SEGURIDAD PERIMETRAL CON ENDİAN FIREWALL PARA LA IMPLEMENTACIÓN DE UNA RED LAN–DMZ–WAN

Yisireth Murcia Ortiz
e-mail:ymurciao@unadvirtual.edu.co
Ana Isabel Agredo Hoyos
e-mail: aiagredoh@unadvirtual.edu.co
pedro sarria encarnacion
e-mail: pedro.s.e.2003@gmail.com
Cristian Xavier Sanchez Valencia
email: cxsanchez@unadvirtual.edu.co
Nicolas Arled Arregoces Sanchez
email: naarregocess@unadvirtual.edu.co

RESUMEN: *Este artículo describe la creación y validación de un entorno de seguridad perimetral para una infraestructura de red, empleando GNU/Linux Endian Firewall (EFW) con zonas LAN (Verde), DMZ (Naranja) y WAN (Roja). Se garantizó la protección de los servidores y bases de datos en la DMZ, así como el control de acceso y comunicación entre zonas, mediante la configuración de NAT, políticas de firewall, reglas interzona y un proxy HTTP autenticado. También se documentó el manejo de servicios por consola, evidenciando cada acción con fecha y hora. El proceso demostró la robustez de la arquitectura, verificando accesos HTTP, FTP, restricciones ICMP y la navegación controlada desde la LAN a Internet***.**
.

PALABRAS CLAVE: DMZ, Endian Firewall, Seguridad Perimetral, NAT, Proxy.

1. INTRODUCCIÓN

La implementación de seguridad perimetral es esencial para proteger la información y garantizar la integridad de los servidores dentro de una organización. Con el uso de la distribución Endian Firewall es posible segmentar la red en zonas con diferentes niveles de confianza, permitiendo un control granular sobre el tráfico. En este artículo se presenta el desarrollo de cinco temáticas fundamentales para la configuración de un entorno seguro mediante la integración de las zonas Verde (LAN), Roja (WAN) y Naranja (DMZ), asegurando el funcionamiento de aplicaciones críticas alojadas en servidores GNU/Linux.

2. FORMATO

La arquitectura se basó en la siguiente segmentación:

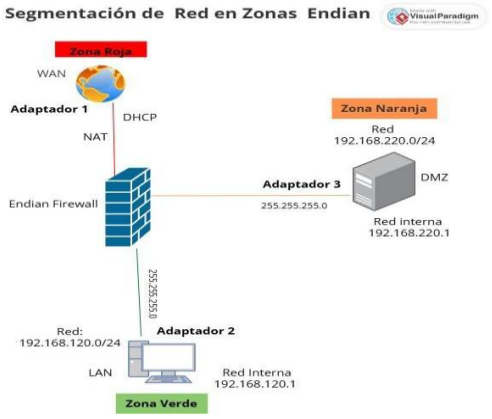
Zona Roja (WAN): acceso a Internet mediante DHCP y NAT.

Zona Verde (LAN): 192.168.120.0/24 – Clientes internos.

Zona Naranja (DMZ): 192.168.220.0/24 – Servidor Web.

El Endian Firewall actuó como núcleo de seguridad filtrando y controlando el tráfico entre cada zona.

figura 1: Esquema de segmentación de red con zonas Endian Firewall

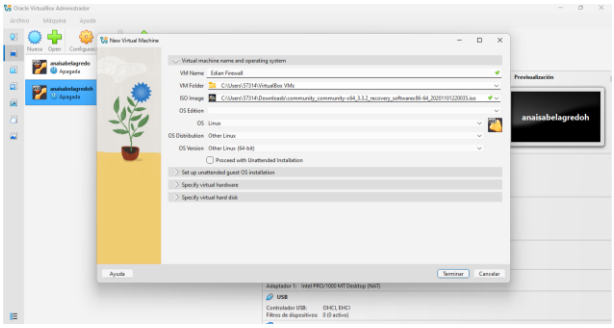


Fuente: Individual Autoría Ana Isabel Agredo

3. Temática 1: Configuración de la instancia para GNU/Linux Endian en VirtualBox (tarjetas de red) e instalación efectiva del mismo.

La implementación de Endian Firewall en un entorno virtualizado requiere una configuración precisa de sus interfaces, zonas y parámetros de red para garantizar un funcionamiento estable y seguro. Este proceso incluye la instalación del sistema, la definición de las zonas de seguridad, la asignación de direccionamiento y la verificación de conectividad entre los distintos segmentos, a lo largo del desarrollo se establecen las bases operativas que permiten asegurar, controlar y monitorear el tráfico dentro de la infraestructura.

Figura 2 Implementación de la imagen ISO de Endian Firewall

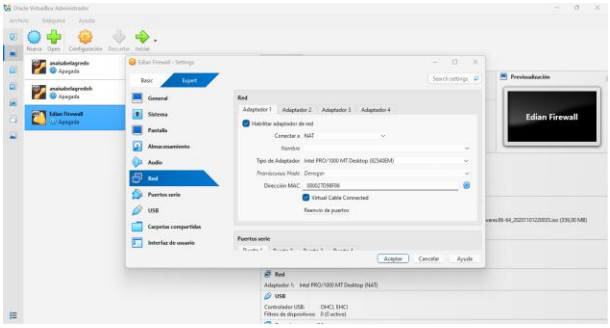


Fuente: Autoría individual Ana Isabel Agredo

La preparación inicial del sistema se realizó mediante la obtención y montaje de la imagen ISO de Endian Firewall. Tras descargar el archivo desde su repositorio oficial, la ISO se incorporó a VirtualBox para crear la máquina virtual correspondiente, permitiendo ejecutar el instalador de Endian dentro del entorno virtualizado, habilitando el despliegue del firewall y dando inicio al proceso de configuración del sistema.

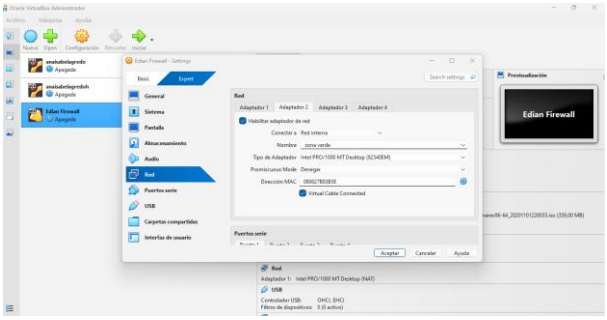
3.1. Configuración de Adaptadores de Red para Zonas Endian

Figura 3 Asignación de Red para el Adaptador 1 (NAT)



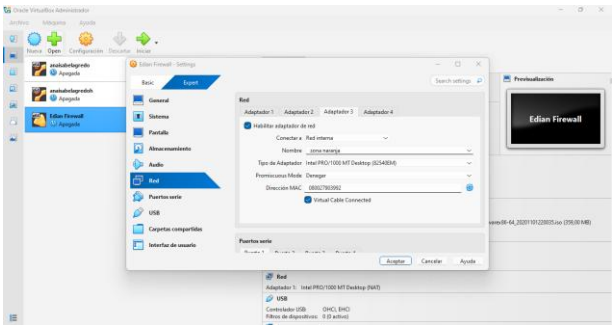
Fuente: Autoría individual Ana Isabel Agredo

Figura 4 Asignación de Red del Adaptador 2 – Zona Verde (Red Interna)



Fuente: Autoría individual Ana Isabel Agredo

Figura 5 Asignación de Red del Adaptador 3 – Zona Naranja (Red Interna – DMZ

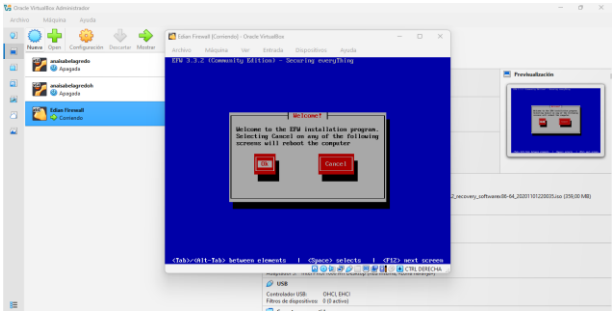


Fuente: Autoría individual Ana Isabel Agredo

La configuración de los tres adaptadores en VirtualBox define la segmentación base de Endian Firewall. El Adaptador 1 en modo NAT proporciona conectividad WAN para instalación y acceso externo. El Adaptador 2 como Red Interna establece la Zona Verde destinada a la LAN segura. El Adaptador 3 también en Red Interna conforma la Zona Naranja o DMZ para servicios expuestos bajo un entorno aislado. Esta estructura garantiza un modelo de segmentación claro y un flujo de tráfico controlado entre los distintos segmentos.

