CONFIGURACIÓN DE SEGURIDAD PERIMETRAL EN GNU/LINUX USANDO ENDIAN FIREWALL Y VIRTUALBOX

Jeferson Leonardo Sandoval Silva
jlsandovals@unadvirtual.edu.co
Evelyn Vanessa Acevedo Reyes
evacevedor@unadvirtual.edu.co
Luis Carlos Leal Jimenez
lclealj@unadvirtual.edu.co
Ellis Orlando Jaimes Sandoval
eojaimess@unadviertual.edu.co
José Andrés Ardila Noguera
jaardilano@unadvirtual.edu.co

RESUMEN: *La presente investigación describe el proceso de implementación de un esquema de seguridad perimetral utilizando GNU/Linux Endian Firewall Community en un entorno virtualizado con VirtualBox. El desarrollo se centró en la configuración de las zonas Verde (LAN), Roja (WAN) y Naranja (DMZ), así como en la aplicación de reglas NAT, políticas de acceso, configuración de servicios HTTP y FTP, y la implementación de un proxy HTTP con autenticación de usuarios. El objetivo principal fue fortalecer la seguridad de una infraestructura de red simulada, garantizando el control del tráfico entre las diferentes zonas y permitiendo la administración segura de los servicios. Los resultados obtenidos evidenciaron el correcto funcionamiento de las políticas de filtrado, traducción de direcciones y autenticación, demostrando que Endian constituye una alternativa eficiente para la administración de seguridad perimetral en sistemas GNU/Linux.*

PALABRAS CLAVE: Endian Firewall, GNU/Linux, Nat, DMZ, Proxy HTTP, Seguridad.

ABSTRACT: This research describes the implementation process of a perimeter security scheme using the GNU/Linux Endian Firewall Community in a virtualized environment with VirtualBox. The development focused on configuring the Green (LAN), Red (WAN), and Orange (DMZ) zones, as well as applying NAT rules, access policies, configuring HTTP and FTP services, and implementing an HTTP proxy with user authentication. The main objective was to strengthen the security of a simulated network infrastructure, ensuring traffic control between the different zones and enabling secure service management. The results obtained demonstrated the correct operation of the filtering, address translation, and authentication policies, proving that Endian is an efficient alternative for perimeter security management in GNU/Linux systems.

KEYWORDS: Endian Firewall, GNU/Linux, Nat, DMZ, HTTP Proxy, Security.

1 INTRODUCCIÓN

En la actualidad, la seguridad de las infraestructuras de red representa uno de los pilares fundamentales para garantizar la continuidad operativa de cualquier organización. El incremento sostenido de amenazas cibernéticas, ataques de intrusión y accesos no autorizados ha impulsado la adopción de arquitecturas de seguridad perimetral que permitan segmentar, controlar y monitorear el tráfico de red de manera efectiva y estructurada.

Una de las estrategias más sólidas en este campo es la implementación de una Zona Desmilitarizada (DMZ), que actúa como red intermedia entre la red interna de la organización (LAN) y la red pública de Internet (WAN). Esta arquitectura garantiza que los servidores que exponen servicios al exterior queden aislados de los sistemas internos críticos, reduciendo significativamente la superficie de ataque ante posibles intrusos.

El presente trabajo documenta la implementación colaborativa de un esquema de seguridad perimetral completo sobre plataforma GNU/Linux, utilizando la distribución Endian Firewall (EFW) como solución central. Endian es una distribución basada en Linux orientada a la seguridad de redes, que integra en una sola plataforma capacidades de firewall por zonas, traducción de direcciones de red (NAT), proxy HTTP, filtrado de contenidos y gestión unificada de amenazas (UTM), siendo ampliamente utilizada en entornos educativos y empresariales.

El desarrollo se organizó en cinco temáticas complementarias. La Temática 1 abordó la instalación y configuración de Endian Firewall en VirtualBox, estableciendo las tres zonas de red: zona verde (LAN), zona roja (WAN) y zona naranja (DMZ). La Temática 2 configuró las reglas NAT para permitir la comunicación desde la LAN hacia Internet y desde la DMZ hacia la WAN, verificando el reenvío de puertos en cada escenario. La Temática 3 habilitó los servicios HTTP (puerto 80) y FTP (puerto 21) en el servidor Ubuntu de la DMZ, y aplicó reglas de firewall para bloquear el protocolo ICMP, impidiendo respuestas al comando ping desde la red. La Temática 4 definió reglas de acceso inter-zona para comunicar la zona verde con la zona naranja, y verificó las directivas de acceso HTTP y FTP en múltiples escenarios de origen y destino. La Temática 5 implementó un proxy HTTP no transparente con autenticación por usuario, listas negras para bloqueo de sitios y verificación desde la LAN.

El objetivo central fue demostrar, de manera práctica y documentada, que una arquitectura de seguridad perimetral correctamente implementada sobre GNU/Linux permite controlar el flujo de tráfico entre zonas, exponer servicios de forma segura y proteger la integridad de los recursos internos. Todos los procedimientos fueron ejecutados exclusivamente desde consola, sin interfaces gráficas, conforme a las directrices de la guía de actividades.

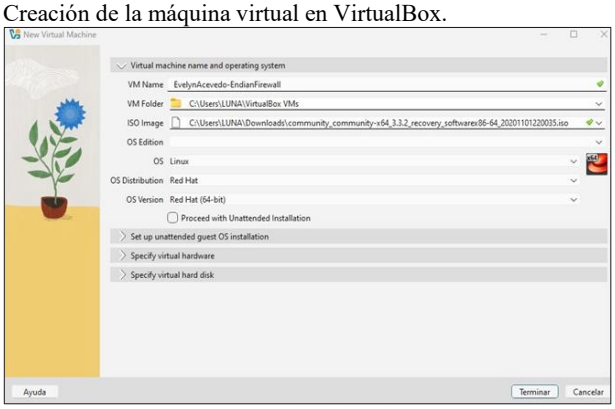
2 TEMÁTICAS

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

Se inicia con la descarga de la imagen ISO de Endian Firewall Community (EFW) desde la página oficial https://sourceforge.net/projects/efw/, ademas se crea la nueva máquina virtual (Endian Firewall) en VirtualBox, la cual actuará como firewall de toda la red.

Al finalizar la descarga de la imagen ISO se procede con la configuración de la máquina virtual (Endian Firewall) como se observa en la Fig. 1, donde se registran los valores del nombre de la máquina, la selección de la imagen ISO, el tipo y la versión.

Figura 1.
Creación de la máquina virtual en VirtualBox.



Fuente: Autoría propia

Luego se especifica el hardware de la máquina virtual, en este caso fue asignó 2048 MB de memoria RAM, 1 CPU de procesador y de disco duro se asigna 20 GB, terminando de esta manera con la creación y configuración de la máquina virtual (Endian Firewall).

Antes de iniciar la máquina virtual creada, se ingresa en configuración en la opción Red para definir los tres adaptadores de Endian. En la Fig. 2. Se observa la configuración del Adaptador 1: WAN (Zona Roja) red NAT, que permite que el firewall tenga acceso a Internet.

Figura 2.
Adaptador 1 de la máquina virtual (Endian Firewall).

Fuente: Autoría propia

En la Fig. 3. Se observa la configuración del Adaptador 2: LAN (Zona Verde) red interna, que permite conectar los equipos internos (clientes).

Figura 3.
Adaptador 2 de la máquina virtual (Endian Firewall).

Fuente: Autoría propia

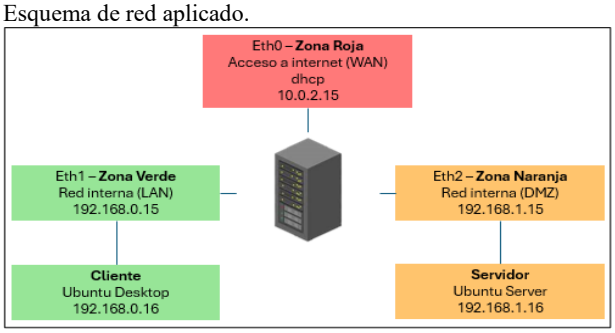
En la Fig. 4. Se observa la configuración del Adaptador 3: DMZ (Zona Naranja) red interna, donde irá el servidor web.

Figura 4.
Adaptador 3 de la máquina virtual (Endian Firewall).

Fuente: Autoría propia

Para continuar con la instalación y configuración de la instancia se realiza el esquema red aplicado al desarrollo de la temática 1 como se observa en la Fig. 5.

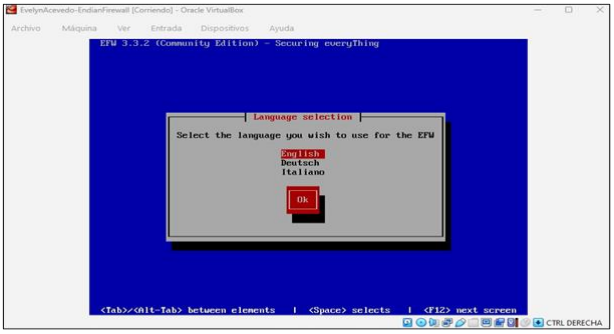
Figura 5.
Esquema de red aplicado.



Fuente: Autoría propia

Al finalizar la configuración de los adaptadores se inicia la máquina virtual (Endian Firewall) para comenzar con la instalación de Endian, se selecciona el idioma como se observa en la Fig. 6, en este caso fue inglés y se selecciona OK.

Figura 6.
Selección del idioma.

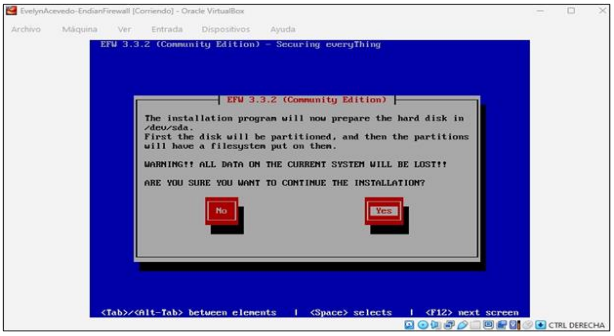


Fuente: Autoría propia

En la pantalla siguiente se muestra el mensaje de bienvenida al programa de instalación, y la observación que al seleccionar Cancelar en cualquiera de las pantallas siguientes se reiniciará el equipo. Se selecciona OK y se empiezan a detectar los discos.

