ENTORNO DE SEGURIDAD PERIMETRAL CON ENDIAN FIREWALL: SEGMENTACIÓN, CONTROL DE TRÁFICO Y SERVICIOS EN DMZ

Francisco Javier Ramos Pungo
e-mail: fjramosp@unadvirtual.edu.co
Daniel Stiven Cardenas Gallego
e-mail: dscardenasga@unadvirtual.edu.co
Santiago Daniel Cortes Cortes
e-mail: sdcortesc@unadvirtual.edu.co
Cristian David Franco Jaimes
e-mail: cdfrancoj@unadvirtual.edu.co
Cristian Urrego
e-mail: cmurreop@unadvirtual.edu.co

RESUMEN: *este artículo presenta la implementación y configuración de una infraestructura de red basada en GNU/Linux Endian dentro de un entorno virtualizado en VirtualBox. Se desarrolla la segmentación de la red en zonas Verde (LAN), Roja (WAN) y Naranja (DMZ), y se establecen reglas de traducción de direcciones (NAT) que permiten la comunicación controlada entre estas áreas. Además, se habilitan y restringen servicios específicos dentro de la DMZ, tales como HTTP y FTP, complementados con políticas de bloqueo para el protocolo ICMP con el fin de fortalecer la seguridad. Posteriormente, se implementan reglas de acceso interzonales para permitir o denegar tráfico según el servicio requerido. Finalmente, se configura un proxy HTTP no transparente con autenticación y listas negras, demostrando un control eficaz del acceso a Internet desde la LAN. Los resultados evidencian un entorno seguro, segmentado y funcional, apto para la simulación de servicios empresariales básicos.*

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

***ABSTRACT*:** *This article presents the implementation and configuration of a network infrastructure based on GNU/Linux Endian within a virtualized environment using VirtualBox. The network is segmented into Green (LAN), Red (WAN), and Orange (DMZ) zones, and Network Address Translation (NAT) rules are established to enable controlled communication between these segments. Additionally, specific services within the DMZ, such as HTTP and FTP, are enabled or restricted, complemented by ICMP blocking policies to enhance security. Inter-zone access rules are later implemented to allow or deny traffic according to required services. Finally, a non-transparent HTTP proxy with user authentication and blacklist policies is configured to control Internet access from the LAN. The results demonstrate a secure, segmented, and functional environment suitable for simulating basic enterprise-level services.*

KEYWORDS: DMZ, Endian Firewall, NAT, Perimeter Security

1 INTRODUCCIÓN

La implementación de infraestructuras de red seguras y segmentadas constituye un elemento fundamental en los entornos empresariales modernos. La separación de redes internas, redes expuestas a Internet y zonas destinadas a servidores permite reducir la superficie de ataque y aplicar políticas de seguridad más precisas. GNU/Linux Endian, como plataforma de firewall y proxy, ofrece capacidades avanzadas para la gestión del tráfico, la traducción de direcciones y el control de servicios, lo que lo convierte en una herramienta adecuada para entornos académicos y empresariales.

En este trabajo se presenta la configuración completa de un sistema Endian implementado en VirtualBox, organizando la red en tres zonas: Verde (LAN), Roja (WAN) y Naranja (DMZ). Se abordan aspectos clave como la configuración de interfaces de red, reglas NAT, filtrado de servicios, creación de políticas de acceso entre zonas y establecimiento de un proxy HTTP no transparente con autenticación. Cada temática se desarrolla con el objetivo de simular un entorno seguro y funcional que permita comprender el funcionamiento de redes segmentadas y los mecanismos de seguridad perimetral. Los resultados obtenidos validan la correcta operación de las reglas y servicios configurados, demostrando la eficacia del sistema para la administración y control del tráfico en redes simuladas.

2 TEMATICA 1: CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN

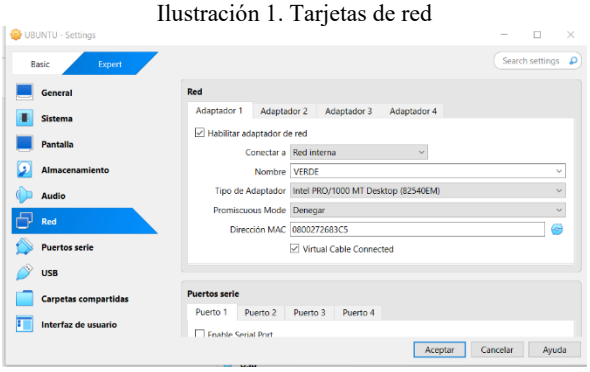
En esta temática se configuró la instancia de GNU/Linux Endian en VirtualBox junto con las máquinas Ubuntu Server y Ubuntu Desktop, con el fin de establecer

las zonas de red LAN, WAN y DMZ. Esta preparación inicial permitió crear el entorno virtual necesario para iniciar las pruebas y configuraciones de seguridad en las siguientes etapas.

2.1 CONFIGURACIÓN TARJETAS DE RED.

Para tener conexión con los diferentes dispositivos se debe configurar las diferentes redes (VERDE, NARANJA Y ROJA). Hay que tener en cuenta que el Sistema endian require tener las 3 interfaces de 3 para que esta las administer y reparta internet y reglas a los distintos dispositivos.

