [En línea]. Disponible en: https://www.debian.org/releases/stable/amd64/index.es.html
[8] Oracle, Manual de usuario VirtualBox, 2020. [En línea]. Disponible en: https://www.virtualbox.org/manual/
[9] Endian, Endian UTM 3.2 Manual referencia, 2016. [En línea]. Disponible en: http://docs.endian.com/3.2/utm/index.html
[10] J. LaCroix, Mastering Ubuntu Server: Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting Ubuntu Server, Packt Publishing, 2020. [En línea]. Disponible en: https://research-ebsco-com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b41952