IMPLEMENTACIÓN DE SEGURIDAD PERIMETRAL EN GNU/LINUX CON ENDIAN FIREWALL (EFW)

David Ricardo Carrasco Cocinero
e-mail: drcarrascoc@unadvirtual.edu.co
Daniel Tomás Cháves Montánchez
dtchavesm@unadvirtual.edu.co
Luis Alberto Pacichaná Domínguez
lapacichanad@unadvirtual.edu.co
Luisa Cristina Mosquera Delgado
luisa.mosquera@escuelanormalpasto.edu.co
Sandra Milena Bolaños Delgado
smbolanosd@unadvirtual.edu.co

RESUMEN: *Este artículo presenta la implementación y configuración de seguridad perimetral en una infraestructura de red mediante la distribución Endian Firewall (EFW) en un entorno virtualizado con VirtualBox. Se describe el proceso de instalación del sistema, la segmentación de las zonas de red (LAN, WAN y DMZ), la creación de reglas de firewall, la configuración de NAT, la definición del tráfico entre zonas, el control de acceso a servicios HTTP y FTP, la denegación de ICMP y la implementación de un servidor proxy HTTP no transparente para el filtrado de contenido. La metodología empleada se basa en prácticas administrativas desde consola, orientadas a garantizar un control riguroso sobre los servicios expuestos en entornos corporativos. Los resultados evidencian que Endian Firewall mejora de forma significativa el nivel de seguridad, constituyéndose en una solución viable y replicable para contextos educativos y empresariales.*

PALABRAS CLAVE: Endian Firewall, Segmentación de redes, Seguridad perimetral, Virtualización.

1 INTRODUCCIÓN

En la administración de sistemas moderna, garantizar la seguridad del perímetro de las redes informáticas es un objetivo de máxima prioridad. Ante el crecimiento de las amenazas cibernéticas, la necesidad de exponer servicios críticos y la alta movilidad de los usuarios, se hace indispensable contar con arquitecturas segmentadas, sólidas y de bajo monitoreo continuo.

La distribución GNU/Linux Endian Firewall (EFW), está diseñada específicamente para esta tarea, ya que ofrece la capacidad de implementar soluciones de seguridad integral que abarcan funcionalidades como firewall, NAT, DMZ y un proxy con mecanismos de autenticación.

En el presente documento se evidenció el proceso de instalación y configuración de Endian Firewall (EFW), desarrollando los siguientes puntos: instalación del sistema operativo Endian Firewall, definición y/o segmentación de zonas de red: LAN (área local), WAN (Red de área amplia), DMZ (zona desmilitarizada); establecimiento de reglas de firewall para controlar el tráfico; Configuración de NAT (Network Address Translation) definición de reglas de tráfico interzona para regular la comunicación entre las diferentes zonas de red (LAN, WAN, DMZ); Permitir servicios de la zona DMZ para la red para los servicios HTTP, FTP y denegar el protocolo ICMP; Establecer las reglas de acceso para permitir o denegar el tráfico interzona e Implementación de un servidor proxy HTTP no transparente con políticas de autenticación y filtrado de contenido.

El propósito principal del proyecto es demostrar la efectividad de Endian Firewall (EFW) como un recurso valioso para la formación, administración de red y protección en entornos educativos y empresariales reales.

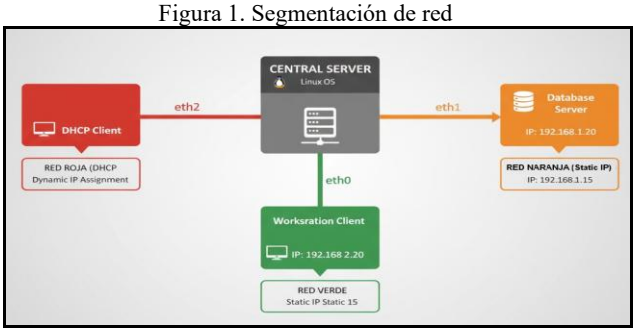
2 METODOLOGÍA

El proceso metodológico se basó en la implementación detallada y secuencial de Endian Firewall (EFW), en un entorno virtualizado, utilizando VirtualBox, con estaciones de trabajo GNU/Linux para la red LAN. La instalación y configuración de EFW se centró en los siguientes aspectos:

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

Se implementó GNU/Linux Endian en VirtualBox, configurando sus interfaces de red para establecer las siguientes zonas y se asignaron direccionamientos IPS pertinentes a toda la red, así:

Figura 1. Segmentación de red



Fuente: Autoría Propia

- **Zona Roja: (DHCP Cliente) eth2c- conecta el sistema a internet o a redes externas (WAN)**
  Tipo de asignación IP: Dinámica (DHCP)
  Propósito: contiene un Cliente DHCP. Esta red está diseñada para la asignación automática de direcciones IP.

- **Zona Naranja (Static IP) Servidores DMZ**
  Interfaz del Servidor Central: eth1
  Dirección IP del Servidor Central (eth1): 192.168.1.15 (esta dirección identifica al Servidor Central dentro de la Red Naranjada)
  Tipo de Asignación IP: Estática. Los dispositivos en esta red tienen direcciones IP fijas, asignadas manualmente.
  Dispositivo Principal: Database Server con la dirección IP 192.168.1.20
  Propósito: esta red es una zona de servidores críticos que requieren direcciones IP fijas para facilitar su acceso y gestión predecible.

- **Zona Verde: (Static IP) – Red Interna (LAN),** red local o intranet, donde residen los usuarios internos.
  Interfaz del Servidor Central: eth0
  Dirección Ip del Workstation Client: 192.168.2.20
  Tipo de Asignación IP: Estática
  Dispositivo principal: Workstation Client con la dirección IP 192.168.2.20
  Propósito: contiene clientes de trabajo (Workstation) con direcciones fijas.

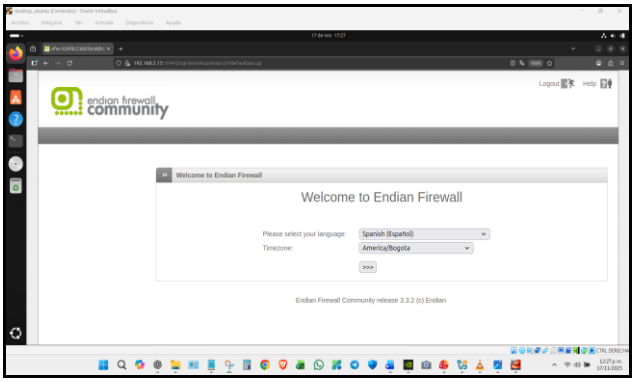
La instalación base del sistema operativo, se llevó a cabo utilizando la imagen ISO oficial de Endian Firewall 3.3.2. Para iniciar el proceso de instalación base, fue necesario preparar un medio de arranque a partir del archivo ISO, posteriormente se procedió a reiniciar el host de virtualización y se modificó la secuencia de boot para asegurar el arranque desde el medio creado. Una vez iniciado el proceso, se siguieron los pasos e indicaciones mostradas en pantalla para completar satisfactoriamente la instalación del sistema.

Figura 2. Instalación y Configuración de Endian 3.3.2

Fuente: Autoría Propia

La Fig. 3, ilustra el primer paso del asistente de configuración post – instalación de Endian Firewall, donde el usuario establece el idioma y la zona horaria del sistema.

Figura 3. Configuración de Endian 3.3.2



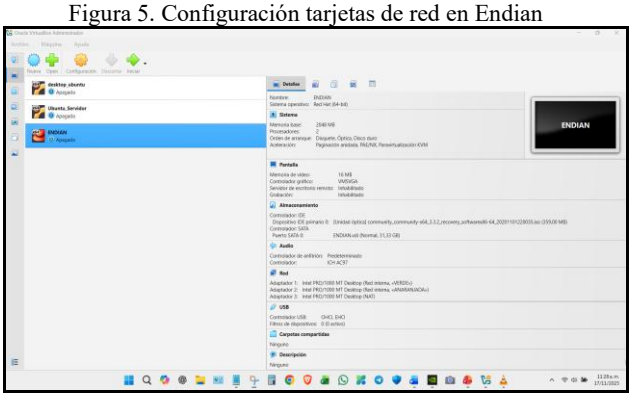
Fuente: Autoría Propia

La Fig. 4, muestra la interfaz de gestión basada en consola de Endian Firewall, la cual permite realizar tareas esenciales de mantenimiento y configuración.