En la Fig. 7, se informa que el programa de instalación particiona el disco e instala un sistema de archivos en las particiones. Para continuar con la instalación se selecciona Yes.

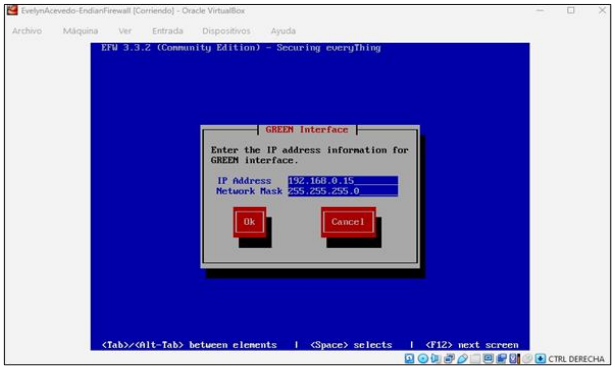
Figura 7.
Instalación de Endian



Fuente: Autoría propia

En la siguiente pantalla se pregunta si se desea habilitar la consola a través del puerto serie, se selecciona Yes. En la Fig. 8 se observa la dirección IP y máscara de red que se registró para la zona verde, luego se selecciona OK.

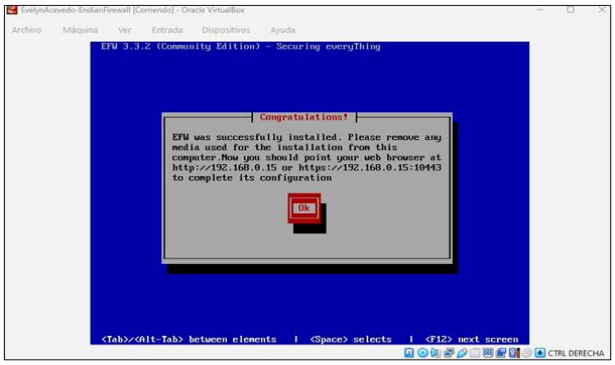
Figura 8.
Dirección IP zona verde



Fuente: Autoría propia

La instalación de Endian fue correcta como se muestra en la Fig. 9. Ahora se debe completar la configuración desde el navegador web del cliente (Ubuntu Desktop), ingresando a: https://192.168.0.15:10443

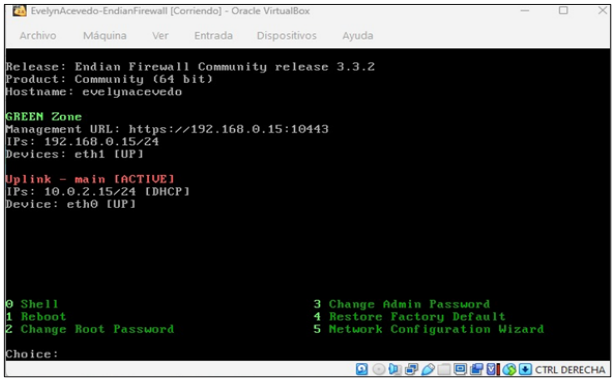
Figura 9.
Instalación correcta de Endian



Fuente: Autoría propia

Se reinicia la máquina virtual (Endian Firewall) y como se observa en la Fig. 10 Endian ya se encuentra instalado y funcionando, luego se selecciona la opción 5 Network Configuration Wizard para continuar con la configuración.

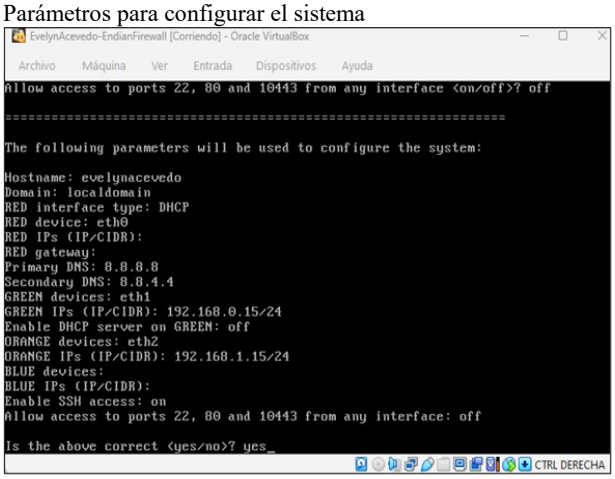
Figura 10.
Endian en funcionamiento



Fuente: Autoría propia

En la Fig. 11, se observa el registro de parámetros utilizados para configurar el sistema, como hostname, el dominio, el dispositivo y la IP de las zonas (verde: 192.168.0.15/24, naranja: 192.168.1.15/24). Al terminar la configuración se reinicia con la opción 1 Reboot.

Figura 11.
Parámetros para configurar el sistema



Fuente: Autoría propia

Se continua con el cambio del adaptador de la máquina virtual cliente (Ubuntu Desktop) por red interna y se selecciona el nombre LAN (Zona Verde) como se observa en la Fig.12, después se inicia la máquina.

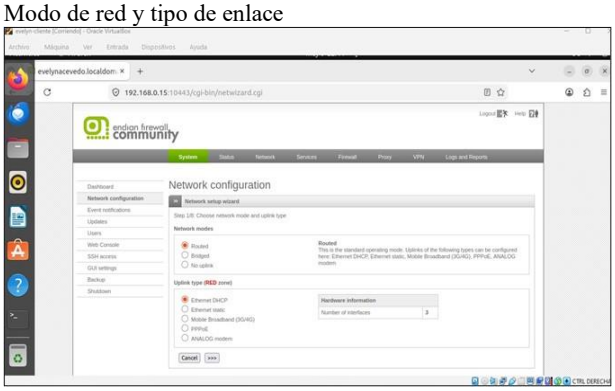
Figura 12.
Adaptador de la máquina virtual cliente (Ubuntu Desktop).

Fuente: Autoría propia

Se inicia la máquina virtual cliente (Ubuntu Desktop), se ingresa a https://192.168.0.15:10443 para completar la configuración, además se selecciona el idioma, la zona horaria, se aceptan los términos y condiciones, en backup se deja por defecto default, se asignan las credenciales de acceso para el administrador y SSH.

En la Fig. 13 se observa el modo de red (enrutamiento), el tipo de enlace Ethernet por DHCP para la zona roja y que el servidor de Endian cuenta con tres interfaces configuradas.

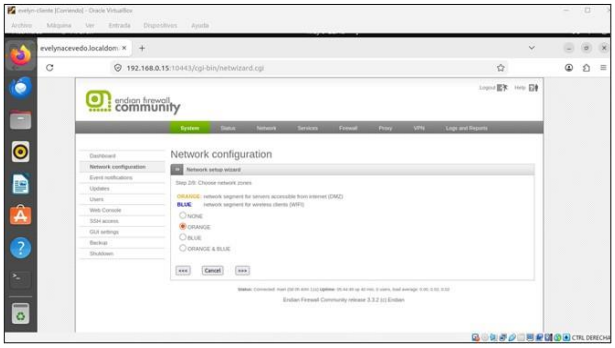
Figura 13.
Modo de red y tipo de enlace



Fuente: Autoría propia

En la Fig. 14 se observa la selección de la zona naranja para habilitar la segmentación DMZ

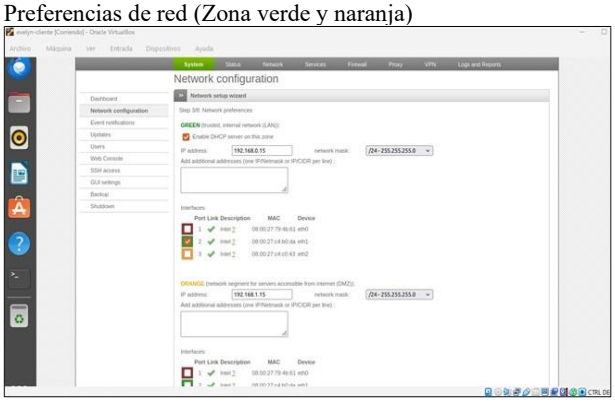
Figura 14.
Zonas de red



Fuente: Autoría propia

En el siguiente paso de configuración se observa la configuración de la zona verde LAN (IP: 192.168.0.15) y la zona naranja DMZ (IP: 192.168.1.15) como se observa en la Fig. 15.

Figura 15.
Preferencias de red (Zona verde y naranja)



Fuente: Autoría propia

En la Fig. 16, se presenta el siguiente paso donde se configura la zona roja (WAN) para el acceso a la conexión de internet.

Figura 16.
Preferencias de acceso a internet (Zona roja)

Fuente: Autoría propia

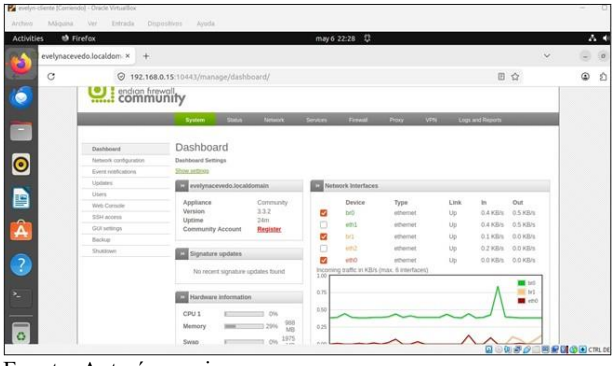
Para el siguiente paso se registran los DNS, luego los campos de la configuración del correo de administrador se dejan en blanco y se aplica la configuración como se muestra en la Fig. 17.

Figura 17.
Configuraciones aplicadas en Endian

Fuente: Autoría propia

Al finalizar la configuración como se observa en la Fig. 18, se presenta el panel de control de Endian donde se cuenta con una visión general del sistema.