Ilustración 1. Tarjetas de red



Fuente: Autoría propia

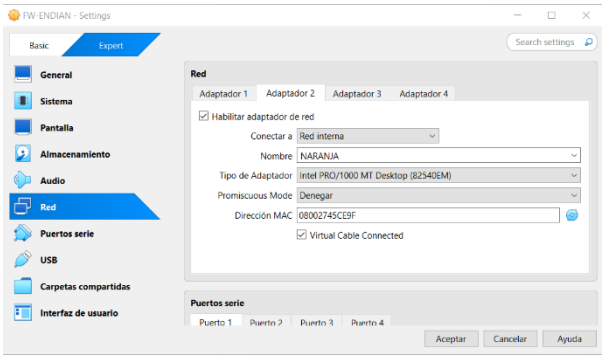
Ilustración 2. Tarjetas de red

Fuente: Autoría propia

Ilustración 3. Tarjetas de red

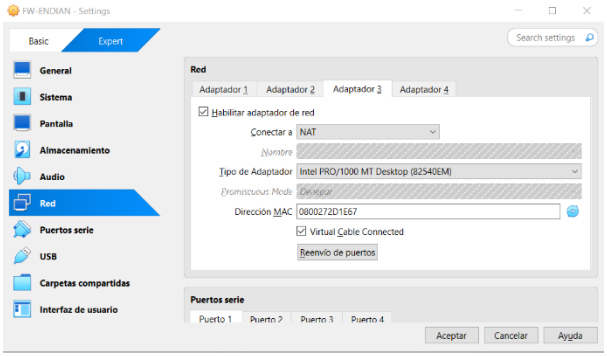
Fuente: Autoría propia

Ilustración 4. Tarjetas de red



Fuente: Autoría propia

Ilustración 5. Tarjetas de red

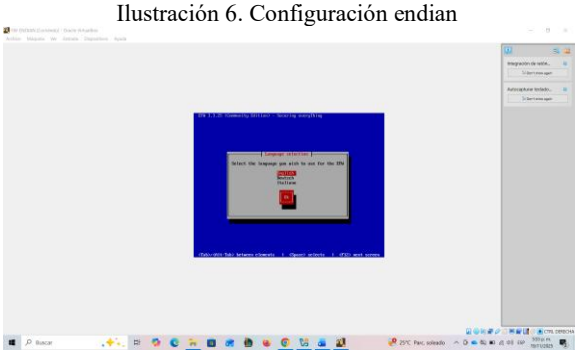


Fuente: Autoría propia

2.2 CONFIGURACIÓN ENDIAN

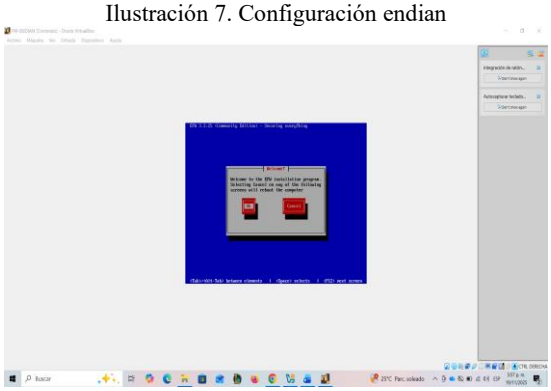
Iniciamos el Sistema

Ilustración 6. Configuración endian



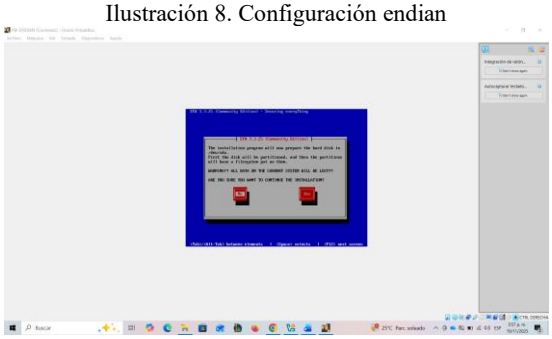
Fuente: Autoría propia

Ilustración 7. Configuración endian



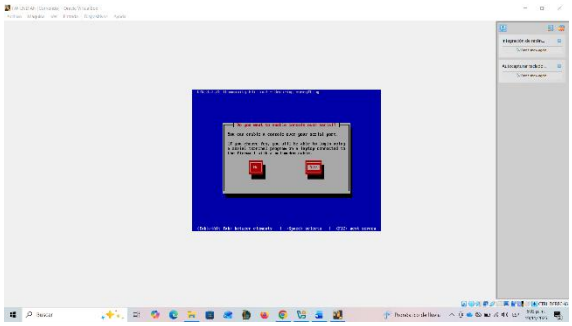
Fuente: Autoría propia

Ilustración 8. Configuración endian



Fuente: Autoría propia

Ilustración 9. Configuración endian



Fuente: Autoría propia

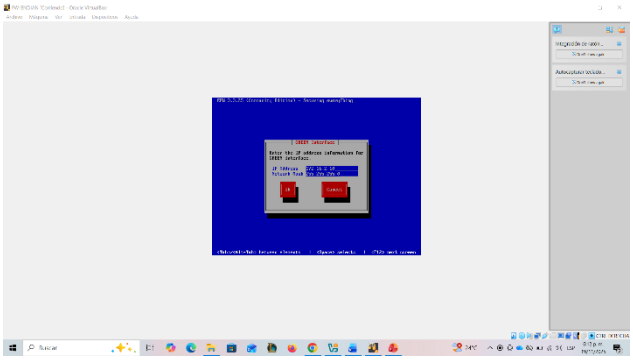
2.3 CONFIGURACIÓN RED VERDE

Configuramos la red verde con el siguiente segmento teniendo en cuenta que al configurar el endian se realiza dicho ajuste

PUERTA DE ENLACE: 172.16.2.10

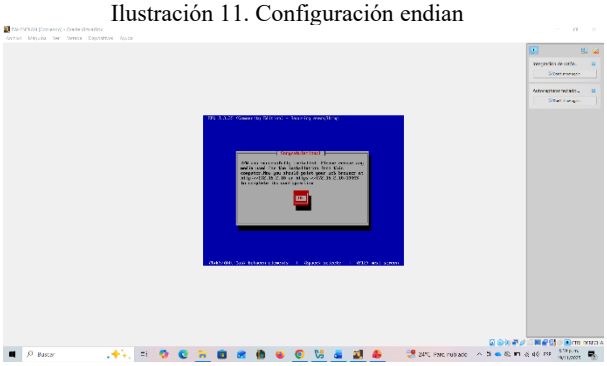
CLIENTE: 172.16.2.20

Ilustración 10. Configuración endian



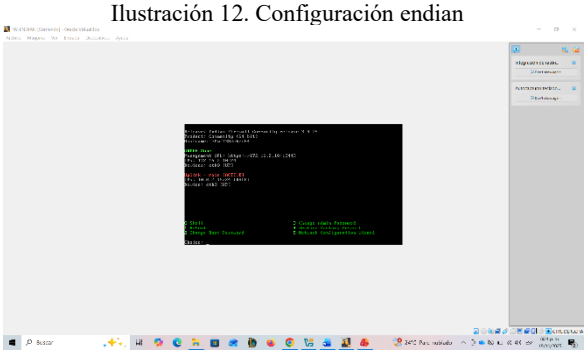
Fuente: Autoría propia

Ilustración 11. Configuración endian



Fuente: Autoría propia

Ilustración 12. Configuración endian

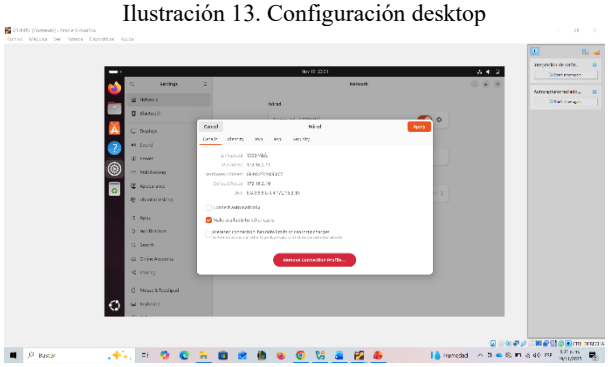


Fuente: Autoría propia

2.4 VALIDAR CONEXIÓN RED VERDE

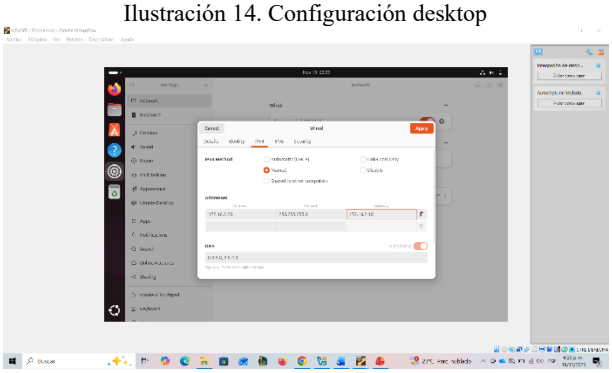
Desde las configuraciones de red validamos el direccionamiento IP que contiene nuestra maquina en la cual se evidencia que adquirio una aleatoria por medio de DHCP. Modificaremos la dirección IP por medio de la opción de IPv4 con los datos indicados anteriormente.

Ilustración 13. Configuración desktop



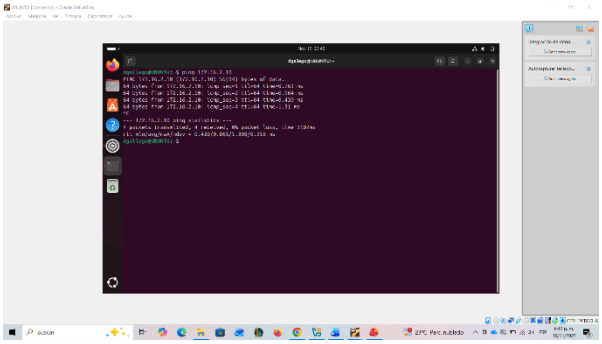
Fuente: Autoría propia

Ilustración 14. Configuración desktop



Fuente: Autoría propia

Ilustración 15. Validación conexión

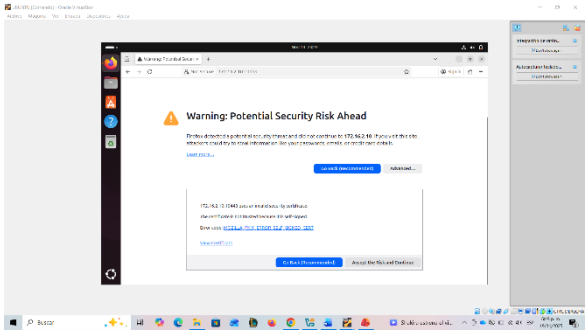


Fuente: Autoría propia

2.5 CONFIGURACIÓN FIREWALL

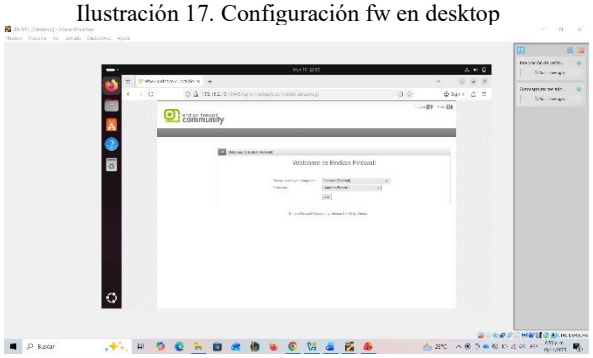
Accedemos al firewall por medio del equipo desktop con la dirección IP que nos dio el endian https://172.16.2.10:10443.