Figura 4. Interfaz de Endian

Fuente: Autoría Propia

Figura 5. Configuración tarjetas de red en Endian

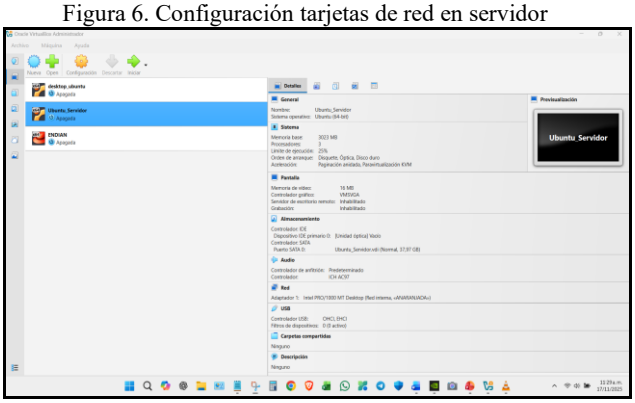


Fuente: Autoría Propia

La Fig. 5, muestra la configuración de las tarjetas de red (adaptadores) para la Endian dentro del administrador de VirtualBox.

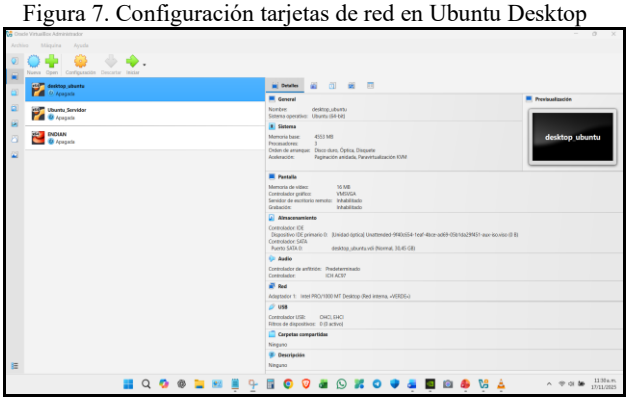
Se procedió a realizar la configuración de las tarjetas de red en el Servidor y en Ubuntu desktop, co mo se muestra en las figuras 6 y 7.

Figura 6. Configuración tarjetas de red en servidor



Fuente: Autoría Propia

Figura 7. Configuración tarjetas de red en Ubuntu Desktop



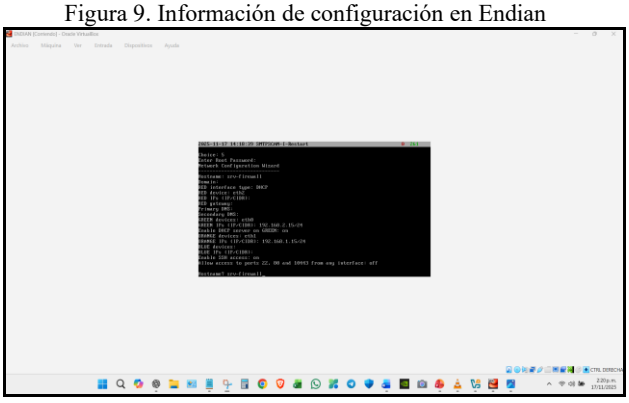
Fuente: Autoría Propia

Figura 8. Zonas verde, naranja y roja, configuradas en Endian

Fuente: Autoría Propia

En la fig. 8, se documenta el proceso crucial donde el administrador mapea las interfaces de red virtuales (eth0, eth1, eth2) a las tres zonas de seguridad (red, Green, Orange) y especifica el método de conexión para la zona externa (Roja).

Figura 9. Información de configuración en Endian



Fuente: Autoría Propia

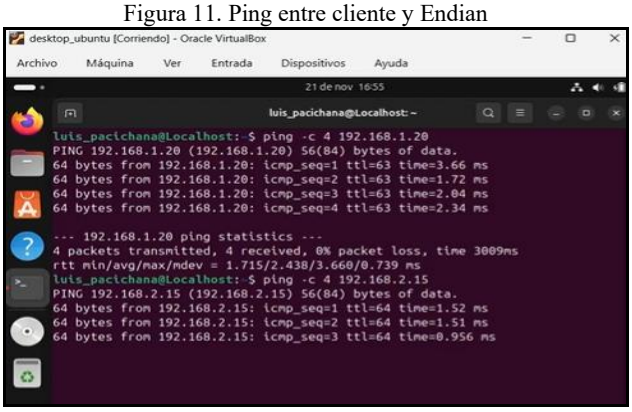
Al finalizar la configuración e instalación del Endian Versión 3.3.2, el usuario es recibido por la interfaz de consola. Se destaca la operatividad de las zonas de seguridad Verde y Roja, cuyas configuraciones de red predefinidas se establecieron automáticamente durante la fase de despliegue del sistema operativo.

Para comprobar la conectividad entre zonas y demostrar que la segmentación funcionó se realizaron las siguientes pruebas, de acuerdo a las figuras 10 y 11.

Figura 10. Ping entre cliente y servidor

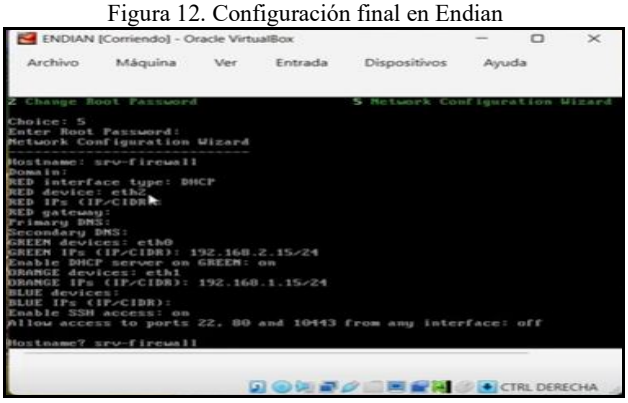
Fuente: Autoría Propia

Figura 11. Ping entre cliente y Endian



Fuente: Autoría Propia

Figura 12. Configuración final en Endian



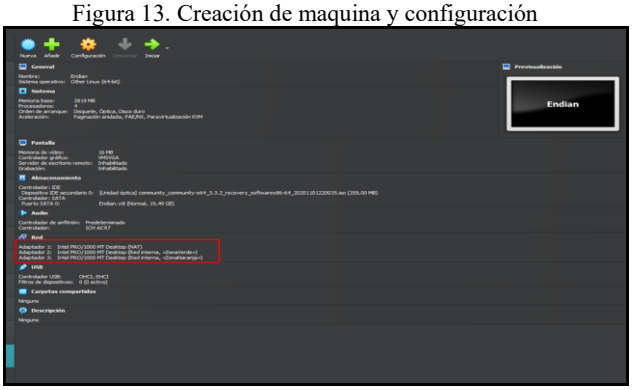
Fuente: Autoría Propia

En la fig. 12, se muestra el resumen de la configuración final de Endian Firewall tal como se presenta en la consola de comandos de ejecutar el asistente de configuración de red.

2.2 TEMÁTICA 2: CONFIGURACIÓN NAT.

En el desarrollo de la etapa 2, inicialmente, se creó la máquina virtual configurando la red como se muestra en la Fig. 13.

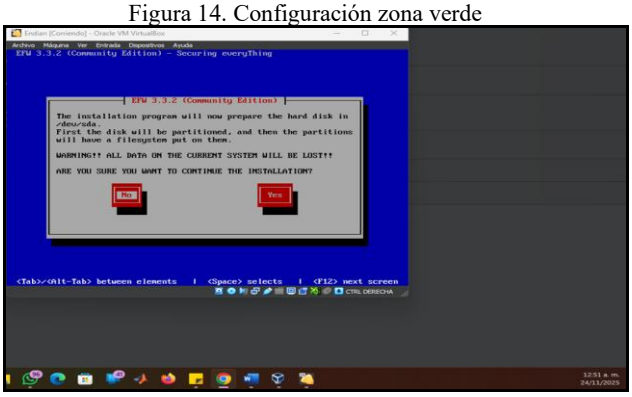
Figura 13. Creación de maquina y configuración



Fuente: Autoría Propia

Se configuró la IP de la zona verde como se muestra e la Fig. 14:

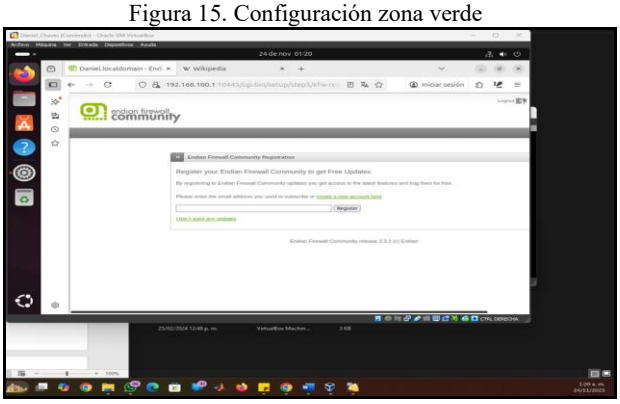
Figura 14. Configuración zona verde



Fuente: Autoría Propia

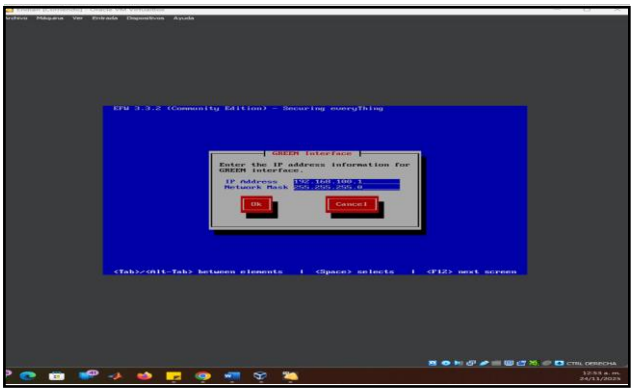
Desde Endian se procedió a realizar las configuraciones correctamente

