# SOLUCIÓN EN SEGURIDAD PERIMETRAL PARA REDES SEGMENTADAS CON GNU/LINUX ENDIAN

Luis Enrique Vergara Clavijo
e-mail: levergaracl@unadvirtual.edu.co
Diego Efrain Solarte Quintero
e-mail: desolarteq@unadvirtual.edu.co
Jhonnyer Alexander González Ospina
e-mail: jagonzalezosp@unadvirtual.edu.co
Andrés Julián Montenegro Luango
e-mail: ajmontenegrol@unadvirtual.edu.co
Maryely Andrea Grajales Narvaez
e-mail: magrajalesn@unadvirtual.edu.co

**RESUMEN:** *Este artículo presenta la implementación de una arquitectura integral de seguridad perimetral en entornos GNU/Linux, orientada a la protección de infraestructuras LAN, WAN y DMZ mediante el uso de la distribución Endian Firewall Community (EFW) en entornos virtualizados. El trabajo aborda de manera conjunta cinco temáticas fundamentales: configuración inicial de Endian con segmentación de zonas de seguridad, implementación de reglas NAT para la traducción y enrutamiento de tráfico, habilitación y restricción de servicios críticos en la DMZ, definición de políticas de control de acceso interzona y despliegue de un proxy HTTP con autenticación y filtrado de navegación. Cada temática se desarrolla mediante una combinación de configuración inicial por consola y administración centralizada a través de la interfaz web de Endian, aplicando principios de administración segura, monitoreo de servicios y políticas de defensa perimetral. Como resultado, se consolida una solución escalable que fortalece la confidencialidad, integridad y disponibilidad de servicios web y de red, permitiendo gestionar de forma centralizada la seguridad de plataformas GNU/Linux empresariales. Este enfoque evidencia la importancia de integrar herramientas de firewall, segmentación de red, control de tráfico y autenticación para la protección efectiva de servicios críticos en infraestructuras de código abierto.*

**PALABRAS CLAVE**: distribución Endian Firewall, DMZ, LAN, seguridad perimetral, WAN.

## 1 INTRODUCCIÓN

La seguridad informática en infraestructuras empresariales representa un componente esencial para garantizar la continuidad operativa y la protección de servicios críticos frente a amenazas internas y externas. En entornos basados en GNU/Linux, la implementación de soluciones de seguridad perimetral permite establecer mecanismos de defensa robustos mediante la segmentación de redes, el control de tráfico y la administración segura de servicios.

En este contexto, la actividad grupal desarrollada se enfoca en el diseño e implementación de una infraestructura de seguridad utilizando GNU/Linux Endian como plataforma central de firewall, permitiendo separar y proteger las zonas LAN, WAN y DMZ dentro de una arquitectura organizacional simulada. A través del desarrollo de cinco temáticas complementarias, se integran procesos de configuración de red, reglas NAT, publicación segura de servicios HTTP y FTP, control de acceso entre zonas y políticas de navegación autenticada mediante proxy.

El presente estudio evidencia cómo las soluciones open source basadas en GNU/Linux pueden implementarse eficazmente para fortalecer infraestructuras empresariales mediante segmentación de red, control de tráfico, publicación segura de servicios y políticas avanzadas de navegación, consolidando un modelo escalable de seguridad perimetral alineado con buenas prácticas de ciberseguridad.

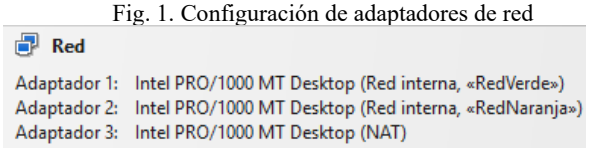
## 2 METODOLOGÍA

Para el desarrollo de esta actividad se requiere la utilización de 3 máquinas virtuales con distribuciones Linux: la primera es el host con Linux Ubuntu Desktop, la segunda es el servidor con Linux Ubuntu Server y la tercera máquina es el Firewall con la distribución Endian, la cual contará con 3 adaptadores de red [1] que se configurarán teniendo en cuenta el siguiente escenario:

- **Adaptador 1:** Red verde (192.168.38.1)
- **Adaptador 2:** Red naranja (10.0.38.1)
- **Adaptador 3:** Red roja – NAT

A continuación, se evidencia la activación de los adaptadores mencionados:

Fig. 1. Configuración de adaptadores de red




Fuente: Autoría propia

# 3 CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN

Luego de configurar los parámetros de hardware en la máquina virtual para la instalación de Endian [2] y de añadir la imagen ISO de la distribución descargada de la pagina oficial, se procede a iniciar el equipo empezando a configurar el idioma en inglés.

Fig. 2. Selección del lenguaje


Fuente: Autoría propia

Se continua con el siguiente paso de bienvenida para lo cual se selecciona la opción Ok.

Fig. 3. Mensaje de bienvenida


Fuente: Autoría propia

En la siguiente imagen se informa que el disco duro de la maquina será borrado completamente y particionado, entonces, se procede confirmando esta acción con Yes.

Fig. 4. Preparación del disco duro


Fuente: Autoría propia

El siguiente paso nos solicita elegir si se desea la habilitación de la consola por el puerto serial. En esta pantalla se escoge la opción Yes.

Fig. 5. Activación de consola


Fuente: Autoría propia

A continuación, se realiza la configuración de la interfaz verde, teniendo en cuenta la ip establecida para esta zona: 192.168.38.1 con mascara 24.

Fig. 6. Configuración de la interfaz verde


Fuente: Autoría propia

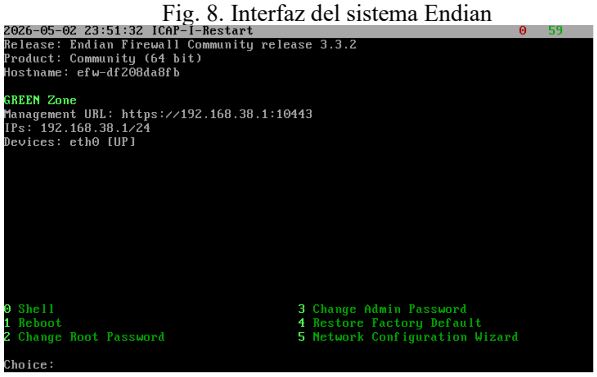
Para finalizar la instalación, la siguiente pantalla evidencia la instalación completa del sistema Endian y la información de la URL para acceder desde navegador a continuar con los ajustes requeridos.

Fig. 7. Instalación completa


Fuente: Autoría propia

Al reiniciarse la maquina virtual, el sistema Endian se inicia correctamente mostrando la interfaz inicial, con la zona verde activa, lo cual indica la activación del servicio de firewall listo para los ajustes deseados.