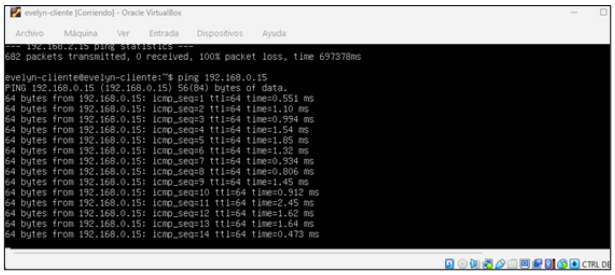
Figura 18.
Panel de control de Endian



Fuente: Autoría propia

Se valida la conexión desde la máquina virtual cliente (Ubuntu Desktop) hacia la zona verde, como se muestra en la Fig. 19.

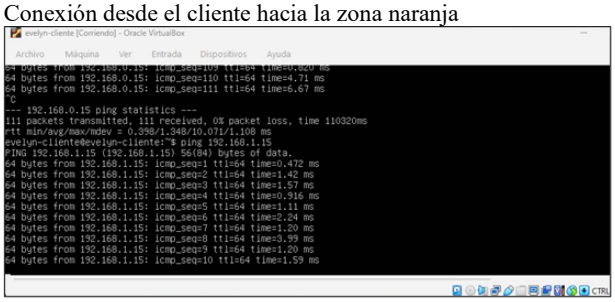
Figura 19.
Conexión desde el cliente hacia la zona verde



Fuente: Autoría propia

Se valida la conexión desde la máquina virtual cliente (Ubuntu Desktop) hacia la zona naranja, como se muestra en la Fig. 20.

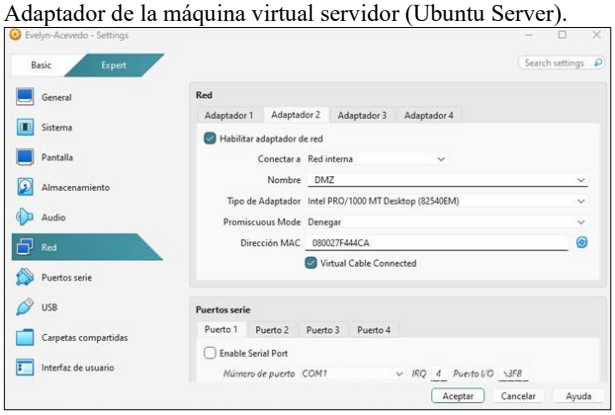
Figura 20.
Conexión desde el cliente hacia la zona naranja



Fuente: Autoría propia

Para continuar con las validaciones se cambia el adaptador de la máquina virtual servidor (Ubuntu Server) por red interna y se selecciona el nombre DMZ (Zona Naranja) como se observa en la Fig. 21, luego se inicia la máquina.

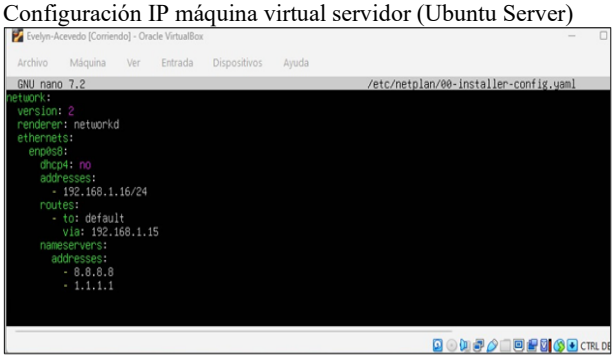
Figura 21.
Adaptador de la máquina virtual servidor (Ubuntu Server).



Fuente: Autoría propia

Se realiza la configuración de la IP estática de la máquina virtual servidor (Ubuntu Server) para conectarla a la zona naranja (DMZ), se consulta el nombre de la interfaz de red con el comando ip a, en este caso será enp0s8, luego se edita el archivo de red con el comando sudo nano /etc/netplan/00-installer-config.yaml, se registran las líneas que se observan en la Fig. 22, y se aplican los cambios con el comando sudo netplan apply

Figura 22.
Configuración IP máquina virtual servidor (Ubuntu Server)



Fuente: Autoría propia

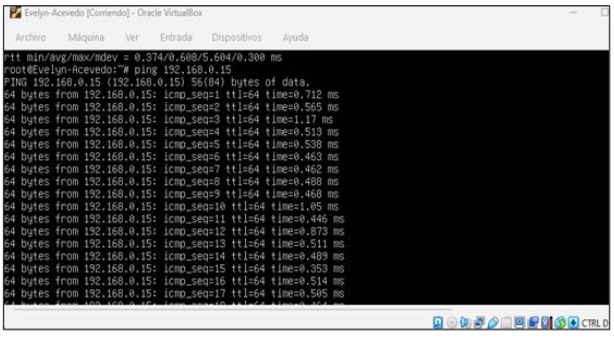
Se valida la conexión desde la máquina virtual servidor (Ubuntu Server) hacia la zona naranja, como se muestra en la Fig. 23.

Figura 23.
Conexión desde el servidor hacia la zona naranja

Fuente: Autoría propia

Se valida la conexión desde la máquina virtual servidor (Ubuntu Server) hacia la zona verde, como se muestra en la Fig. 24.

Figura 24.
Conexión desde el servidor hacia la zona verde

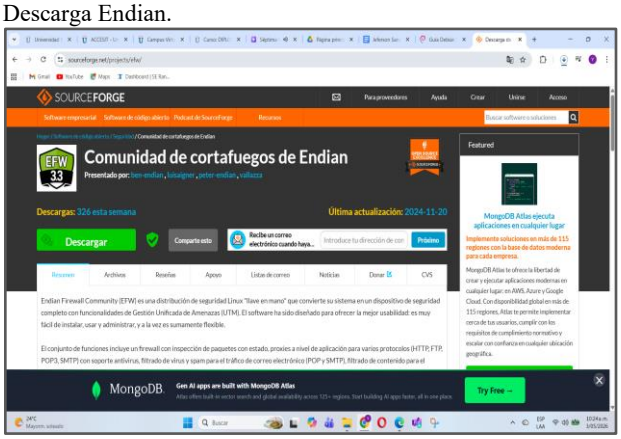


Fuente: Autoría propia

2.2 TEMÁTICA 2: CONFIGURACIÓN NAT.

Fig 25. se aprecia donde se inicia con la descarga de la imagen ISO de Endian Firewall.

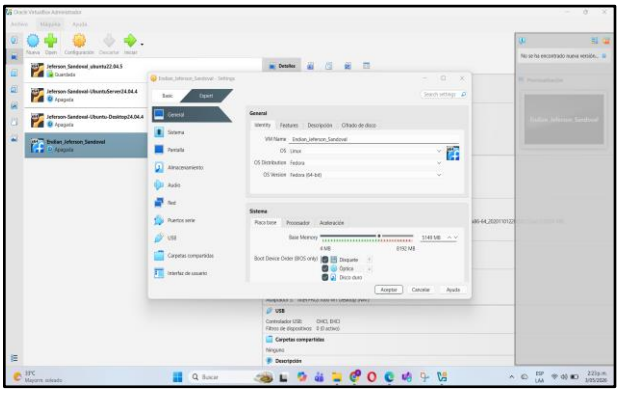
Figura 25.
Descarga Endian.



Fuente: Autoría propia.

Fig 26. Se crea máquina virtual en virtualbox con el sistema operativo Endian.

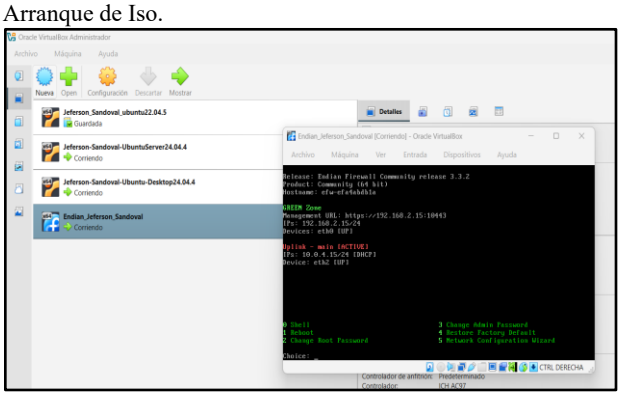
Figura 26.
Creación de un entorno virtual.



Fuente: Autoría propia.

Fig 27. Se evidencia el arranque de la máquina virtual en virtualbox con el sistema operativo Endian.

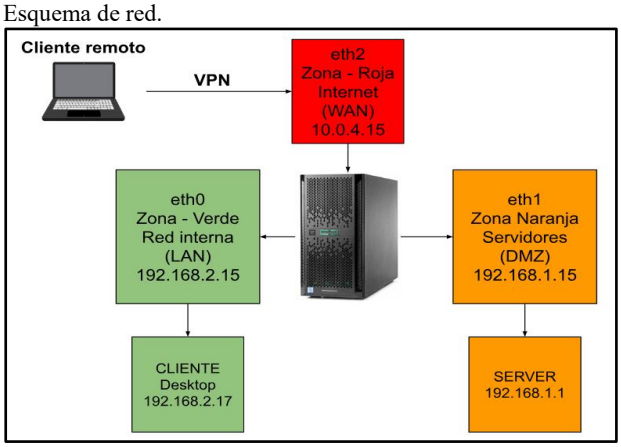
Figura 27.
Arranque de Iso.



Fuente: Autoría propia.

Fig 28. Esquema de red con las ip asignadas para el desarrollo de la actividad.

Figura 28.
Esquema de red.



Fuente: Autoría propia.

Fig 29. Configuración de adaptador de red Verde en virtualbox.

Figura 29.
Configuración de adaptador.

Fuente: Autoría propia.

