IMPLEMENTACION Y CONFIGURACION DE UN ENTORNO PERIMETRAL CON GNU/LINUX ENDIAN FIREWALL EN INFRAESTRUCTURA VIRTUALIZADA

Andres Felipe Rincon Núñez
e-mail: afrinconn@unadvirtual.edu.co
Jeniffer Camila Castiblanco Albarracín
e-mail: jccastiblancoa@unadvirtual.edu.co
Jhojan Yadir Quintero Cortes
e-mail: jyquinteroc@unadvirtual.edu.co
Andres Felipe Olmos Rojas
e-mail: afolmosr@unadvirtual.edu.co
Vivian Yulieth Conde Leon
e-mail: vycondel@unadvirtual.edu.co

RESUMEN: *Este documento detalla la implementación de una infraestructura de seguridad perimetral utilizando la distribución Endian Firewall en un entorno virtualizado con VirtualBox. El proyecto consistió en el despliegue de una topología de red segmentada en tres zonas (Verde/LAN, Naranja/DMZ y Roja/WAN), configurando adaptadores virtuales y asignando direccionamiento IP específico para cada segmento. La metodología incluyó la configuración de reglas de NAT para permitir la conectividad a Internet desde las redes internas, la implementación de políticas de firewall para controlar el acceso a servicios HTTP y FTP en la DMZ, el bloqueo de tráfico ICMP y la configuración de un proxy HTTP con autenticación y listas negras de filtrado. Los resultados confirmaron la conectividad exitosa entre zonas, el acceso controlado a los servicios, la efectividad del bloqueo de protocolos y la funcionalidad del proxy, logrando una arquitectura segura y aislada que cumple con los objetivos de seguridad perimetral establecidos.*

PALABRAS CLAVE: Endian, Linux, Seguridad, Segmentación

1 INTRODUCCIÓN

La presente sección documenta la implementación de un entorno de seguridad perimetral basado en la distribución GNU/Linux Endian Firewall, desplegada sobre una infraestructura virtualizada mediante VirtualBox. El objetivo de esta primera fase consiste en la correcta configuración de la instancia del firewall, incluyendo la asignación y gestión de tres zonas de red fundamentales para la protección de servicios y recursos: la zona verde (LAN) destinada a los usuarios internos, la zona roja (WAN) como enlace hacia Internet y la zona naranja (DMZ) concebida para alojar servidores expuestos o semiexpuestos. Para ello se realizó la instalación efectiva de Endian, la definición de la topología de red, la creación y vinculación de adaptadores virtuales y la validación funcional de conectividad entre las diferentes zonas. Esta configuración inicial constituye la base técnica sobre la cual se desarrollarán las temáticas posteriores relacionadas con traducción de direcciones, políticas de acceso, control de tráfico y servicios de seguridad avanzados.

2 TEMATICAS

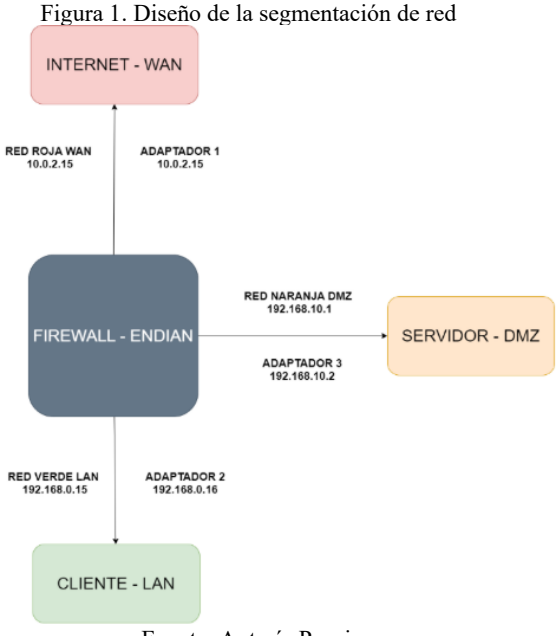
2.1 TEMATICA 1: CONFIGURACION DE LA INSTACIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX (TARJETAS DE RED) E INSTALACIÒN EFECTIVA DEL MISMO

Implementación de GNU/Linux Endian con las zonas verde, roja y naranja, así: Zona verde: Red interna (LAN), Zona roja: Acceso a internet (WAN) y Zona naranja: Servidores (DMZ).