Fig. 8. Interfaz del sistema Endian




Fuente: Autoría propia

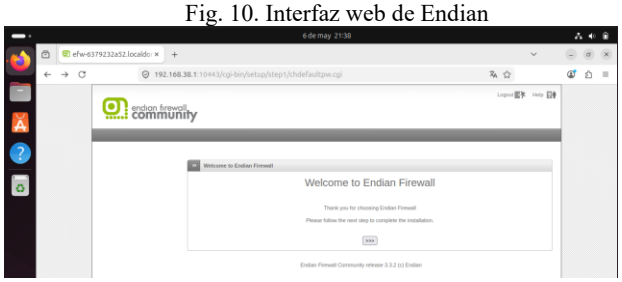
Se puede observar en la Fig 9 el acceso a la máquina virtual de Ubuntu Desktop, la cual se ajusta con adaptador en red interna hacia la RedVerde. Por DHCP toma la ip 192.168.38.2/24.

Fig. 9. Configuración ip de la máquina cliente Ubuntu

Fuente: Autoría propia

Se realiza ingreso al panel administración web de Endian por la URL sugerida en la interface de Endian https://192.168.38.1:10443

Fig. 10. Interfaz web de Endian




Fuente: Autoría propia

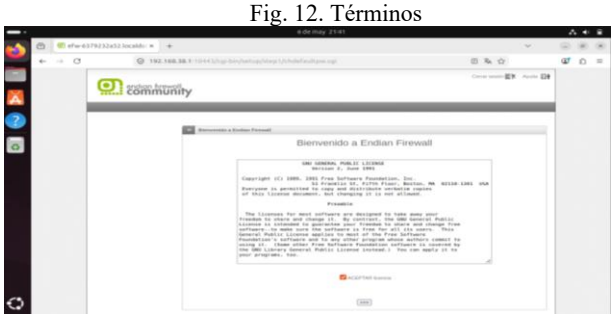
Se procede con la selección del idioma español y región para el panel de administración web de Endian.

Fig. 11. Idioma en portal de Endian


Fuente: Autoría propia

Se aceptan los términos y condiciones.

Fig. 12. Términos




Fuente: Autoría propia

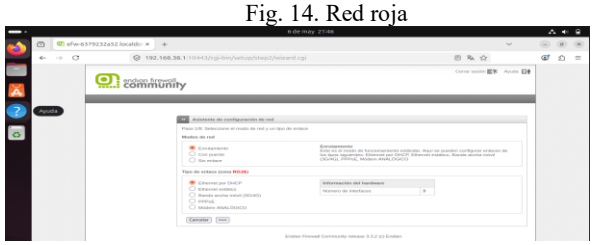
Se establece la contraseña del usuario admin del panel de administración web y del usuario root de Endian.

Fig. 13. Configuración usuarios de administración

Fuente: Autoría propia

En la siguiente evidencia se observa la configuración de la zona roja, lo cual se deja por defecto como está.

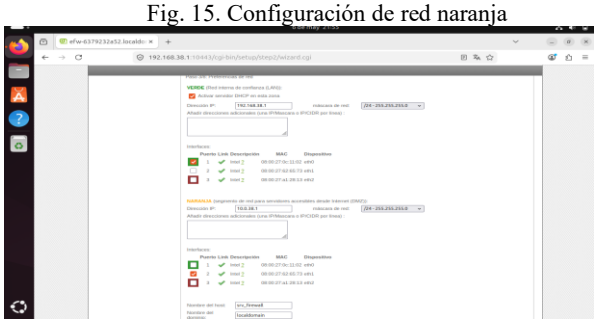
Fig. 14. Red roja



Fuente: Autoría propia

A continuación de selecciona la zona naranja para proceder con la configuración con la ip 10.0.38.1/24 y cuyo nombre será srv_firewall.

Fig. 15. Configuración de red naranja



Fuente: Autoría propia

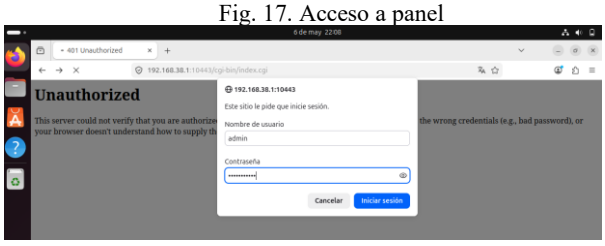
Se evidencia que las 3 zonas necesarias están activas, se dejan los DNS como automáticos, se siguen los siguientes pasos sin modificar nada y se aplican los ajustes.

Fig. 16. Verificación de zonas

Fuente: Autoría propia

Se realiza el logueo con las credenciales de admin.

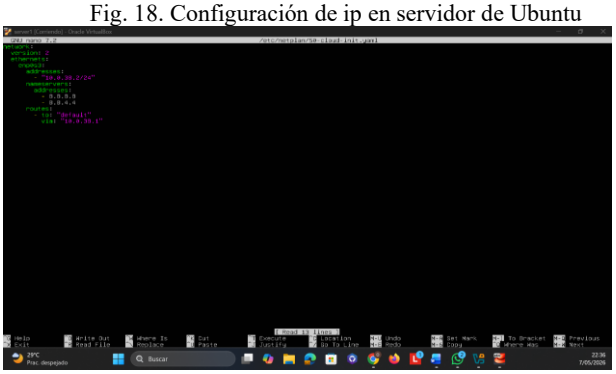
Fig. 17. Acceso a panel




Fuente: Autoría propia

Se asigna la dirección ip 10.0.38.2 con puerta de enlace 10.0.38.1 y DNS 8.8.8.8 en el servidor, para lo cual se hace necesario modificar el archivo de configuración /etc/netplan/50-cloud-init.yaml.

Fig. 18. Configuración de ip en servidor de Ubuntu



Fuente: Autoría propia

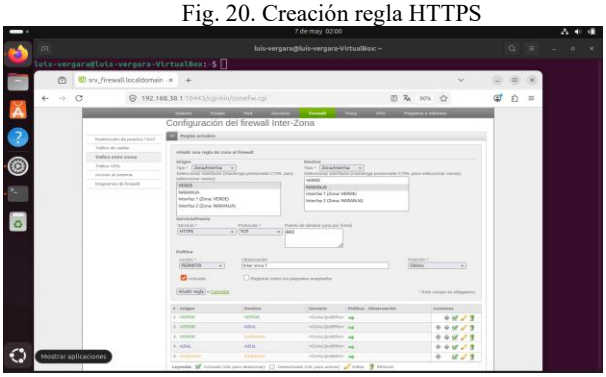
Se reinicia el servidor, se verifica la dirección ip con ifconfig y se procede a ejecutar un ping a la puerta de enlace con ping -c 6 10.0.38.1, como se evidencia en la Fig 19.

Fig. 19. Comunicación en servidor

Fuente: Autoría propia

Ahora se procede a configurar las reglas de firewall Inter – Endian UTM Firewall entre la zona Verde (origen) y Naranja (destino) en este caso para acceder solo a los servicios (HTTPS 443), la configuración aplicada se muestra en la imagen.

