GUÍA PARA CONFIGURAR ENDIAN EN VIRTUALBOX: IMPLEMENTANDO SEGURIDAD EN GNU/LINUX

Lindsay Andrea Quintero Hernández
e-mail: laquinterohe@unadvirtual.edu.co
Dimas Eduardo Bustos Sosa
e-mail: debustoss@unadvirtual.edu.co
Ángel José Contreras Reyes
e-mail: ajcontrerasre@unadvirtual.edu.co
Keller Emmanuel Beltran Vivas
e-mail: kebeltranv@unadvirtual.edu.co
Jhoan David Gomez Suarez
e-mail: jdgomezsua@unadvirtual.edu.co

RESUMEN: *Este articulo presenta la implementación y configuración del firewall Endian en máquina virtual "VirtualBox", estructurado en cinco ejes temáticos. Se inicia con la arquitectura de la red, se procede con la configuración de reglas SNAT y DNAT con el fin de permitir la comunicación controlada de servicios internos, del servidor web sin afectar la red LAN, se continua con activación de servicios HTTP y FTP desde DMZ, además de denegar el protocolo ICMP como medida preventiva. Para la temática cuatro se definen las reglas de acceso que filtran el tráfico; y se finaliza con la implementación de un Proxy HTTP no transparente con política de autenticación para navegación en internet.*

PALABRAS CLAVE: UTM (Sistema de gestión de amenazas unificadas), DMZ (Zona desmilitarizada), NAT (Network Address Translation), SNAT (Source NAT).

1 INTRODUCCIÓN

En la actualidad la seguridad no es opcional, y el primer parámetro fundamental es el firewall (o cortafuegos), como "protector" de la infraestructura digital aplica un filtro selectivo para protección de los datos; entre estos se encuentra Endian (sistema de gestión de amenazas unificadas "UTM"), que incluye el conjunto de herramientas "todo en uno". Garantiza la protección de los servicios que conforman la intranet (LAN)/extranet (WAN), limita por medio de la zona desmilitarizada (DMZ), asegura la integridad y seguridad de la base de datos y aplicaciones bajo plataformas GNU/Linux.

A lo largo del desarrollo de esta fase practica se detalla la guía de su aplicación, desde la descarga, instalación y configuración de distribución GNU/Linux Endian (EFW), hasta la gestión de servicios.

Se incluye el paso a paso para realizar la comunicación NAT y así demostrar la comunicación entre LAN hacia la WAN, además se permiten servicios de la zona DMZ, se configuran las reglas de acceso para permitir o denegar el tráfico con el objetivo de evidenciar los conocimientos para implementar solución de seguridad.

2 OBJETIVOS DEL PROYECTO

Objetivo General

Implementar y desplegar el firewall Endian "UTM" mediante la configuración de interfaces de red y reglas de administración, con el fin de fortalecer la seguridad perimetral de un entorno Linux, verificando su funcionamiento óptimo antes de finalizar la etapa actual.

Objetivos Específicos

- Instalar y configurar el direccionamiento IP de Endian Firewall en VirtualBox, definiendo las interfaces de red requeridas, en un plazo máximo de 5 días tras iniciar la etapa 7.
- Implementar y validar reglas NAT para tráfico bidireccional entre zonas Verde (LAN) y Roja (WAN), configurando el reenvío de puertos para servicios en la zona Naranja (DMZ).
- Habilitar los puertos 80 (HTTP) y 21 (FTP) en el servidor Ubuntu (DMZ), aplicando reglas granulares para bloquear respuestas ICMP tipos 8 y 30.
- Configurar políticas de acceso inter-zona (Verde, Roja, Naranja) en Endian Firewall para administrar el flujo de datos mediante permisos específicos de entrada y salida.
- Implementar un Proxy HTTP no transparente con autenticación y filtrado de contenido por lista negra, validando el bloqueo de sitios desde un cliente LAN.

3 METODOLOGIA

Este estudio emplea una metodología de investigación aplicada y desarrollo técnico para la implementación de seguridad perimetral mediante Endian Firewall. El proceso describe la configuración de un Proxy HTTP con autenticación y filtrado por listas negras, estructurándose como una guía técnica. La validez del sistema se determinó mediante pruebas de acceso y control de tráfico desde la zona LAN, resolviendo requerimientos de seguridad en redes segmentadas.

4 DESARROLLO DE CONTENIDOS

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

4.1.1 INSTALACIÓN Y CONFIGURACIÓN DE ENDIAN

Se realizó Subneteo para 30 direcciones en cada subred, con 8 subredes disponibles, como se observa en la Fig. 1.

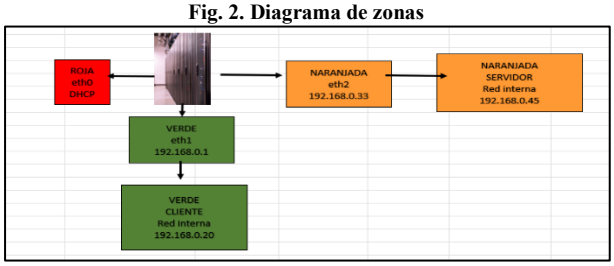
Fig. 1. Subneteo de red

Roja	Adaptador puente	eth0	DHCP	ENDIA	Mascara	Rango host
Verde	Red interna NAT	eth1	192.168.0.0 /27	192.168.0.1	255.255.255.224	.2 hasta .30
Naraja	Red interna DMZ	eth2	192.168.0.32 /27	192.168.0.33	255.255.255.224	.34 hasta .62
Cliente	192.168.0.20 /27	LAN				
Servidor red interna	192.168.0.45 /27	DMZ		Modo Promiscuo esté en "Permitir todo"		
	Id inicio	Gateway	Inicio	Fin	Broadcast	
Verde (LAN)	192.168.0.0/27	192.168.0.1/27	192.168.0.2/27	192.168.0.30/27	192.168.0.31/27	<Saltos de 32
Naranja (DMZ)	192.168.0.32/27	192.168.0.33/27	192.168.0.34/27	192.168.0.62/27	192.168.0.63/27	

Fuente: Autoría Propia

En Fig. 2 se evidencia el diagrama de zonas para la configuración de zonas (roja, verde, naranja) en Endian.

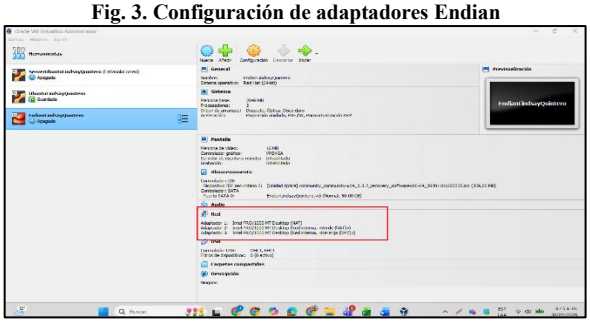
Fig. 2. Diagrama de zonas



Fuente: Autoría Propia

Se procede con la creación de nueva máquina virtual Endian en VirtualBox, se selecciona 2048MG, dos procesadores y 50GB de memoria virtual, a continuación, se procede con la configuración de los adaptadores de la siguiente manera:
-Adaptador 1: NAT
-Adaptador 2: Red interna (Verde)
-Adaptador 3: Red interna (Naranja DMZ)

Fig. 3. Configuración de adaptadores Endian



Fuente: Autoría Propia

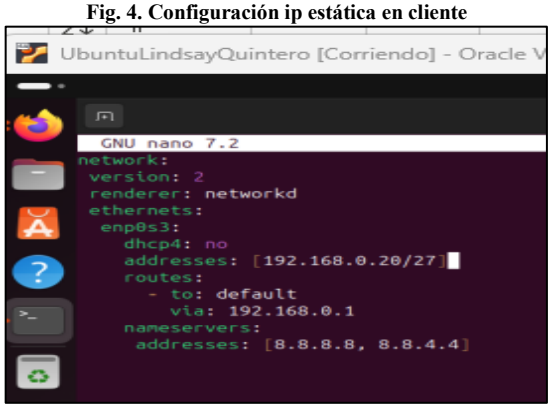
Se procede con la configuración de adaptadores de red en el cliente (Ubuntu/Linux Desktop) y servidor (Ubuntu Server), de la siguiente manera:
-Adaptador cliente (Ubuntu Desktop): Red interna (Verde)
-Adaptador cliente (Ubuntu Server): Red interna (Naranja DMZ)

Se procede con la configuración de la ip estática para el cliente (Ubuntu Desktop)
Se accede al archivo de configuración de red con permisos de administración utilizando el editor de texto nano:

sudo nano /etc/netplan/00-installer-config.yaml

Se incluye el contenido del archivo Fig. 4 se incluye en la línea addresses la dirección de 192.168.0.20/27 que será la ip del cliente "ip disponibles dentro de la subred verde" incluyendo su mascará de red, además, se incluye el Gateway 192.168.0.1 en la línea "via".