Figura 15. Configuración zona verde



Fuente: Autoría Propia

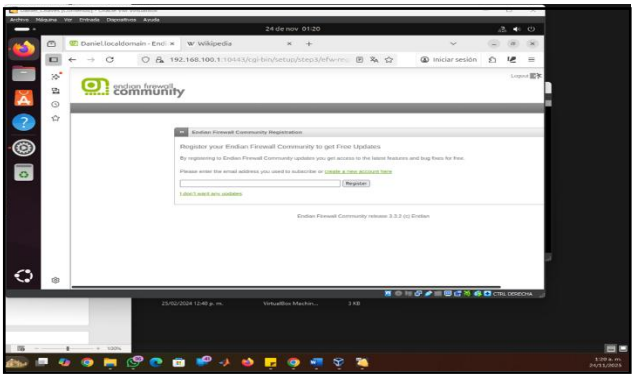
Figura 16. Asignación de IP zona verde



Fuente: Autoría Propia

Al tener acceso a Endian pueden observar todas las configuraciones como se muestran en la figura:

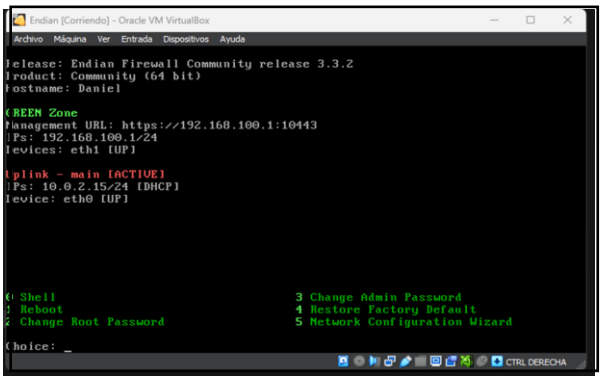
Figura 17. Asignación de IP zona verde



Fuente: Autoría Propia

Se observó que se tiene la comunicación esperada.

Figura 18. Configuración en Endian



Fuente: Autoría Propia

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

Permitir los servicios HTTP (Puerto 80) y FTP (Puerto 21) desde el servidor Web bajo Ubuntu Server. 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.

Siguiendo la configuración de la red, de acuerdo a la segmentación realizada en la temática 1, se realizó la configuración de Endian en la máquina virtual VirtualBox y versión Red Had 64 bits.

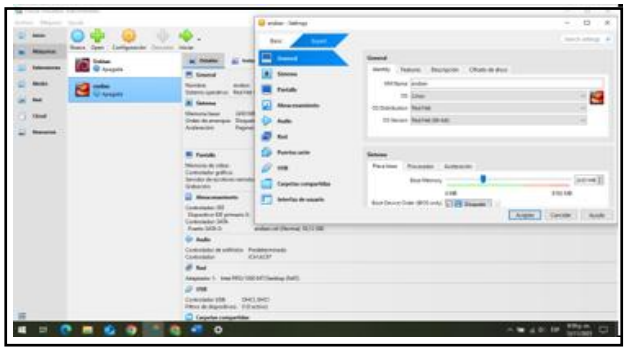
En el icono de configuración se ingresó a la Red en los adaptadores de red (RedVerde, RedNaranja y RedRoja)

Adaptador 1 / conectar Red Interna / nombre RedVerde/ Tipo de adaptador intelPRO/1000 MT.

Adaptador 2 / nombre RedNaranja / Tipo de adaptador intelPRO/1000 MT.

Adaptador 3 / conectar NAT / Tipo de adaptador intelPRO/1000 MT / Guardar.

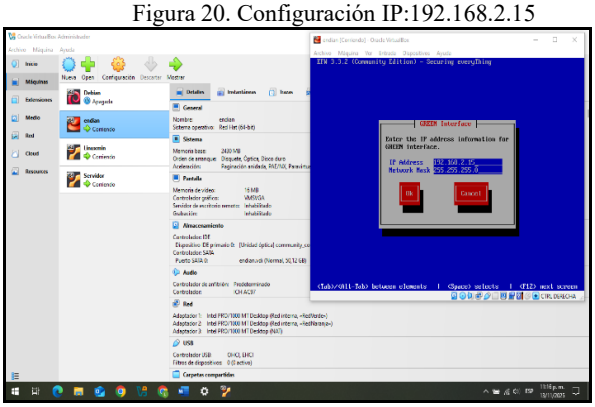
Figura 19. Validación del adaptador 1 en Endian



Fuente: Autoría Propia

Una vez realizada la configuración se procedió a iniciar la instalación, se seleccionó el idioma inglés ok

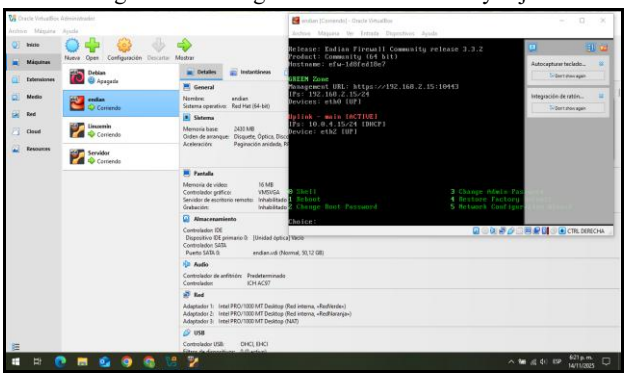
Figura 20. Configuración IP:192.168.2.15



Fuente: Autoría Propia

Con la configuración que se realizó se obtuvieron las zonas verde y roja de forma automática IP 10.0.4.15/24 DHCP:

Figura 21. Configuración de zona verde y roja.



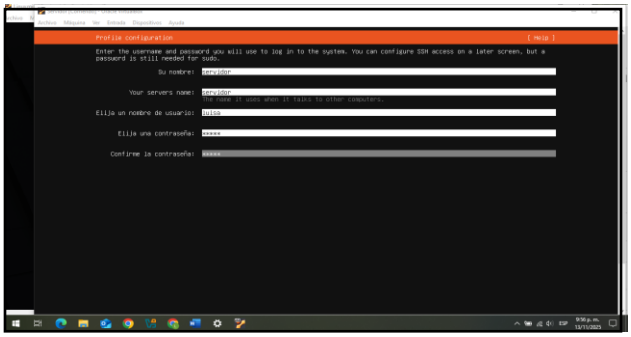
Fuente: Autoría Propia

Se realizó la instalación del Ubuntu Server 24.04.3, descargado de la página oficial: https://ubuntu.com/download/server, se procedió a realizar la configuración inicial, de memoria 2048 MB, y un disco 51,30 GB.

Configuración Ubuntu server – nombre Servidor/ selección ISO Ubuntu24.04.3, OS: Linux, distribución Ubuntu y 64 bit. configuración Red /conectar a Red interna /nombre: RedNaranja /aceptar. Se seleccionó el idioma español y el teclado.

Se continuó con la configuración de interfaz para el servidor en enp03 /edit IPv4, se configura IPv4, se configuró nombre de servidor, usuario y contraseña.

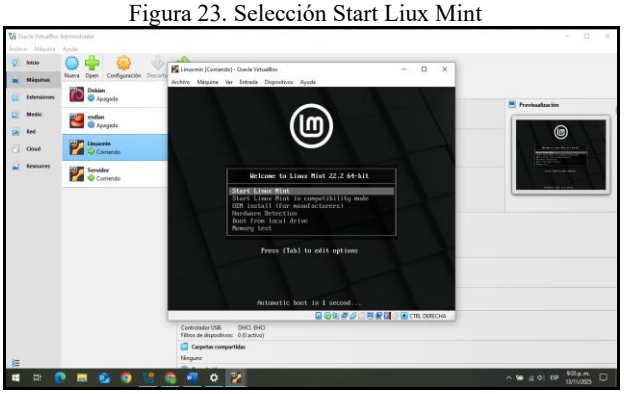
Figura 22. Configuración en el servidor



Fuente: Autoría Propia

De igual manera se procedió con la instalación de Linux mint 22.2 desde la página oficial: https://linuxmint-installation-guide.readthedocs.io/en/latest/index.html, se realizó la configuración inicial, de memoria 2048 MB, y un disco 52,48 GB. En configuración se dio un nombre Linuxmin, se seleccionó ISO Linux mint, SO Linux, distribución: Ubuntu y la versión x 64. Clic en configuración, red y Adaptador 1 conectar a una red interna /nombre redverde/ aceptar.