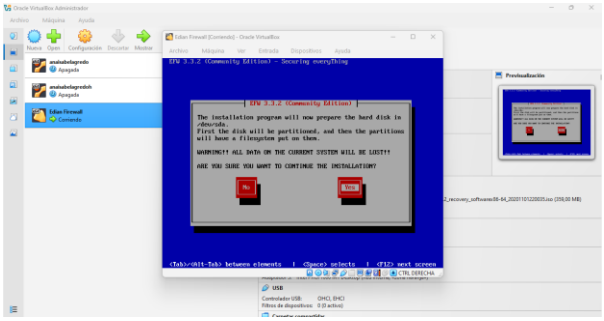
3.2 Proceso de Instalación Inicial de Endian Firewall

Figura 6 Pantalla de Bienvenida del Proceso de Instalación



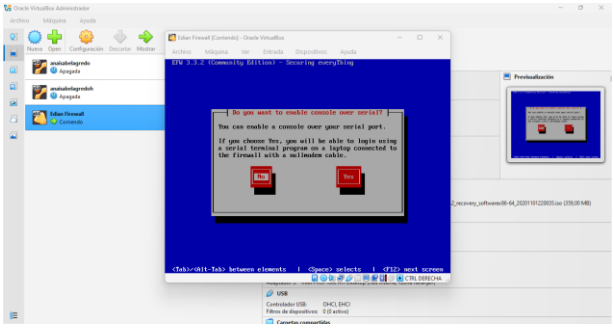
Fuente: Autoría individual Ana Isabel Agredo

Figura 7 Preparación del Disco para la Instalación



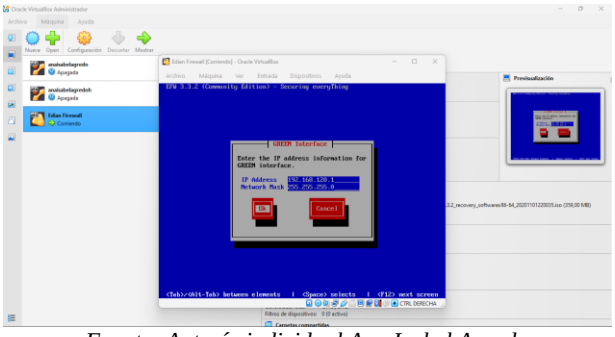
Fuente: Autoría individual Ana Isabel Agredo

Figura 8 Habilitación de Consola por Puerto Serial



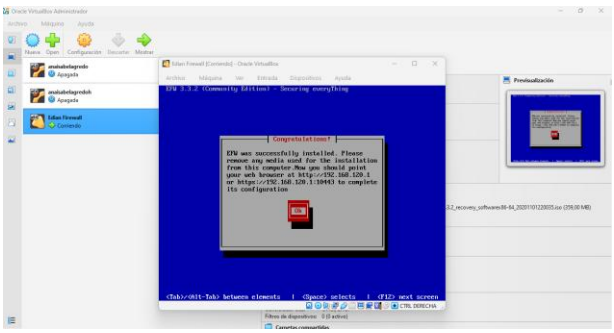
Fuente: Autoría individual Ana Isabel Agredo

Figura 9 Configuración de la Interfaz GREEN (LAN)



Fuente: Autoría individual Ana Isabel Agredo

Figura 10 Finalización de la Instalación del Sistema

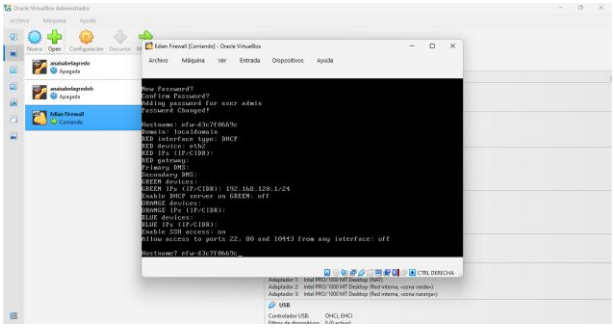


Fuente: Autoría individual Ana Isabel Agredo

Describe la instalación básica de Endian Firewall desde el instalador, la pantalla de bienvenida confirma el inicio del proceso, el instalador procede a preparar el disco (/dev/sda) indicando que se formateará para crear las particiones del sistema, lo cual se autoriza aceptando la advertencia de pérdida de datos, también se ofrece habilitar una consola serial, opción que se descarta para continuar la instalación convencional, posteriormente se configura la interfaz GREEN asignando su dirección IP y la máscara de red para el segmento LAN. Completado la copia e instalación del sistema, se extrae el medio y se continúa con la configuración inicial a través de la interfaz web administrativa.

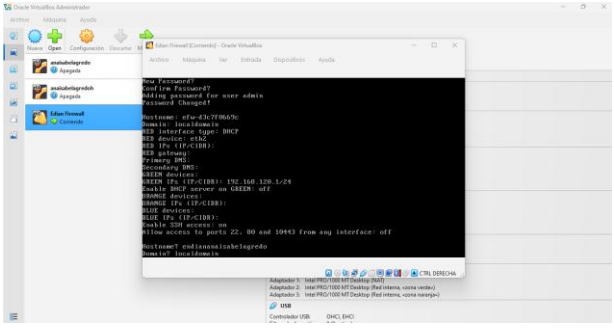
3.3 Configuración Inicial del Sistema y Definición de Zonas de Red

Figura 11 Acceso al Asistente de Configuración de Red



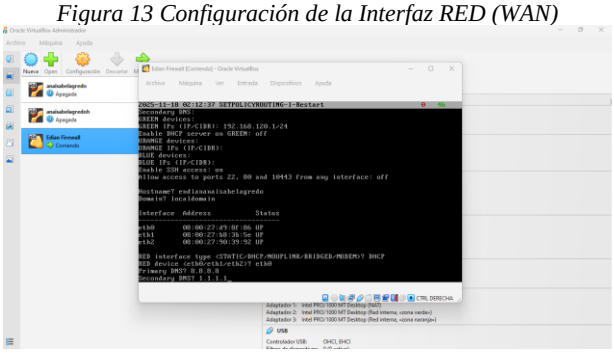
Fuente: Autoría individual Ana Isabel Agredo

Figura 12 Configuración del Hostname y Dominio



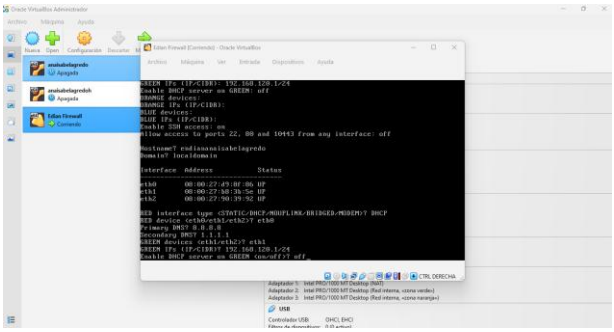
Fuente: Autoría individual Ana Isabel Agredo

Figura 13 Configuración de la Interfaz RED (WAN)



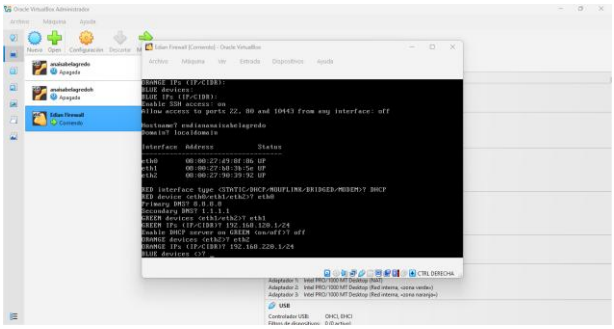
Fuente: Autoría individual Ana Isabel Agredo

Figura 14 Configuración de la Interfaz GREEN (LAN)



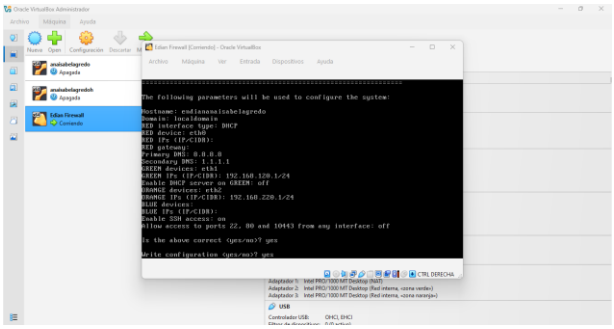
Fuente: Autoría individual Ana Isabel Agredo

Figura 15 Configuración de la Interfaz ORANGE (DMZ)



Fuente: Autoría individual Ana Isabel Agredo

Figura 16 Ajustes de Acceso y Confirmación de la Configuración

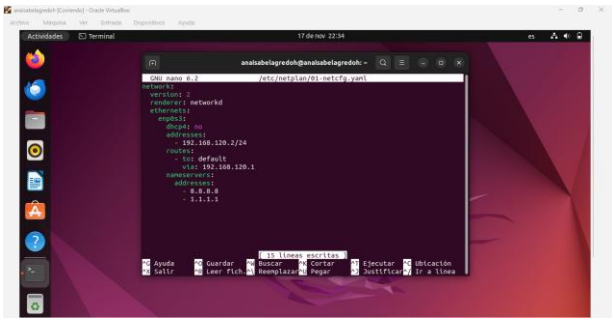


Fuente: Autoría individual Ana Isabel Agredo

El asistente de configuración solicita crear una contraseña administrativa segura y definir los parámetros básicos de identificación del sistema, incluyendo el hostname y el dominio. Posteriormente se establecen las tres zonas principales: la interfaz RED se configuró como WAN usando DHCP y DNS públicos, la interfaz GREEN se definió como LAN interna con direccionamiento estático y sin DHCP para un control total del segmento y la interfaz ORANGE se creó como DMZ con una red independiente para servicios expuestos. Se habilitó el acceso SSH para administración remota y se confirmaron los ajustes dejando el firewall operativo con su estructura de red adecuadamente segmentada.