Fig. 4. Configuración ip estática en cliente



Fuente: Autoría Propia

Se aplican los cambios con:

sudo netplan apply

Se realizan pruebas de ip y ruta con los comandos

ip addr

Fig. 5. Verificación de configuración ip estática en cliente

Fuente: Autoría Propia

Se realiza el mismo procedimiento para el servidor, ingresando al archivo con permisos de administración y el editor nano:

sudo nano /etc/netplan/00-installer-config.yaml

Se incluye el contenido del archivo Fig. 6. Se incluye en la línea addresses la dirección de 192.168.0.45/27 que será la ip del servidor "ip disponibles dentro de la subred naranja" incluyendo su mascará de red, además, se incluye el Gateway 192.168.0.33 en la línea "via".

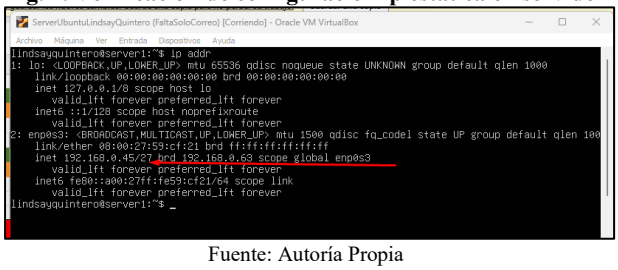
Fig. 6. Verificación de configuración ip estática en servidor

Fuente: Autoría Propia

Se realizan pruebas de ip y ruta con los comandos

ip addr

Fig. 7. Verificación de configuración ip estática en servidor



Fuente: Autoría Propia

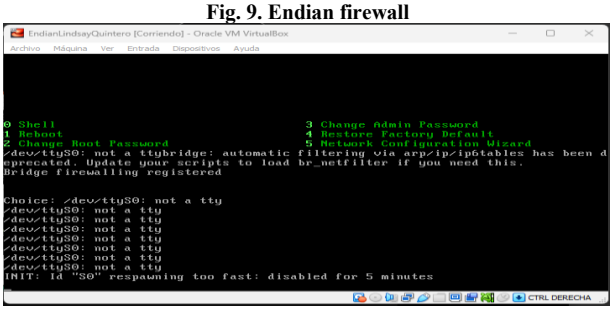
Se procede con la instalación de la maquina Endia, se selecciona el idioma, y se aceptan, para continuar con la configuración de la red verde (se ingresa su Gateway con la máscara de red 192.168.0.1) Fig. 8.

Fig. 8. Instalación de Endian

Fuente: Autoría Propia

Una vez se aplique la configuración se obtendrá Fig 9.

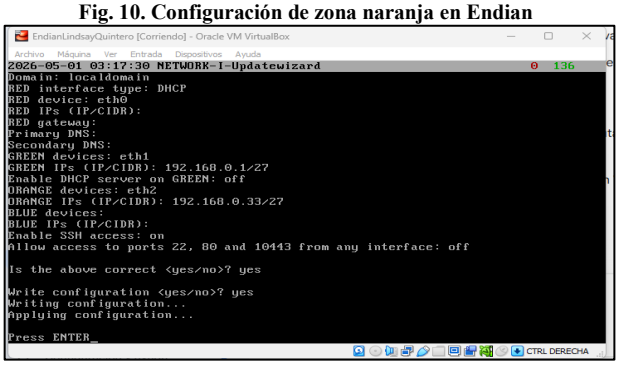
Fig. 9. Endian firewall



Fuente: Autoría Propia

Para proceder con la configuración de la zona verde se accede a la opción 5, se ingresa el usuario "login" y la clave (por defecto es Endian", en esta fase se puede verificar la configuración anterior de eth0 (roja-DHCP) y eth1 (verde "192.168.0./27"), al llegar a eth2 (zona naranja) se ingresa la ip Gateway que se ha definido en la configuración de red "192.168.0.33/27" Fig 10.

Fig. 10. Configuración de zona naranja en Endian



Fuente: Autoría Propia

Verificación

Se verifica la zona verde Fig. 11, se obtiene éxito del 100%.

Fig. 11. Verificación conexión zona verde

Fuente: Autoría Propia

Se verifica la zona naranja Fig. 12, se envían paquetes, pero no hay comunicación (perdida de paquetes), esto indica seguridad, cualquier cosa que venga de zona naranja tiene prohibido entrar a la zona verde.

Fig. 12. Verificación conexión zona naranja

Fuente: Autoría Propia

Validación de ip y pruebas cruzadas.

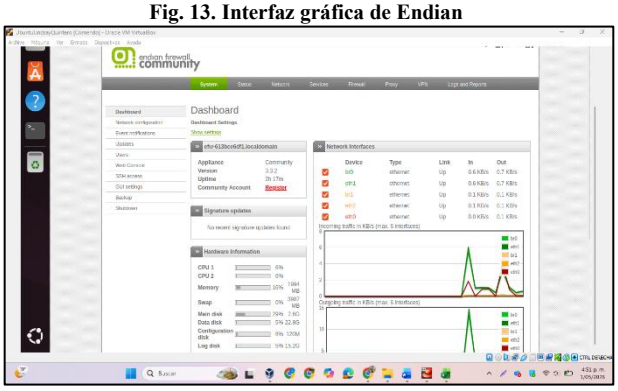
Ingreso a Interfaz gráfica de Endian desde el navegador del cliente:

Se usa el Gateway de la zona verde:

https://192.168.0.1:10443

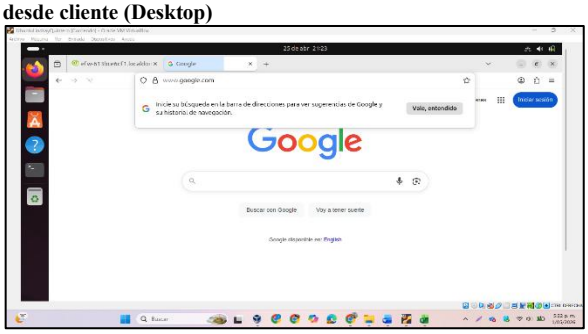
Indicará advertencia de riesgo potencial de seguridad, se selecciona avanzado, aceptar el riesgo, "no quiero ninguna actualización" y se ingresa con el usuario y la clave de Endian.