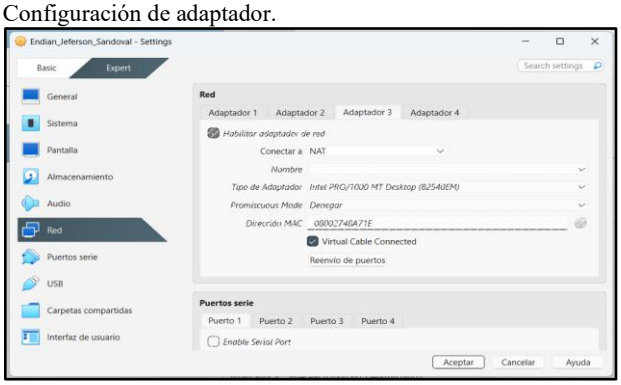
Fig 30. Configuración de adaptador de red Naranja en virtualbox.

Figura 30.
Configuración de adaptador.

Fuente: Autoría propia.

Fig 31. Configuración de adaptador de red Roja en virtualbox

Figura 31.
Configuración de adaptador.



Fuente: Autoría propia.

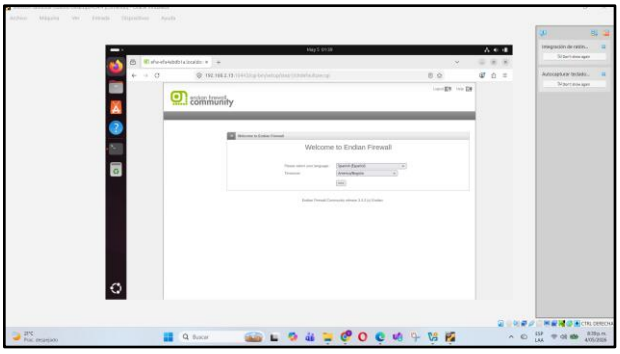
Fig 32. Se procede a asignarle la ip a Endian.

Figura 32.
Instalación y configuración Endian firewall.

Fuente: Autoría propia.

Fig 33. Se abre navegador en el Desktop para dirigirnos al administrador web de Endian firewall por medio del adaptador verde con la ip 192.168.2.15

Figura 33.
Accedo administrador web.



Fuente: Autoría propia.

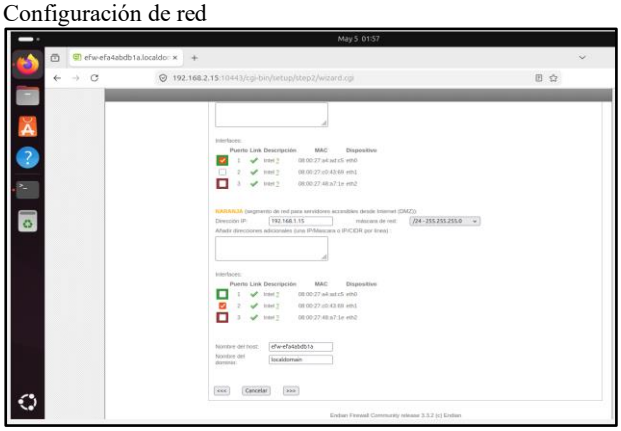
Fig 34. Creamos la credencial de acceso tanto para administrador web y usuario root de consola.

Figura 34.
Asignación de credenciales.

Fuente: Autoría propia.

Fig 35. Configuramos la red naranja con la respectiva ip 192.168.1.15

Figura 35.
Configuración de red



Fuente: Autoría propia.

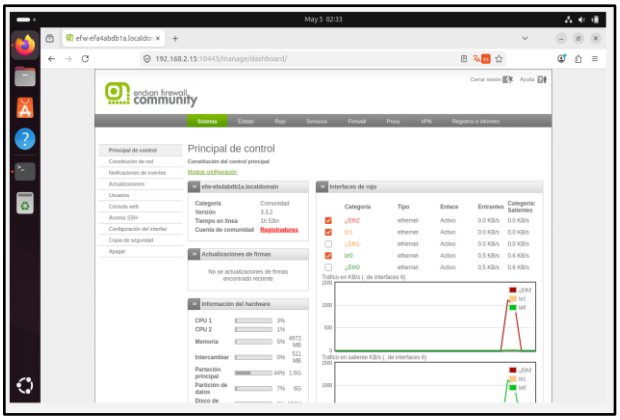
Fig 36. Podemos validar que los adaptadores 0, 1 y 2 quedaron correctamente configurados.

Figura 36.
Configuración de adaptadores

Fuente: Autoría propia.

Fig 37. Ingresamos por medio del administrador web y podemos ver la lista de las tarjetas de red verde, naranja y roja.

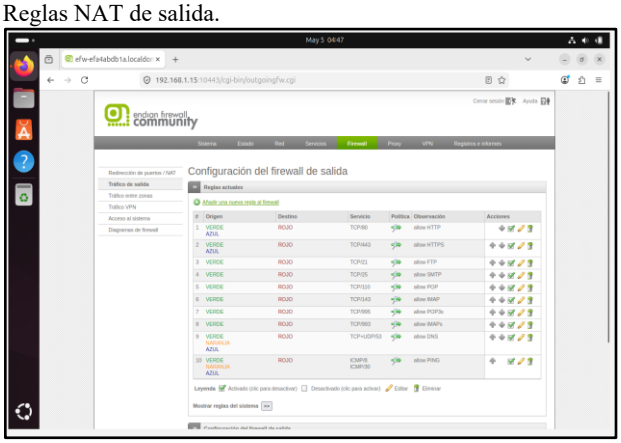
Figura 37.
Administrador web



Fuente: Autoría propia

Fig 38. Desde el administrador web firewall ingresamos a la opción firewall - NAT de salida. Se puede ver que por defecto Endian permite el tráfico de LAN a WAN de forma automatizada como se puede ver en la regla.

Figura 38.
Reglas NAT de salida.



Fuente: Autoría propia.

Fig 39. Regla con sus respectivos permisos.

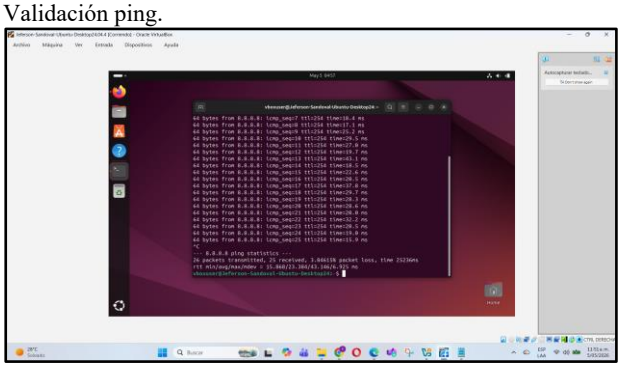
Figura 39.
Característica regla.

Origen	Destino	Servicio	Observación	Acción
Verde (LAN)	Rojo (Internet)	TCP/80	HTTP, HTTP/S, FTP, SMTP, POP, IMAP	Permitir

Fuente: Autoría propia

Fig 40. En la siguiente imagen se puede ver que se valida por medio de ping 8.8.8.8 desde máquina cliente conectada a la red-nat el cual está operando correctamente.

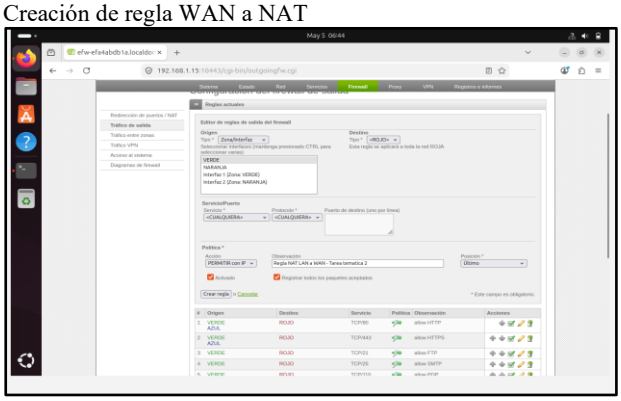
Figura 40.
Validación ping.



Fuente: Autoría propia

Fig 41. Lo anterior ha sido una configuración casi automatizada ahora se procede a llevar a la práctica la creación de reglas de navegación de WAN a LAN de forma manual ajustada.

Figura 41.
Creación de regla WAN a NAT



Fuente: Autoría propia

Fig 42. Lo anterior ha sido una configuración casi automatizada ahora se procede a llevar a la práctica la creación de reglas de navegación de WAN a LAN de forma manual ajustada. Ingresamos a firewall y buscamos la opción de crear nueva regla con los siguientes parámetros.

Figura 42.
Ítems para regla.

Origen:

Tipo: Cambia "Red/IP" por <VERDE> (Que es la red LAN).

DESTINO:

Tipo: Seleccionamos <ROJO> (Que representa Internet).

SERVICIO/PUERTO:

Servicio: Dejar por defecto cualquiera

Protocolo: Dejar por defecto cualquiera

POLÍTICA:

Acción: Permitir con IPS

Observación: NAT LAN a WAN - Tarea Temática 2

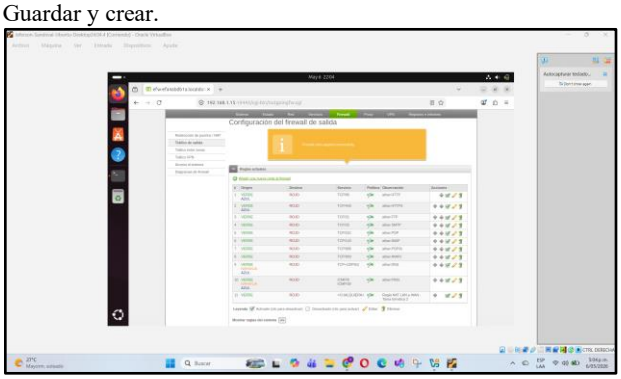
Registrar todos los paquetes aceptados: Seleccionamos todos

Posición: Primero

Fuente: Autoría propia

Fig 43. Damos crear reglas, aplicar. Por defecto se creará con los parámetros establecidos previamente.