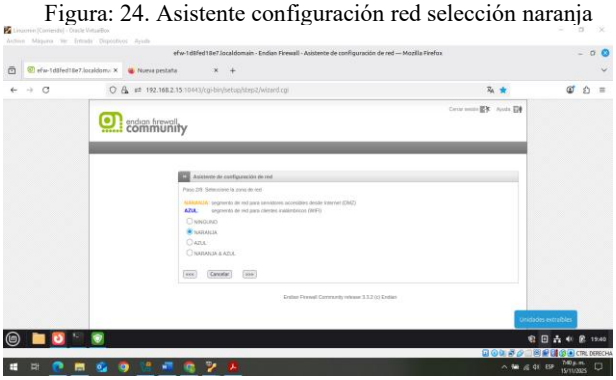
Figura 23. Selección Start Liux Mint



Fuente: Autoría Propia

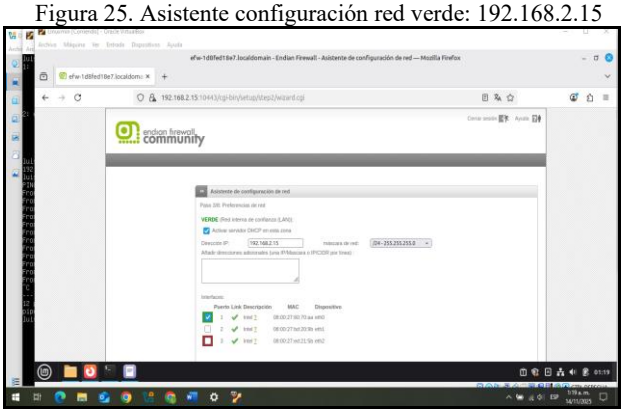
Paso seguido se realizó la instalación y configuración de Endian, siguiendo los pasos de selección de idioma, configuración de contraseña, entre otros. De igual manera se realizó la configuración de cada una de las redes, naranja, verde, roja y DNS automático y correo electrónico por defecto.

Figura: 24. Asistente configuración red selección naranja



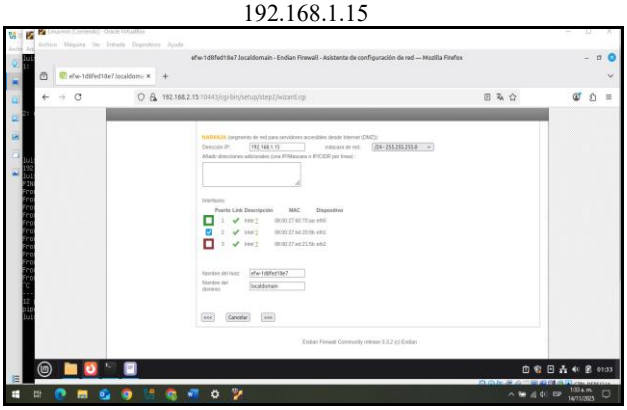
Fuente: Autoría Propia

Figura 25. Asistente configuración red verde: 192.168.2.15



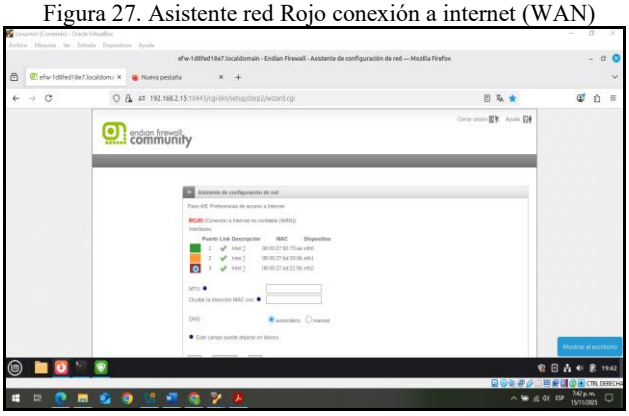
Fuente: Autoría Propia

Fuente: 26. Asistente de configuración red Naranja IP 192.168.1.15



Fuente: Autoría Propia

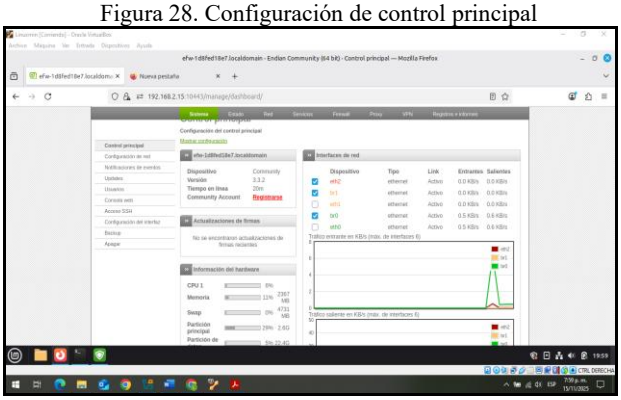
Figura 27. Asistente red Rojo conexión a internet (WAN)



Fuente: Autoría Propia

Se aplicó la configuración y se evidenció la configuración de control principal.

Figura 28. Configuración de control principal

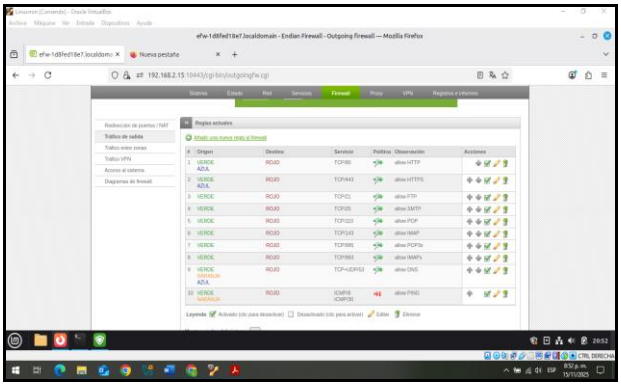


Fuente: Autoría Propia

Para ver la configuración seleccionar tráfico de salida y seleccionar Firewall, se mostró el servicio TCP 80 con allow HTTP y el servicio TCP 21 allow FTP.

Configuración de firewall de salida: para poder cambiar origen:Verde y destino Rojo de servicio ICMP/8 y ICMP/30 se editó por lápiz y cambió el origen a verde y destino rojo y proxy apagado.

Figura 29. Reglas actuales



Fuente: Autoría Propia

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

Preparación de Servicios (Ubuntu Server - Zona DMZ)

Antes de crear las reglas, se aseguró que el servidor en la DMZ tuviera qué mostrar.

1. Se fue a la consola de tu **Ubuntu Server (DMZ)**.
2. Se verificó que el servicio Web y FTP estuvieran corriendo.
   - sudo systemctl status apache2
   - sudo systemctl status vsftpd, instalamos SFTP si fueran necesario: sudo apt install vsftpd.

Figura 30. Preparación de servicios Ubuntu Server

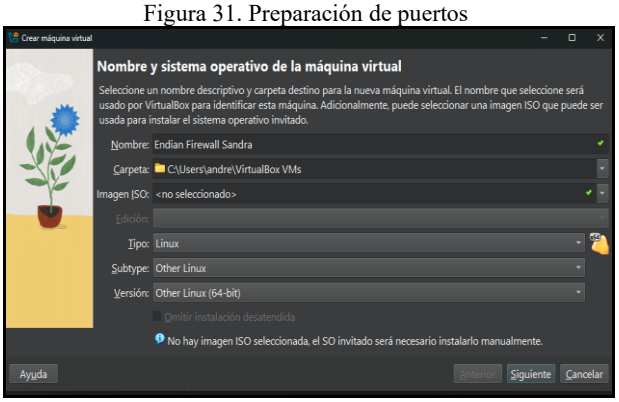
Fuente: Autoría Propia

Se configuró la red en VirtualBox con la máquina de ENDIAN

A. Se configuró la Máquina de Endian (El Guardián):

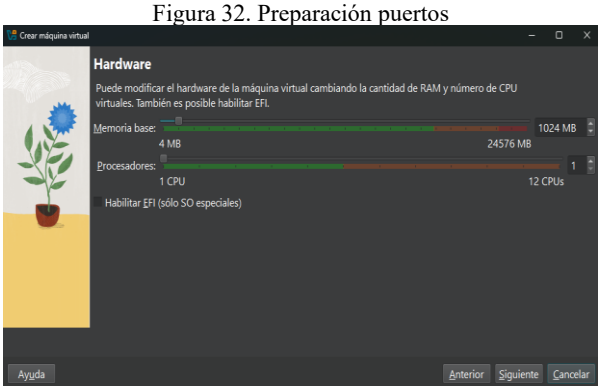
1. En VirtualBox, se creó una nueva máquina virtual.
   a. Nombre: Endian Firewall Sandra
   b. Tipo: Linux
   c. Versión: Other Linux (64-bit)
   d. RAM: 1024 MB (1GB)
   e. Disco duro: Crea uno nuevo de 20GB.