Fig. 13. Interfaz gráfica de Endian



Fuente: Autoría Propia

Fig. 14. Comprobación exitosa de ingreso a página en internet desde cliente (Desktop)



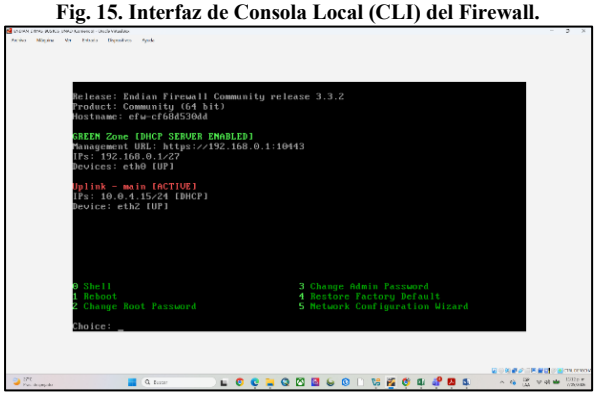
Fuente: Autoría Propia

4.2 TEMATICA 2: CONFIGURACIÓN NAT

Para la implementación de las reglas NAT, se utilizó una instancia de Endian Firewall 3.3.2 configurada en VirtualBox con tres interfaces de red debidamente segmentadas: eth0 vinculada a la zona verde (LAN: 192.168.0.0/27), eth1 vinculada a la zona NARANJA (DMZ: 192.168.0.32/27) y eth2 vinculada a la zona ROJA (WAN: 192.168.1.50) para el acceso a Internet. Esta arquitectura permitió aplicar políticas de traducción de direcciones mediante la cadena MASQUERADE, garantizando que los equipos internos puedan navegar de forma segura hacia el exterior.

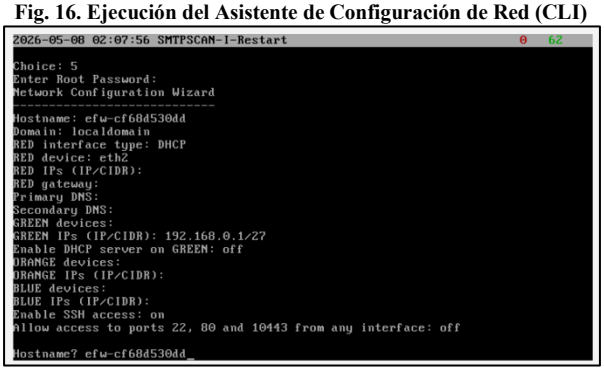
La validación técnica incluyó la auditoría de las tablas de IPTables desde la consola del firewall, donde se confirmó la activación del enmascaramiento de red para todo el tráfico saliente. Asimismo, se verificó la conectividad desde la estación de trabajo en la zona LAN y el servidor en la zona DMZ (IP 192.168.0.33), permitiendo servicios críticos como HTTP (puerto 80), HTTPS (puerto 443) y consultas DNS hacia la zona WAN. Se comprobó que el Gateway predeterminado (192.168.1.1) gestiona correctamente el enrutamiento, cumpliendo con los requisitos de seguridad perimetral y disponibilidad de servicios establecidos para la actividad.

Fig. 15. Interfaz de Consola Local (CLI) del Firewall.



Fuente: Autoría propia

Fig. 16. Ejecución del Asistente de Configuración de Red (CLI)



Fuente: Autoría propia

El uso del Network Configuration Wizard dentro de la consola del firewall, un paso crítico para la definición de la topología lógica del sistema. En la imagen se observa la parametrización de las diversas zonas de seguridad antes de su despliegue final.

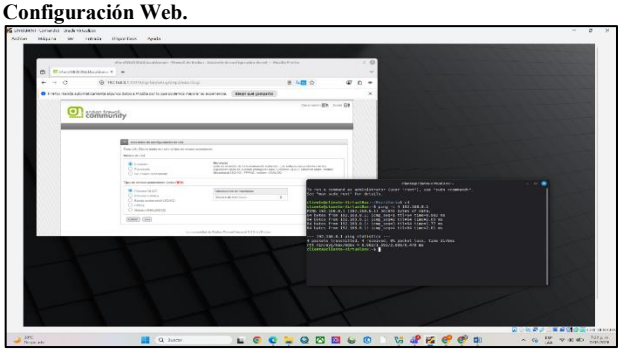
Identificación del Sistema: Se establece el nombre de host como efw-cf68d530dd dentro del dominio localdomain.

Configuración de la Zona RED: Se define el dispositivo eth2 con un tipo de interfaz DHCP, lo que permite la obtención automática de parámetros de red externos para la conectividad WAN.

Configuración de la Zona GREEN: Se asigna de forma estática la dirección IP 192.168.0.1/27, estableciendo la puerta de enlace para la red interna protegida (LAN). Se observa además que el servidor DHCP interno para esta zona se encuentra desactivado (off).

Se evidencia la activación del acceso vía SSH (on), mientras que el acceso abierto a los puertos administrativos (22, 80 y 10443) desde cualquier interfaz se mantiene desactivado para reforzar la seguridad perimetral inicial.

Fig. 17. Validación de Conectividad Inicial y Asistente de Configuración Web.

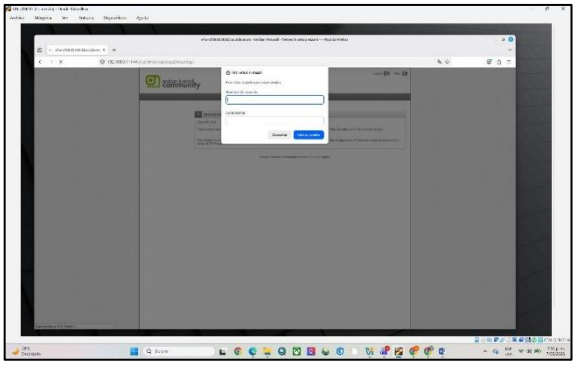


Fuente: Autoría propia

Interfaz Gráfica de Configuración (GUI): Se visualiza el primer paso del asistente de configuración de red de Endian Firewall Community 3.3.2, donde se define el modo de operación como "Enrutado" y se selecciona el tipo de enlace ascendente para la Zona Roja (RED) mediante el protocolo Ethernet DHCP. El sistema reconoce automáticamente la existencia de tres interfaces de hardware en la plataforma virtual.

Resultados de Conectividad: La evidencia muestra un éxito absoluto en la transmisión de paquetes, con un 0% de pérdida y un tiempo de respuesta promedio de 1.691 ms. Este resultado confirma la estabilidad del enlace entre el cliente y el firewall, asegurando que la infraestructura de la Zona Verde está preparada para la implementación de reglas de tráfico superiores.

Fig. 18. Finalización de la Configuración y Autenticación Administrativa.



Fuente: Autoría propia

Aplicación de Cambios: Se observa en el fondo el paso final ("Step 8/8: End") del asistente de configuración de Endian Firewall Community, indicando que la nueva arquitectura de red ha sido procesada y guardada en el sistema.

Seguridad de Acceso (Autenticación): En primer plano, se visualiza una ventana emergente de autenticación HTTP para la dirección IP 192.168.0.1 a través del puerto seguro 10443. Este mecanismo garantiza que solo el personal autorizado con credenciales administrativas

pueda acceder al panel de control una vez establecida la nueva configuración.

Fig. 19. Panel de Control Principal y Monitoreo del Sistema.

Fuente: Autoría propia

El Dashboard principal de la interfaz web de Endian Firewall Community release 3.3.2, el cual centraliza el monitoreo en tiempo real de los recursos y el tráfico de red.

Estado de Interfaces de Red: Se verifica que los dispositivos lógicos y físicos (eth2, br1, eth1, br0, eth0) se encuentran en estado "Up".

Gestión de Enlaces (Uplinks): El sistema reporta el enlace principal (Main uplink) con estado operativo "UP", operando bajo la dirección IP 10.0.4.15.

Recursos de Hardware: El panel de Hardware information refleja un consumo de memoria del 14% (1994 MB) y una carga mínima en los cuatro núcleos de la CPU.

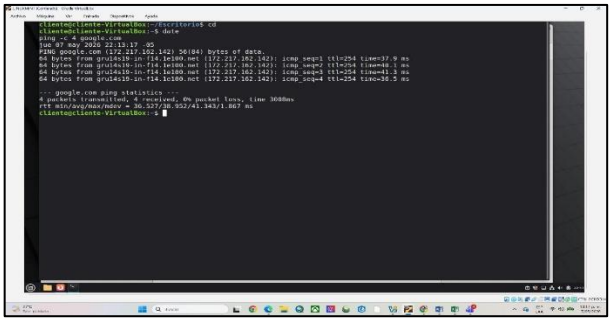
Fig. 20. Información de Estado de Red y Diagnóstico de Interfaces.