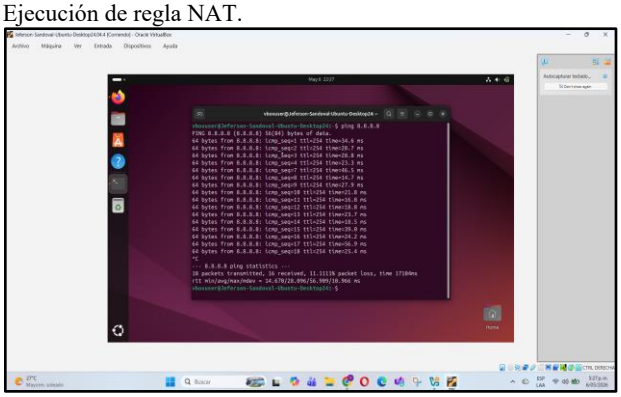
Figura 43.
Guardar y crear.



Fuente: Autoría propia

Fig 44. Ponemos a prueba la regla creada por medio de ping 8.8.8.8 ejecutada en la terminal consola de cliente (Desktop). Podemos ver que de los 18 paquetes se recibieron correctamente 16.

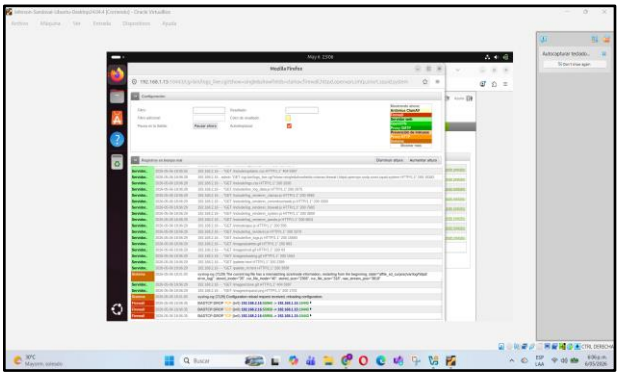
Figura 44.
Ejecución de regla NAT.



Fuente: Autoría propia

Fig 45. Ahora verificamos el tráfico de ip de Ubuntu hacia afuera que fue aceptado.

Figura 45.
Verificación de tráfico.



Fuente: Autoría propia

Fig 46. Esta es la parte donde se procede a configurar la configuración DMZ hacia la internet NAT. Para ello elegimos la opción de crear nueva regla para este caso va a ser la NARANJA con los siguientes parámetros.

Figura 46.
Configuración DMZ.

ORIGEN:

Tipo: Cambia "Red/IP" por <NARANJA>

DESTINO:

Tipo: Seleccionamos <ROJO> (Que representa Internet).

SERVICIO/PUERTO:

Servicio: Dejar por defecto CUALQUIERA

Protocolo: Dejar por defecto CUALQUIERA

POLÍTICA:

Acción: Permitir con IPS

Observación: NAT DMZ a WAN - Temática 2

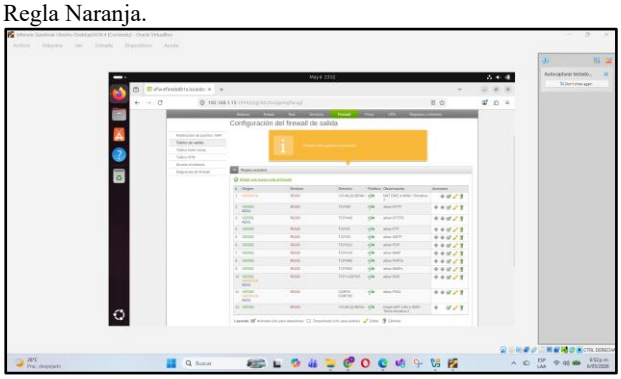
Registrar todos los paquetes aceptados: Seleccionamos todos

Posición: Primero

Fuente: Autoría propia

Fig 47. Podemos ver la imagen que se creó la regla naranja correctamente y se ubicó en primer puesto.

Figura 47.
Regla Naranja.



Fuente: Autoría propia

Fig 48. Ahora creamos la regla de reenvíos de puertos con los siguientes parámetros.

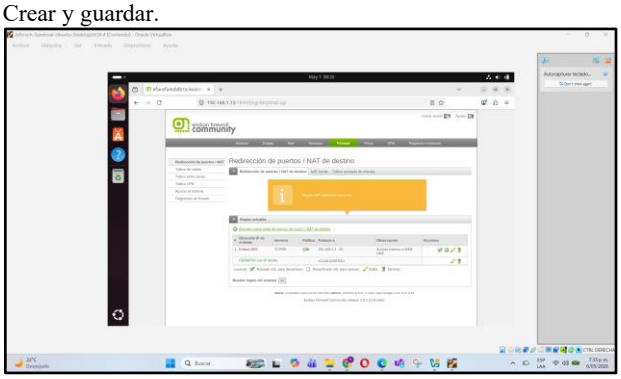
Figura 48.
Regla de reenvíos de puertos.

- **IP de entrada:** Selecciona <CUALQUIERA>
- **Servicio: HTTP** (o el puerto 80).
- **Protocolo:** TCP.
- **Traducir a (Destino):** IP 192.168.1.1 privada del servidor en la zona naranja.
- **Puerto de destino:** Escribe 80.
- **Observación:**Acceso externo a Web DMZ.
- **Posición**: De primero

Fuente: Autoría propia

Fig 49. Creamos reglas y las aplicamos como se puede ver a continuación.

Figura 49.
Crear y guardar.

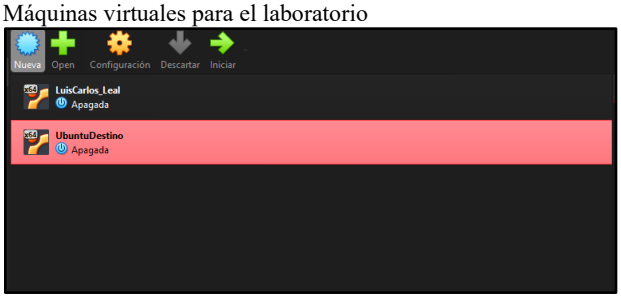


Fuente: Autoría propia

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

Se inicia con la descarga de la imagen ISO de Endian Firewall

Figura 50.
Máquinas virtuales para el laboratorio



Fuente: Autoría propia.

Instalación de las dos máquinas virtuales para proceder con la configuración necesaria de implementar y demostrar el control de servicios en una zona DMZ.