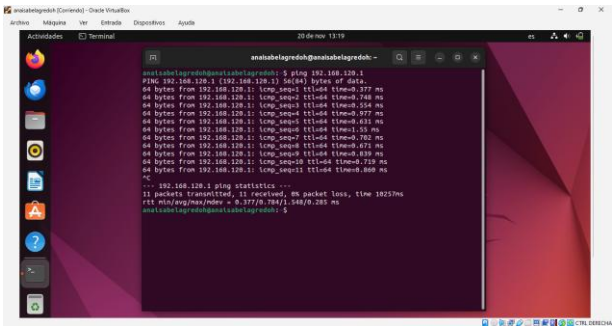
3.4 Configuración y Validación de la Conectividad en Ubuntu Desktop (Zona Verde)

Figura 17 Configuración de IP Estática en Ubuntu Desktop (Zona Verde)



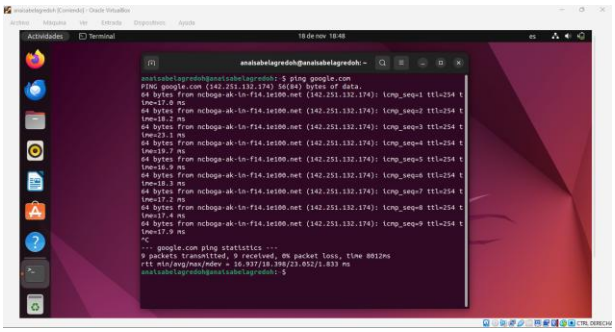
Fuente: Autoría individual Ana Isabel Agredo

Figura 18 Verificación de Conectividad



Fuente: Autoría individual Ana Isabel Agredo

Figura 19 Verificación de Conectividad Externa

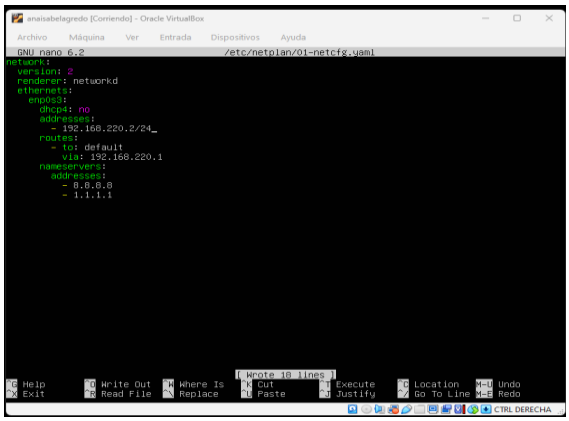


Fuente: Autoría individual Ana Isabel Agredo

Se configuró una IP estática en Ubuntu Desktop dentro de la Zona Verde para establecer un direccionamiento fijo dentro del segmento LAN, luego se validó la comunicación interna mediante pruebas de conectividad hacia la interfaz GREEN de Endian Firewall confirmando la correcta operación dentro de la red local. Se verificó el acceso externo mediante un ping a google.com, garantizando la salida funcional hacia la red WAN a través del firewall y confirmando el adecuado funcionamiento del entorno en la Zona Verde.

3.5 Configuración y Validación de la Conectividad en Ubuntu Server (Zona Naranja – DMZ)

Figura 20 Configuración de IP Estática en Ubuntu Server (Zona Naranja)

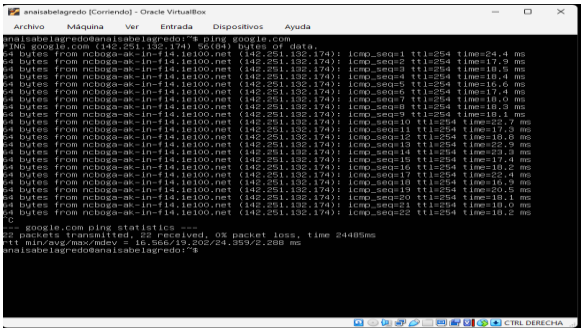


Fuente: Autoría individual Ana Isabel Agredo

Figura 21 Verificación de Conectividad

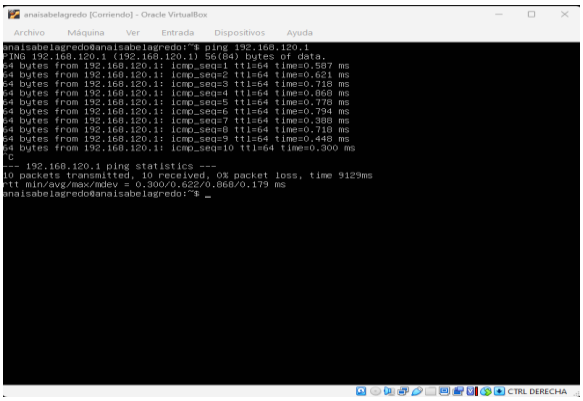
Fuente: Autoría individual Ana Isabel Agredo

Figura 22 Comprobación de Conectividad Externa



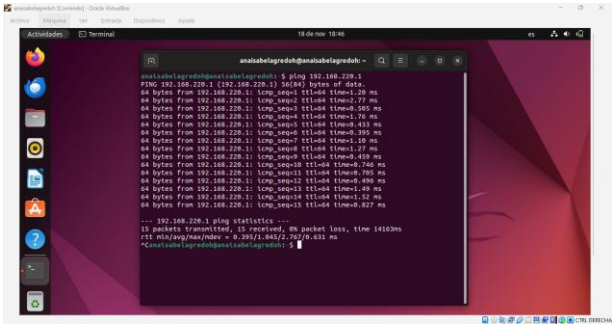
Fuente: Autoría individual Ana Isabel Agredo

Figura 23 Verificación de Conectividad con la Zona Verde



Fuente: Autoría individual Ana Isabel Agredo

Figura 24 Verificación de Conectividad con la Zona Naranja

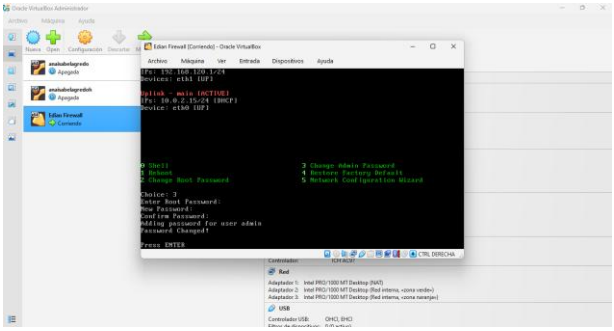


Fuente: Autoría individual Ana Isabel Agredo

Se configuró una IP estática en Ubuntu Server para integrarlo correctamente en la Zona Naranja (DMZ) garantizando un direccionamiento estable para servicios expuestos o segmentados. Luego de ajustar la configuración de red, se validó la comunicación interna con Endian Firewall mediante pruebas de ping confirmando la operatividad dentro del segmento DMZ. Posteriormente se verificó el acceso externo mediante pruebas de conectividad hacia Internet asegurando la salida adecuada a través de la zona RED. Se realizaron pruebas cruzadas entre la Zona Naranja y la Zona Verde validando el enrutamiento interno y confirmando que Endian Firewall gestiona correctamente el tráfico entre ambas zonas manteniendo la segmentación y las políticas definidas.

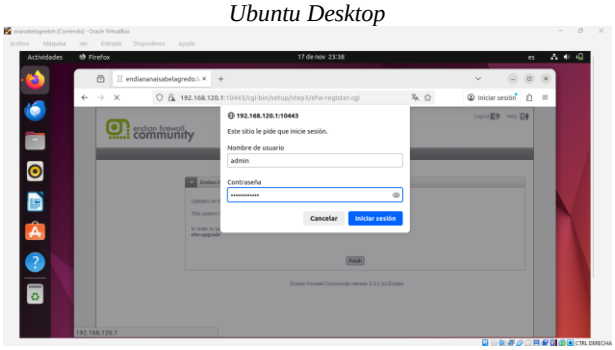
3. 6 Gestión de Acceso y Verificación del Estado del Sistema en Endian Firewall

Figura 25 Cambio de la Contraseña del Administrador en Endian Firewall



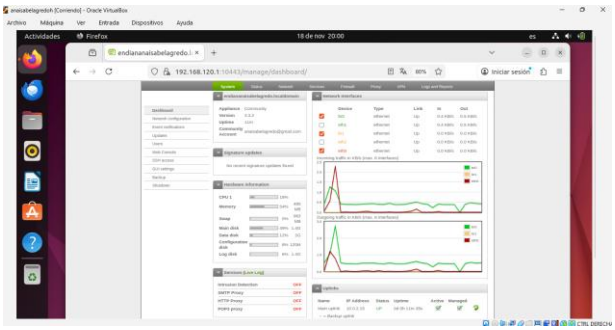
Fuente: Autoría individual Ana Isabel Agredo

Figura 26 Acceso a la Interfaz Web de Endian Firewall desde Ubuntu Desktop



Fuente: Autoría individual Ana Isabel Agredo

Figura 27 Acceso a la Consola de Gestión del Sistema Endian Firewall



Fuente: Autoría individual Ana Isabel Agredo

Se reforzó la seguridad del sistema mediante el cambio de la contraseña del usuario administrador desde la consola local, posteriormente desde Ubuntu Desktop se accedió a la interfaz web utilizando la dirección de gestión en la Zona Verde, autenticando el ingreso con las credenciales configuradas. Dentro del panel principal de Endian Firewall se verificó el estado general del sistema y el funcionamiento de las interfaces eth0, eth1 y eth2, confirmando su correcta asignación a las zonas WAN, LAN y DMZ, así como el monitoreo del tráfico entrante validando la operación estable de la infraestructura implementada.

4. Temática 2

En el ámbito de seguridad de redes, las redes NAT esto se coloca como un mecanismo fundamental para regular el flujo de tráfico entre dominios de varios niveles de confianza. la correcta implementación para poder establecer conexiones controladas de firewall en Endian, ya que lo que se garantiza es que tanto los equipos de red interna LAN como el servidor o el escritorio que están ubicados en la zona (DMZ) es que puedan dar o tener una conexión de (WAN/INTERNET) de una forma muy complementaria segura, teniendo a la misma vez una conexión segura.