Fuente: Autoría propia

La sección de Network status information dentro de la interfaz de gestión de Endian Firewall, la cual proporciona una vista detallada de la configuración lógica y el estado del hardware de red.

Configuración de Direccionamiento Lógico: Se confirma el estado operativo de las interfaces lógicas y sus respectivas subredes. La interfaz br0 (Zona Verde) opera bajo 192.168.0.1/27, mientras que la interfaz br1 (Zona Naranja) utiliza 192.168.0.33/27.

Fig. 21. Validación de Conectividad WAN y Resolución de Nombres en la Zona Verde.

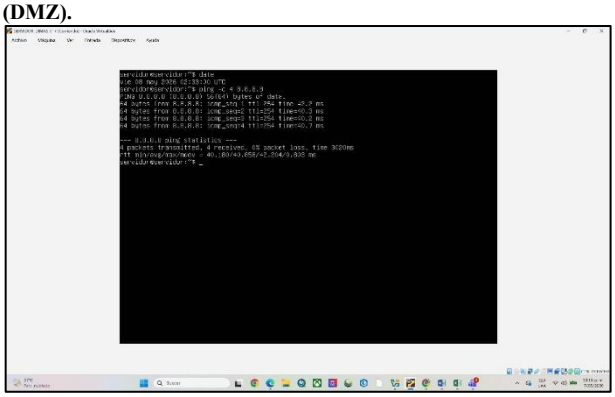


Fuente: Autoría propia

Prueba final de conectividad a nivel de aplicación desde la estación de trabajo situada en la Zona Verde (LAN).

Se demuestra el éxito en la comunicación extremo a extremo a través del firewall.

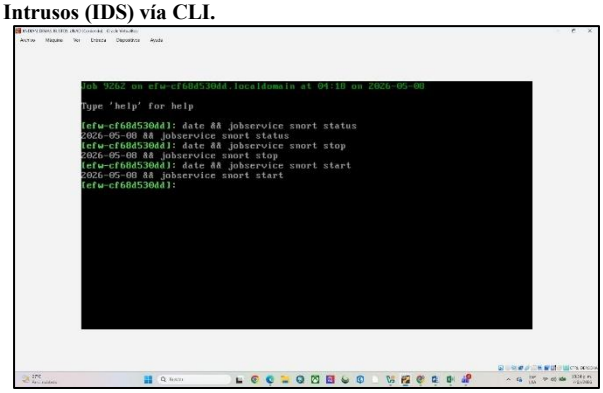
Fig. 22. Verificación de Conectividad WAN desde la Zona Naranja (DMZ).



Fuente: Autoría propia

La prueba de alcance hacia redes externas realizada desde el servidor ubicado en la Zona Naranja (DMZ). La captura de pantalla en la terminal del sistema operativo Linux permite validar los siguientes puntos técnicos: sincronización temporal, prueba de enlace exterior, integridad de la transmisión, validación de reglas de firewall.

Fig. 23. Gestión Administrativa del Sistema - Detección de Intrusos (IDS) vía CLI.



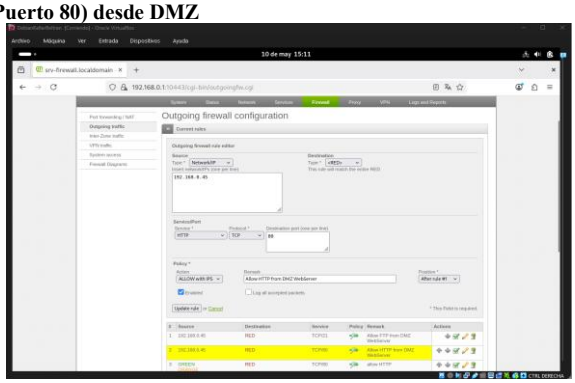
Fuente: Autoría propia

La interacción técnica con el sistema operativo del firewall para la gestión de servicios de seguridad avanzados. La imagen captura la administración por la línea de comandos del motor de prevención de intrusiones Snort.

4.3 Temática 3: Permitir servicios de la Zona DMZ para la red

Para la gestión del tráfico de red, se realizó la configuración de una regla de salida en el firewall con el objetivo de habilitar el servicio web desde la zona desmilitarizada hacia el exterior, dicho procedimiento consistió en definir una directiva que permite la comunicación a través del protocolo TCP en el puerto 80 (HTTP), tomando como origen la dirección IP 192.168.0.45, la cual identifica al servidor web en la DMZ, estableciendo el destino hacia la interfaz RED (Internet) y aplicar la política de "Permitir con IPS", se garantiza que el flujo de datos no solo sea autorizado, sino también inspeccionado por el sistema de prevención de intrusiones, asegurando un equilibrio entre la disponibilidad del servicio y la integridad de la infraestructura.

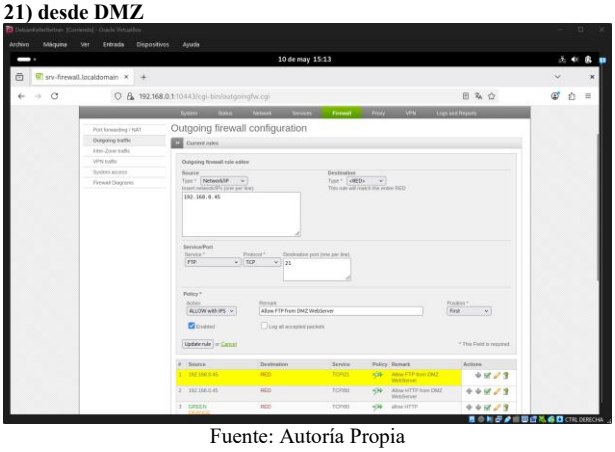
Fig. 24. Creación de la regla para permitir el servicio HTTP (Puerto 80) desde DMZ



Fuente: Autoría Propia

Por otra parte, se estableció una regla de salida diseñada para facilitar el intercambio de información mediante el protocolo FTP, dicho proceso involucró la creación de una excepción específica al servidor web con IP 192.168.0.45, ubicado en el segmento de la DMZ, permitiéndole establecer conexiones hacia la zona RED (Internet) mediante el puerto 21 (TCP), la configuración se definió bajo la acción de "Permitir con IPS", lo que asegura que las sesiones de transferencia de archivos sean monitoreadas activamente contra amenazas potenciales.

Fig. 25. Creación de la regla para permitir el servicio FTP (Puerto 21) desde DMZ



Fuente: Autoría Propia

Como alternativa técnica para obtener un control más preciso sobre el protocolo ICMP, se accedió a la gestión del cortafuegos mediante una conexión SSH, se sincroniza la fecha y hora del sistema para fines de auditoría, se procedió a inspeccionar el estado de la cadena FORWARD en iptables, este análisis previo por consola permite verificar las directivas de red actuales y aplicar restricciones granulares que la interfaz gráfica no permite, garantizando una administración más rigurosa de la seguridad.