Fig. 20. Creación regla HTTPS




Fuente: Autoría propia

Para verificar que la regla se creó con éxito se ingresa a la URL https://10.0.38.1 en la cual cargará un formulario de registro con conexión a una base de datos previamente configurada.

Fig. 21. Prueba de HTTPS


Fuente: Autoría propia

# 4 CONFIGURACIÓN NAT

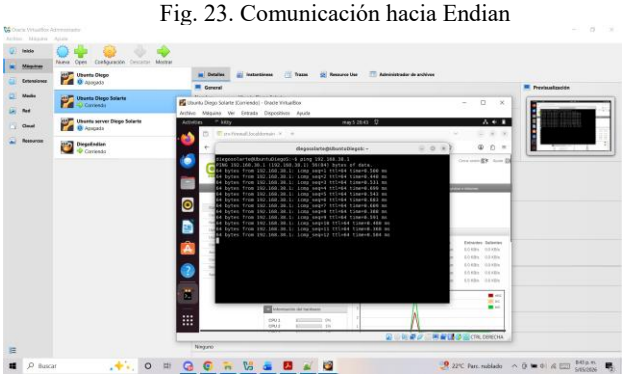
Se verifica que la máquina Ubuntu desktop esté dentro del rango de la zona verde, en este caso se generó por DHCP la ip 192.168.38.2 que se encuentra correcta.

Fig. 22. Direccionamiento del host

Fuente: Autoría propia

Se valida que la maquina Ubuntu desktop tenga comunicación con Endian por medio de ping hacia la ip 192.168.38.1

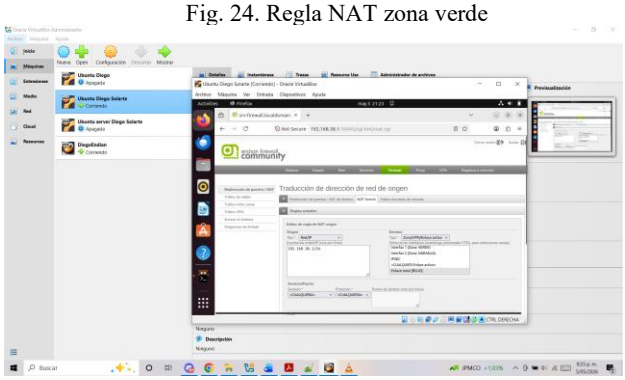
Fig. 23. Comunicación hacia Endian



Fuente: Autoría propia

Se procede con la configuración de la regla NAT para la salida a internet por la zona verde [3].

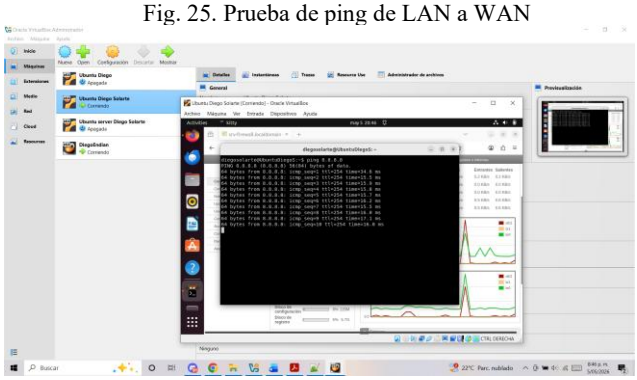
Fig. 24. Regla NAT zona verde



Fuente: Autoría propia

Se valida que se tenga navegación en el equipo desktop, realizando un ping hacia los dns de Google 8.8.8.8

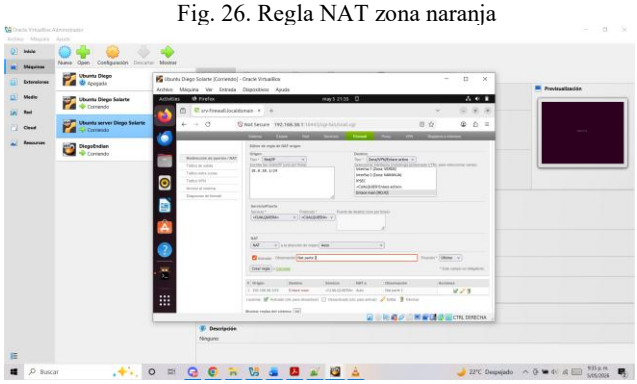
Fig. 25. Prueba de ping de LAN a WAN



Fuente: Autoría propia

Ahora, se genera una regla NAT para la salida a internet de la zona naranja [4].

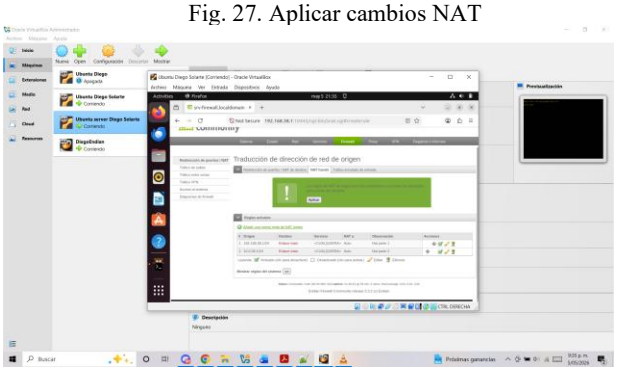
Fig. 26. Regla NAT zona naranja



Fuente: Autoría propia

Se aplican los cambios para guardar las configuraciones de las reglas NAT.

Fig. 27. Aplicar cambios NAT



Fuente: Autoría propia

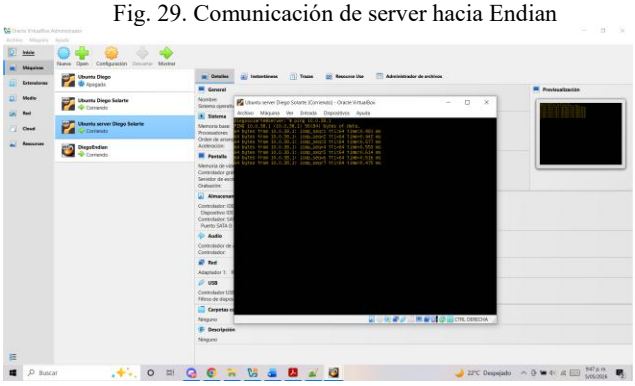
Se verifica que la máquina Ubuntu server esté en la zona naranja, la máquina tiene asignada por defecto la ip 10.0.38.10 que se encuentra dentro de la red naranja.

Fig. 28. Direccionamiento del server

Fuente: Autoría propia

Se realiza la validacion de comunicación entre la maquina server y el Endian por medio de ping.