4.1. Arquitectura de Red

Tabla 1: Arquitectura de Red

zona	interfaz VirtualBox	Tipo De Red VirtualBox	Rango IP
VERDE(LAN)	adaptador 1	Red Interna	192.168.120.2
Naranja(DMZ)	adaptador 2	Red interna	192.168.120.1
Roja(WAN)	adaptador 3	Res NAT	192.168.120.0/24

fuente: autoría pedro sarria

4.2. Configuración De Práctica de SNAT para el Acceso a internet desde LAN

El objetivo de la temática es permitir que la zona verde (LAN) acceda a internet. con las direcciones de IP privadas no son enrutables para dar conexión, para esto es necesario agregar una regla NAT dentro del endian de la zona (VERDE).

4.3. Procedimiento en la interfaz de web Endian

se accede en el menú de firewall para poder dar conexión a internet desde LAN para esto se sigue los siguientes pasos.

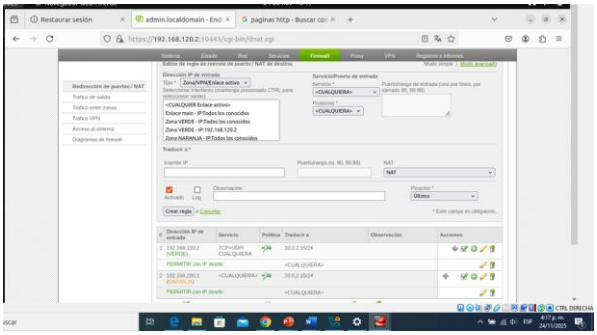
1. se hace al menú de firewall
2. dentro del firewall se da la opción port forwarding / NAT
3. se selecciona la pestaña Source NAT
4. hacer clic en add a new source NAT rule se coloca para crear una nueva regla de SNAT
5. después de esto se configuran los parámetros de regla:

6. Se selecciona la ZONA VERDE como origen de tráfico y como destino se establece la ZONA ROJA y por defecto se deja en any para aplicar todo el tráfico.

Figura 28: Configuración del firewall

fuente: Autoría pedro sarria

Figura 29: creación de regla source nat

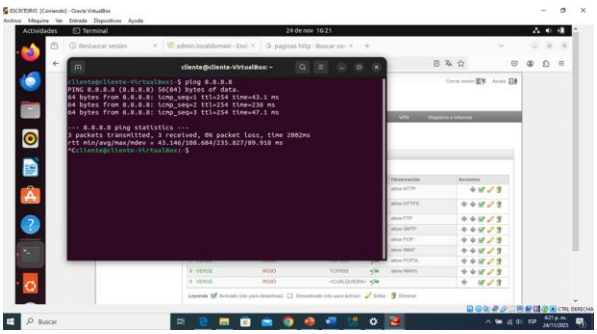


fuente Autoría pedro sarria

4.4. verificación de funcionamiento de conexión y salida del equipo verde

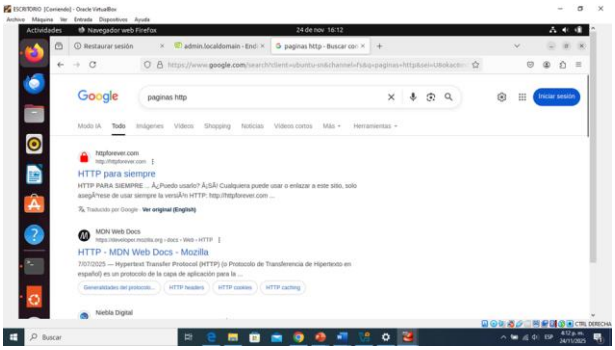
Desde la consola de la máquina se consulta la dirección de la IP de la máquina para demostrar se encuentra dentro de la red verde y se realizan pruebas de conexión con PING y navegación de internet.

Figura 30: dirección IP máquina PING 8.8.8.8



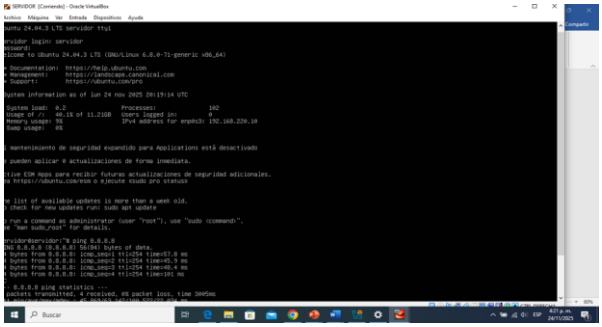
fuente: Autoría pedro sarria

Figura 31: Navegador Web



fuente: Autoría pedro sarria

Figura 32: verificación conexión a internet



fuente: Autoría pedro sarria

La correcta configuración de NAT y de reenvío de puertos en Endian es importante, para establecer un acceso seguro y controlado a los equipos de red interna y los servidores en el DMZ, y comprender la arquitectura de la zona de endian Firewall.

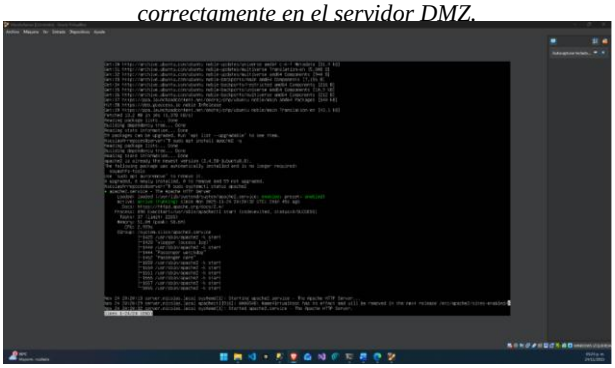
5. Temática 3: Permitir servicios de la Zona DMZ para la Red

La Temática 3 se centró en la configuración de los servicios esenciales del servidor ubicado en la Zona Naranja (DMZ), el cual opera bajo Ubuntu Server. El propósito principal fue habilitar los servicios HTTP y FTP para permitir el consumo desde otras zonas de la red, garantizando a la vez la restricción del protocolo ICMP con el fin de mejorar la seguridad perimetral del servidor. Todas las acciones fueron realizadas mediante consola, y se documentó la ejecución de cada comando con su respectiva fecha y hora.

5.1. Habilitación del servicio HTTP (Puerto 80)

Para permitir el acceso mediante HTTP desde otras zonas hacia el servidor en la DMZ, se instaló y configuró el servicio Apache2. La instalación se efectuó desde la terminal mediante los comando **sudo apt install apache2 y sudo systemctl status apache2.** La activación del servicio se verificó observando el estado “active (running)”, lo cual confirmó su correcto funcionamiento.

Figura 33: Estado del servicio Apache2 inicializado correctamente en el servidor DMZ.



Fuente: Autoría individual Nicolás Arregoces.

A continuación, se procedió a habilitar el puerto 80 en el firewall UFW con **sudo ufw allow 80/tcp.** Con ello se garantizó que cualquier cliente de la red pudiera acceder al sitio web alojado en la DMZ.

5.2. Habilitación del servicio HTTP (Puerto 80)

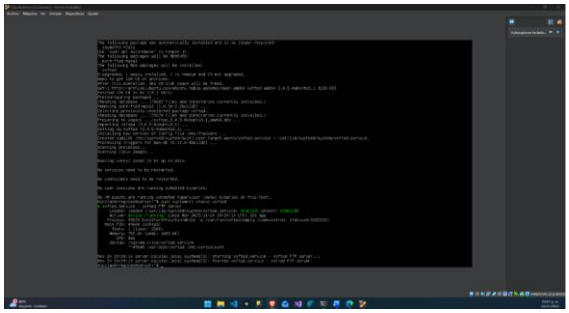
Para permitir transferencia de archivos desde clientes internos y externos autorizados, se instaló el servidor FTP vsftpd mediante:

sudo apt install vsftpd

sudo systemctl status vsftpd

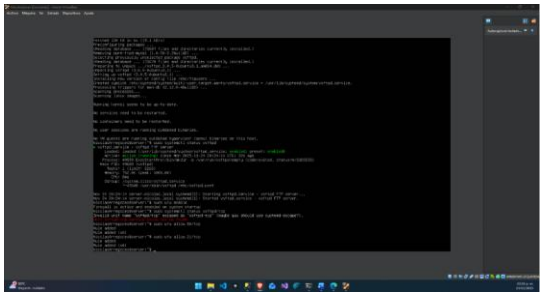
Tras verificar que el servicio se encontraba en ejecución, se habilitó el puerto correspondiente: **sudo ufw allow 21/tcp**

Figura 34: Servicio vsFTPd habilitado y operativo en el servidor DMZ.



Fuente: Autoría individual Nicolás Arregoces.

Figura 35: Configuración del firewall (UFW), HTTP y FTP habilitado.



Fuente: Autoría individual Nicolás Arregoces.

Estas configuraciones permiten el acceso remoto controlado al servicio FTP ubicado en la DMZ.