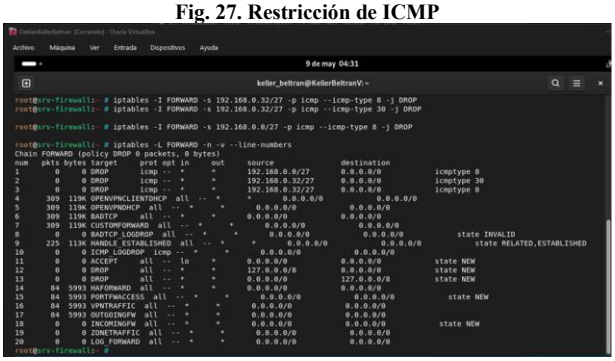
Fig. 26. Auditoría de reglas mediante consola SSH

Fuente: Autoría Propia

Para robustecer la seguridad perimetral, se ejecutó la restricción directa de mensajes de diagnóstico en el firewall mediante el uso de iptables, se insertaron reglas en la cadena de reenvío para denegar peticiones ICMP

Echo Request (tipo 8) y Traceroute (tipo 30) provenientes de los segmentos de red locales y la zona desmilitarizada, este filtrado manual impide que hosts internos o externos realicen un mapeo de la infraestructura, mitigando posibles ataques de reconocimiento, además se verificó la correcta implementación de las directivas.

Fig. 27. Restricción de ICMP



Fuente: Autoría Propia

Se procedió a su almacenamiento para asegurar que las políticas de bloqueo permanezcan activas incluso tras un reinicio del sistema.

Fig. 28. Persistencia de reglas

Fuente: Autoría Propia

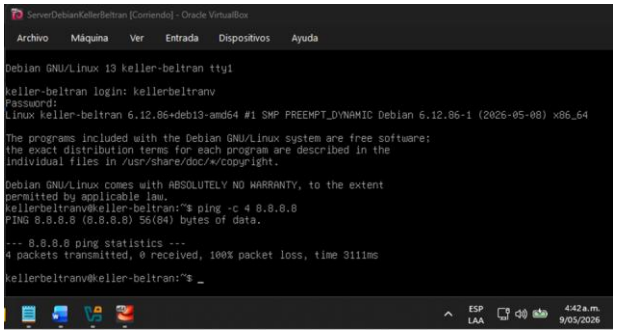
La ejecución del comando de listado permite verificar la correcta integración de las nuevas directivas de seguridad en la cadena de reenvío del sistema.

Fig. 29. Título Validación de directivas en la cadena FORWARD

Fuente: Autoría Propia

A continuación, se valida la efectividad de las restricciones mediante un intento de conexión desde el servidor en la DMZ.

Fig. 30. Prueba de conectividad denegada



Fuente: Autoría Propia

Para asegurar la segmentación de la red, se ejecutó una prueba de diagnóstico desde un equipo cliente hacia la zona desmilitarizada.

Fig. 31. Comprobación de aislamiento en la LAN

Fuente: Autoría Propia

Se confirma la salida efectiva a la red externa mediante una petición de cabeceras web desde el servidor.

Fig. 32. Verificación de navegación HTTP en DMZ

Fuente: Autoría Propia

Se presenta el listado final de las políticas configuradas en el cortafuegos para gestionar las comunicaciones hacia el exterior.

Fig. 33. Consolidado de reglas de tráfico saliente

Fuente: Autoría Propia

Se realizó la comprobación de conectividad mediante la terminal, documentando la fecha y hora exacta de cada ejecución para fines de auditoría.

Fig. 34. Contraste de servicios con registro temporal

Fuente: Autoría Propia

4.4 Temática 4: Reglas de Acceso a Inter-Zona

Para el tráfico entre zonas se crearon distintas reglas permisos desde la interfaz web de ENDIAN dentro del apartado Firewall→Inter-Zone traffic. Encontraremos unas reglas en blanco allí inicialmente. Las ignoramos o eliminamos.

Fig. 35. ENDIAN→Firewall→Inter-Zone

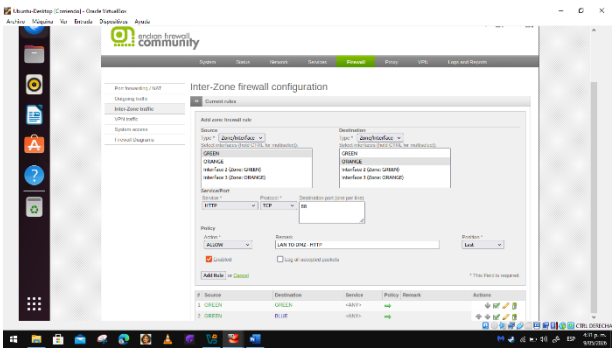
Fuente: Autoría propia

Se añaden las reglas. Se presenta la siguiente plantilla para configurar todas y cada una de las reglas.

Son 2 reglas por conexión entre zonas aplicando los dos servicios que ocupamos para este artículo: HTTP y FTP
Puertos:
HTTP: 80
FTP: 21
Protocolo:
TCP
Acción: ALLOW
Status: Enabled
Para crear las reglas, hacemos click en “Add a new inter-zone firewall rule”
Reglas para Verde (LAN) ↔ Naranja (DMZ)

- Green-Orange a LAN TO DMZ (HTTP)
- Green-Orange a LAN TO DMZ (FTP)

Fig. 36. Configuración de reglas Verde (LAN) ↔ Naranja (DMZ)



Fuente: Autoría propia

Reglas para Internet (WAN) ↔ DMZ

En los casos de la Zona Roja (RED), establecemos el tipo de Origen/Destino en <ANY>, (RED de las reglas de la temática 2).

- Red-Orange a WAN TO DMZ (HTTP)
- Red-Orange a WAN TO DMZ (FTP)

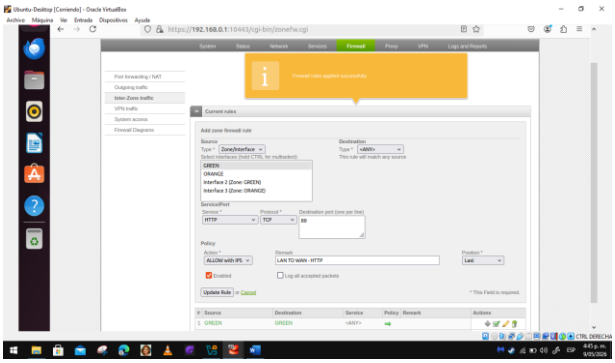
Fig. 37. Configuración de Reglas para Internet (WAN) ↔ DMZ

Fuente: Autoría propia

Reglas para LAN → WAN

- Green-Red à LAN TO WAN (HTTP)
- Green-Red à LAN TO WAN (FTP)

Fig. 38. Configuración de reglas para LAN → WAN

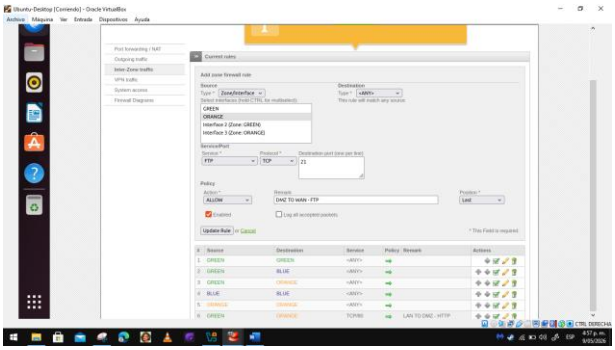


Fuente: Autoría propia

Reglas para DMZ → WAN

- Orange-Red à LAN TO WAN (HTTP)
- Orange-Red à LAN TO WAN (FTP)

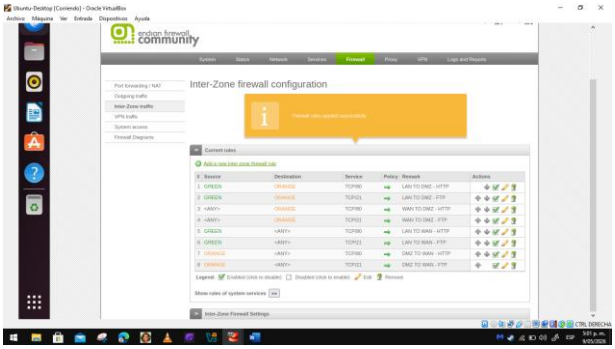
Fig. 39. Configuración de reglas



Fuente: Autoría propia

Se aplican los cambios de todas las reglas.