2.1.1 PLAN GENERAL Y ESQUEMA DE DIRECCIONES

Se usaron redes internas para separar zonas y el NAT de VirtualBox para simular la Internet.

Figura 1. Diseño de la segmentación de red



Fuente: Autoría Propia

2.1.2 DESCARGA DE ENDIAN FIREWALL COMMUNITY

Se realizo la descarga de Endian Firewall Community desde la página web oficial

Figura 2. página de principal de Endian

Fuente: Autoría Propia

Se realizo descarga de ISO

Figura 3. página de descarga ISO Endian

Fuente: Autoría Propia

Se realizo descarga de ISO

Figura 4. ISO descargado

Fuente: Autoría Propia

2.1.3 CREAR LA MÁQUINA VIRTUAL EN VIRTUALBOX

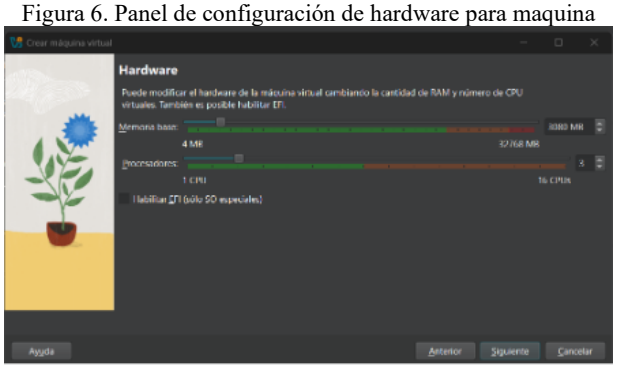
Se realizo creación de máquina virtual en virtual vox con la siguiente configuración

Figura 5. panel de configuración VirtualBox para maquina Endian

Fuente: Autoría Propia

Se realizo asignación de nombre y sistema operativo ahora se asignará el hardware de la maquina

Figura 6. Panel de configuración de hardware para maquina



Fuente: Autoría Propia

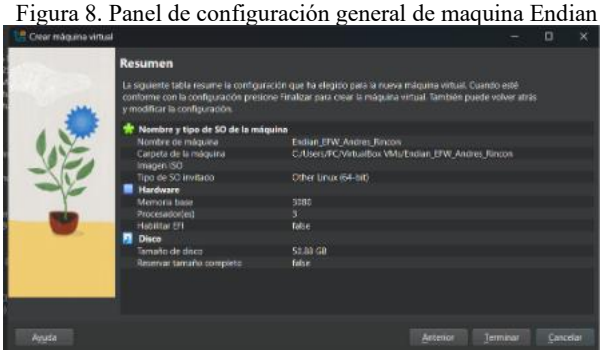
Ahora se asignará la cantidad de espacio que tendrá en disco la maquina

Figura 7. Panel de configuración de almacenamiento para maquina

Fuente: Autoría Propia

Finalizando, terminaríamos la creación de la maquina en Virtual box

Figura 8. Panel de configuración general de maquina Endian



Fuente: Autoría Propia

Ya una vez creada se procederá a crear y configurar los tres adaptadores de red para maquina endian, maquina DEBIAN servidor y maquina Ubuntu cliente.

- MAQUINA FIREWALL ENDIAN

ADAPTADOR 1 (RED ROJA WAN)

Será de la conexión NAT como parte de la zona roja de red WAN

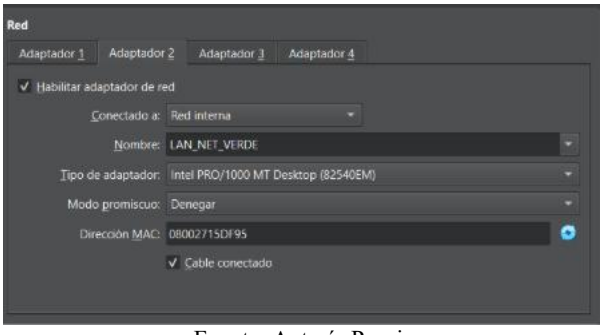
Figura 9. Configuración adaptador 1 red NAT maquina Endian

Fuente: Autoría Propia.