5.3. Restricción del protocolo ICMP (Ping)

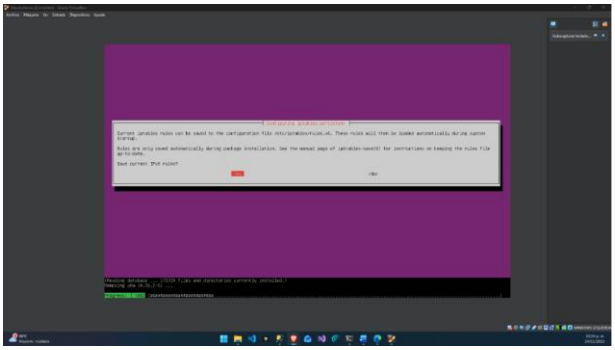
Como medida de seguridad perimetral, se denegó el protocolo ICMP tipo *echo-request* (puerto lógico 8) y tipo 30, evitando que el servidor responderá a solicitudes de ping. La configuración se aplicó con las siguientes reglas de iptables:

sudo iptables -A INPUT -p icmp --icmp-type echo-request -j DROP

sudo iptables -A INPUT -p icmp --icmp-type 30 -j DROP

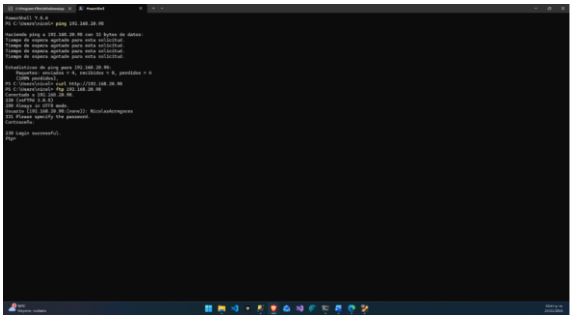
Posteriormente, las reglas persistieron con **sudo netfilter-persistent save.** Para comprobar su efectividad, desde una máquina cliente se ejecutó **ping 192.168.20.98.** El resultado esperado fue la ausencia total de respuesta.

Figura 36: Reglas iptables aplicadas



Fuente: Autoría individual Nicolás Arregoces.

Figura 37: Intento fallido de ping hacia la DMZ tras aplicar la denegación de ICMP.

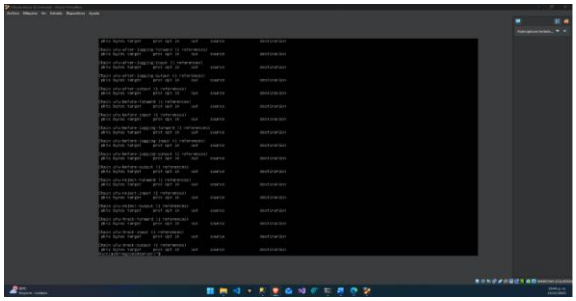


Fuente: Autoría individual Nicolás Arregoces.

5.4. Verificación de tráfico y reglas de firewall

Una vez configurados los servicios y restricciones, se verificó el estado de las reglas aplicadas en UFW mediante **sudo ufw status verbose**. Y la visualización completa de las reglas activas en iptables **sudo iptables -L -n -v**. La salida mostró los puertos 80 y 21 permitidos correctamente, así como la regla de bloqueo de ICMP activa.

Figura 38: Listado de reglas activas en UFW mostrando acceso HTTP y FTP habilitado.



Fuente: Autoría individual Nicolás Arregoces.

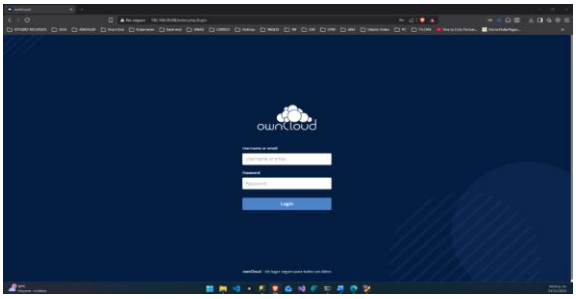
5.5. Pruebas funcionales de acceso

Se llevaron a cabo pruebas desde las diferentes zonas:

5.5.1 Acceso HTTP al servidor DMZ

Desde un cliente en la LAN, se realizó: **curl http://192.168.20.98.** El servidor respondió con la página por defecto de Apache.

Figura 39: Acceso exitoso al servicio HTTP alojado en la DMZ.

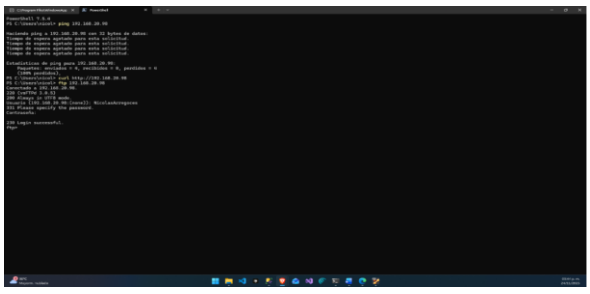


Fuente: Autoría individual Nicolás Arregoces.

5.5.2. Acceso FTP al servidor DMZ

ftp 192.168.20.98 El servidor vsFTPd devolvió el mensaje de bienvenida.

Figura 40: Conexión exitosa al servicio FTP ubicado en la DMZ.



Fuente: Autoría individual Nicolás Arregoces.

5.5.3. ICMP denegado

Como resultado de las reglas configuradas, la prueba **ping 192.168.20.98** arrojó la ausencia de respuesta, evidenciando correctamente la restricción.

6.Temática 4: Reglas de acceso para permitir o denegar el tráfico

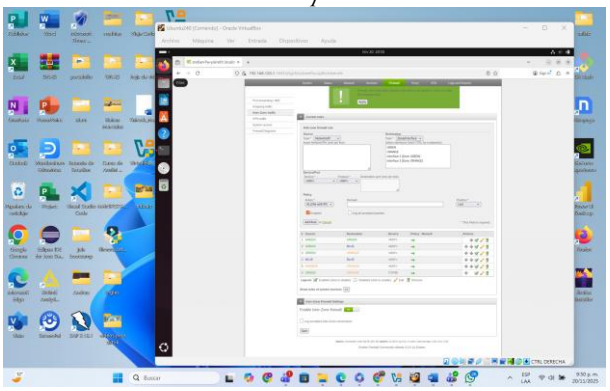
La Temática 4 se enfocó en la creación de políticas de acceso entre las diferentes zonas del Endian Firewall —Zona Verde (LAN), Zona Naranja (DMZ) y Zona Roja (WAN)— con el fin de controlar el flujo de datos y garantizar la seguridad perimetral de la infraestructura. Estas políticas fueron implementadas desde el módulo Firewall → Inter-Zone Traffic, definiendo qué tipo de comunicación se permite o se deniega entre los segmentos de red.

6.1. Comunicación entre Zona Verde y Zona Naranja

Se configuraron reglas específicas para permitir la comunicación desde la LAN hacia la DMZ utilizando los protocolos HTTP (puerto 80) y FTP (puerto 21). Estas reglas habilitan a los clientes de la Zona Verde (192.168.120.0/24) el acceso al servidor ubicado en la DMZ (192.168.220.0/24), necesario para consultar sitios web internos y transferir archivos hacia el servicio FTP del servidor.

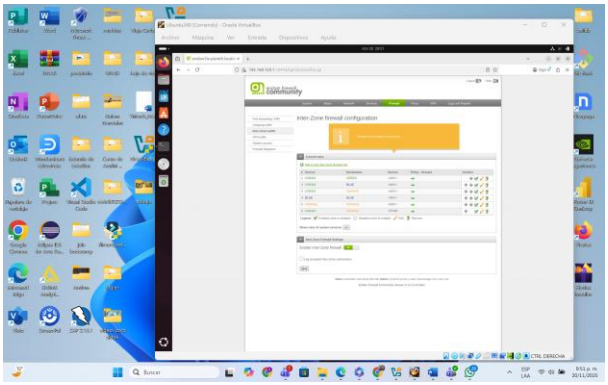
Regla creada:
Origen: GREEN
Destino: ORANGE
Servicio: HTTP, FTP
Acción: Allow.

figura 41: Regla de acceso GREEN→ORANGE permitiendo HTTP y FTP.



Fuente: Autoría individual Yisireth murcia

figura 42: Visualización de las reglas creadas



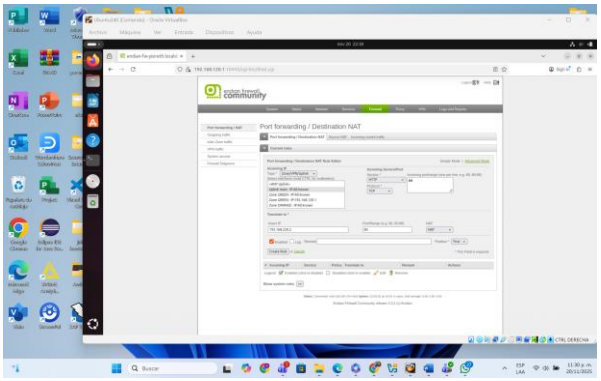
Fuente:Autoria individual Yisireth murcia

6.2 Comunicación entre Zona Roja (Internet) y la DMZ

Debido a que los servidores ubicados en la DMZ deben ser accesibles desde Internet, se habilitaron reglas de acceso desde la WAN hacia la Zona Naranja. Estas reglas permiten el ingreso de solicitudes HTTP provenientes de Internet hacia los servicios web publicados en la DMZ.

Firewall → Port Forwarding / NAT y luego en
Add a new port forwarding / Destination NAT rule
Crear regla RED → ORANGE (HTTP)
Configura así:
Incoming interface: Uplink main – IP: All known que representa a ROJO
Service: HTTP (TCP 80)
Destination: 192.168.220.2 esta es la ip estatica del server
Port/Range: 80
NAT: NAT
Enabled: Sí.
Esta configuración es fundamental para que el servidor web pueda ser accedido desde el exterior sin comprometer la seguridad de la LAN.