Fig. 40. Reglas de Acceso



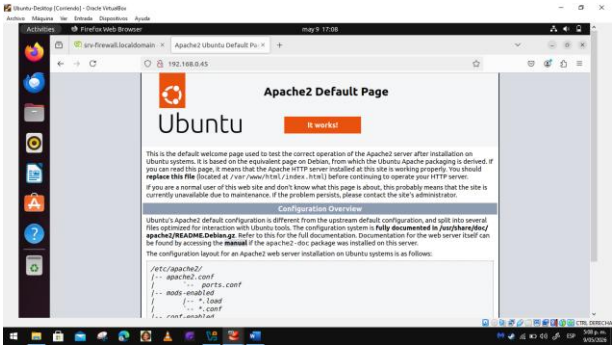
Fuente: Autoría propia.

Con las reglas ya configuradas, procedemos a hacer las pruebas pertinentes.

Prueba 1: LAN→DMZ

Se abre la dirección ip del servidor por medio del navegador del Desktop para comprobar que servicios como apache estén activos. Se verifica instalación de apache en el DMZ (servidor) y verificar que esté activo con un systemctl status apache2 en el ubuntu server. Luego, en el desktop se ingresa: http://192.168.0.45

Fig. 41. Acceso web al servidor



Fuente: Autoría propia

Ahora, en la terminal del desktop, usamos curl -I http://192.168.0.45 para comprobar acceso por terminal.

Fig. 42. Acceso terminal al servidor

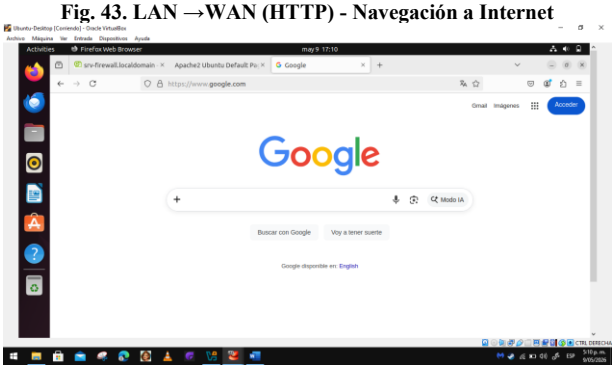
```
root@Ubuntu-Desktop:~# curl -I http://192.168.0.45
HTTP/1.1 200 OK
Date: Sat, 09 May 2026 22:15:52 GMT
Server: Apache
Upgrade: h2,h2c
Connection: Upgrade
Last-Modified: Tue, 21 Apr 2026 19:52:54 GMT
ETag: "29af-64ffdc2de4de4"
Accept-Ranges: bytes
Content-Length: 10671
Vary: Accept-Encoding
Content-Type: text/html

root@Ubuntu-Desktop:~#
```

Fuente: Autoría propia

Prueba 2: LAN → WAN (HTTP) - Navegación a Internet

Se repite los mismos pasos de la prueba anterior para confirmar la salida a internet. Podemos hacer una búsqueda cualquiera, usaremos en este caso: http://www.google.com
Navegador web:

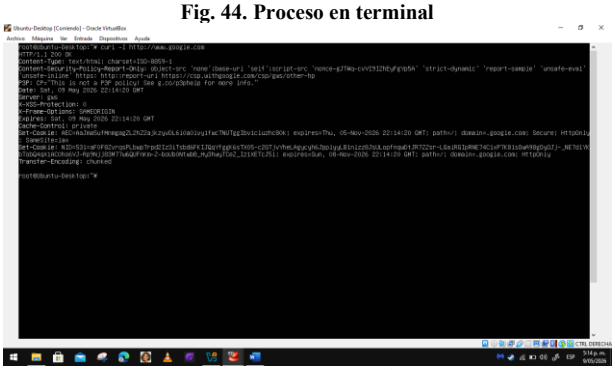
Fig. 43. LAN →WAN (HTTP) - Navegación a Internet



Fuente: Autoría propia

Terminal:

Fig. 44. Proceso en terminal



Fuente: Autoría propia

Prueba 3: DMZ → WAN (HTTP) - Servidor DMZ sale a Internet
Comandos date && curl -I http://www.ubuntu.com o cualquier otra página web como google

Fig. 45. Salida a internet DMZ - WAN

Fuente: Autoría propia

Prueba 4: WAN → DMZ (HTTP) - Acceso externo al servidor web
Desde la consola de Endian (que tiene acceso a todas las zonas):

ssh root@192.168.0.1

Si pide contraseña se usa la configurada en el Wizard.

Desde Endian, se simula acceso externo al servidor DMZ:

curl -I http://192.168.0.45

Se confirma con un mensaje HTTP/1.1 200 OK

Fig. 46. ssh al servidor desde ENDIAN

Fuente: Autoría propia

Prueba 5: LAN → WAN (FTP)

Se conecta al servidor FTP externo (simulado):

Se usa ftp.gnu.org como destino externo real:

date && ftp -n ftp.gnu.org

En el prompt de FTP:

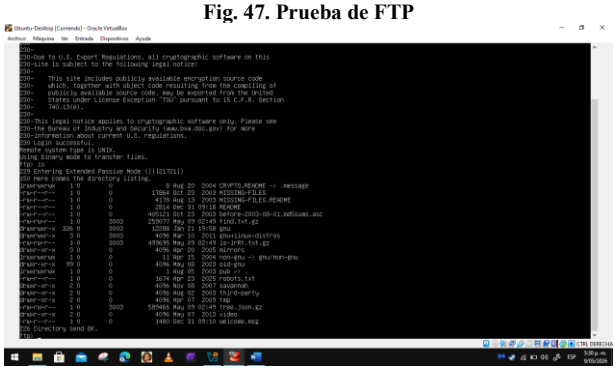
ftp> user anonymous

ftp> ls

ftp> quit

Si conecta, se debe permitir listar con ls y confirmar con un mensaje de login successful.

Fig. 47. Prueba de FTP



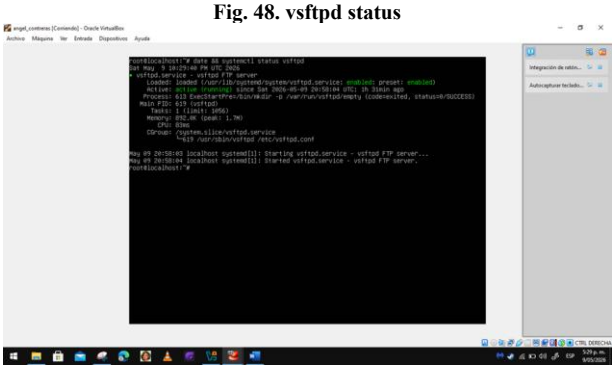
Fuente: Autoría propia

Prueba 6: WAN → DMZ (FTP) - Acceso FTP externo al servidor DMZ

Desde Ubuntu-Server-DMZ, se verifica que vsftpd esté corriendo:

date && sudo systemctl status vsftpd

Fig. 48. vsftpd status



Fuente: Autoría propia

Desde Ubuntu-LAN-Cliente (simulando acceso externo):

ftp 192.168.0.45

Name: usuario del servidor (en mi caso fue "angel_contreras")

Password: en mi caso fue 1234

SALIDA ESPERADA: 230 Login successful.