ADAPTADOR 2 (RED VERDE LAN)

Sera conectada a red interna como parte de la zona verde LAN

Figura 10. Configuración adaptador 2 red LAN maquina Endian

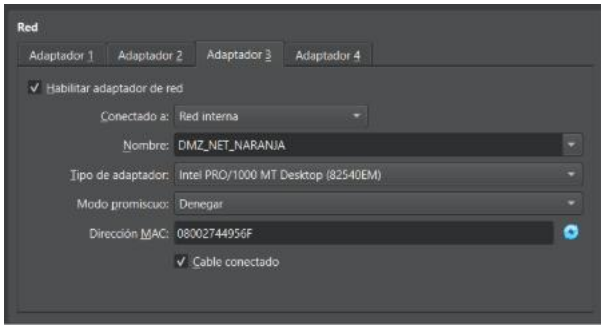


Fuente: Autoría Propia.

ADAPTADOR 3 (RED NARANJA DMZ)

Sera conectada a una red interna como parte de la zona naranja DMZ

Figura 11. Configuración adaptadora 3 red DMZ maquina Endian

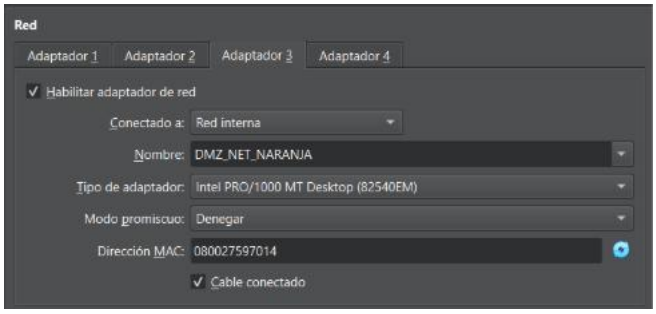


Fuente: Autoría Propia

- MAQUINA SERVIDOR QUE MANEJA LA RED NARANJA DMZ DEBIAN SERVER

ADAPTADOR 3 INTERCONEXIÓN A RED NARANJA DMZ

Figura 12. Configuración adaptador 3 red DMZ maquina Debian Server



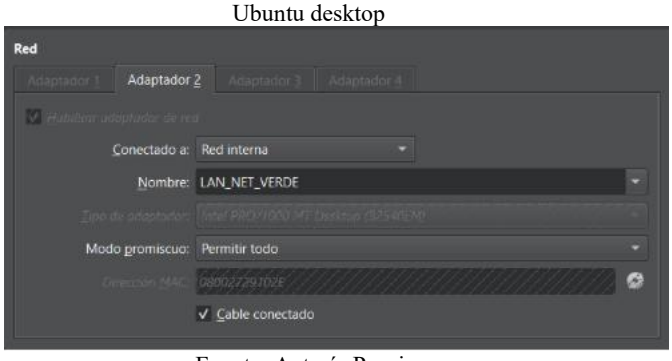
Fuente: Autoría Propia.

- MAQUINA UBUNTU DESKTOP

ADAPTADOR 2 INTERCONEXIÓN A RED VERDE LAN

Ahora ya configuradas los adaptadores de red en cada maquina ahora se montará la ISO de Endian para arrancar con su instalación

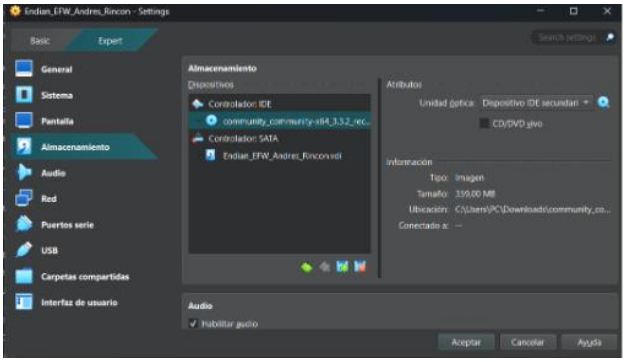
Figura 13. Configuración adaptador 2 red LAN maquina Ubuntu desktop



Fuente: Autoría Propia.