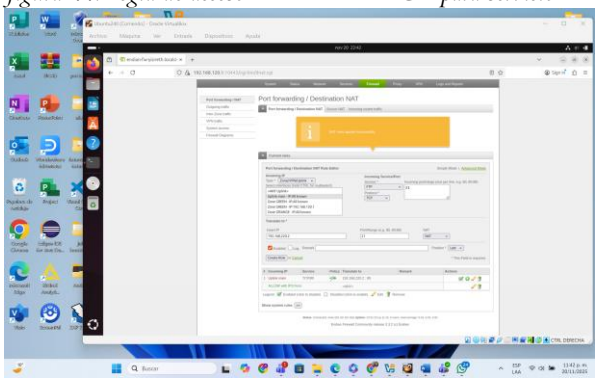
figura 43 : Regla de acceso RED→ORANGE para servicio HTTP



Fuente: Autoria individual yisireth murcia

continuamos creando la regla de FTP (21) similar a http

figura 44:Regla de acceso RED→ORANGE para servicio FTP



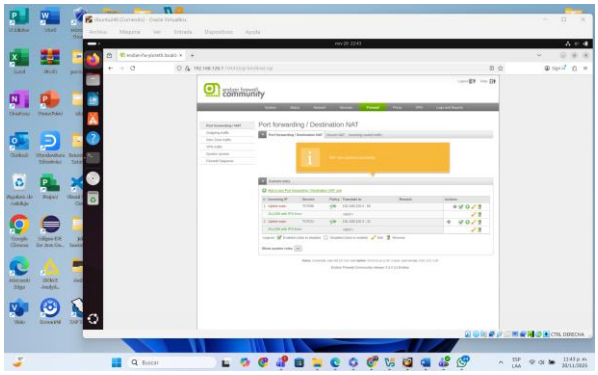
Fuente: Autoria individual Yisireth Murcia

6.3 Verificación del Tráfico Inter-Zona

Una vez implementadas las reglas, se verificó su creación en:

Firewall → Inter-Zone Traffic
Se confirmó que:
Las reglas se encuentran activas.
El orden de procesamiento es coherente con las políticas de seguridad.
No existe conflicto entre reglas de denegación y permisos establecidos.
La verificación se complementó con pruebas de conectividad y accesibilidad mediante navegación web y conexión FTP.

figura 45:Visualizacion de las dos reglas creadas htpp y ftp



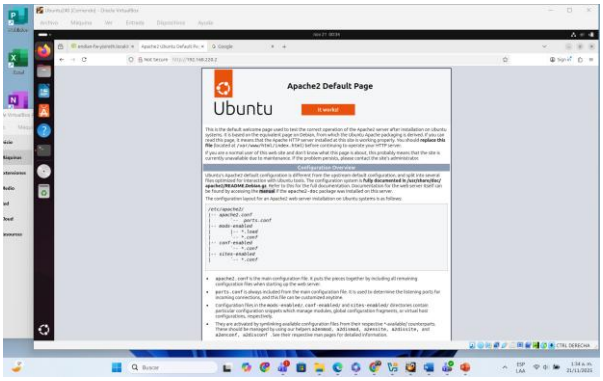
Fuente:Autoría individual Yisireth murcia

6.4 Pruebas Funcionales de Acceso entre Zonas

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

Para comprobar la correcta aplicación de las reglas de acceso entre la Zona Verde (LAN) y la Zona Naranja (DMZ), se realizó una prueba de conectividad mediante el protocolo HTTP. Desde un equipo cliente ubicado en la red LAN (192.168.120.1/24), se abrió un navegador web e ingresa la dirección IP del servidor web ubicado en la DMZ (192.168.220.2).

figura 46: Acceso HTTP desde la LAN al servidor Apache en la DMZ

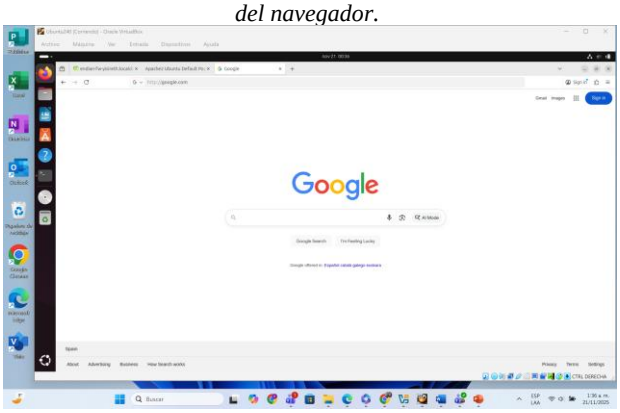


Fuente:Autoría individual Yisireth murcia

6.4.2 Del servicio HTTP desde la LAN hacia la WAN.

Esta prueba valida que los equipos ubicados en la Zona Verde (LAN) pueden acceder correctamente a servicios HTTP disponibles en la Zona Roja (WAN), es decir, a sitios web externos en Internet. Para ello, desde una estación de trabajo ubicada en la red LAN (192.168.120.0/24), se abrió un navegador web y se ingresó la dirección de un sitio público, como http://www.google.com. La carga exitosa del sitio confirma que la regla configurada en el firewall permite el tráfico HTTP desde la LAN hacia la WAN.

figura 47:Acceso HTTP desde la LAN hacia la WAN a través del navegador.

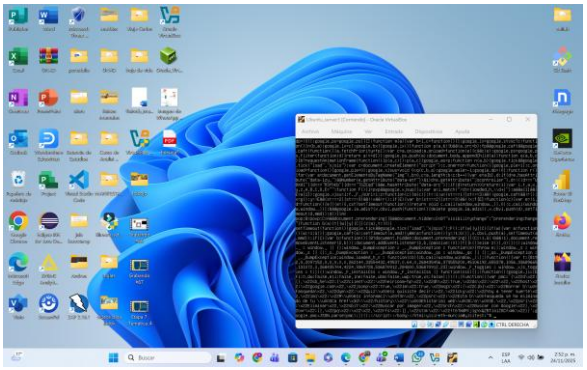


Fuente:Autoría individual Yisireth murcia

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

Para comprobar que los servidores ubicados en la Zona Naranja (DMZ) pueden establecer conexiones HTTP hacia Internet, se realizó una prueba de navegación directamente desde el servidor web alojado en esta zona (192.168.220.10). Desde la terminal del servidor, se ejecuta el comando: curl http://www.google.com
Esta prueba demuestra que la política configurada en Firewall → Inter-Zone Traffic permite la salida del tráfico HTTP desde la DMZ, garantizando que el servidor pueda acceder a repositorios externos, recursos en línea y actualizaciones.

figura 48: Respuesta HTML obtenida desde la DMZ mediante el comando curl hacia la WAN.



Fuente:Autoría individual Yesireth murcia

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

La prueba se realizó desde un equipo externo simulado en la Zona Roja, ingresando en un navegador web la dirección IP pública asignada a la interfaz Red del Endian Firewall. Al cargar la página web, se confirmó que la solicitud HTTP fue enviada correctamente a través de Internet, recibida por el firewall y reenviada al servidor ubicado en la DMZ. El servidor respondió devolviendo la página alojada en Apache, demostrando que la regla de publicación y el proceso de NAT funcionan adecuadamente.

figura 49:se muestra la página Apache cargada desde la WAN, evidenciando el acceso HTTP hacia la DMZ

Fuente:Autoría individual Yisireth murcia

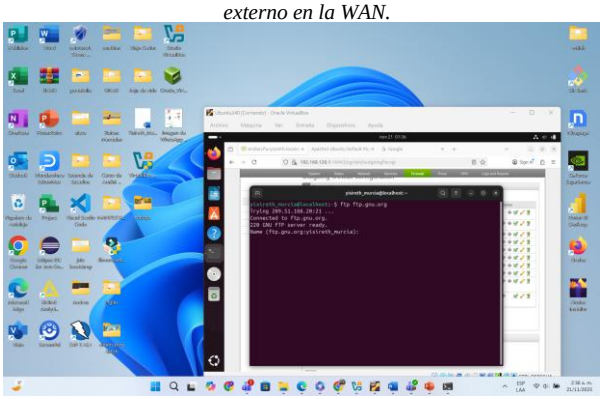
6.4.5 El ingreso del servicio FTP desde la LAN hacia la WAN.

Para validar la salida del protocolo FTP desde la Zona Verde (LAN) hacia la Zona Roja (WAN), se configuró una regla de tráfico inter-zona que permite el acceso al puerto 21 desde la red 192.168.120.0/24 hacia Internet. Posteriormente, desde un equipo en la LAN se ejecutó el comando ftp ftp.gnu.org, intentando establecer conexión con un servidor FTP público.

La conexión fue recibida correctamente por el servidor remoto, mostrando el mensaje “220 GNU FTP server ready”, lo que confirma que el firewall permite el tráfico FTP hacia la WAN y que el mecanismo de traducción de direcciones (NAT) funciona adecuadamente para este protocolo. Esta prueba

demuestra que la LAN tiene capacidad para comunicarse con servidores FTP externos sin restricciones.

Figura 50:Prueba de conexión FTP desde la LAN hacia un servidor externo en la WAN.



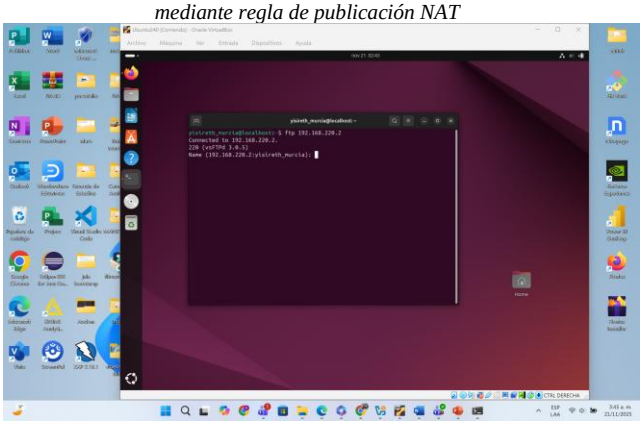
Fuente:Autoría individual Yisireth murcia

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

Para habilitar el acceso al servicio FTP del servidor ubicado en la Zona Naranja (DMZ) desde la Zona Roja (WAN), fue necesario configurar previamente una regla de publicación mediante Port Forwarding / NAT. En esta regla se redirigió el tráfico entrante al puerto 21 (FTP) desde la interfaz WAN hacia la dirección interna del servidor DMZ (ftp 192.168.220.2).