Fig. 49. FTP → DMZ

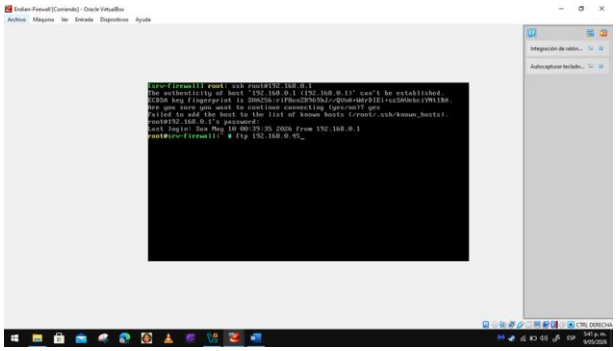
Fuente: Autoría propia

Desde Endian (simulando WAN):

ssh root@192.168.0.1

ftp 192.168.0.45

Fig. 50. SSH WAN→DMZ



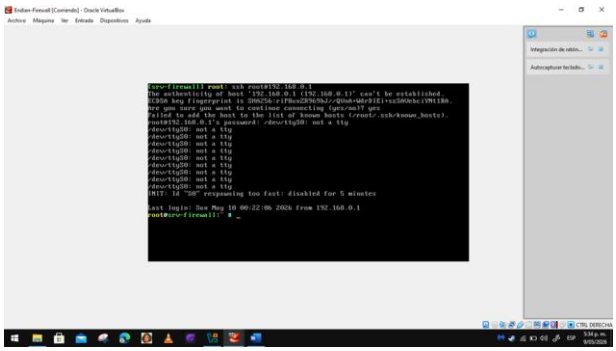
Fuente: Autoría propia

Verificación desde Consola de Endian (iptables)

Conectar a Endian:

ssh root@192.168.1.1

Fig. 51. SSH ENDIAN→WAN

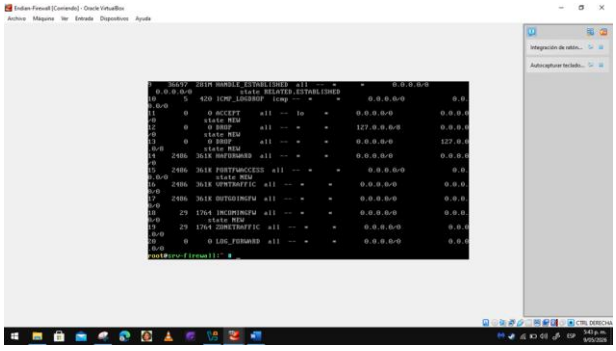


Fuente: Autoría propia

Ver todas las reglas del firewall con contadores:

iptables -L FORWARD -n -v --line-numbers

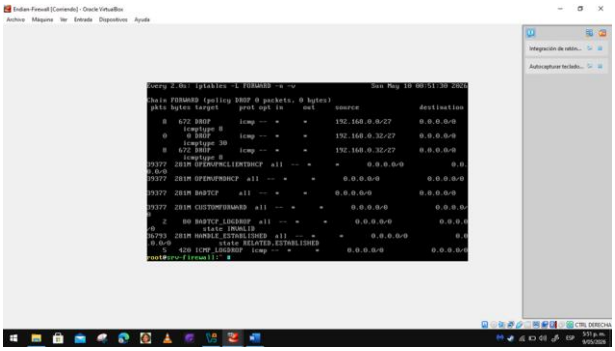
Fig. 52. Reglas Firewall



Fuente: Autoría propia

Ahora, se ejecuta el comando: watch -n 2 'iptables -L FORWARD -n -v'

Fig. 53. Conteo

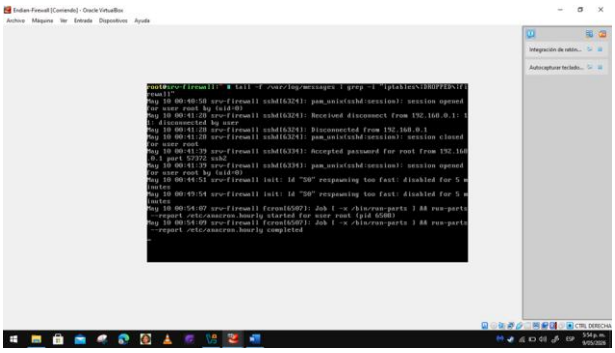


Fuente: Autoría propia

Nota: Para volver al control de la terminal, ctrl + c.

Se Verifica los logs del firewall para ver qué está siendo bloqueado:tail -f /var/log/messages | grep -i "iptables\|DROPPED\|firewall"

Fig. 54. logs del Firewall

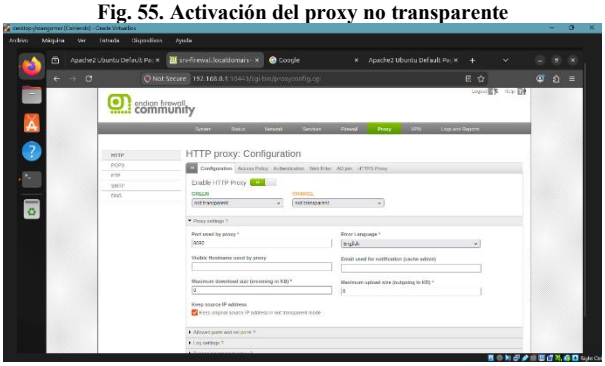


Fuente: Autoría propia

4.5 Temática 5: Proxy HTTP No Transparente con Autenticación

Para la implementación del Proxy HTTP no transparente se utilizó Endian Firewall como servidor proxy basado en Squid. En primer lugar, se habilitó el servicio proxy HTTP desde la interfaz web de Endian en la sección Proxy ----> HTTP, configurándolo en modo no transparente sobre la interfaz GREEN con el puerto 8080.

Fig. 55. Activación del proxy no transparente



Fuente: Autoría propia

Posteriormente se creó un perfil de filtrado con una lista negra de dominios que contiene los siguientes: www.hotmail.com, www.youtube.com y www.elnuevodia.com.co.

Fig. 56. Activación del proxy no transparente

Fuente: Autoría propia

Posteriormente se configuró la autenticación local, se creó el usuario *estudiante_1* como usuario para acceder. Este usuario fue asociado al grupo *Usuarios_LAN*, y se le vinculó una política de acceso que exige autenticación y aplica el perfil de filtrado creado.

Fig. 57. Creación del usuario

Fuente: Autoría propia

Fig. 58. Creación del grupo y asignación del usuario estudiante_1

Fuente: Autoría propia

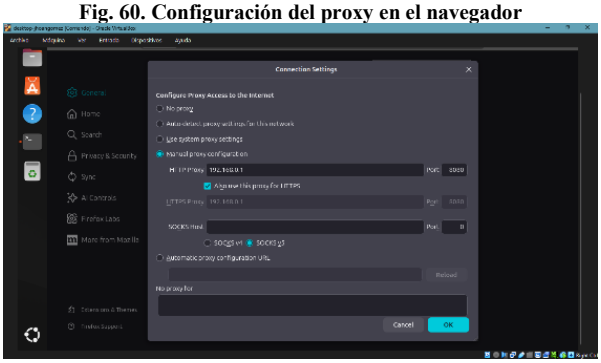
Para la configuración de la política se debe definir la ip la cual es 192.168.0.1 que apunta a Endian, se configura para que la autenticación sea basada en el grupo del usuario.

Fig. 59. Creación de la política de acceso a la red

Fuente: Autoría propia

Para que funcione adecuadamente el proxy es necesario que el cliente lo configure en su navegador, la ip de este debe apuntar a Endian quien se encarga de redirigir el tráfico.