Instalación y habilitación de servicios HTTP y FTP

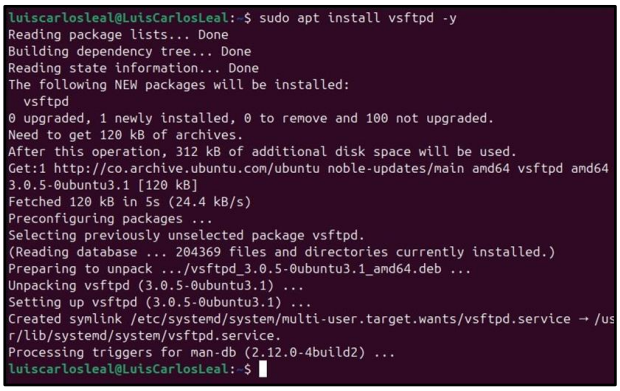
Figura 51.
Instalación y configuración de las máquinas virtuales en VirtualBox para la implementación de la zona DMZ.

```
luiscarlosleal@LuisCarlosLeal:~$ date
Tue May  5 11:56:29 AM UTC 2026
luiscarlosleal@LuisCarlosLeal:~$ sudo apt update
[sudo] password for luiscarlosleal:
Hit:1 http://co.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://co.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://co.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:5 https://ppa.launchpadcontent.net/ondrej/php/ubuntu noble InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
100 packages can be upgraded. Run 'apt list --upgradable' to see them.
luiscarlosleal@LuisCarlosLeal:~$ sudo apt install apache2 -y
[sudo] password for luiscarlosleal:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
apache2 is already the newest version (2.4.58-1ubuntu8.11).
0 upgraded, 0 newly installed, 0 to remove and 100 not upgraded.
luiscarlosleal@LuisCarlosLeal:~$ sudo apt install vsftpd -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

Fuente: Autoría propia.

Se inició verificando la fecha y hora del sistema, seguido de la actualización de los repositorios con sudo apt update. Apache2 ya se encontraba instalado en su versión 2.4.58. Se procedió a instalar el servicio FTP mediante sudo apt install vsftpd -y, el cual se instaló en la versión 3.0.5.

Figura 52.
Verificación de fecha y hora del sistema con el comando date e inicio de la actualización de repositorios con sudo apt update en el servidor DMZ.

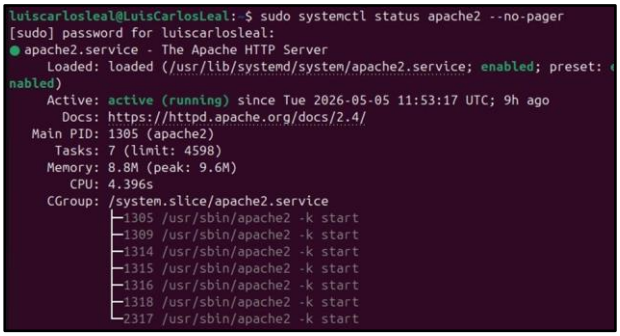


Fuente: Autoría propia.

Figura 53.
Confirmación de Apache2 versión 2.4.58 ya instalado en el servidor e inicio de la instalación del servicio vsftpd con sudo apt install vsftpd -y.

Fuente: Autoría propia.

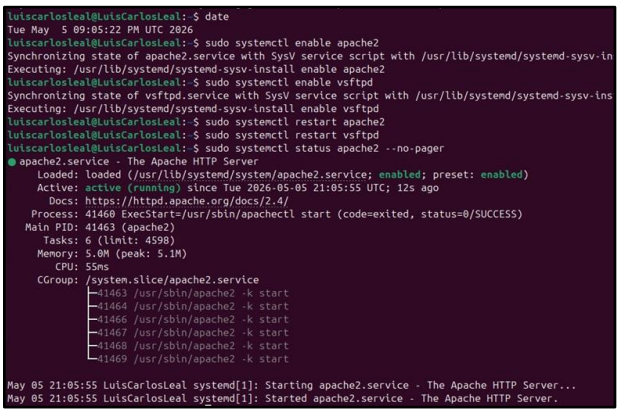
Figura 54.
stalación exitosa de vsftpd versión 3.0.5 en el servidor de la zona DMZ con descarga desde los repositorios oficiales de Ubuntu.



Fuente: Autoría propia.

Se verificó el estado de ambos servicios con el comando systemctl status, comprobando que se encontraban activos y en ejecución.

Figura 55.
Verificación del estado del servicio Apache2 mediante sudo systemctl status apache2, mostrando estado active (running) y habilitado al inicio del sistema.



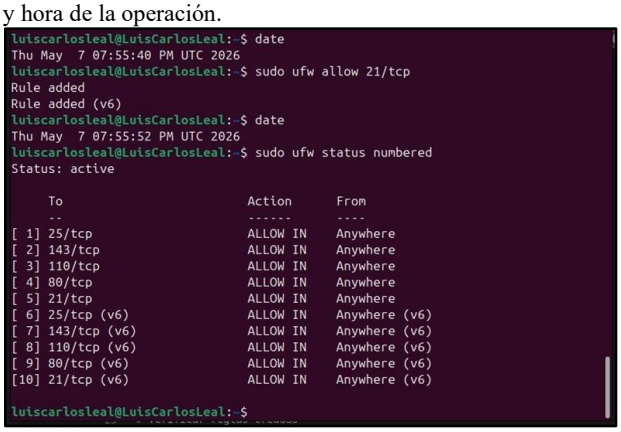
Fuente: Autoría propia.

Figura 56.
Verificación del estado del servicio vsftpd mediante sudo systemctl status vsftpd, mostrando estado active (running) y habilitado al inicio del sistema.

Fuente: Autoría propia.

Se habilitaron ambos servicios para que inicien automáticamente con el sistema operativo, y se reiniciaron para aplicar cualquier cambio de configuración pendiente.

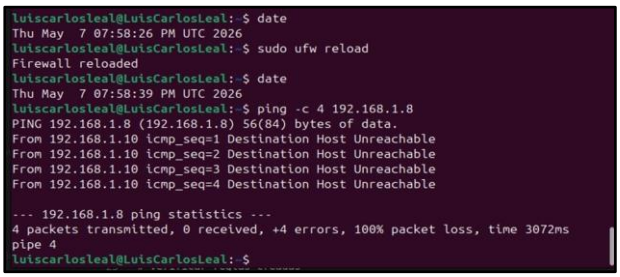
Figura 57.
Habilitación con systemctl enable y reinicio con systemctl restart de los servicios Apache2 y vsftpd, con registro de fecha y hora de la operación.



Fuente: Autoría propia.

Se activó el firewall UFW (Uncomplicated Firewall) y se crearon las reglas para permitir el tráfico entrante en el puerto 80 (HTTP) y puerto 21 (FTP), correspondientes a los servicios instalados en la zona DMZ.

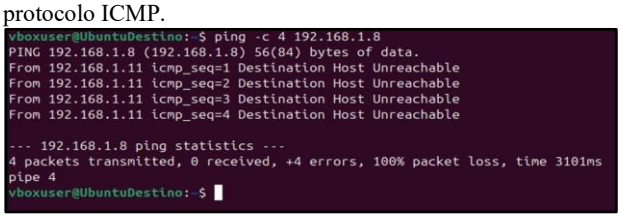
Figura 58.
Activación del firewall UFW y creación de reglas ALLOW para los puertos 80/tcp (HTTP) y 21/tcp (FTP), verificadas con sudo ufw status numbered.



Fuente: Autoría propia.

Para denegar el protocolo ICMP y evitar que se pueda hacer ping a la red, se editó el archivo /etc/ufw/before.rules modificando la regla de echo-request de ACCEPT a DROP. Posteriormente se recargó UFW para aplicar los cambios.

Figura 59.
Edición del archivo /etc/ufw/before.rules para modificar la directiva echo-request de ACCEPT a DROP y bloquear el protocolo ICMP.

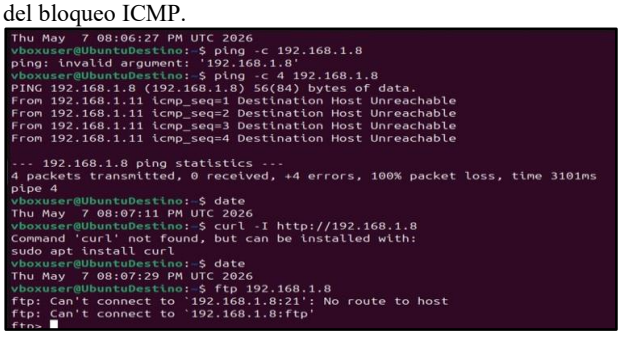


Fuente: Autoría propia.

Figura 60.
Recarga del firewall UFW con sudo ufw reload para aplicar el bloqueo del protocolo ICMP configurado en before.rules.

Fuente: Autoría propia.

Figura 61.
Prueba de ping desde el servidor hacia su propia IP 192.168.1.8, obteniendo 100% packet loss como confirmación del bloqueo ICMP.



Fuente: Autoría propia.

Desde la máquina cliente con IP 192.168.1.11 se realizaron las pruebas de verificación para comprobar el correcto funcionamiento de las reglas implementadas.

Se ejecutó el comando ping desde UbuntuDestino hacia el servidor 192.168.1.10, obteniendo como resultado 100% packet loss, confirmando que el protocolo ICMP está correctamente bloqueado.

Figura 62.
Prueba de ping desde la máquina cliente UbuntuDestino (192.168.1.11) hacia el servidor DMZ (192.168.1.10), obteniendo 100% packet loss.

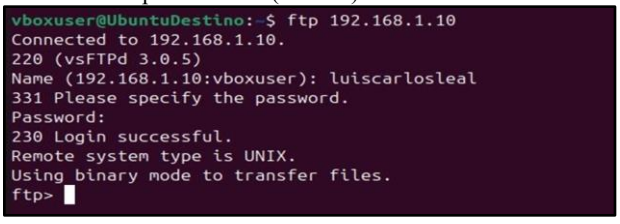
Fuente: Autoría propia.

Figura 63.
Confirmación de bloqueo ICMP desde la máquina cliente con fecha Thu May 7 08:06:27 PM UTC 2026, verificando Destination Host Unreachable en cada paquete.

Fuente: Autoría propia.

Se instaló curl en la máquina cliente y se realizó una petición HTTP al servidor. La respuesta fue HTTP/1.1 200 OK, confirmando que el servicio Apache está funcionando correctamente y accesible desde la red.

Figura 64.
Instalación de curl en la máquina cliente e ingreso exitoso al servicio HTTP del servidor, obteniendo respuesta HTTP/1.1 200 OK con Apache/2.4.58 (Ubuntu).