La conexión fue recibida correctamente por el servidor vsFTPd, que responde con el mensaje de bienvenida “220 (vsFTPd 3.0.5)”. Esto confirma que el firewall permite las conexiones FTP procedentes de la WAN y que el mecanismo de redireccionamiento hacia la DMZ está funcionando adecuadamente.

figura 51:Conexión FTP desde la WAN hacia el servidor DMZ mediante regla de publicación NAT



Fuente:Autoría individual Yisireth murcia

6. Temática 5: Implementar un Proxy HTTP (No transparente) con políticas de autenticación para navegación en Internet.

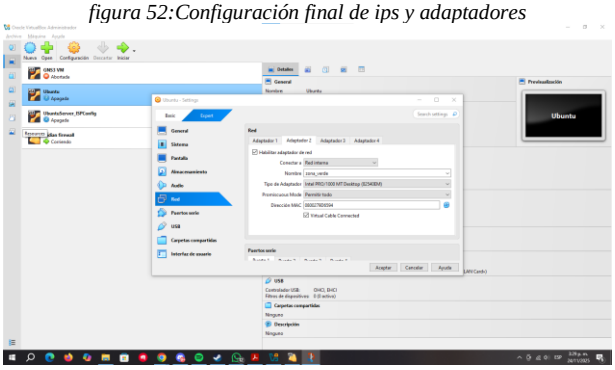
Para esta temática se solicitó realizar 3 distintas actividades las cuales fueron crear un perfil y establecer una lista negra bloqueando 3 sitios en específico crear un usuario y asociarlo a un grupo y establecer una política de acceso que se vincule con las anteriores reglas de bloqueo y por último realizar una prueba de conexión mediante un navegador a estas 3 páginas o sitios web.

7.1. Configuración del desktop

una vez terminado de configurar en su totalidad endian booteamos nuestro desktop preferido en mi caso ubuntu desktop y empezamos a configurar las ultimas cosas que hacen falta las cuales son: la ip, la lista de usuarios y grupo, las restricciones y la contraseña.

Pero primero tenemos que cambiar los adaptadores del ubuntu desktop desde virtual box para asegurarnos de usar el diagrama de red y que use de manera obligatoria el endian

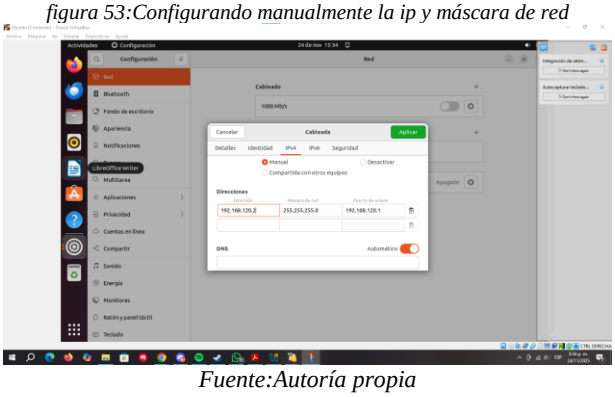
figura 52:Configuración final de ips y adaptadores



Fuente:Autoría propia

una vez hecho esto podemos empezar a configurar la ip que usaremos para nuestro desktop

figura 53:Configurando manualmente la ip y máscara de red

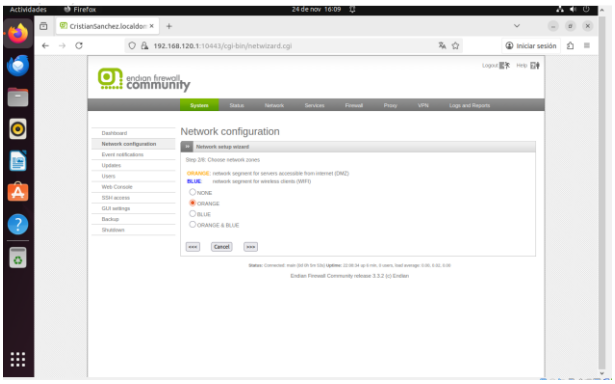


Fuente:Autoría propia

7.2. Configuración del proxy

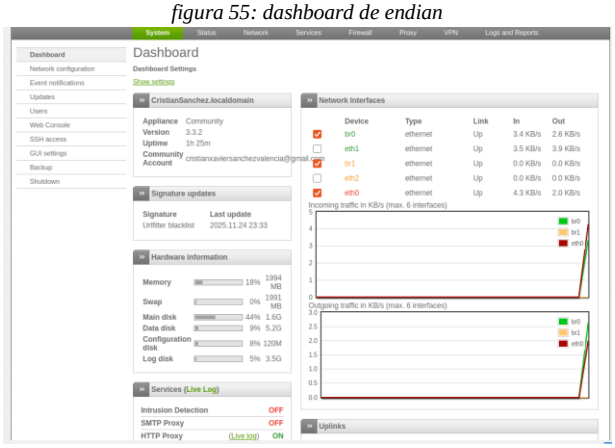
una vez configurada la ip de manera manual podemos empezara configurar los ultimos pasos necesarios y lo vamos a hacer desde endian mediante una ip que el mismo endian nos proporcionó para poder terminar de configurarlo desde un navegador web insertando la ip, en la siguiente imagen se observa los primeros pasos de la configuracion asi como se ve el dashboard de endian

figura 54:Configurando las distintas zonas



Fuente:Autoría propia

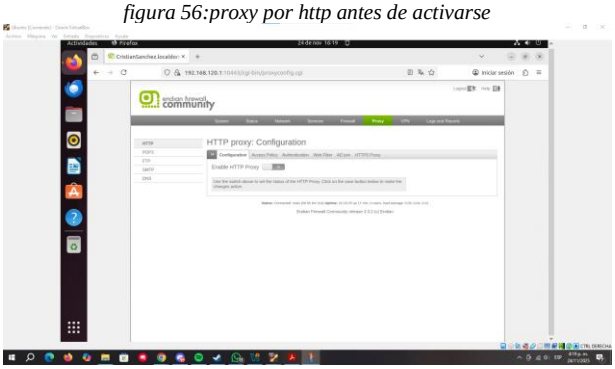
figura 55: dashboard de endian



Fuente:Autoría propia

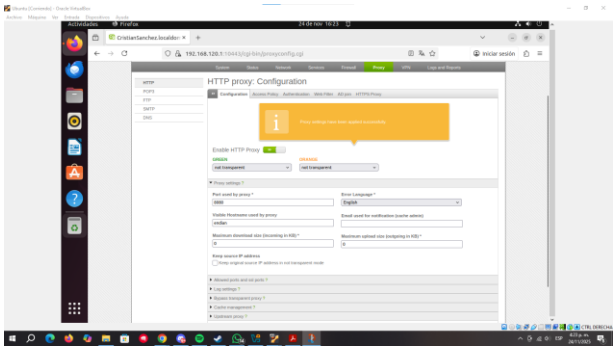
En la siguiente imagen se podrá observar cómo se habilita la opción de un proxy mediante http y desde ahí también podremos hacer que sean no transparentes entre otras configuraciones como puertos limite de descarga o subida etc..

figura 56:proxy por http antes de activarse



Fuente:Autoría propia

figura 57:proxy por http después de activarse con sus opciones

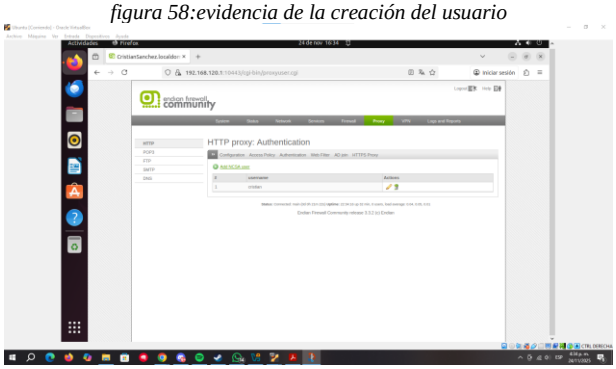


Fuente:Autoría propia

7.4. Creando usuarios

Empezamos a crear usuarios de prueba para esta actividad en este caso solo creamos 1 usuario con el nombre de cristian y su respectiva contraseña para que luego podamos usarlo en la sección de crear una blacklist y asociarlo al usuario/grupo

figura 58:evidencia de la creación del usuario

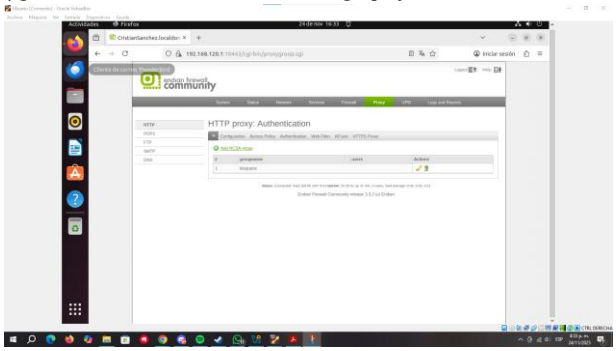


Fuente:Autoría propia

7.5. Creando grupos

Una vez creado un usuario que podamos asignar podemos empezar a crear un grupo de prueba el cual servirá para las pruebas de bloqueo de páginas