Ilustración 16. Configuración fw en desktop



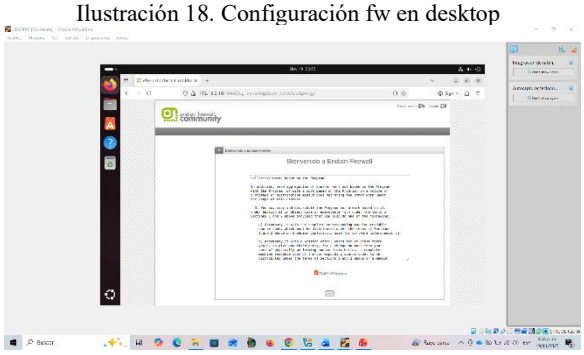
Fuente: Autoría propia

Ilustración 17. Configuración fw en desktop



Fuente: Autoría propia

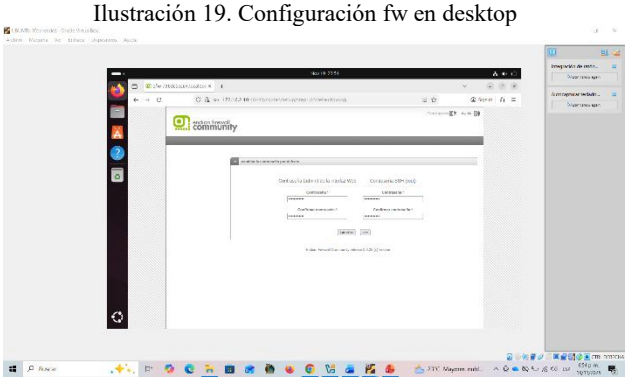
Ilustración 18. Configuración fw en desktop



Fuente: Autoría propia

Para acceder al firewall por medio de SSH o por interfaz gráfica configuramos los datos de acceso a continuación.

Ilustración 19. Configuración fw en desktop

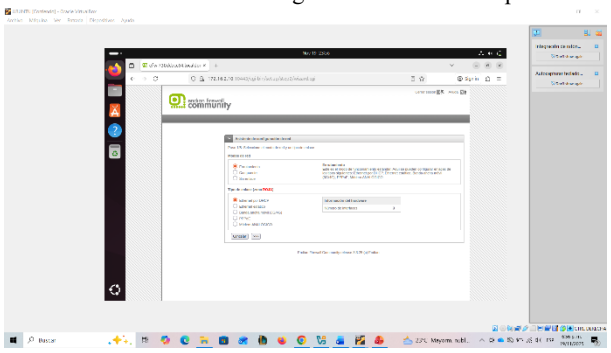


Fuente: Autoría propia

2.6 CONFIGURACIÓN RED ROJA

Para la conexión del ISP (Porveedor de internet) y el firewall se require una configuración de entrada. Siendo esta brindada por el DHCP en este caso siendo brindada por el router o modem suministrado por el proveedor de internet

Ilustración 20. Configuración fw en desktop

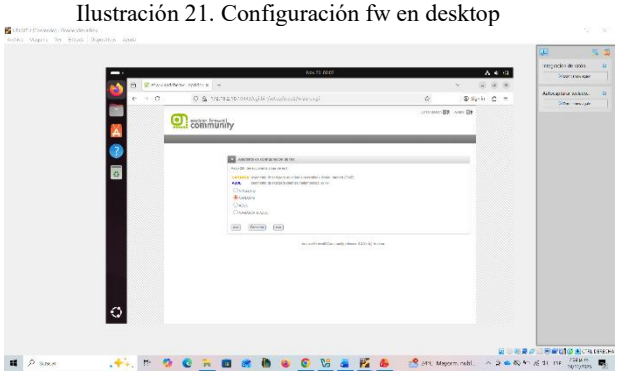


Fuente: Autoría propia

2.7 CONFIGURACIÓN RED NARANJA

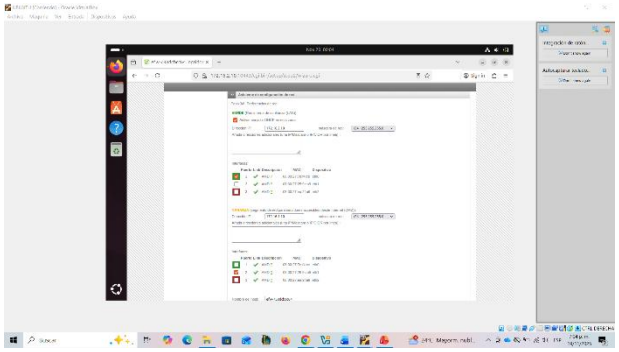
Configuramos red Naranja para la conexión del firewall con el servidor que se tiene, para los diferentes servicios que Brinda el mismo. IP la Puerta de enlace es 172.16.1.10

Ilustración 21. Configuración fw en desktop



Fuente: Autoría propia

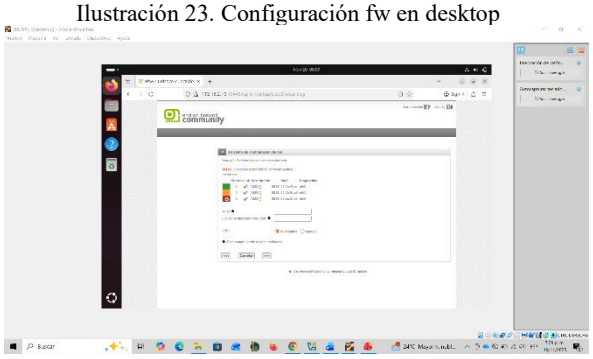
Ilustración 22. Configuración fw en desktop



Fuente: Autoría propia

Una vez se termina la configuración de las diferentes redes, el firewall nos da un resumen de las mismas con sus respectivas MAC.

Ilustración 23. Configuración fw en desktop

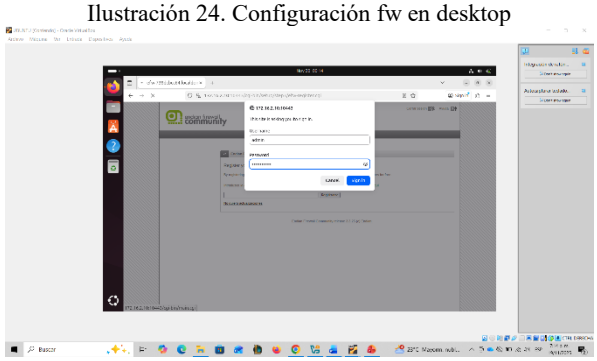


Fuente: Autoría propia

2.8 FIN CONFIGURACIÓN FW

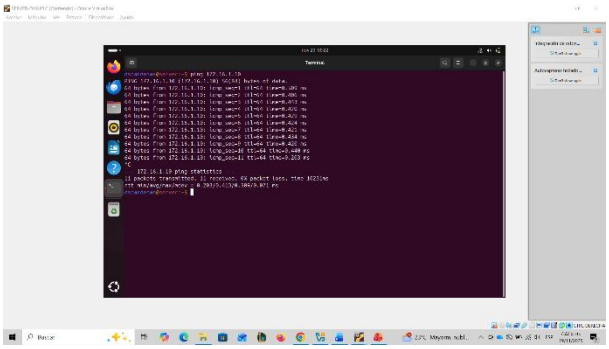
Una vez finalizamos la configuración, la plataforma nos solicitara datos de acceso, siendo los configurados en el firewall.

Ilustración 24. Configuración fw en desktop



Fuente: Autoría Propia

Ilustración 25. Validación de conexión



Fuente: Autoría Propia

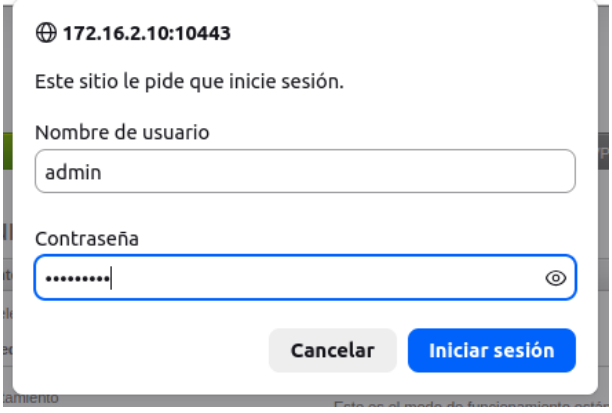
3 TEMATICA 2: CONFIGURACION NAT

3.1 ACCESO AL PORTAL DE ADMINISTRACIÓN

Desde el equipo de la LAN (172.16.2.20) se accedió a la consola web del firewall mediante: https://172.16.2.10:10443.

Se ingresó con las credenciales del usuario administrador.