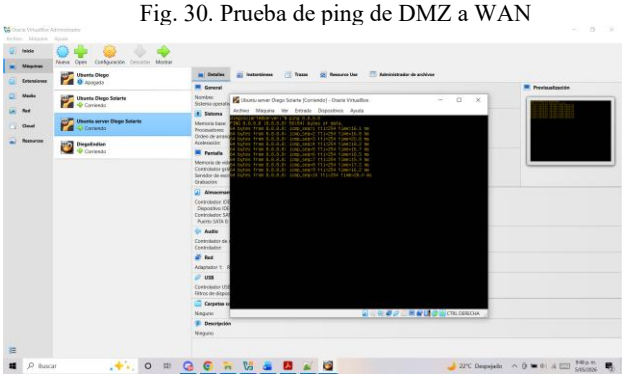
Fig. 29. Comunicación de server hacia Endian



Fuente: Autoría propia

Se confirma tambien que desde el servidor se tenga acceso a internet por medio de ping hacia 8.8.8.8

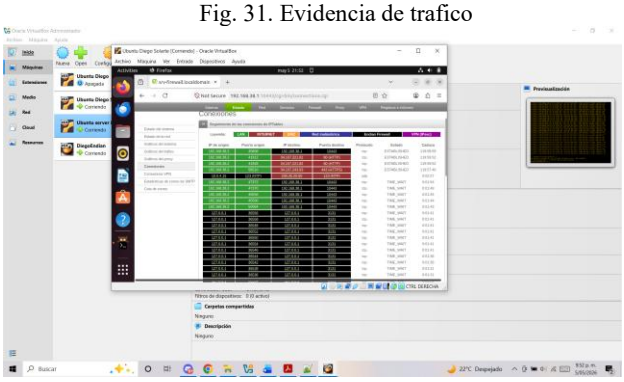
Fig. 30. Prueba de ping de DMZ a WAN



Fuente: Autoría propia

Se verifica la existencia de trafico revisando en el dashboard del portal de Endian el estado de las conexiones.

Fig. 31. Evidencia de trafico



Fuente: Autoría propia

# 5 PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

Se deshabilitan todas las reglas del tráfico de salida que están creadas predeterminadas.

Fig. 32. Configuración del firewall de salida


Fuente: Autoría propia

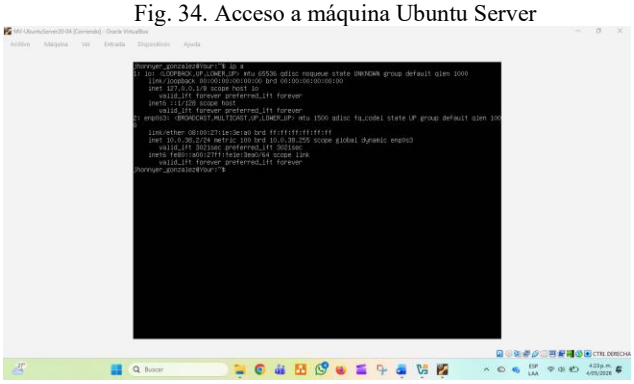
Se desactivan las reglas predeterminadas del tráfico entre zonas.

Fig. 33. Configuración del firewall inter-zona


Fuente: Autoría propia

Se realiza acceso a la máquina virtual de Ubuntu Server, la cual se ajustó con adaptador en red interna hacia la RedNaranja. Por DHCP toma la ip 10.0.38.2/24.

Fig. 34. Acceso a máquina Ubuntu Server



Fuente: Autoría propia

Al intentar acceder a la URL http://10.0.38.2 se evidencia que la página no carga bajo el Ubuntu Server.

Fig. 35. Prueba de servicio HTTP sin reglas


Fuente: Autoría propia

La siguiente evidencia nos muestra que no se tiene acceso a ftp 10.0.38.2

Fig. 36. Prueba de servicio FTP sin reglas


Fuente: Autoría propia

Desde la configuración de firewall inter-zona se crea la regla para permitir acceso al servicio HTTP [5] con el puerto 80 desde la zona verde hacia la zona naranja.

Fig. 37. Creación de regla para servicio HTTP

Fuente: Autoría propia

Desde la misma configuración de tráfico entre zonas se genera la regla para permitir acceso al servicio FTP por el puerto 21 desde la zona verde hacia la zona naranja.

Fig. 38. Creación de regla para servicio FTP

Fuente: Autoría propia

Se observa que las reglas anteriores quedaron creadas y activas de manera correcta, las cuales corresponden a las reglas 6 y 7 en este caso.

Fig. 39. Configuración de reglas HTTP y FTP


Fuente: Autoría propia

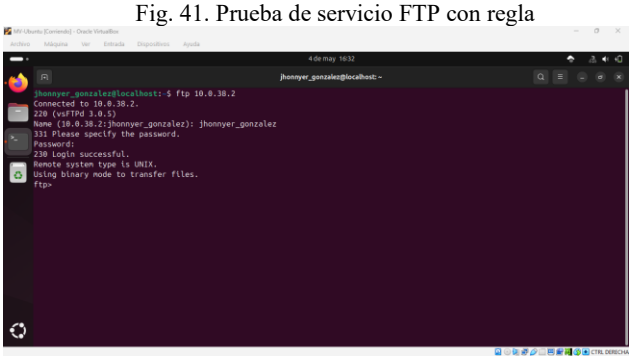
Al verificar nuevamente el acceso a http://10.0.38.2 se evidencia que ya carga un servicio del servidor de Ubuntu, en este caso el portal de ownCloud.

Fig. 40. Prueba de servicio HTTP con regla


Fuente: Autoría propia

Al verificar nuevamente el acceso por consola a ftp 10.0.38.2, se evidencia que ya se obtiene acceso al servidor Ubuntu por medio del servicio de transferencia de archivos [6].

Fig. 41. Prueba de servicio FTP con regla




Fuente: Autoría propia

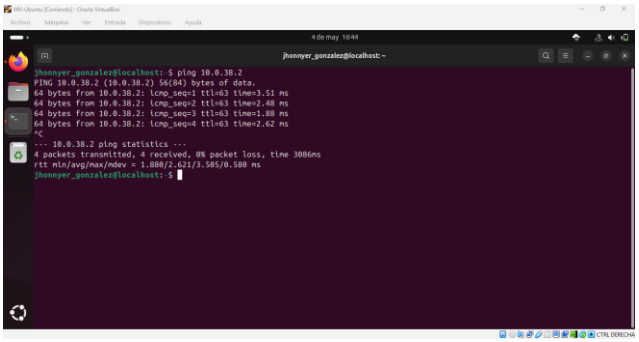
A manera de prueba, se configura una regla para permitir el protocolo ICMP.

Fig. 42. Permitir el protocolo ICMP

Fuente: Autoría propia

La siguiente imagen nos evidencia que al realizar ping hacia la ip del servidor Ubuntu 10.0.38.2, esta responde de manera correcta.