Fuente: Autoría propia.

Se realizó la conexión FTP al servidor desde la máquina cliente. El servidor vsftpd respondió correctamente aceptando la conexión y autenticando al usuario luiscarlosleal con el mensaje 230 Login successful

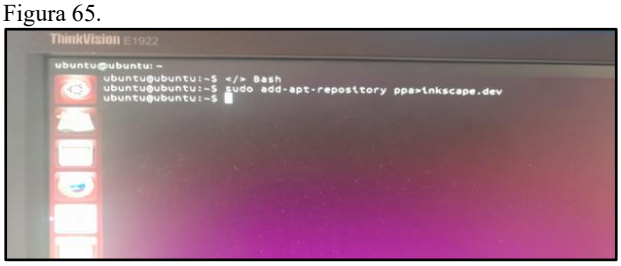
2.4 TEMÁTICA 4: REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO. PRODUCTO ESPERADO.

Se inicia con la descarga de la imagen ISO de Endian Firewall

Paso 1. Verificar conectividad inicial

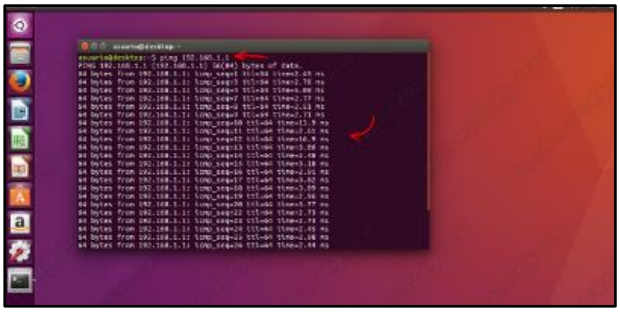
Antes de crear reglas, verificar que el firewall Endian esté encendido y que Ubuntu Desktop tenga conectividad. pin 192168.0.15

Figura 65.



Fuente: Autoría Propia

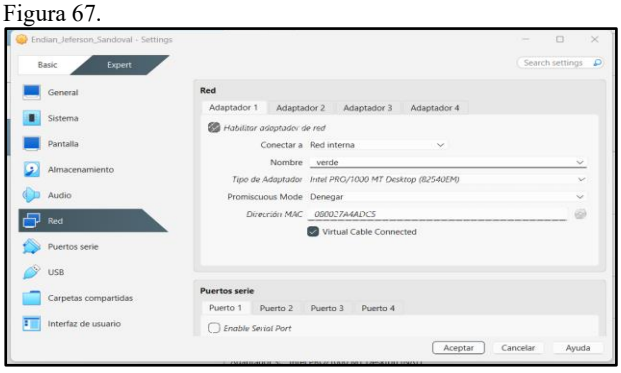
Figura 66.
Validamos internet



Fuente: Autoría Propia

Paso 2. Ingresar al administrador web de Endian

Figura 67.



Fuente: Autoría Propia

Paso 3. Ingresar a Firewall → Inter-Zone Traffic

Firewall → Inter-Zone Traffic

Esta sección controla el tráfico entre zonas:

GREEN (LAN) = red interna
ORANGE (DMZ) = servidores
RED (WAN) = Internet

Paso 4. Crear una regla para PERMITIR tráfico

Crear una regla para permitir tráfico desde la red LAN hacia Internet.

Seleccionar:

Add New Firewall Rule

Configurar:

Figura 68.

Origen: Verde
Destino: Rojo
Servicio: HTTP /HTTPS
Acción: Aceptar
Remark: Permitir Navegación Web
Enabled: Activado

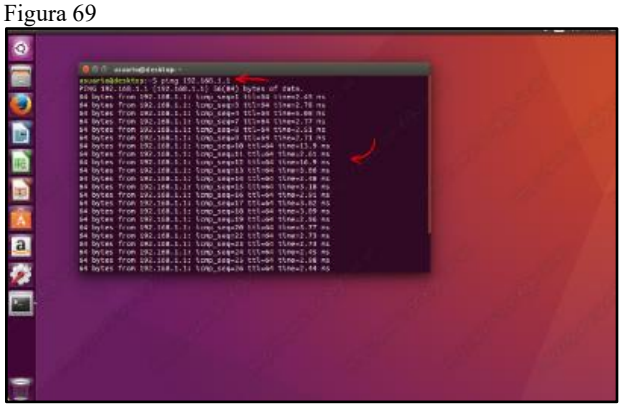
Add → Apply Changes

Esto permitirá navegación web desde Ubuntu Desktop hacia Internet.

Paso 5. Validar regla de permitir tráfico

ping 8.8.8.8

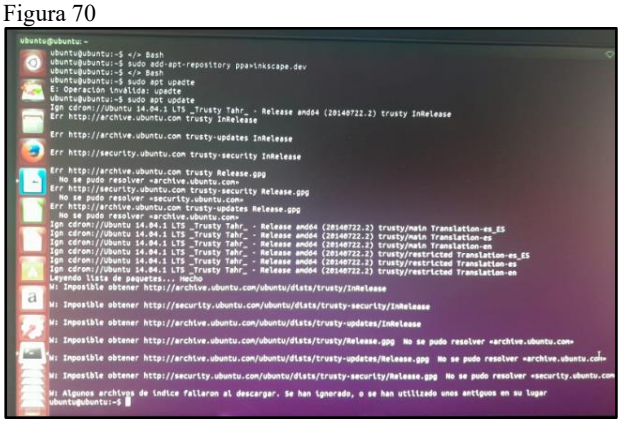
Figura 69



Fuente: Autoría Propia

curl google.com

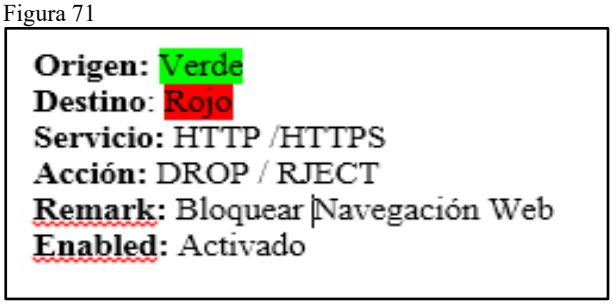
Figura 70



Fuente: Autoría Propia

Paso 6. Crear regla para DENEGAR tráfico

Figura 71



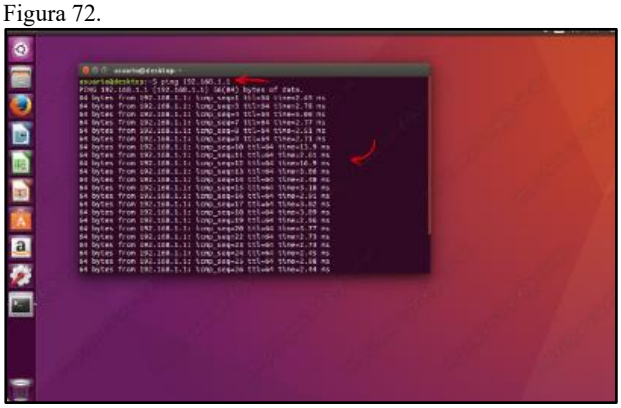
Paso 7. Subir prioridad de la regla

Muy importante: Mover la regla de denegar hacia arriba usando las flechas de prioridad.

Paso 8. Probar el bloqueo

Desde Ubuntu Desktop probar:

Figura 72.



Fuente: Autoría Propia

Paso 9. Revisar logs del firewall

Logs → Firewall Logs

Aquí se observan paquetes:

ACCEPT
DROP
REJECT

Esto sirve como evidencia de que la política está funcionando.

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

Se inicia con la descarga de la imagen ISO necesarias para la práctica

La imagen ISO de Endian Firewall Community fue utilizada para implementar el firewall encargado del control de acceso a Internet y administración del proxy.

Ubuntu Server fue instalado para disponer de un entorno Linux orientado a servicios y pruebas de conectividad.

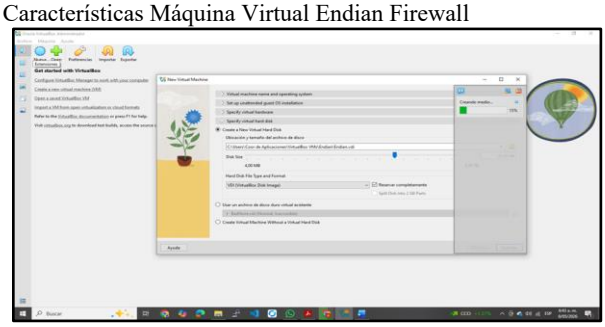
Ubuntu Desktop fue utilizado como cliente para realizar las pruebas de navegación web y autenticación mediante Firefox.

Posteriormente se procedió a crear las máquinas virtuales dentro de Oracle VirtualBox.

Máquina Virtual Endian Firewall

La máquina virtual de Endian fue configurada con las siguientes características:

Figura 73.
Características Máquina Virtual Endian Firewall



Fuente: Autoría Propia

El primer adaptador se configuró en modo NAT para permitir el acceso a Internet.

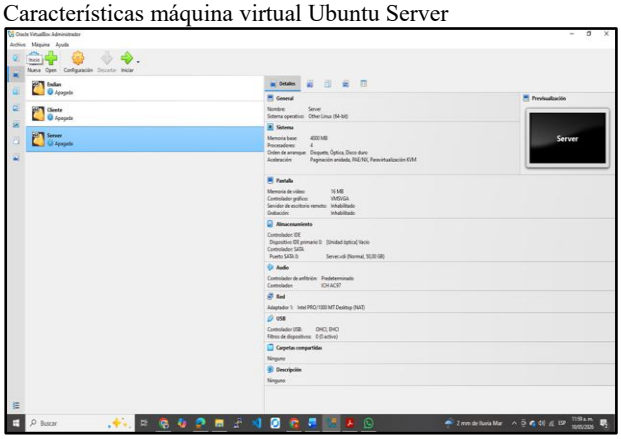
El segundo adaptador se configuró en Red Interna para establecer comunicación con el cliente Ubuntu.

Durante la instalación se configuraron las interfaces GREEN y ORANGE:

Máquina Virtual Ubuntu Server

La máquina Ubuntu Server fue creada con los siguientes recursos:

Figura 74.
Características máquina virtual Ubuntu Server



Fuente: Autoría propia

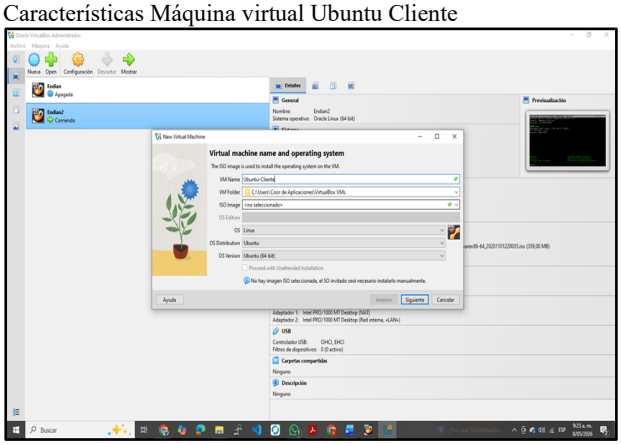
El objetivo de esta máquina fue validar conectividad y pruebas de red dentro de la infraestructura virtual.

Máquina Virtual Ubuntu Cliente

La máquina Ubuntu Desktop fue utilizada como cliente final para validar el funcionamiento del proxy.

La configuración implementada fue:

Figura 75
Características Máquina virtual Ubuntu Cliente



Fuente: Autoría Propia

Esta máquina fue conectada a la interfaz GREEN de Endian Firewall.

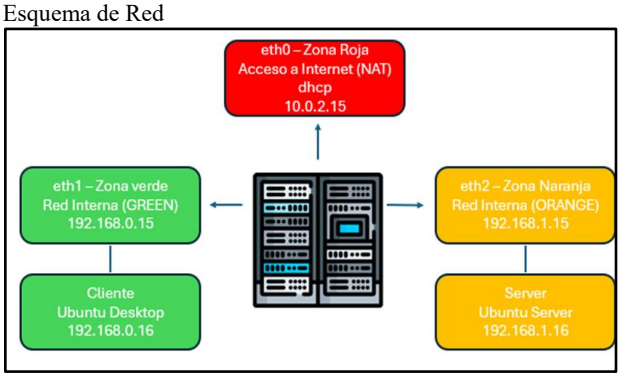
Configuración de Red

Una vez instaladas las máquinas virtuales se procedió a configurar el direccionamiento IP.

La interfaz GREEN del firewall Endian fue configurada como puerta de enlace principal para los clientes internos.

Posteriormente se verificó la conectividad mediante pruebas de ping entre las máquinas virtuales.

Figura 76.
Esquema de Red



Fuente: Autoría Propia

Instalación de Endian Firewall Community

Durante el proceso de instalación de Endian Firewall se seleccionó la opción de instalación estándar. Posteriormente se configuraron los parámetros básicos del sistema:

- Contraseña de administración.
- Configuración de interfaces de red.
- Asignación de IP para la red GREEN.
- Configuración de acceso web administrativo.

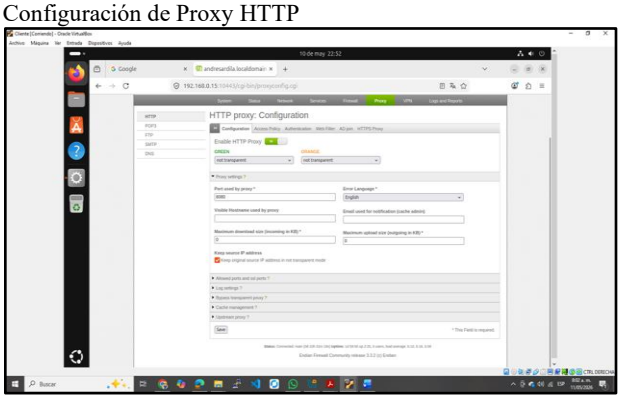
Una vez finalizada la instalación, se accedió a la consola web administrativa desde el navegador mediante la dirección IP configurada para la interfaz GREEN.

Configuración de Proxy HTTP

Dentro de la interfaz administrativa se habilitó el servicio Proxy HTTP.

La configuración realizada fue la siguiente:

Figura 77.
Configuración de Proxy HTTP



Fuente: Autoría Propia