Ilustración 26. Credenciales



Fuente: Autoría Propia

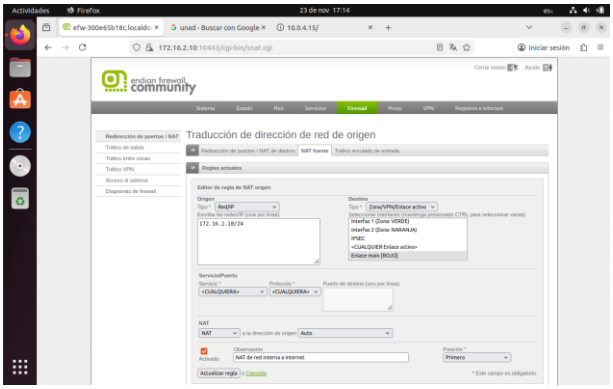
3.2 CONFIGURACIÓN DE SNAT PARA LA RED VERDE

En Firewall → Port Forwarding / NAT → Source NAT, se creó una regla con los siguientes parámetros:

- **Source:** Network/IP → 172.16.2.0/24
- **Destination:** Uplink Main (ROJA)
- **Acción NAT:** Masquerading
- **Posición:** First
- **Comentario:** "NAT para LAN hacia Internet"

La regla se guardó y quedó activa tras seleccionar **Apply**.

Ilustración 27**.** Creación de la nueva regla NAT – Zona Verde



Fuente: Autoría Propia

3.3 CONFIGURACIÓN DE SNAT PARA LA RED NARANJA

Se agregó una segunda regla SNAT:

- **Source:** Network/IP → 172.16.1.0/24
- **Destination:** Uplink Main
- **Acción NAT:** Masquerading
- **Posición:** Last
- **Comentario:** "NAT DMZ hacia Internet"

La regla quedó registrada en el panel de Source NAT.

Ilustración 28. Creación de la nueva regla NAT – Zona Verde

Fuente: Autoría propia

3.4 RESULTADOS Y VALIDACIÓN

Una vez se terminaron las configuraciones de las reglas para el ejercicio se procedió a ejecutar en ambas maquinas, Desktop y server, los comandos ping 8.8.8.8 y ping google.com para determinar si las reglas quedaron configuradas correctamente.

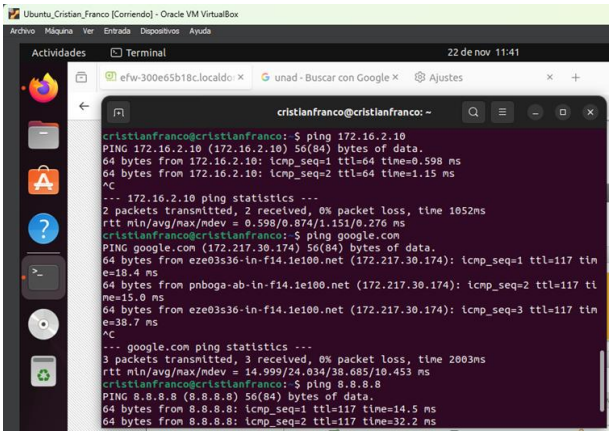
PRUEBAS EN LA RED VERDE

Desde el equipo 172.16.2.20 se ejecutaron:

- ping 8.8.8.8
- ping google.com

Los resultados confirmaron acceso a Internet y resolución DNS correcta.

Ilustración 29. Prueba de conexión desde la LAN

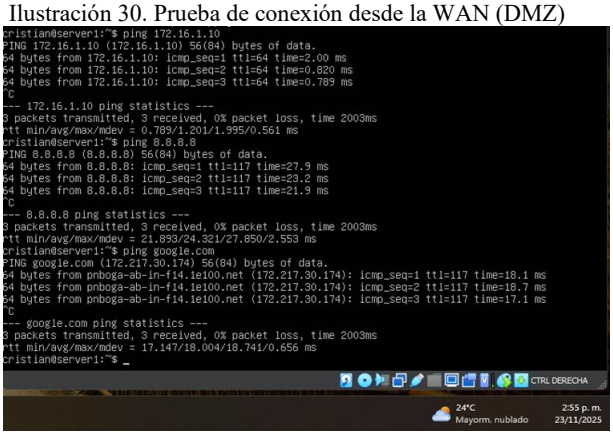


Fuente: Autoría propia

PRUEBAS EN LA RED NARANJA

En el servidor de la DMZ (172.16.1.10) se realizaron los mismos comandos, obteniendo respuesta exitosa, lo cual confirmó la correcta aplicación del SNAT.

Ilustración 30. Prueba de conexión desde la WAN (DMZ)



Fuente: Autoría propia

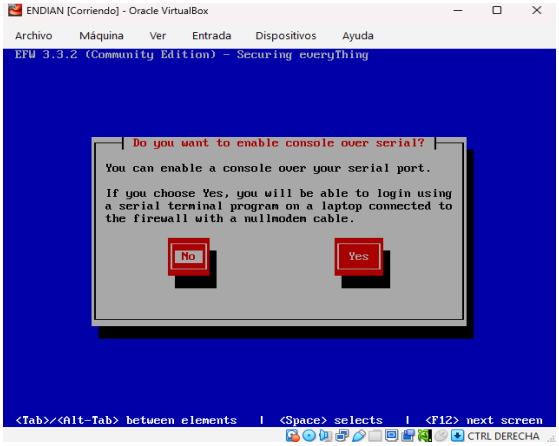
4 TEMATICA 3: SERVICIOS DMZ DEFINICIÓN DE ZONAS

En esta fase se habilitan servicios específicos en el servidor ubicado en la zona DMZ, utilizando Ubuntu Server como plataforma base. El objetivo es permitir el acceso controlado a servicios web y FTP, al tiempo que se restringe el uso del protocolo ICMP para mejorar la seguridad perimetral.

- IP de zona verde: 172.16.1.10
- IP de naranja: 172.16.2.20

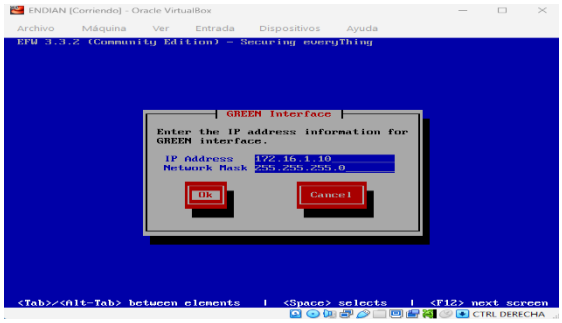
INSTALACIÓN Y DEFINICIÓN DE LA ZONA VERDE EN ENDIAN.