Figura 31. Preparación de puertos



Fuente: Autoría Propia

Figura 32. Preparación puertos



Fuente: Autoría Propia

Se configuraron las redes.
-> Configuración -> Red.
Endian necesita 3 tarjetas (adaptadores):

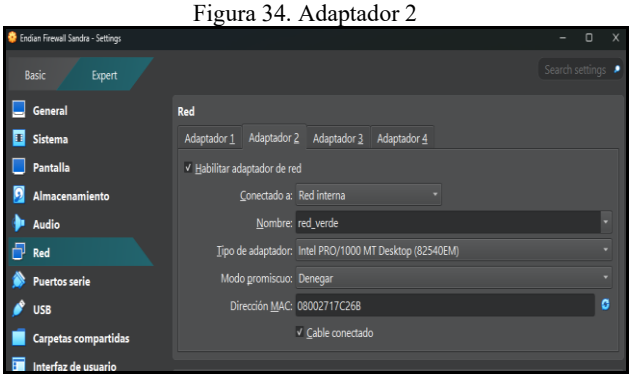
- Adaptador 1 (Zona ROJA/Internet)
- Conectado a: Adaptador Puente (Bridged Adapter).
  - *Esto hará que Endian tome router real.*

Figura 33. Adaptador 1

Fuente: Autoría Propia

Adaptador 2 (Zona VERDE/LAN):
Conectado a: Red Interna (Internal Network).
Nombre: red_verde.

Figura 34. Adaptador 2

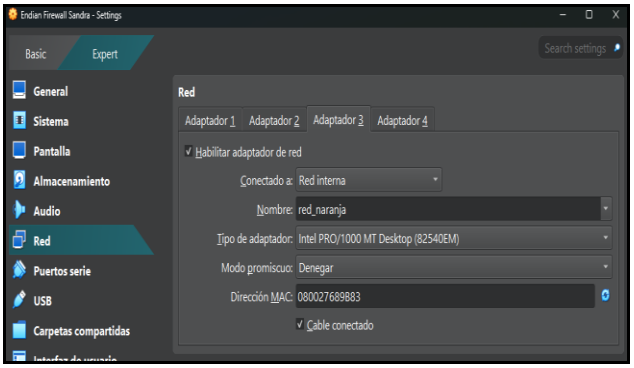


Fuente: Autoría Propia

Adaptador 3 (Zona NARANJA/DMZ):
Conectado a: Red Interna.
Nombre: red_naranja.

La Fig. 34, muestra la configuración del Adaptador 2 de red para la máquina virtual de Endian Firewall dentro de la configuración de VirtualBox.

Figura 35. Adaptador 3



Fuente: Autoría Propia

Ahora se continua con la configuración e instalación de la ISO de Endian,

B. Configuración de Ubuntu Desktop

Se realizó la configuración de la red, los adaptadores 1

Figura 36. Configuración de Desktop

Fuente: Autoría Propia

C. Configuración de Ubuntu Server (El Servidor)

Adaptador 1: Conectado a Red Interna.
Nombre: red_naranja.
Explicación: Este PC ahora está aislado en la zona naranja.

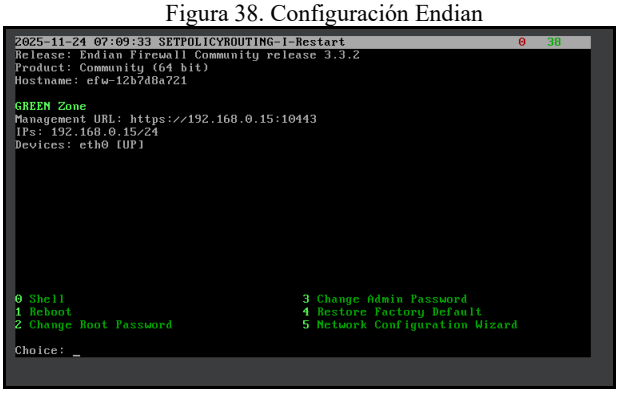
Figura 37. Configuración Ubuntu Server

Fuente: Autoría Propia

Instalación y configuración de Endian

Se configuró ENDIAN con la ip 192.168.10.1 (Mascara: 255.255.255.0 / 24).

Figura 38. Configuración Endian



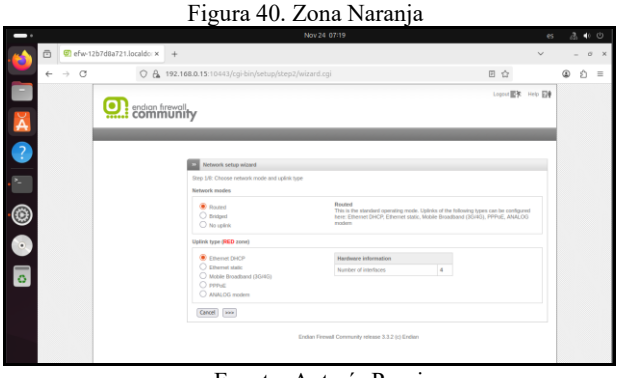
Fuente: Autoría Propia

Configuración de las IPs Ubuntu Desktop y Server

Figura 39. Zona verde

Fuente: Autoría Propia

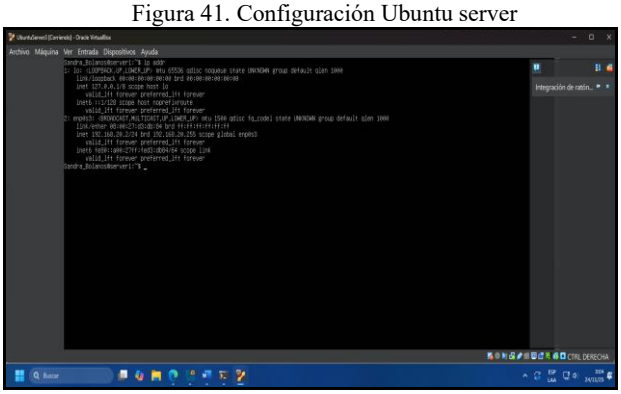
Figura 40. Zona Naranja



Fuente: Autoría Propia

Se continuó con la configuración de Ubuntu Server. Se asignó una Ip a ubuntuserver a través del comando sudo nano /etc/netplan/00-installer-config.yaml :

Figura 41. Configuración Ubuntu server



Fuente: Autoría Propia

Ya realizadas todas las configuraciones iniciales, se procedió a realizar la configuración de lo solicitado en la temática 4.

Endian: El cerebro (192.168.10.1 y 192.168.20.1).
Ubuntu Desktop: El empleado (192.168.10.2).
Ubuntu Server: El servidor (192.168.20.2).

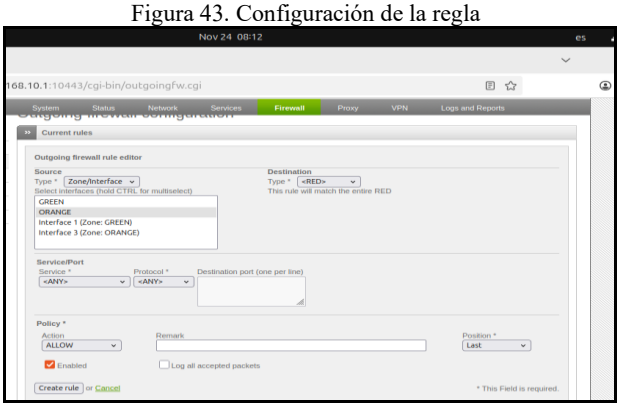
Asignación de reglas y verificación de conexiones

Se da acceso a internet al servidor agregando una nueva regla en endian

Figura 42. Acceso a internet con nueva regla

Fuente: Autoría Propia

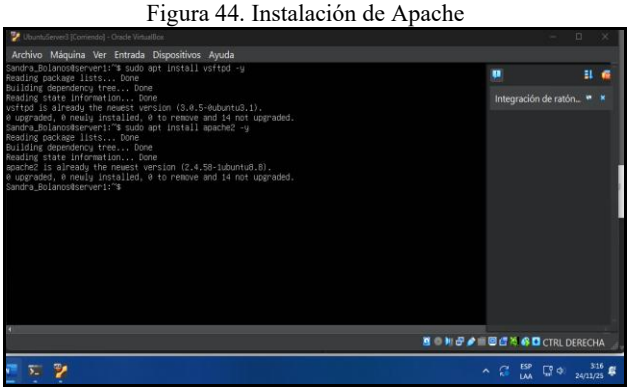
Figura 43. Configuración de la regla



Fuente: Autoría Propia

Se procedió a realizar la instalación de apache en el servidor FPT, utilizando el comando sudo apt update.