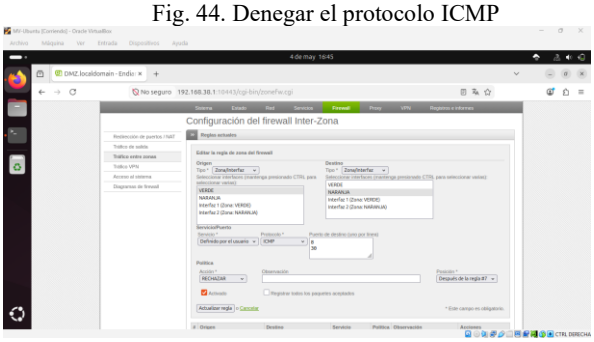
Fig. 43. Prueba de ping con protocolo ICMP




Fuente: Autoría propia

Como se debe denegar el protocolo, se procede a realizar el ajuste para rechazar el servicio ICMP desde la zona verde hacia la naranja en el tráfico entre zonas.

Fig. 44. Denegar el protocolo ICMP




Fuente: Autoría propia

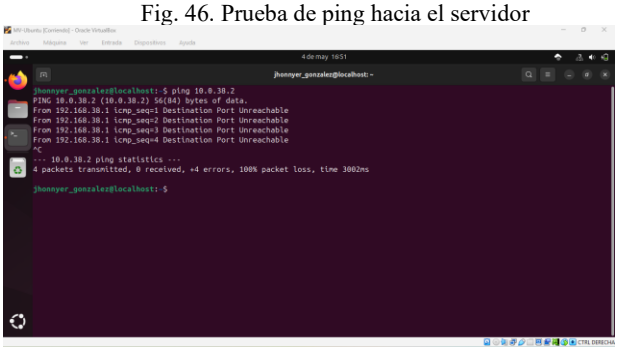
La siguiente evidencia nos muestra la regla ajustada para denegar el protocolo ICMP desde el firewall inter-zona. Toma como numero de regla el 8.

Fig. 45. Evidencia de ajuste en la regla inter-zona


Fuente: Autoría propia

Al realizar ping nuevamente a la ip 10.0.38.2 se evidencia que no alcanza el destino, lo cual indica que la regla queda configurada de manera correcta.

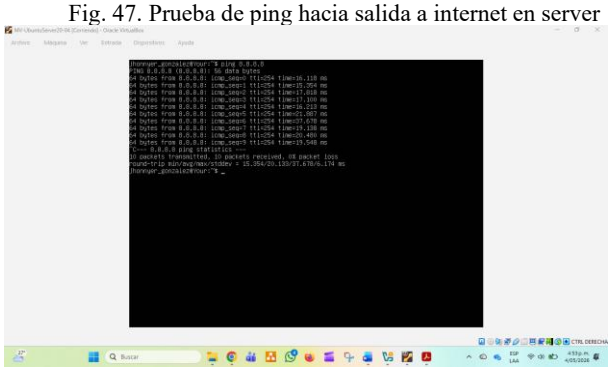
Fig. 46. Prueba de ping hacia el servidor




Fuente: Autoría propia

Al hacer ping a los dns de Google 8.8.8.8 se evidencia que responde, lo cual indica conexión de internet en el server.

Fig. 47. Prueba de ping hacia salida a internet en server



Fuente: Autoría propia

Se genera una regla en el firewall de salida desde las zonas verde y naranja hacia la zona roja para denegar el protocolo ICMP con salida a internet, tanto en el host como en el server.

Fig. 48. Creación de regla para el tráfico de salida

Fuente: Autoría propia

La imagen siguiente nos muestra la regla creada para denegar el protocolo ICMP desde el firewall de salida. Toma como numero de regla el 11.

Fig. 49. Evidencia de configuración de regla de salida

Fuente: Autoría propia

Al validar nuevamente el ping desde el Server hacia 8.8.8.8, se evidencia que ya no hay comunicación.

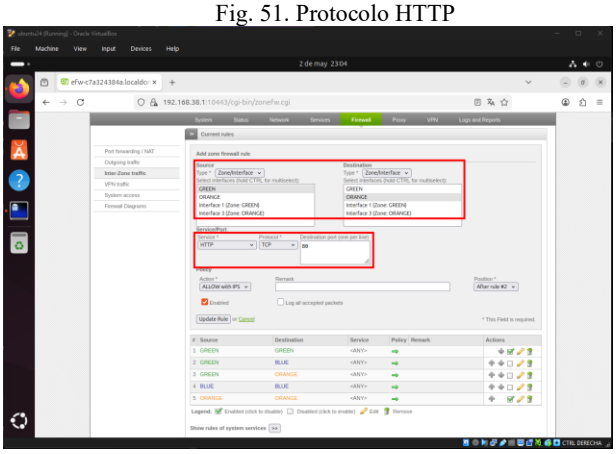
Fig. 50. Prueba de ping en Server con la regla

Fuente: Autoría propia

# 6 REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO

Se requiere permitir la comunicación entre la zona Verde y la zona Naranja con el protocolo HTTP por el puerto 80.

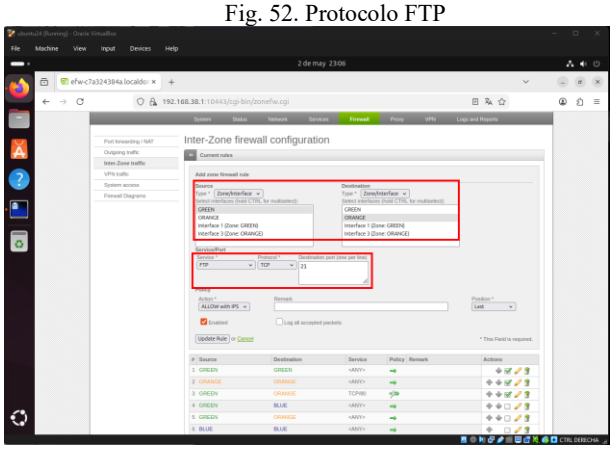
Fig. 51. Protocolo HTTP



Fuente: Autoría propia

De igual manera, se desea generar la configuracion del servicio FTP por el puerto 21.

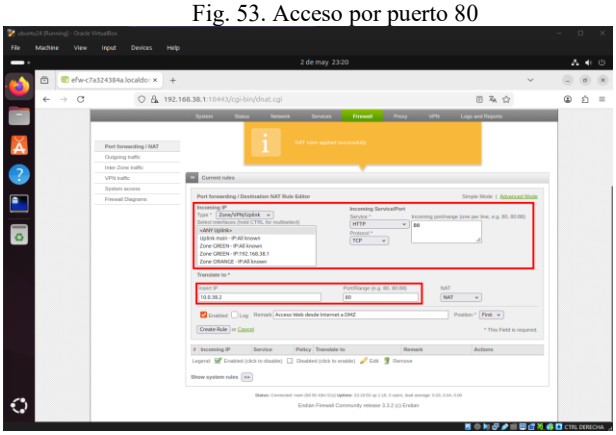
Fig. 52. Protocolo FTP




Fuente: Autoría propia

Se realiza la configuración del forwarding para permitir el acceso WEB desde la zona roja(WAN) a la zona naranja (DMZ).