Ilustración 31. Demostración en Endian



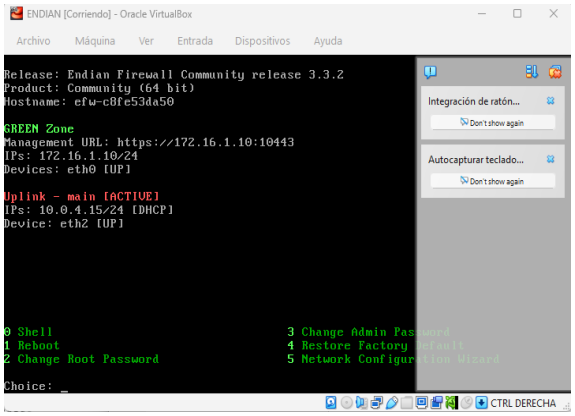
Fuente: Autoría propia

Ilustración 32. Demostración en Endian



Fuente: Autoría propia

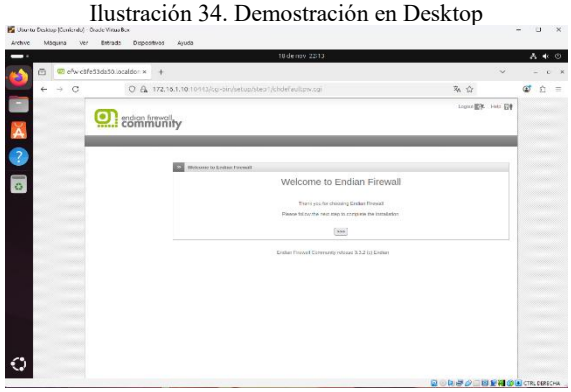
Ilustración 33. Demostración en Endian



Fuente: Autoría propia

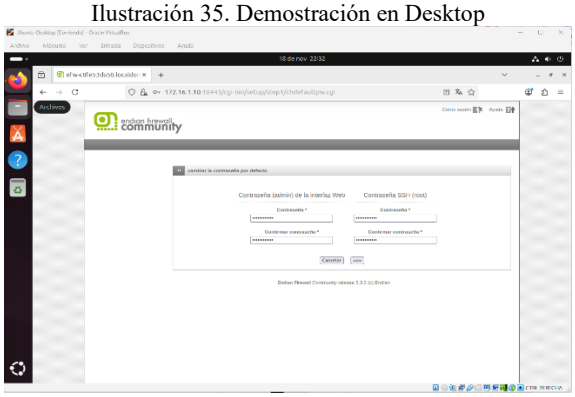
4.1 CONFIGURACIÓN DE ENDIAN

Ilustración 34. Demostración en Desktop



Fuente: Autoría propia

Ilustración 35. Demostración en Desktop

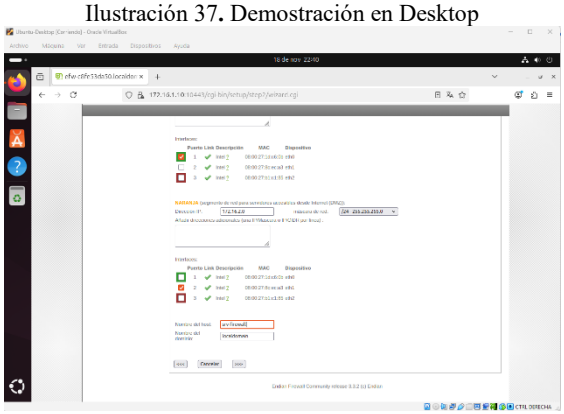


Fuente: Autoría propia

Ilustración 36. Demostración en Desktop

Fuente: Autoría propia

Ilustración 37. Demostración en Desktop



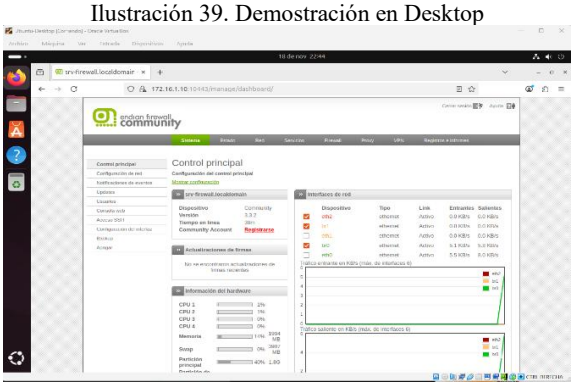
Fuente: Autoría propia

Ilustración 38. Demostración en Desktop

Fuente: Autoría propia

Se habilitan los puertos correspondientes a los servicios HTTP (puerto 80) y FTP (puerto 21) en el firewall Endian, permitiendo la comunicación desde la LAN hacia el servidor ubicado en la DMZ. Las reglas se crean desde la interfaz gráfica de Endian y se validan mediante pruebas de conexión desde estaciones cliente.

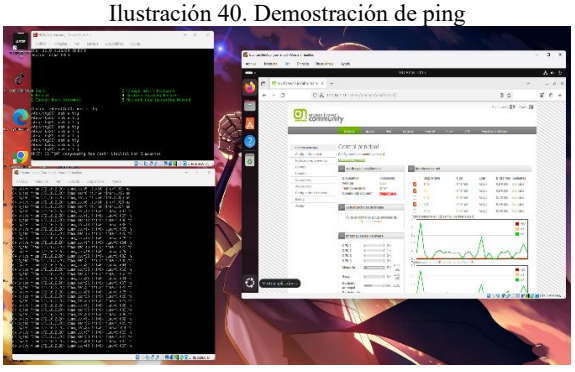
Ilustración 39. Demostración en Desktop



Fuente: Autoría propia

Después de la configuración en desktop probamos el ping con servidor 172.16.2.20, obteniendo respuesta.

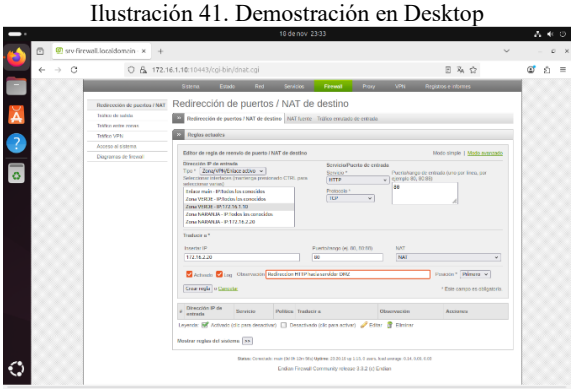
Ilustración 40. Demostración de ping



Fuente: Autoría propia

Se crea la regla de acceso puerto 80.

Ilustración 41. Demostración en Desktop



Fuente: Autoría propia

Redireccionamiento puerto 21.

Ilustración 42. Demostración en Desktop

Fuente: Autoría propia

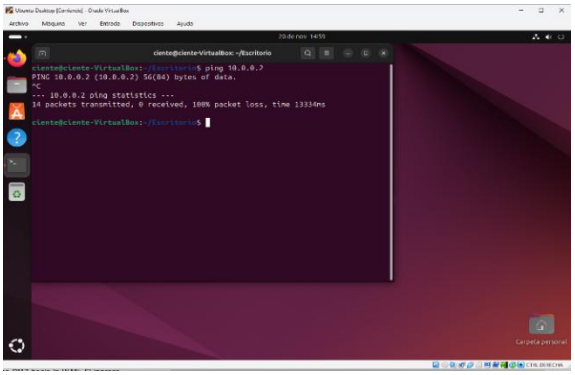
Reglas creadas.

Ilustración 43. Demostración en Desktop

Fuente: Autoría propia

Para evitar que se realicen pruebas de conectividad mediante ping, se bloquea el protocolo ICMP (puertos 8 y 30) desde la zona verde hacia la DMZ. Esta acción se realiza mediante la creación de reglas específicas en el tráfico de salida.

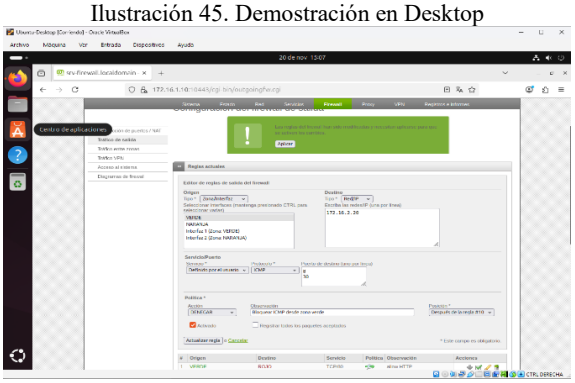
Ilustración 44. Demostración en Endian



Fuente: Autoría propia

Creación de regla para bloquear ICMP desde zona verde.

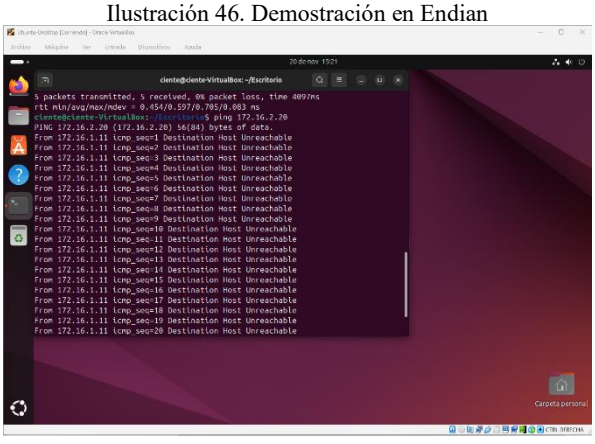
Ilustración 45. Demostración en Desktop



Fuente: Autoría propia

La prueba se realiza desde una estación en la LAN, intentando hacer ping al servidor en la DMZ (IP: 172.16.2.20), confirmando que no se recibe respuesta, lo que valida la efectividad de la regla.

Ilustración 46. Demostración en Endian

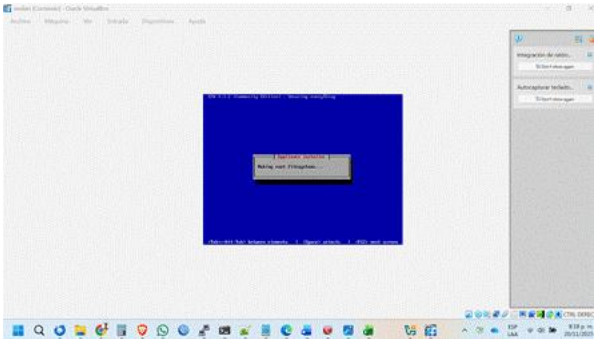


Fuente: Autoría propia

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

5.1 INSTALANDO ENDIAN FIREWALL

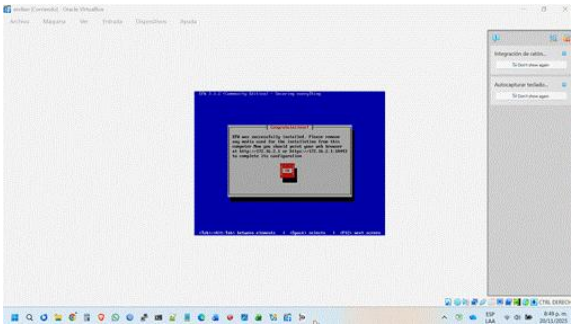
Ilustración 47. Demostración en Endian



Fuente: Autoría propia

Instalación de ISO completada se muestra que quedo configurada la IP 172.16.2.1 en la zona verde.