Figura 44. Instalación de Apache



Fuente: Autoría Propia

Se comprobó que el servidor esté funcionando en DMZ.

Se configuró la comunicación VERDE ->NARANJA, Primero en HTTP:

Figura 45. Configuración en HTTP

Fuente: Autoría Propia

Se configura en FTP:

Figura 46. Configuración en FPT

Fuente: Autoría Propia

Se logró acceder a través de la IP 192.168.20.2

Figura 47. Comprobación de conexión

Fuente: Autoría Propia

Se configura INTERNET -> DMZ

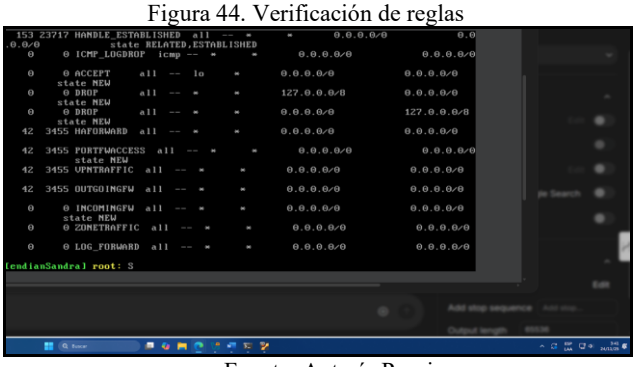
Se creó la regla NAT

Figura 48. Creación de la regla NAT

Fuente: Autoría Propia

Luego, se verificaron las reglas en consola

Figura 44. Verificación de reglas



Fuente: Autoría Propia

Ejecución de pruebas finales

A. Ingreso a HTTP LAN hacia DMZ:

En Ubuntu Desktop:

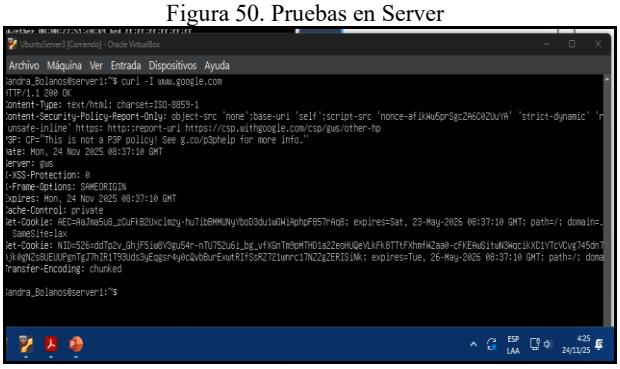
Figura 49. Pruebas en Desktop

Fuente: Autoría Propia

B. Ingreso a HTTP WAN hacia DMZ

Se encontró la IP ROJA en Endian:

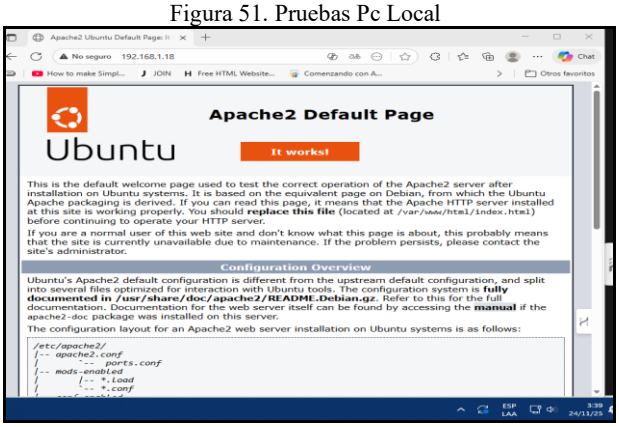
Figura 50. Pruebas en Server



Fuente: Autoría Propia

Se realizó la prueba desde PC local

Figura 51. Pruebas Pc Local



Fuente: Autoría Propia

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

En esta temática se creó un perfil y se estableció una lista negra para bloquear los sitios

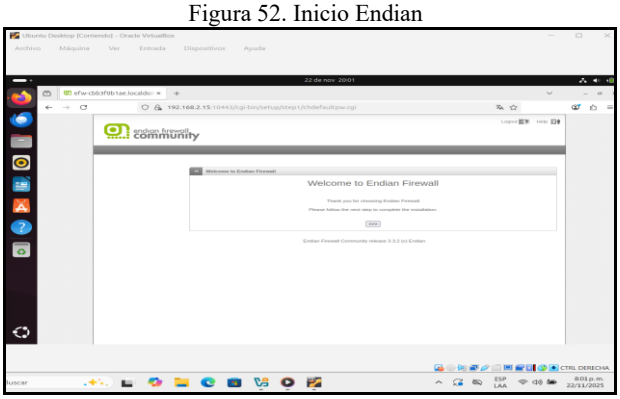
- www.hotmail.com
- www.youtube.com
- www.elnuevodia.com.co

Además, se debió implementar la autenticación por usuario, creando un usuario y asignándole a un grupo, estableciendo una política de acceso y vinculando esta política con el perfil creado. Finalmente, se probó el acceso a los sitios bloqueados desde la LAN utilizando un navegador web.

De acuerdo al diagrama de segmentación de red anteriormente creado, una vez realizada la instalación y configuración de redes en los sistemas ubuntu server, ubuntu desktop y Endian.

Se dio inicio a la temática ingresando a la página de configuraciones de firewall en Endian

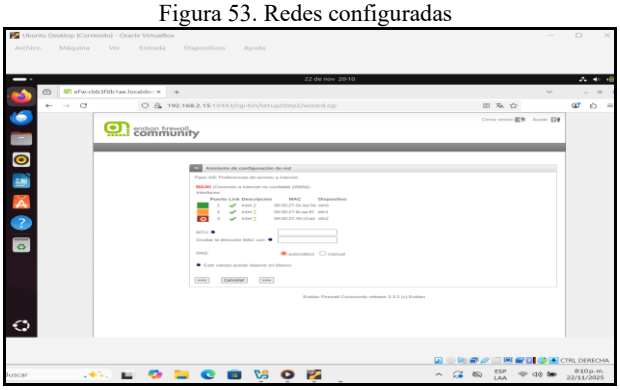
Figura 52. Inicio Endian



Fuente: Autoría Propia

Se continuó ejecutando el asistente de configuración y una vez se tuvo configurada la segmentación de redes, éstas aparecieron como se muestra en ala Fig. 53

Figura 53. Redes configuradas



Fuente: Autoría Propia

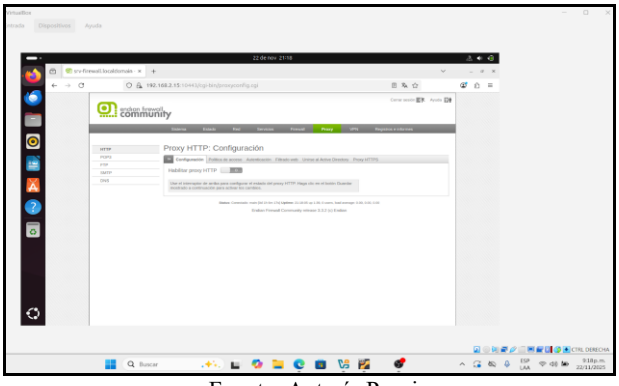
Para finalmente tener acceso al panel de control principal de Endian

Figura 54. Panel de control

Fuente: Autoría Propia

Navegando por este panel de control se encontró con la sección Proxy HTTP Configuración

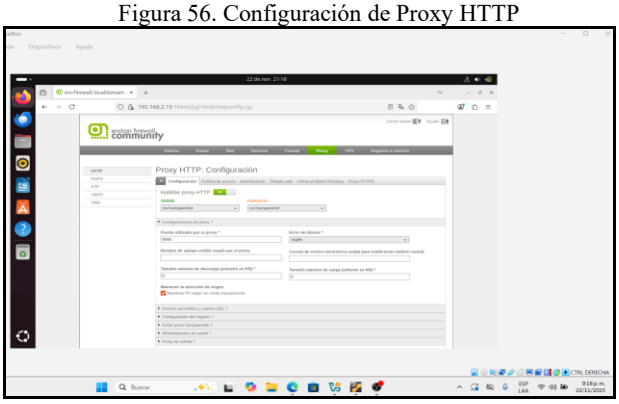
Figura 55. Sección Proxy HTTP Configuración



Fuente: Autoría Propia

Se habilitó el proxy HTTP, apareciendo las redes y configuraciones adicionales del Proxy