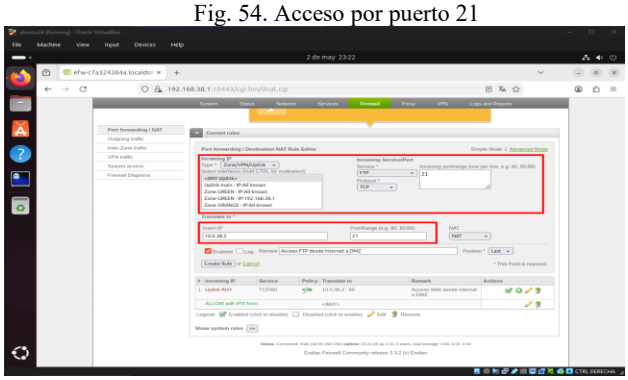
Fig. 53. Acceso por puerto 80



Fuente: Autoría propia

Se realiza la configuración del forwarding para permitir el acceso FTP desde la zona roja (WAN) a la zona naranja (DMZ).

Fig. 54. Acceso por puerto 21



Fuente: Autoría propia

Al realizar reenvío de puertos desde la zona roja hacia la DMZ, se recomienda evitar rangos amplios de puertos y limitar la exposición exclusivamente a servicios específicos, reduciendo riesgos de redirección no controlada y superficie de ataque [7].

Fig. 55. Creación de reglas para FTP y HTTP


Fuente: Autoría propia

Deshabilitar el firewall de inter-zona está totalmente desaconsejado, ya que permite que todo el tráfico fluya sin restricciones entre las zonas GREEN y ORANGE, eliminando la segmentación de seguridad [8] aunque para este caso de uso se comunican por puertos específicos.

Fig. 56. verificación del tráfico inter-zona

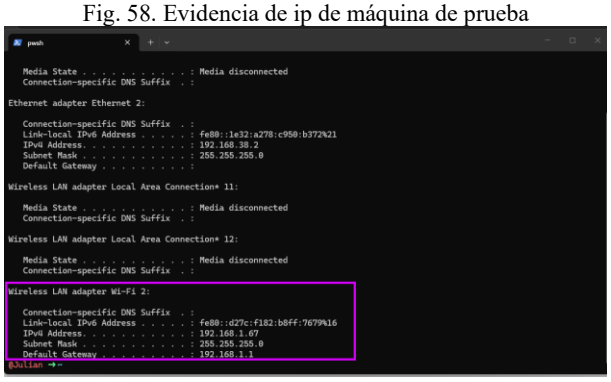

Fuente: Autoría propia

Para las validaciones se va a usar las ip de la red roja (192.168.1.73) y la de una maquina local de windows (192.168.1.67) de prueba las cuales estan conectadas a la WAN (router de un proveedor de internet).

Fig.57. Evidencia de ip roja

Fuente: Autoría propia

Fig. 58. Evidencia de ip de máquina de prueba




Fuente: Autoría propia

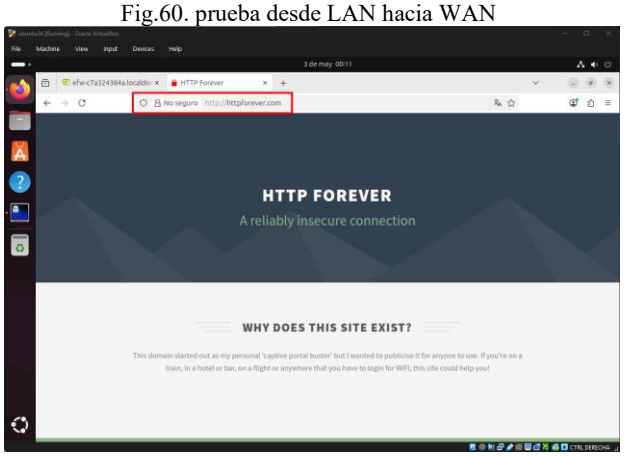
Se realiza el acceso a un portal web de ejemplo como Wordpress para realiza la validacion de acceso por HTTP en el servidor de Ubuntu (10.0.38.2)-

Fig.59. ingreso a portal web con HTTP


Fuente: Autoría propia

Se lleva a cabo la validación desde dispositivo en red LAN hacia WAN con la página http://httpforever.com

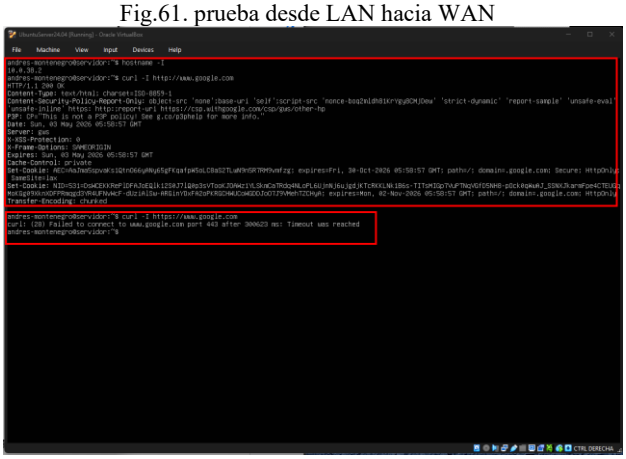
Fig.60. prueba desde LAN hacia WAN




Fuente: Autoría propia

Se valida desde línea de comandos con curl en el ubuntu server para traer la cabecera de la página http en la red WAN - con validación de no acceso otros protocolos como https.

Fig.61. prueba desde LAN hacia WAN



Fuente: Autoría propia

Fig.62. Traza de peticiones en google


Fuente: Autoría propia

Para el ingreso desde el servicio HTTP desde la WAN hacia la zona DMZ, se usa la ip que de la zona Roja asignada en el endian (192.168.1.73). Se muestra una página de prueba realizada anteriormente porque está usando el puerto 80 desde el alojamiento.

Fig. 63. prueba de acceso WAN a DMZ por HTTP


Fuente: Autoría propia

El ingreso del servicio FTP desde la LAN hacia la WAN se lleva a cabo desde el explorador de ubuntu desktop donde se accede al ftp publico de ftp://ftp.pureftp.org para validar el acceso desde la zona verde (LAN) por el puerto 21 a la (WAN)

Fig. 64. evidencia de acceso desde LAN a WAN por FTP

Fuente: Autoría propia

Por ultimo, se usa el explorador de windows con la ip de la zona Roja (192.168.1.73) para realizar la prueba de conexión al servicio ftp instalado en el ubuntu server, que permite su ingreso con credenciales.

Fig. 65. Ingreso desde WAN a DMZ por FTP

Fuente: Autoría propia

# 7 IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE) CON POLÍTICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET

Inicialmente se valida en la configuración del Proxy HTTP que el servicio se encuentre habilitado y funcionando correctamente.