figura 59:Evidencia de la creación del grupo y asociación del usuario

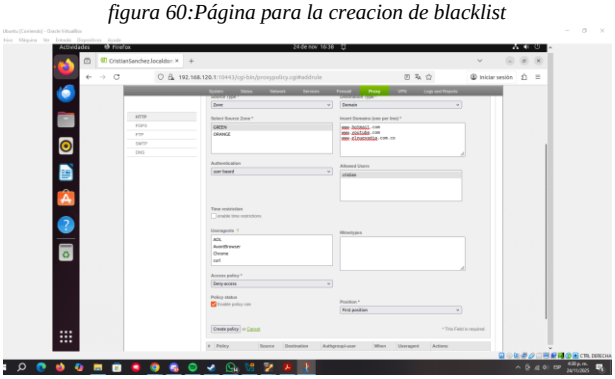


Fuente:Autoría propia

7.6. Creando la lista de bloqueo

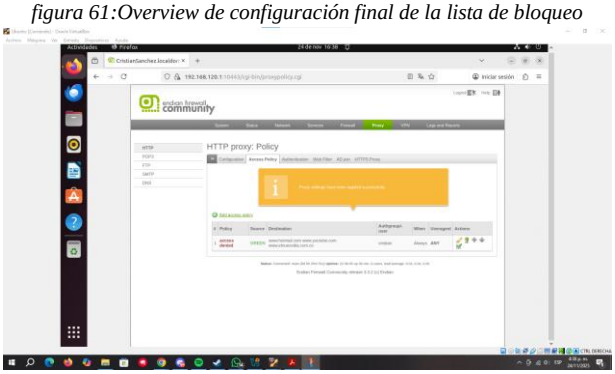
con todo lo anterior ya creado tendremos todo lo que necesitamos para poder empezar a crear la lista de bloqueo, esta parte fue la que personalmente me dio más problemas primero se observará unas imágenes de como lo estaba configurando inicialmente, pero esta configuración no satisfacía las necesidades para esta actividad

figura 60:Página para la creacion de blacklist



Fuente:Autoría propia

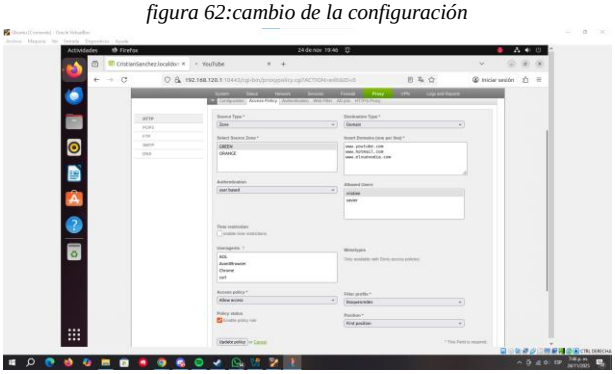
figura 61:Overview de configuración final de la lista de bloqueo



Fuente:Autoría propia

Como mencione antes esta configuración no me sirvio ya que al usarla me generaba problemas como que otras paginas no cargan tampoco a pesar de poner que solo las 3 paginas especificas fueran bloqueadas y lo solucione de la siguiente manera:

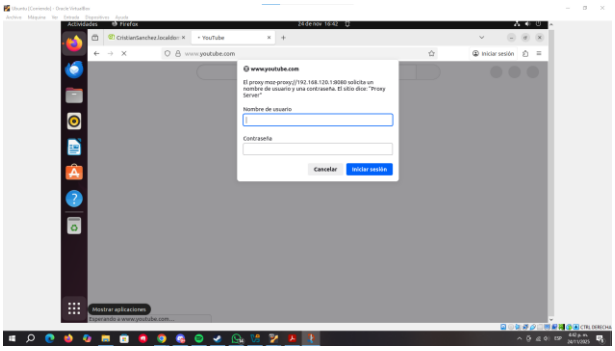
figura 62:cambio de la configuración



Fuente:Autoría propia

con esta configuración ahora si cumplía todos los requisitos necesarios para esta actividad por ende podríamos empezar a realizar las pruebas que darian los siguientes resultados:

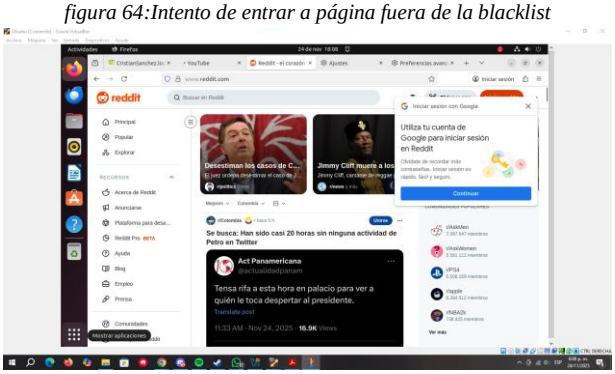
figura 63:Intento de entrar a página en blacklist



Fuente:Autoría propia

Como se observa la página pide usuario y contraseña y si ingresa con el usuario bloqueado no le dejara entrar a la pagina

figura 64:Intento de entrar a página fuera de la blacklist



Fuente:Autoría propia

y como se observa en esa última imagen se puede entrar a otras páginas que no estén bloqueadas para este ejemplo use la página llamada reddit

7. Conclusiones.

8. 1 Temática 1:

La implementación de GNU/Linux Endian en un entorno virtualizado permitió construir una arquitectura segmentada con las zonas Verde (LAN), Roja (WAN) y Naranja (DMZ). La configuración de los adaptadores en VirtualBox y el ajuste inicial del sistema aseguraron el aislamiento del tráfico y el control de cada segmento, la Zona Verde ofreció un entorno seguro interno, la Roja habilitó la salida hacia Internet y la Naranja permitió alojar servicios expuestos bajo condiciones controladas. El resultado fue una infraestructura funcional y coherente con los principios de seguridad perimetral.

conclusión temática 2:

Durante esta actividad, se adquirieron habilidades esenciales para manejar sistemas Linux de manera efectiva, abarcando desde la detección y solución de fallos de hardware y arranque, hasta el uso de comandos de diagnóstico clave como lspci y ldd. Esto permitió comprender cómo cada componente del sistema interactúa para garantizar estabilidad y rendimiento.

Al mismo tiempo, la práctica con Systemd fortaleció la capacidad de administrar servicios y procesos de manera ordenada y eficiente. La experiencia brindó una base sólida para enfrentar desafíos reales en entornos Linux, fomentando confianza y autonomía en la gestión de sistemas operativos modernos.

conclusión Temática 3:

La configuración realizada cumple satisfactoriamente con los requerimientos de la Temática 3. Se habilitaron correctamente los servicios HTTP (puerto 80) y FTP (puerto 21) en el servidor Ubuntu dentro de la zona DMZ, permitiendo que los equipos de la red accedan a estos servicios sin restricciones. Asimismo, se implementaron reglas de firewall para bloquear el protocolo ICMP, impidiendo respuestas a solicitudes de ping desde la red, lo cual refuerza la seguridad al evitar reconocimiento no autorizado del servidor. Las pruebas ejecutadas en consola demostraron que las reglas aplicadas funcionan adecuadamente y fueron reflejadas en el tráfico de salida del firewall, evidenciando una correcta gestión del control de acceso en la DMZ.

conclusión Temática 4:

Se demostró la importancia del filtrado y la segmentación para proteger los servicios ubicados en la DMZ.
La correcta configuración de reglas HTTP y FTP, junto con las pruebas desde la LAN y la WAN, permitió validar la efectividad del firewall al permitir únicamente el tráfico autorizado.

conclusión Temática 5:

La implementación del Proxy HTTP no transparente en Endian Firewall permitió comprender de manera práctica el funcionamiento de los mecanismos de control de navegación basados en políticas de autenticación y filtrado de contenido. A través de la creación de usuarios locales, grupos, perfiles de filtrado y reglas de acceso, fue posible gestionar adecuadamente el tráfico proveniente de la red interna, garantizando que solo los usuarios autorizados puedan navegar y que determinados sitios sean bloqueados mediante listas negras.

8. REFERENCIAS

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

[2] Endian Community. (2023). Endian Firewall Documentation. https://www.endian.com/ [4] LaCroix, J. (2020). Mastering Ubuntu Server: Gain expertise in the art of deploying, configuring, managing, and troubleshooting

[3] LPI LPIC-1 Exam 101. (2022). Tema 101: Determinar y configurar los ajustes de hardware. https://learning.lpi.org/es/learning materials/101-500/101/101.1/

.

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

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

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

[7] Endian Firewall Community, "HTTP Proxy and Web Filter Configuration," *Endian Documentation*, 2024. [Online]. Available: https://docs.endian.com/community/.

[8] Mozilla Foundation, "Firefox Proxy Configuration," *Mozilla Support*, 2024. [Online]. Available: https://support.mozilla.org/.

[9] Squid Proxy Developers, "Squid: Optimising Web Delivery," *Squid Official Documentation*, 2024. [Online]. Available: http://www.squid-cache.org/Doc/.

[10] Ubuntu Documentation Team, "Networking and Proxy Settings," *Ubuntu Official Documentation*, 2024. [Online]. Available: https://help.ubuntu.com/.

[11] The Linux Foundation, "Network Security and Proxy Architectures," *Linux Networking Standards*, 2024. [Online]. Available: https://www.linuxfoundation.org/.