Fig. 60. Configuración del proxy en el navegador

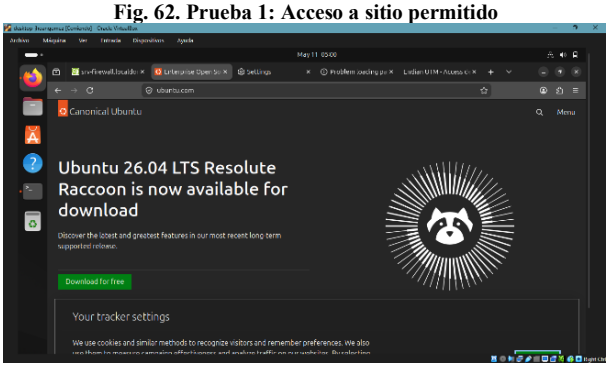


Fuente: Autoría propia

Fig. 61. Solicitud de autenticación al acceder al navegador

Fuente: Autoría propia

Fig. 62. Prueba 1: Acceso a sitio permitido

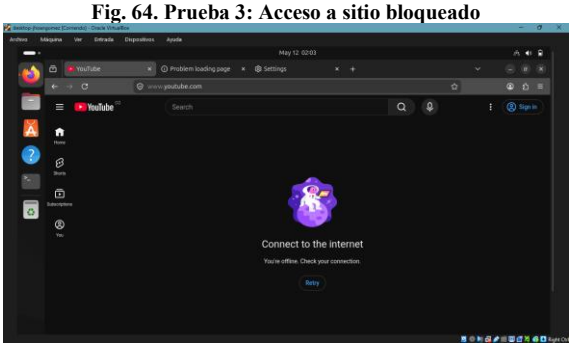


Fuente: Autoría propia

Fig. 63. Prueba 2: Acceso a sitio bloqueado (hotmail.com)

Fuente: Autoría propia

Fig. 64. Prueba 3: Acceso a sitio bloqueado

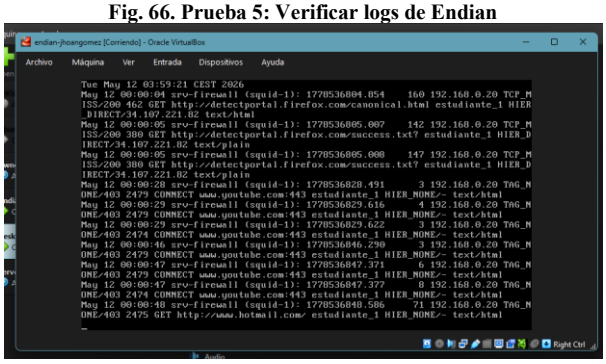


Fuente: Autoría propia

Fig. 65. Prueba 4: Acceso a sitio bloqueado

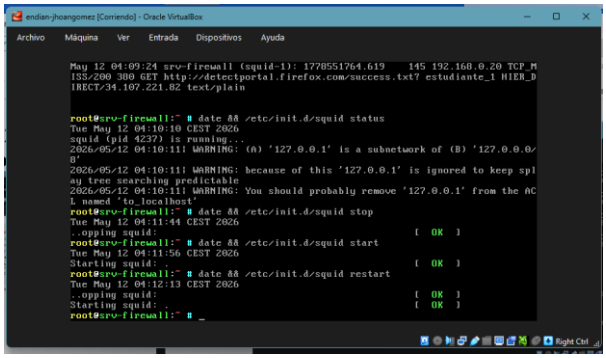
Fuente: Autoría propia

Fig. 66. Prueba 5: Verificar logs de Endian



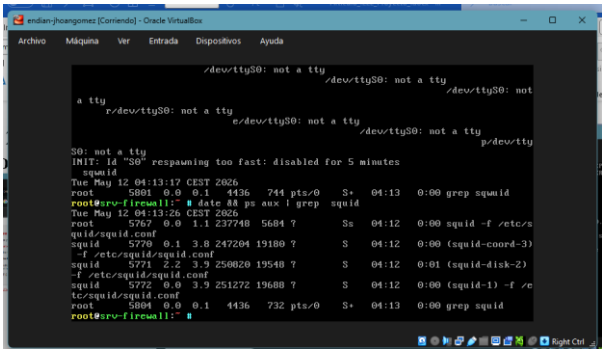
Fuente: Autoría propia

Fig. 67. Prueba 6: Verificar servicios desde la consola



Fuente: Autoría propia

Fig. 68. Prueba 6: Verificar que el proceso está corriendo



Fuente: Autoría propia

Para poder hacer uso de este proxy las personas deben configurar su propio proxy manualmente en su navegador para acceder a Internet.

5 CONCLUSIONES

Es indispensable la adecuada segmentación y configuración de la red para garantizar el funcionamiento, las zonas deben tener una subred diferente y cada interfaz con su propio segmento, se debe verificar el estado de las interfaces, las máscaras correctas y el Gateway para cada zona; existe comunicación de la zona verde al servidor por tanto la configuración es exitosa, La validación de zonas consistió en comprobar la correcta segmentación de subredes, configuración de Gateway, conectividad interna y aplicación de políticas de seguridad.

Efectividad de la traducción de direcciones: Se ha comprobado que la implementación de la regla MASQUERADE en la cadena de SOURCENAT es fundamental para la seguridad perimetral, ya que permite que los dispositivos internos de la LAN y la DMZ naveguen hacia internet ocultando su direccionamiento privado bajo la IP de la interfaz WAN. Asimismo, la verificación de las tablas de rutas y el estado de las interfaces confirma que el Firewall gestiona correctamente la segmentación, permitiendo un acceso controlado y seguro hacia el exterior sin comprometer la integridad de la infraestructura interna.

La integración de directivas de seguridad en el segmento perimetral demuestra que es viable mantener la operatividad de servicios públicos críticos sin exponer la topología interna de la organización, permitiendo únicamente el tráfico estrictamente necesario y bloquear los protocolos de reconocimiento como ICMP, se mitiga el riesgo de escaneo de red por parte de agentes externos. Con el levantamiento de reglas garantizamos que nuestro Firewall actúe de forma estricta para garantizar que las zonas no se comuniquen entre sí sin un permiso específico. Incluso si un servidor en la DMZ es comprometido, la red interna (LAN) permanezca

protegida al no haber permisos de acceso libre desde la zona naranja hacia la verde.

La implementación del Proxy HTTP no transparente en Endian Firewall permitió controlar la navegación de los usuarios de la red LAN mediante autenticación y lista negra. Se verificó el bloqueo efectivo de sitios HTTP restringidos y el correcto funcionamiento de squid.

6 REFERENCIAS

[1] Oracle Corporation, *Oracle VM VirtualBox*, v. 7.0. Palo Alto, CA, USA: Oracle Corp., 2024.

[2] Canonical, *Guía del Ubuntu desktop 20.04 LTS*, Help Ubuntu, 2023. [En línea]. Disponible en: https://help.ubuntu.com/

[3] Á. J. Cervelión Bastidas, "Instalación de Nagios Core 4.4 en Ubuntu 22.04," Repositorio Institucional UNAD, Objeto Virtual de Información (OVI), ene. 27, 2023. [En línea]. Disponible en: https://repository.unad.edu.co/handle/10596/54230

[4] Debian Project, *El manual del administrador de Debian 12.5.0*, 2023. [En línea]. Disponible en: https://www.debian.org/releases/stable/amd64/index.es.html

[5] Endian, *Endian UTM 3.2 Manual de referencia*, 2016. [En línea]. Disponible en: https://docs.endian.com/3.2/utm/index.html

[6] Linux Professional Institute (LPI), "Tema 101: Arquitectura del Sistema," *Linux Essentials*, 2022. [En línea]. Disponible en: https://learning.lpi.org/es/learning-materials/101-500/101/101.1/101.1_01/

[7] J. LaCroix, *Mastering Ubuntu Server: Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting Ubuntu Server*, Packt Publishing, 2020. [En línea]. Disponible en: https://research-ebsco-com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b41952

[8] Linux Professional Institute (LPI), "Certificaciones," 2026. [En línea]. Disponible en: https://www.lpi.org/es/our-certifications/open-source-essentials/

[9] Oracle, *Manual de usuario VirtualBox*, VirtualBox documentation, 2020. [En línea]. Disponible en: https://www.virtualbox.org/manual/

[10] Universidad Nacional Abierta y a Distancia (UNAD), "Guía de aprendizaje - Etapa 7 - Implementando Seguridad en GNU/Linux," en *Diplomado de profundización en administración de sistemas operativos open source con certificación en Linux*, 2026. [En línea]. Disponible en: https://campus151.unad.edu.co/ses62/mod/resource/view.php?id=4464