Fig. 66. Servicio de Proxy


Fuente: Autoría propia

Además, se verifica que el modo transparente del Proxy HTTP esté desactivado correctamente [9], con el fin de garantizar que toda la navegación web requiera una configuración manual del proxy en los navegadores de las estaciones de trabajo de la red LAN. Esta validación permite confirmar que los usuarios deben ingresar obligatoriamente.

Fig. 67. Configuración transparente


Fuente: Autoría propia

Posteriormente se verifica la correcta creación de los perfiles de navegación configurados dentro del Proxy HTTP de Endian Firewall, validando dos perfiles diferenciados con políticas específicas de acceso y filtrado web para usuarios autenticados [10].

Fig. 68. Perfiles de navegación


Fuente: Autoría propia

Se crea una lista de acceso libre destinada a los usuarios que no presentan restricciones de navegación dentro de la red. Esta configuración permite establecer un perfil con permisos completos de acceso a Internet, garantizando que dichos usuarios puedan ingresar libremente a los diferentes sitios web sin que se apliquen políticas de bloqueo o filtrado.

Fig. 69. Lista de acceso libre


Fuente: Autoría propia

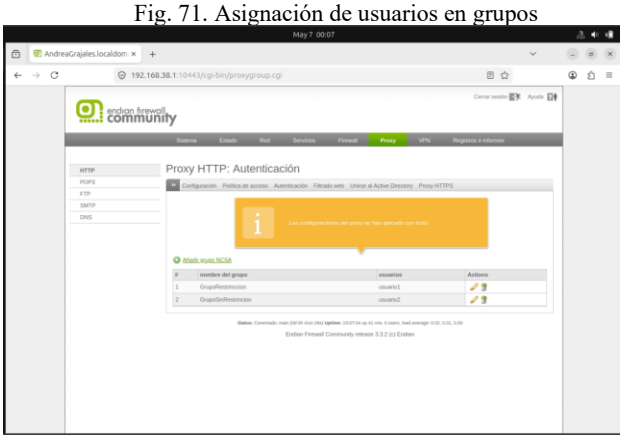
Se realiza la creación de los usuarios que utilizarán los perfiles de navegación configurados anteriormente dentro del Proxy HTTP. Para ello, se registra cada usuario con su respectivo nombre de usuario y contraseña, permitiendo implementar el proceso de autenticación requerido para el acceso a Internet.

Fig. 70. Creación de usuarios


Fuente: Autoría propia

Se asigna un grupo para usuario. Esta asignación se realiza desde la sección de autenticación, donde se gestionan los permisos.

Fig. 71. Asignación de usuarios en grupos




Fuente: Autoría propia

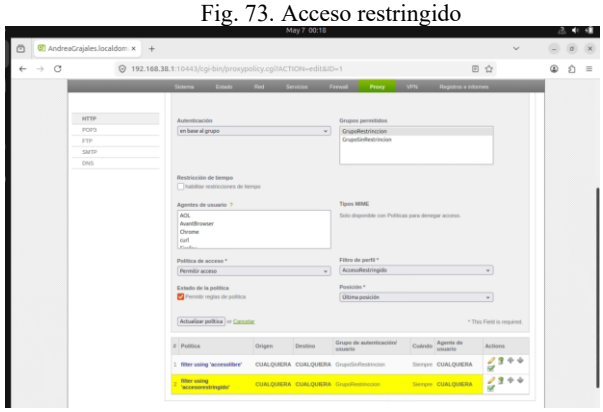
Después de crear los dominios solicitados, estos quedan registrados dentro de las políticas de filtrado del proxy. Esta configuración permite gestionar y controlar el acceso a dichos dominios, aplicando las restricciones o permisos.

Fig. 72. Política de acceso


Fuente: Autoría propia

En la configuración se observa la aplicación de políticas de acceso restringidas, junto con la asignación del perfil de filtro denominado “AccesoRestringido”.

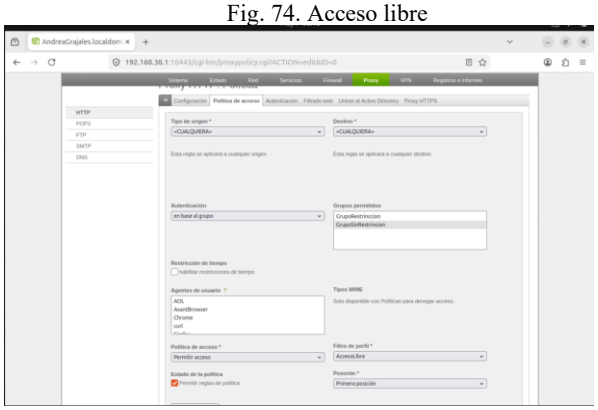
Fig. 73. Acceso restringido



Fuente: Autoría propia

En la configuración también se observa la aplicación de políticas de acceso permitidas, junto con la asignación del perfil de filtro denominado “AccesoLibre”.

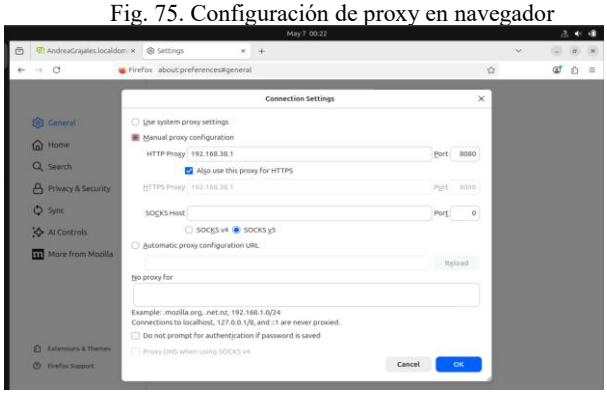
Fig. 74. Acceso libre



Fuente: Autoría propia

Se realiza la asignación del proxy 192.168.38.1 manualmente desde los ajustes del navegador sobre el puerto 8080.

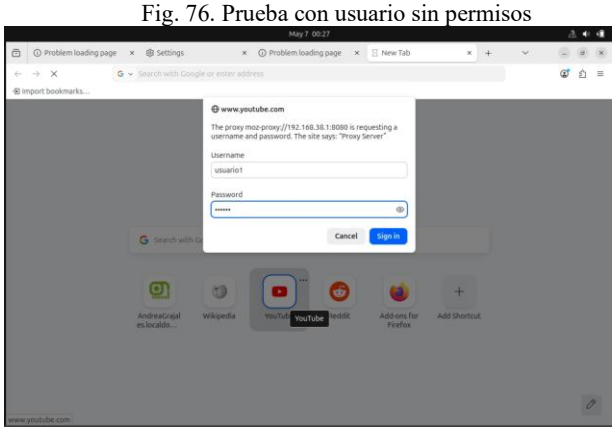
Fig. 75. Configuración de proxy en navegador



Fuente: Autoría propia

Se realiza la prueba de acceso con el usuario que no cuenta con permisos de navegación a determinados sitios de la lista negra.