Ilustración 48. Demostración en Endian



Fuente: Autoría propia

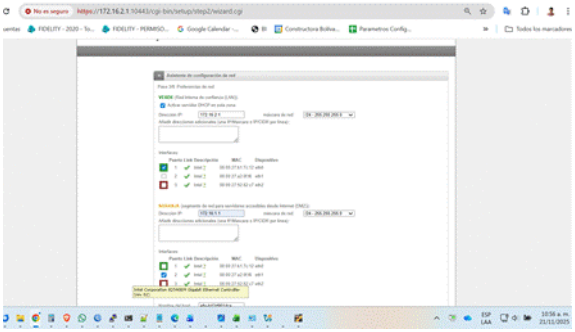
Se inicia Wizard de configuración web para el EFW.

Ilustración 49. Demostración en Desktop

Fuente: Autoría propia

Configuración de IP en la zona verde y Naranja los cuales pasarán a ser los gateways de cada red respectivamente.

Ilustración 50. Demostración en Desktop



Fuente: Autoría propia

Se completa instalacion y configuración básica mediante Wizard web cargado desde MV debian en la zona verde

Ilustración 51. Demostración en Desktop

Fuente: Autoría propia

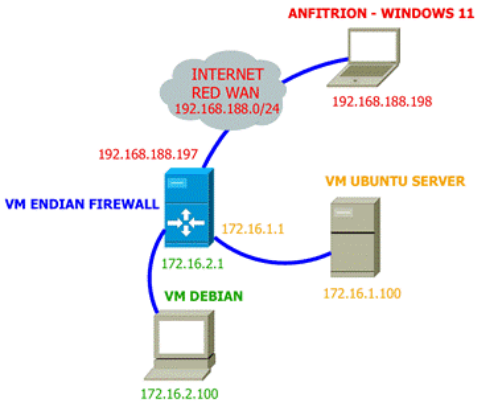
Se valida estado de tarjetas de red y funcionalidad normal de EFW.

Ilustración 52. Demostración en Desktop

Fuente: Autoría propia

5.2 TOPOLOGÍA DE RED

Ilustración 53



Fuente: Infraestructura de red

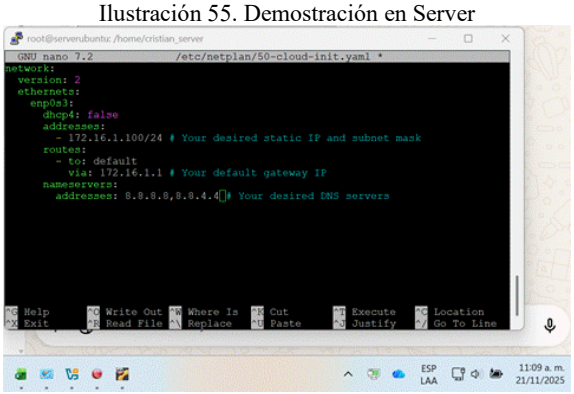
Maquinas virtuales : Debian, Servidor Ubuntu y EFW

Ilustración 54. Configuración virtual Box

Fuente: Autoría propia

5.3 CONFIGURACIÓN DE IPS ESTÁTICA EN SERVIDOR UBUNTU HACIENDO USO DE NETPLAN

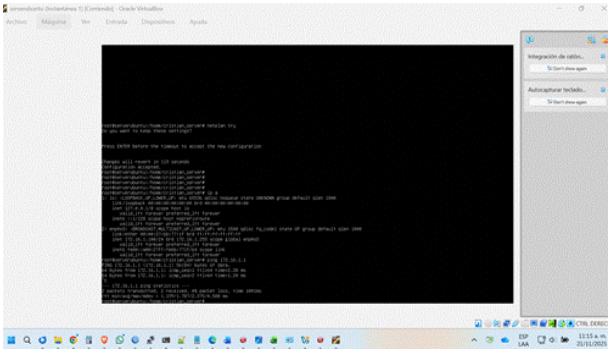
Ilustración 55. Demostración en Server



Fuente: Autoría propia

Prueba de ping al GW de la zona naranja EFW 172.16.1.1:

Ilustración 56. Demostración en Server



Fuente: Autoría propia

5.4 CONFIGURACIÓN DE IPS ESTÁTICA EN VM DEBIAN HACIENDO USO DE KDE

Ilustración 57. Configuración en Desktop

Fuente: Autoría propia

5.5 VALIDACIÓN DE TRÁFICO Y COMUNICACIÓN INTERZONAS VERDE – NARANJA

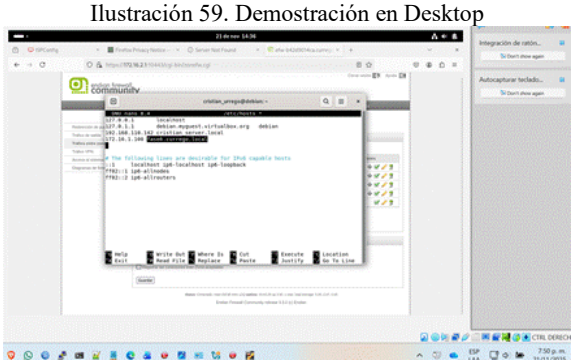
Se cuenta con comunicación habilitada entre Zona verde -verde, Zona verde-naranja y Zona naranja-naranja.

Ilustración 58. Demostración en Desktop

Fuente: Autoría propia

Carga correcta de aplicativo web creado en la fase 6 en servidor Ubuntu desde VM Debian:

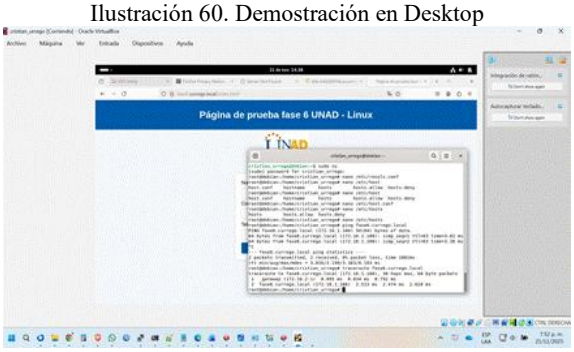
Ilustración 59. Demostración en Desktop



Fuente: Autoría propia

Se modifica /etc/hosts para agregar registro estatico de fase5.curregо.local hacia la IP del servidor Ubuntu. Esto debido que para que cargue correctamente la página debe de hacerse por el dominio y no la IP.

Ilustración 60. Demostración en Desktop



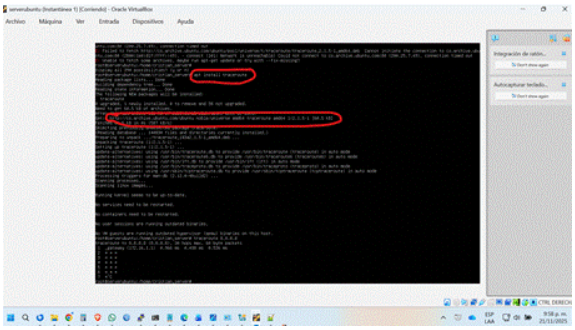
Fuente: Autoría propia

5.6 SE HABILITA HTTP HACIA ZONA ROJA PARA SERVIDOR UBUNTU – NAVEGACIÓN EN SERVIDOR HTTP:

Ilustración 61. Demostración en Desktop

Fuente: Autoría propia

Ilustración 62. Demostración en Server



Fuente: Autoría propia

Con esta prueba se puede confirmar la navegación del servidor Ubuntu ubicado en la zona naranja hacia http en la zona roja

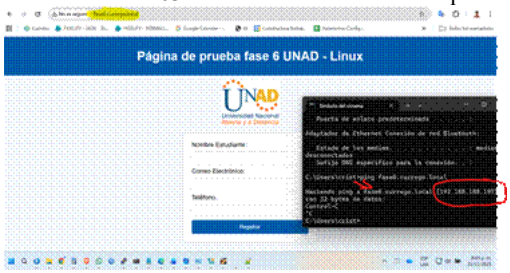
5.7 CONFIGURACIÓN NAT PARA CARGAR SERVIDOR WEB UBUNTU Y FTP DESDE WAN: ZONA ROJA NAT HACIA IP SERVER 172.16.1.100

Ilustración 63. Demostración en Desktop

Fuente: Autoría propia

Pruebas desde Anfitrión Windows cargando aplicativo WEB de server Ubuntu mediante NAT creado en el cual se redirigen los puertos 21,80 y 443 desde zona roja hacia la IP del servidor Ubuntu.