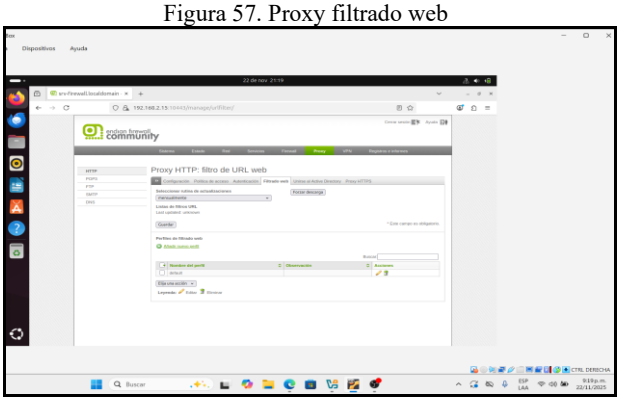
Figura 56. Configuración de Proxy HTTP



Fuente: Autoría Propia

Se recorrió la barra de opciones horizontal hasta la pestaña filtrado web

Figura 57. Proxy filtrado web

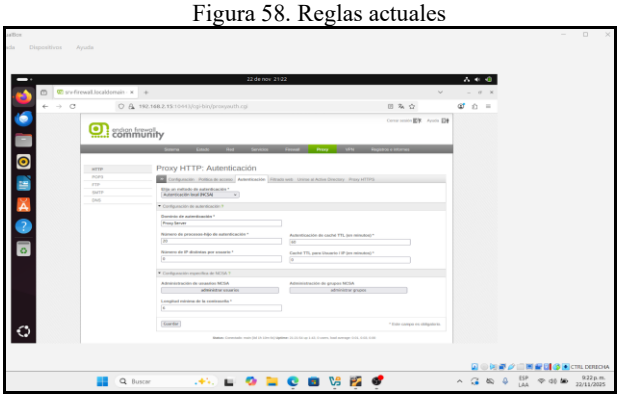


Fuente: Autoría Propia

Se creó un nuevo perfil de filtrado web con el nombre bloqueado y los requerimientos iniciales y se guardó está configuración.

Se recorrió la barra de opciones horizontal nuevamente hasta la pestaña Autenticación y se recorrió el botón administración de usuarios y administración de grupos

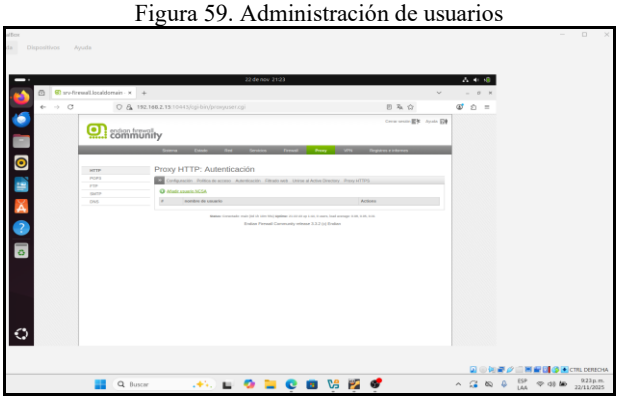
Figura 58. Reglas actuales



Fuente: Autoría Propia

Se seleccionó administración de usuarios, y se escogió la opción de añadir usuario NCSA.

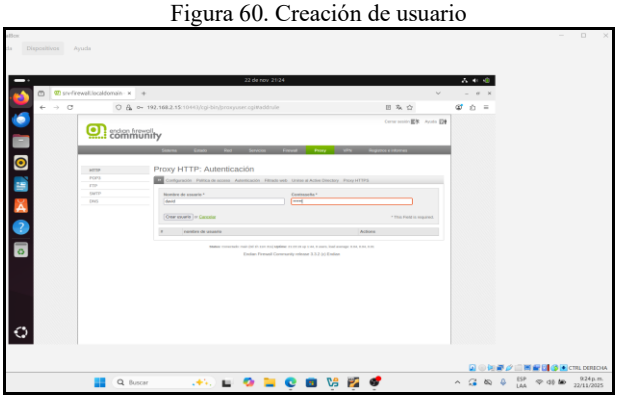
Figura 59. Administración de usuarios



Fuente: Autoría Propia

Se seleccionó añadir usuario NCSA y se creó el usuario David con contraseña.

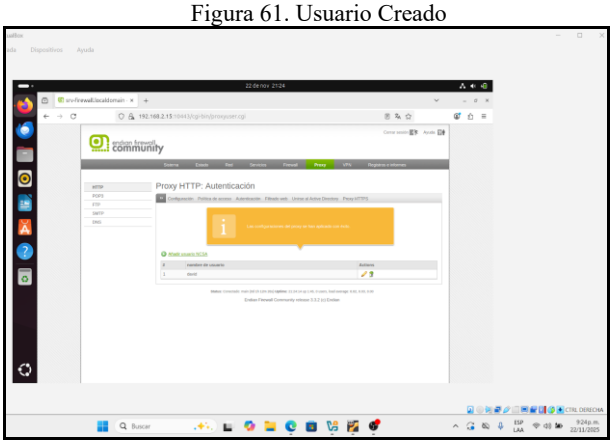
Figura 60. Creación de usuario



Fuente: Autoría Propia

Usuario creado exitosamente.

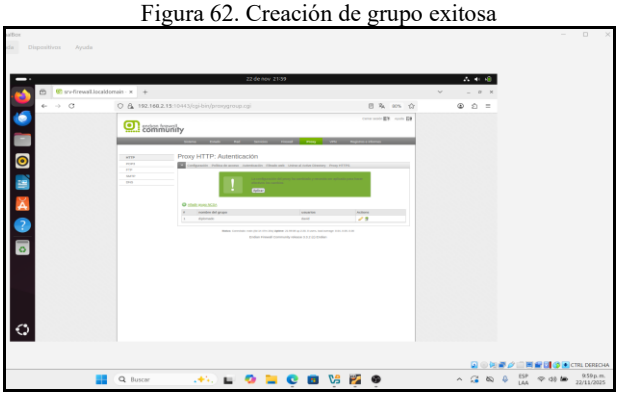
Figura 61. Usuario Creado



Fuente: Autoría Propia

Se seleccionó administración de grupos y apareció la opción de añadir grupo NCSA, se creó el grupo diplomado y se agregó el usuario david.

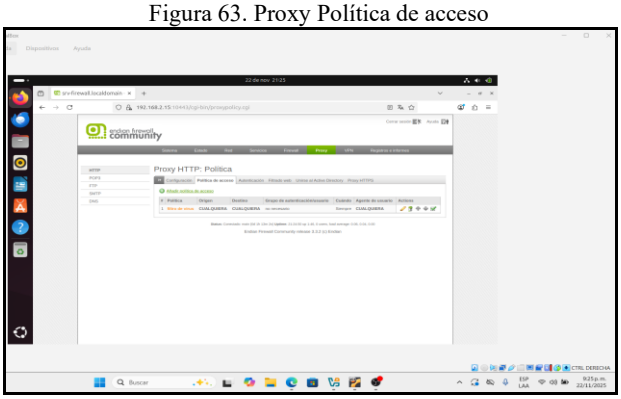
Figura 62. Creación de grupo exitosa



Fuente: Autoría Propia

Se recorrió la barra de opciones horizontal hasta la pestaña Política de acceso

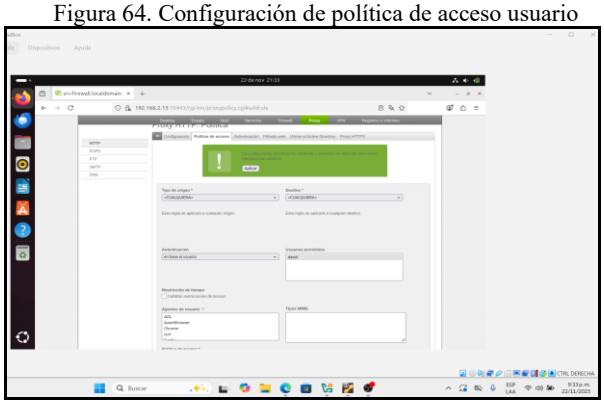
Figura 63. Proxy Política de acceso



Fuente: Autoría Propia

Se seleccionó añadir política de acceso y en el formulario para autenticación se seleccionó de acuerdo a al usuario, apareciendo el usuario david.

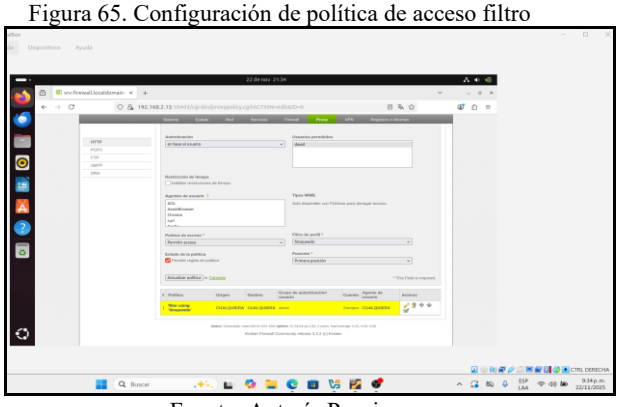
Figura 64. Configuración de política de acceso usuario



Fuente: Autoría Propia

Se seleccionó **permitir acceso** y se despliegan los filtros creados, encontrando el anteriormente creado bloqueado y se actualiza la política.