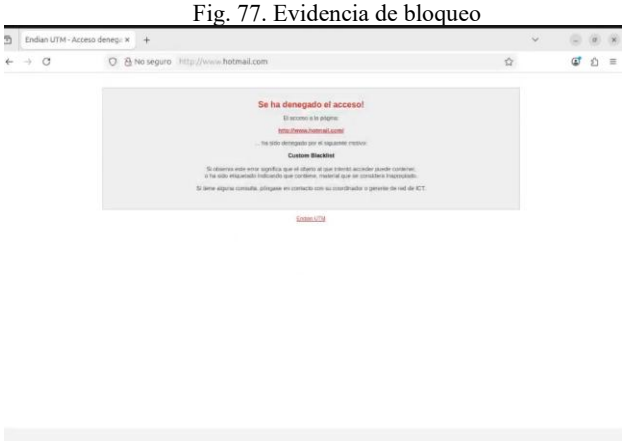
Fig. 76. Prueba con usuario sin permisos



Fuente: Autoría propia

Entonces se verifica que efectivamente no tiene acceso, garantizando las restricciones establecidas de bloqueo.

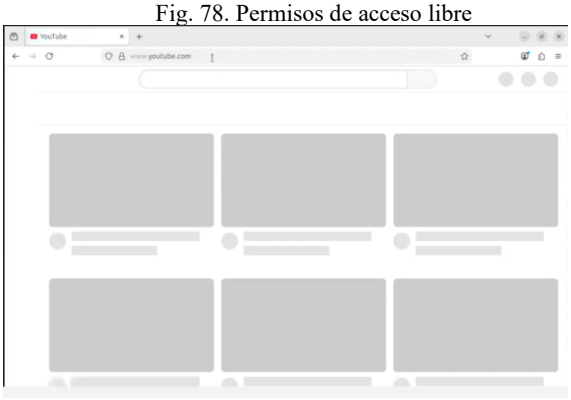
Fig. 77. Evidencia de bloqueo



Fuente: Autoría propia

En cambio, si se intenta con el otro usuario que está permitido a esos sitios, si tendrá acceso.

Fig. 78. Permisos de acceso libre



Fuente: Autoría propia

# 8 CONCLUSIONES

La aplicación técnica desarrollada demuestra que el uso de un firewall UTM como Endian permite establecer un perímetro de seguridad robusto mediante la segmentación de redes en zonas diferenciadas (Verde y Naranja). La correcta configuración de las interfaces y las reglas de tráfico de salida es fundamental para proteger la infraestructura, ya que, aunque el sistema facilita la visibilidad básica mediante protocolos como DNS e ICMP, restringe servicios críticos para prevenir accesos no autorizados hacia la zona Roja o Internet. Finalmente, la validación de la conectividad inter-zona a través de servicios específicos (HTTPS) confirma que un buen diseño de la arquitectura no solo garantiza la integridad de los datos en el servidor, sino que también optimiza la administración de servicios en entornos virtualizados.

La configuración de reglas NAT permitió establecer una comunicación eficiente y segura entre las redes internas, la zona de servidores y el entorno externo, optimizando el flujo de tráfico sin comprometer la protección de la infraestructura. La correcta administración de NAT facilitó el acceso controlado a Internet desde segmentos protegidos, preservando el direccionamiento privado y reduciendo la exposición directa de los sistemas internos. Este proceso evidenció que la gestión adecuada de NAT, junto con el enrutamiento y reenvío de tráfico, constituye una base esencial dentro de la seguridad perimetral, fortaleciendo la conectividad, la administración de recursos y la protección de plataformas GNU/Linux frente a amenazas externas.

Los ajustes en la zona DMZ fortaleció la habilitación controlada de servicios esenciales como HTTP y FTP, asegurando la disponibilidad de recursos web y transferencia de archivos para usuarios autorizados, mientras se restringieron protocolos potencialmente vulnerables como ICMP para evitar procesos de reconocimiento y diagnóstico no autorizados dentro de la red. Esta configuración demostró la importancia de aplicar políticas específicas de filtrado de tráfico para minimizar riesgos de exposición, mejorar el control sobre los servicios publicados y reforzar la protección perimetral del servidor GNU/Linux. En consecuencia, se evidenció que una correcta administración de reglas de salida y acceso en la DMZ constituye un componente clave para preservar la integridad, disponibilidad y seguridad de los servicios empresariales expuestos a redes internas y externas.

La implementación exitosa de reglas inter-zona demuestra que la seguridad de la red no depende solo de bloquear el exterior, sino de segmentar el tráfico interno. Al permitir específicamente los protocolos y puertos estrictamente necesarios entre las zonas, se garantiza que los servicios sean administrables sin exponer innecesariamente el resto de la red local. El uso de reglas específicas (en lugar de permitir todo el tráfico) mitiga el riesgo, asegurando que, si un servidor en la zona específica se ve comprometido, el atacante no tenga acceso automático a las demás zonas.

La creación de una infraestructura de seguridad perimetral mediante la distribución EFW permite fortalecer la protección de la red interna (LAN), la zona desmilitarizada (DMZ) y la red externa (WAN). A través de la configuración del proxy HTTP con autenticación de usuarios y políticas de filtrado, se controla el acceso a Internet de forma eficiente, garantizando que únicamente los usuarios autorizados puedan navegar libremente, mientras que los usuarios restringidos se bloquean de acuerdo con la lista negra definida.

# 9 REFERENCIAS


[1] Oracle. (2020). Oracle VM VirtualBox User Manual: Network Adapter Configuration. Oracle Corporation.

[2] Endian. (s.f.). Endian UTM Installation and Setup Guide. Endian Official Documentation.

[3] Endian. (s.f.). Port forwarding / NAT — Endian UTM 5.0 Reference Manual. Endian Documentation.

[4] Cisco Systems. (2025). Network Address Translation (NAT) fundamentals and enterprise deployment. Cisco Security Documentation.

[5] Endian. (s.f.). Firewall rules and inter-zone traffic management — Endian UTM Administration Guide. Endian Documentation.

[6] Ubuntu Documentation Team, "Ubuntu Server Guide: Secure deployment of Apache2 and FTP services," Canonical Ltd., 2026. [Online]. Available: URL. [Accessed: May 11, 2026].

[7] Cisco Systems. (2025). Secure Port Forwarding and DMZ Service Exposure Guidelines. Cisco Security Documentation.

[8] The firewall menu — endian UTM 5.0 reference manual. (s/f). Endian.com.

[9] Fortinet, "What is a Transparent Proxy?," Fortinet Cybersecurity Glossary, 2026. [Online]. Available: URL. [Accessed: May 11, 2026].

[10] Endian. (s.f.). Web Proxy and Content Filter Configuration — Endian UTM Administration Guide. Endian Documentation.