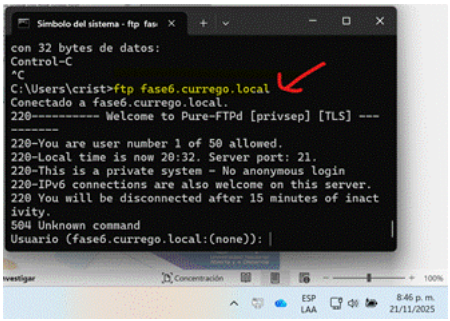
Ilustración 63.1. Demostración en Desktop



Fuente: Autoría propia

Prueba FTP desde Anfitrion Windows hacia servidor LAMP por medio de NAT creado:

Ilustración 64



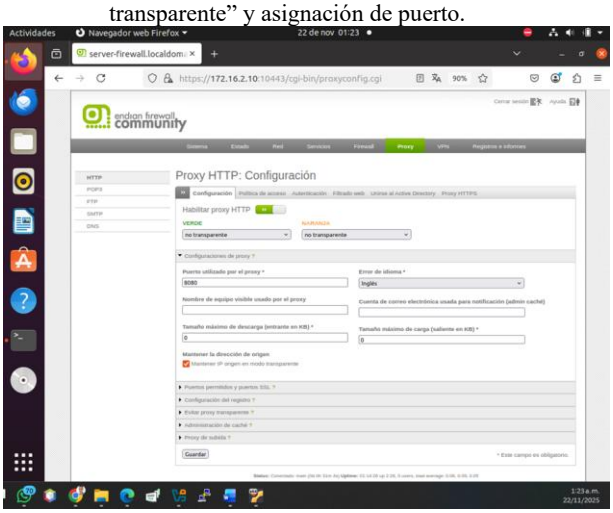
Fuente: Demostración en Desktop

Se valida que desde el anfitrión en Windows se puede cargar el aplicativo web que se encuentra en el Ubuntu server.

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

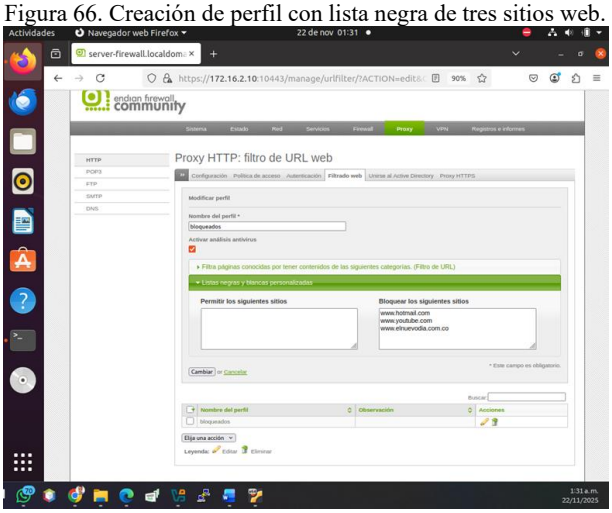
A continuación, se expondrá la Implementación y configuración de una solución de Proxy HTTP No Transparente sobre Endian Firewall, con el propósito de establecer un control de acceso estricto y centralizado para la navegación de la Red Local (LAN), garantizando que solo los usuarios autenticados puedan acceder a Internet y aplicando políticas de filtrado de contenido para dominios específicos.

Figura 65. Habilitación del proxy de manera “no transparente” y asignación de puerto.



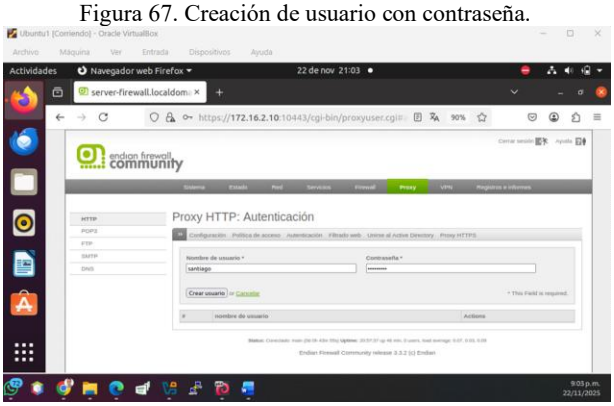
Fuente: Autoría Propia

Figura 66. Creación de perfil con lista negra de tres sitios web.



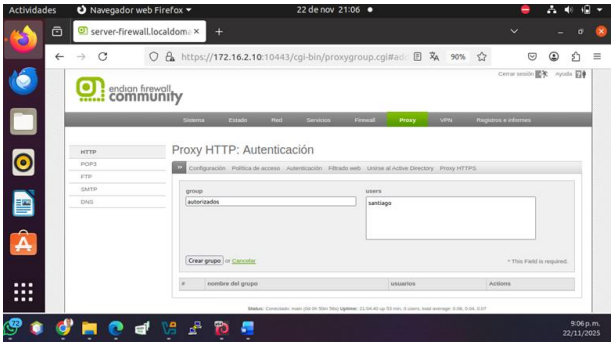
Fuente: Autoría Propia

Figura 67. Creación de usuario con contraseña.



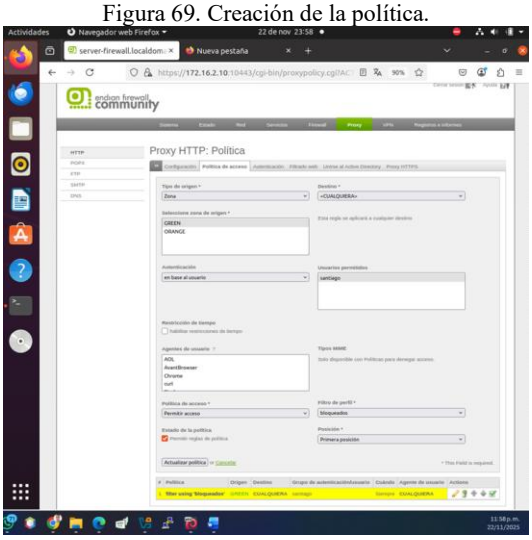
Fuente: Autoría Propia

Figura 68. Creación de grupo al cual se le añade el usuario creado anteriormente.



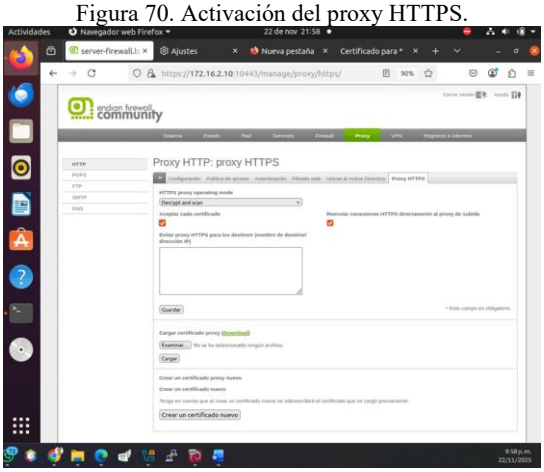
Fuente: Autoría Propia

Figura 69. Creación de la política.



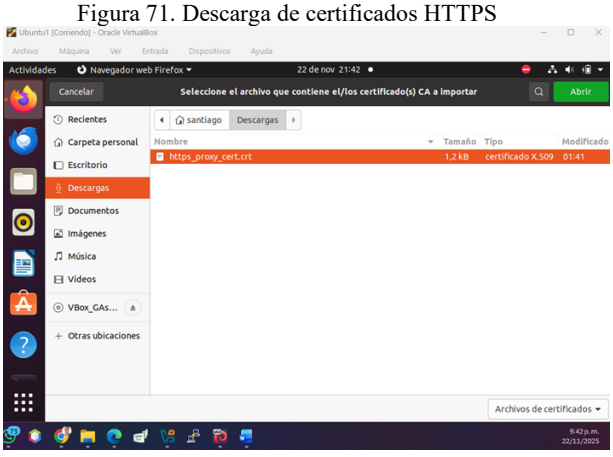
Fuente: Autoría Propia

Figura 70. Activación del proxy HTTPS.