El modo no transparente requirió configurar manualmente el proxy dentro del navegador Firefox del cliente Ubuntu.

Configuración de Usuarios y Grupos

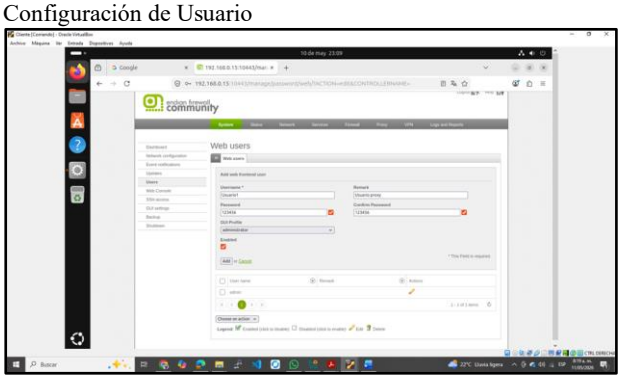
Posteriormente se creó un usuario local mediante autenticación NCSA.

El procedimiento consistió en:

1. Crear el usuario.
2. Asignar contraseña.
3. Crear un grupo de acceso.
4. Asociar el usuario al grupo.

Esta configuración permitió aplicar políticas de navegación basadas en grupos.

Figura: 78.
Configuración de Usuario



Fuente: Autoría Propia

Creación del Perfil de Filtrado

Se creó un perfil de filtrado denominado: BLOQUEO_WEB

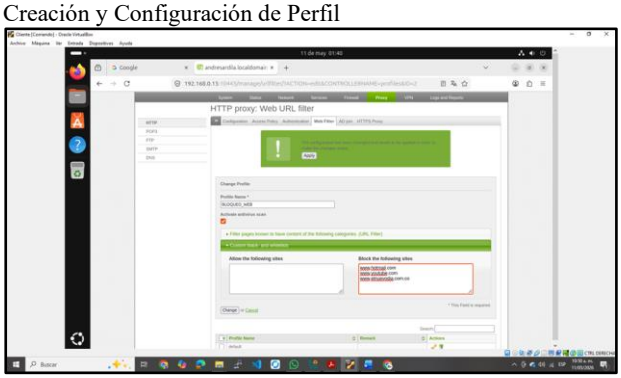
Dentro del perfil se habilitó la opción de listas negras personalizadas.

Posteriormente se agregaron los siguientes dominios:

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

Estos dominios fueron configurados para ser bloqueados por el proxy HTTP.

Figura 79.
Creación y Configuración de Perfil



Fuente: Autoría Propia

Configuración de la Política de Acceso

Después de crear el perfil de filtrado se configuró una política de acceso dentro del proxy HTTP.

La política incluyó los siguientes parámetros:

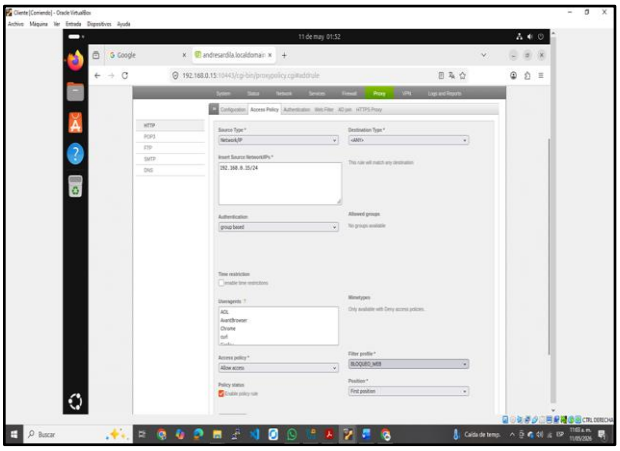
Tabla 1.
Parámetros de Configuración de la Política de Acceso

Parámetro	Configuración
Source Type	Network/IP
Destination	ANY
Authentication	Group Based
Access Policy	Allow Access
Filter Profile	BLOQUEO_WEB
Estado	Habilitado

Fuente: Autoría Propia

La política fue ubicada en la primera posición para garantizar prioridad sobre otras reglas existentes.

Figura 80.
Creación Política de Acceso



Fuente: Autoría Propia

Configuración del Navegador Firefox

En el cliente Ubuntu se configuró manualmente el proxy HTTP dentro de Firefox.

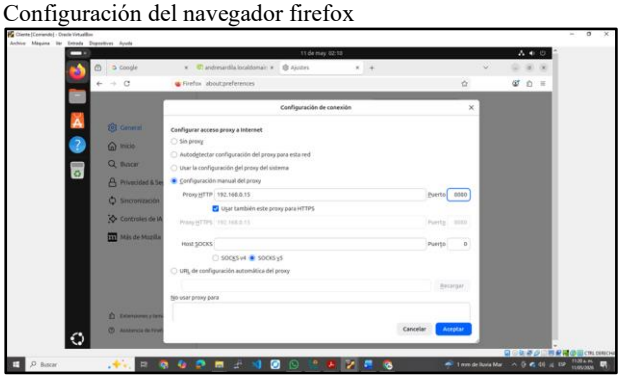
Los parámetros utilizados fueron:

Tabla 2
Parámetros de Configuración Proxy del navegador

Parámetro	Valor
Proxy HTTP	192.168.0.15
Puerto	8080

Fuente: Autoría Propia

Figura 81.
Configuración del navegador firefox



Fuente: Autoría Propia

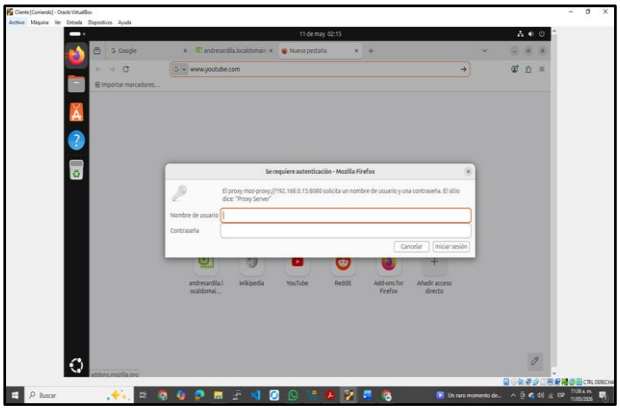
Pruebas de Funcionamiento

Finalmente se realizaron pruebas desde Firefox intentando acceder a los sitios web restringidos.

El sistema solicitó autenticación mediante usuario y contraseña antes de permitir el acceso a Internet.

Posteriormente el proxy bloqueó correctamente los dominios configurados dentro de la blacklist.

Figura 82.
Pruebas de Acceso



Fuente: Autoría Propia

3 CONCLUSIONES

La implementación de GNU/Linux Endian en VirtualBox permite configurar de manera adecuada las zonas Roja (WAN), Verde (LAN) y Naranja (DMZ), logrando la segmentación y administración del tráfico de red entre los diferentes entornos. Asimismo, la configuración de las interfaces de red fortaleció la seguridad perimetral, permitiendo controlar la comunicación entre la red interna, los servidores y el acceso a Internet.

La correcta configuración del NAT permite una separación clara de roles; mientras que la LAN mantiene total privacidad, la DMZ se posiciona como una zona intermedia segura, mitigando riesgos de intrusión directa desde la WAN hacia el núcleo de la red.

Se determinó que la configuración del firewall es solo la mitad del proceso; la comunicación efectiva depende de que los hosts finales (como el Ubuntu Server) tengan correctamente definida su ruta por defecto (default gateway), apuntando hacia la interfaz correspondiente del firewall.

La configuración de reglas de acceso en Endian Firewall permite controlar el tráfico de red entre las diferentes zonas (WAN, LAN y DMZ), fortaleciendo la seguridad perimetral del entorno virtual implementado. Mediante la creación de políticas para permitir y denegar conexiones, fue posible gestionar el acceso a Internet y restringir servicios específicos, garantizando un mayor control sobre la comunicación de los dispositivos conectados a la red.

La implementación de reglas de firewall en Endian facilitó la validación práctica de políticas de seguridad informática, evidenciando la importancia del filtrado de tráfico en la protección de redes. Asimismo, las pruebas de conectividad y la revisión de registros del firewall permitieron verificar el correcto funcionamiento de las reglas establecidas, asegurando una administración eficiente del tráfico de datos según los requerimientos definidos.

La implementación del Proxy HTTP no transparente utilizando Endian Firewall Community permitió comprender el funcionamiento de los mecanismos de autenticación y filtrado web dentro de una infraestructura de red.

Mediante la configuración de usuarios, grupos y políticas de acceso fue posible controlar la navegación web de manera eficiente. Asimismo, el uso de listas negras permitió restringir el acceso a sitios específicos, fortaleciendo la seguridad de la red.

La práctica evidenció la importancia de los servicios proxy en la administración de redes empresariales y en la aplicación de políticas de seguridad informática.

4 REFERENCIAS

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/

Canonical (2023). Guía del Ubuntu desktop 20.04 LTS. Help Ubuntu. https://help.ubuntu.com/

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

Oracle (2020), Manual de usuario VirtualBox. VirtualBox. https://www.virtualbox.org/manual/

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