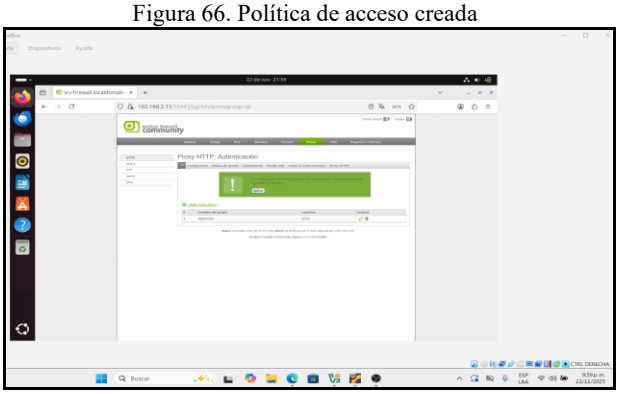
Figura 65. Configuración de política de acceso filtro



Fuente: Autoría Propia

La Política de acceso se creó exitosamente, por lo tanto se aplicó la configuración.

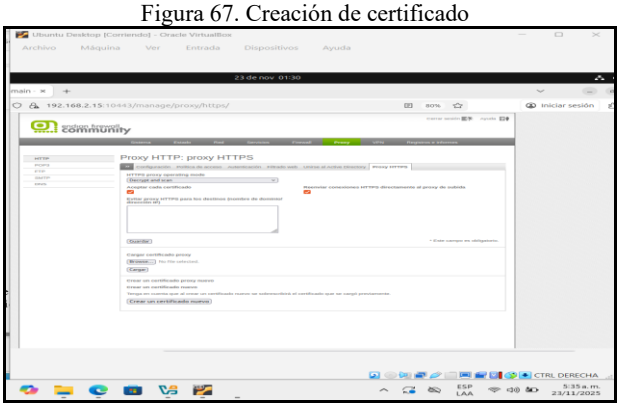
Figura 66. Política de acceso creada



Fuente: Autoría Propia

Dado que la configuración es proxy no transparente se recorrió la barra de opciones horizontal hasta la pestaña Proxy HTTPS y se seleccionó la opción Decrypt and scan y luego se creó un certificado nuevo.

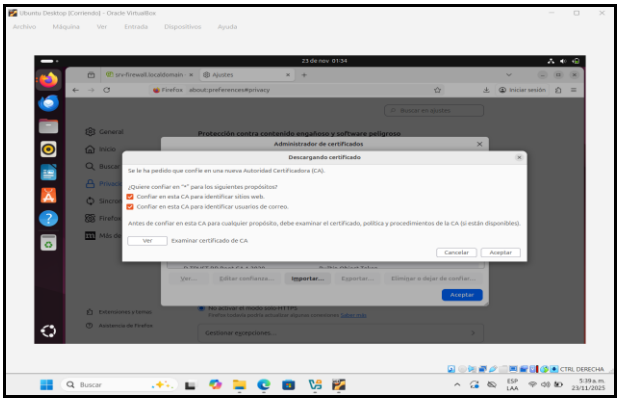
Figura 67. Creación de certificado



Fuente: Autoría Propia

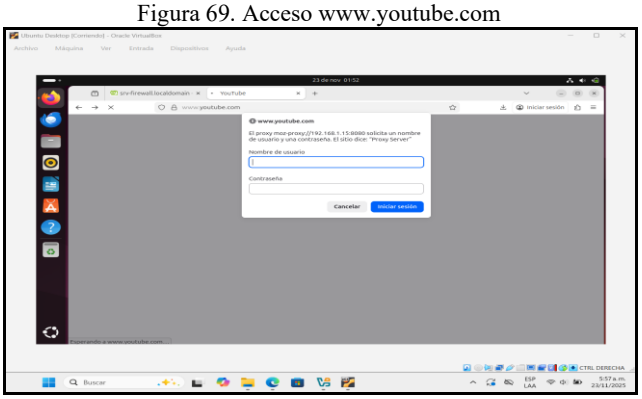
Este certificado al ser guardado se importa en el navegador en este caso en la sección administración de certificados de Firefox.

Figura 68. Creación de certificado



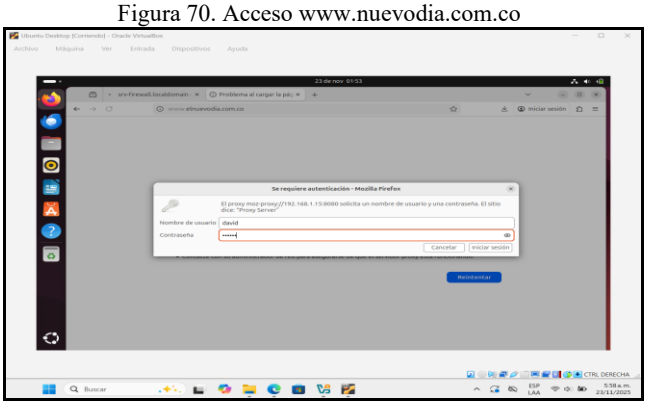
Fuente: Autoría Propia

Figura 69. Acceso www.youtube.com



Fuente: Autoría Propia

Figura 70. Acceso www.nuevodia.com.co



Fuente: Autoría Propia

De esta manera se implementó un proxy http (no transparente) con políticas de autenticación para navegación en internet

3 RESULTADOS

Al realizar la implementación y configuración de seguridad perimetral utilizando la distribución Endian Firewall (EFW), se puedo confirmar la efectividad de EFW como una solución de seguridad perimetral integral y viable.

Segmentación de red y arquitectura zonal: se implementaron con éxito las tres zonas de seguridad esenciales: Roja, Verde y Naranja,

La configuración de cada interfaz (eth0, eth1, eth2) en VirtualBox, a la red lógica correspondiente, permitió simular un entorno de seguridad real y lograr el aislamiento de trafico requerido a través del control de trafico y reglas de Firewaall/NAT.

Se demostró el control de tráfico Inter zona mediante el establecimiento de reglas específicas.

Se configuró NAT (Network Address Translation) y se establecieron reglas para permitir servicios críticos desde la DMZ (Zona Naranja) hacia la LAN (Zona Verde) y la WAN

(Zona Roja/Internet), específicamente HTTP (Puerto 80) y FTP (Puerto 21).

Se validó la denegación del protocolo ICMP (ping) para el control del tráfico, cumpliendo con el objetivo de limitar la capacidad de sondeo de la red.

Se configuró un servidor proxy HTTP no transparente

Se implementaron políticas de autenticación (creación de usuario y grupo NCSA) y filtrado de contenido mediante la creación de un perfil y la definición de una lista negra para bloquear sitios web específicos.

Conclusiones.

La implementación de GNU/Linux Endian en VirtualBox, con la segmentación de redes en zonas Verde, Roja y Naranja, permitió simular un entorno de seguridad real debido a la correcta configuración de las tarjetas de red de la máquina virtual, asignando cada interfaz (eth0, eth1, eth2) a la red lógica correspondiente (LAN, WAN o DMZ).

Segmentación: se logró el objetivo de aislamiento de tráfico, donde la Zona Verde (LAN) quedando protegida del tráfico externo (Roja) y de los servidores expuestos (Naranja).

Entorno de Pruebas: VirtualBox demostró ser una herramienta ideal y de bajo costo para practicar la administración de firewalls sin comprometer una red física real.

El esquema de zonas (Roja, Naranja, Verde) proporcionó el cimiento esencial para la seguridad perimetral. Esta segmentación robusta valida el principio de defensa en profundidad y permite al administrador aplicar reglas estrictas para el filtrado de paquetes y mitigar activamente el riesgo de intrusiones.

La configuración de tres tarjetas de red en VirtualBox junto con las tres zonas de Endian 3.3.2 Verde (interna), Naranjada (servidores) y Roja (internet) permite establecer una arquitectura de red segmentada, segura y funcional. Esta separación garantiza que cada zona cumpla un rol específico: la Zona Verde para la red interna de usuarios, la Zona Naranja para aislar y proteger los servicios expuestos, y la Zona Roja como punto de salida hacia internet.

Gracias a esta estructura, es posible mejorar el control del tráfico, aplicar políticas de seguridad más precisas y reducir riesgos, logrando así un entorno más organizado y confiable para la gestión y protección de los recursos de la red.

Endian Firewall es una solución funcional y replicable para ambientes que requieren una arquitectura segmentada, sólida y con mecanismos integrales de protección perimetral.

4 REFERENCIAS

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

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

[3] J. Sanchez Geraldo (2021). VirtualBox con Endian 3.3.2, 3 Zonas: Verde, Naranja y Roja. https://www.youtube.com/watch?v=Dvht5wCPIrI