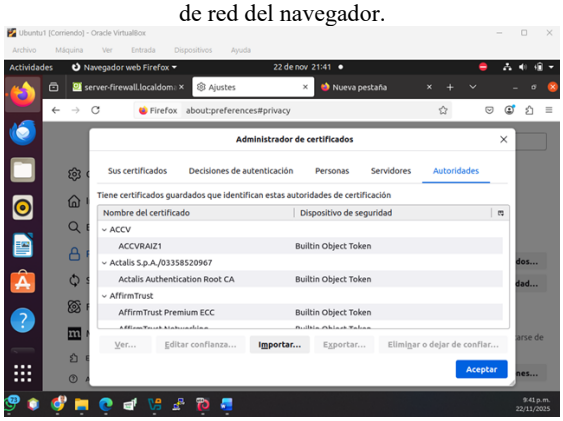
Fuente: Autoría Propia

Figura 71. Descarga de certificados HTTPS



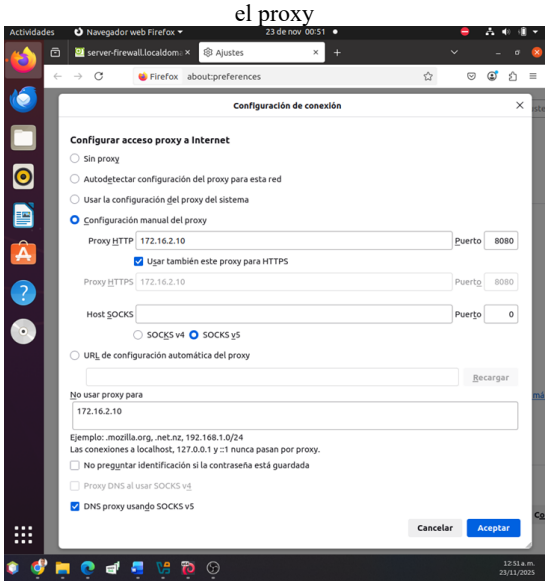
Fuente: Autoría Propia

Figura 72. Importación de certificado desde la configuración de red del navegador.



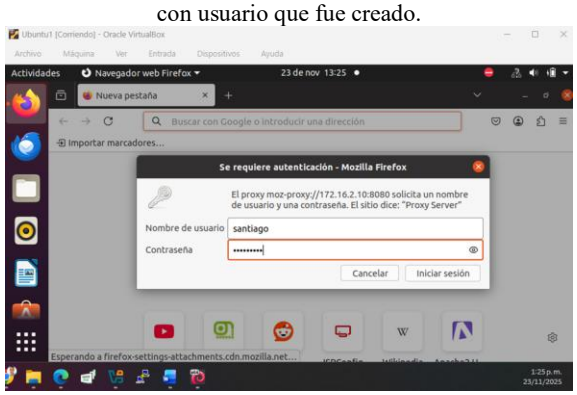
Fuente: Autoría Propia

Figura 73. Configuración de conexión de manera manual con el proxy



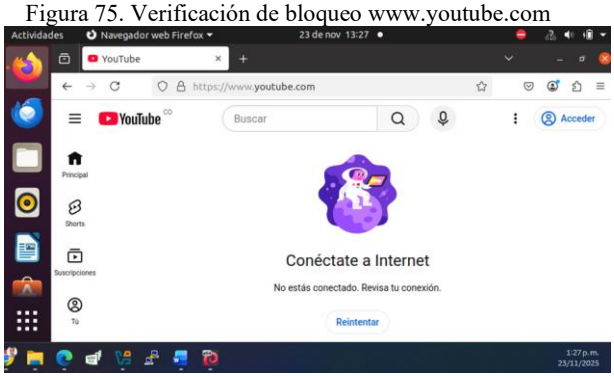
Fuente: Autoría Propia

Figura 74. Autenticación para ingresar al navegador Firefox con usuario que fue creado.



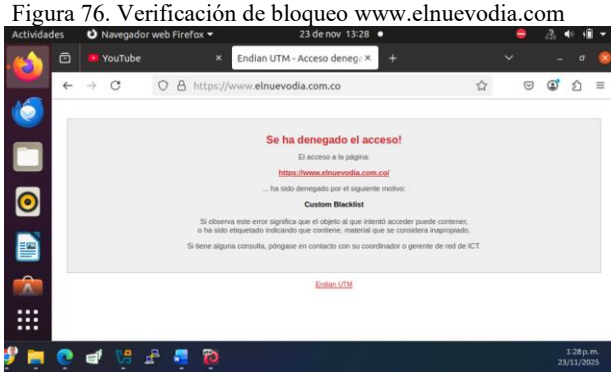
Fuente: Autoría Propia

Figura 75. Verificación de bloqueo www.youtube.com



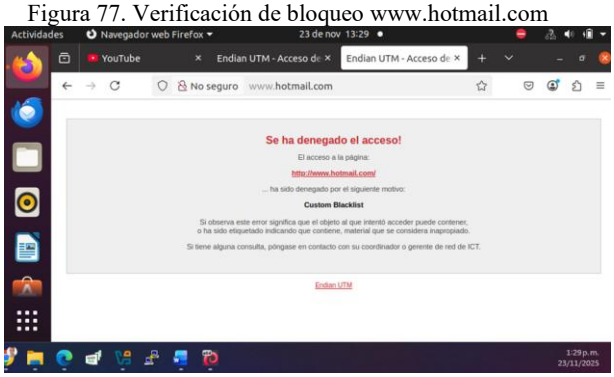
Fuente: Autoría Propia

Figura 76. Verificación de bloqueo www.elnuevodia.com



Fuente: Autoría Propia

Figura 77. Verificación de bloqueo www.hotmail.com



Fuente: Autoría Propia

7 Conclusiones.

La configuración de la instancia Endian y su integración con las máquinas virtuales Ubuntu Server y Ubuntu Desktop permitió establecer correctamente las zonas LAN, WAN y DMZ en VirtualBox. Con esto quedó funcionando la estructura básica de red necesaria para continuar con las siguientes etapas de seguridad y administración, asegurando un entorno virtual estable y operativo **(Temática 1)**.

La configuración del servicio NAT en Endian Firewall

permitió habilitar la salida a Internet tanto para la red LAN como para la DMZ, manteniendo al mismo tiempo la segmentación de seguridad. Las reglas SNAT garantizaron el enmascaramiento de direcciones internas, mientras que el DNAT permitió la publicación segura de servicios ubicados en la DMZ. Las pruebas demostraron que la red opera según lo esperado, cumpliendo con los lineamientos de seguridad y conectividad requeridos para la práctica. **(Temática 2).**

La configuración de servicios en la zona DMZ mediante el uso de Endian y Ubuntu Server permitió establecer un entorno controlado y funcional para la exposición de servicios HTTP y FTP. La correcta aplicación de reglas de acceso y la restricción del protocolo ICMP evidencian una gestión efectiva del tráfico entre zonas, fortaleciendo la seguridad perimetral. Las pruebas realizadas desde la LAN confirmaron la operatividad de los servicios habilitados y la eficacia de las políticas de bloqueo, demostrando que es posible implementar controles granulares en entornos virtuales con plataformas GNU/Linux. **(Temática 3).**

Durante las prácticas se aplicaron estos conceptos mediante la instalación y configuración de Endian Firewall en un entorno virtualizado, trabajando de forma integrada con una máquina virtual Debian, una máquina virtual Ubuntu Server y el equipo anfitrión en Windows. Esta experiencia permitió entender el funcionamiento real de un firewall basado en Linux, la gestión de interfaces, zonas de seguridad, ruteo, NAT y servicios asociados. **(Temática 4).**

El trabajo con el Endian Firewall me enseñó que la función principal de un proxy en cualquier organización es garantizar visibilidad y control sobre el tráfico de red, lo cual es vital para la seguridad y el cumplimiento normativo. Comprobé que la solución requiere disciplina en la configuración, ya que la seguridad es una pirámide: la base es una red estable con IP estática, el segundo nivel es la autenticación para asignar responsabilidades a cada usuario, y la cúspide es la inspección SSL (HTTPS), que es esencial para aplicar políticas de filtrado de contenido y no operar a ciegas en el internet moderno. **(Temática 5).**

8 REFERENCIAS

[1] PI 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/

[2] Arifin, F. M., Mutiara, G. A., & Ismail, I. (2017). Implementation of management and network security using endian UTM firewall. *IJAIT (International Journal of Applied Information Technology)*, 43-51.

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