El Ahora ya configuradas los adaptadores de red en cada maquina ahora se montará la ISO de Endian para arrancar con su instalación

Figura 14. Panel de configuración almacenamiento maquina Endian



Fuente: Autoría Propia.

2.1.4 INSTALACIÓN DE ENDIAN FIREWALL

Se iniciará la instalación respectiva de Endian, primero se dará selección del lenguaje en este caso ingles ya que no está el español

Figura 15. panel de instalación Endian selección de idioma

Fuente: Autoría Propia.

Se realizo configuración de disco como tal la predeterminada

Figura 16. panel de instalación Endian

Fuente: Autoría Propia.

Después se solicitará la dirección IP y la máscara de subred de la interfaz de zona verde.

Figura 17. panel de instalación Endian

Fuente: Autoría Propia.

Se agrego la IP 192.168.0.15 y mascara de subred 255.255.255.0; ya se finalizó la instalación de Endian de forma exitosa en virtual box con las zonas de red configuradas exitosamente

Figura 17. panel de instalación Endian finalización instalación

Fuente: Autoría Propia.

Ya después se realizó automáticamente el reinicio del sistema y ya después de realizado empieza a cargar la consola de Endian, aclaro que la IP direccionada para la red verde se cambió más adelante por protocolo de red y funcionamiento de conexiones

Figura 18. panel de arranque firewall Endian

Fuente: Autoría Propia.

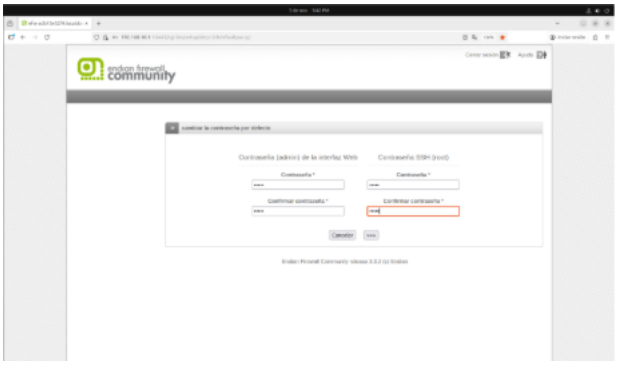
Como se evidencia cargo de forma exitosa y ya se pueden realizar procedimientos administrativos del panel y consola de Endian con el enlace que nos proporciona que es https://192.168.0.15:10443 con la IP de zona verde o la URL https://192.168.10.1:10443 que es la IP zona naranja DMZ entonces desde el Ubuntu desktop se ingresara al panel Endian

Figura 19. panel de administración general Endian

Fuente: Autoría Propia.

Como se evidencia se ingresó de forma exitosa al Endian panel, ya después se ingresan a las opciones del idioma y contrato de licencia todo ok, pero ya en la parte llegamos a la sección de asignar contraseña.

Figura 20. Panel de administración Endian credenciales de acceso



Fuente: Autoría Propia.

Se asigno la respectiva contraseña de forma exitosa

2.1.5 CONFIGURAR INTERFACES Y ZONAS DESDE WEBADMIN

Se realizará configuración desde el asistente de configuración de red el modo de red y tipo de enlace para la Zona roja WAN como modo de red por enrutamiento y tipo de enlace por DHCP

Figura 21. Panel de administración Endian configuración red roja WAN

Fuente: Autoría Propia.

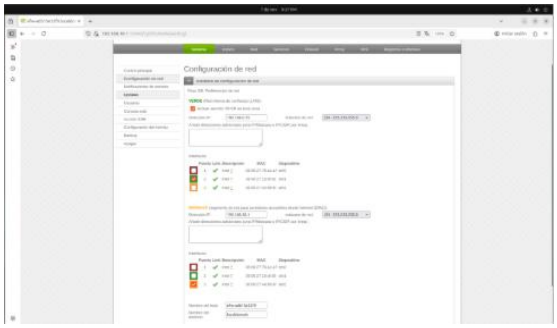
Luego el asistente ha detectado que hay más de 2 tarjetas de red en el hardware de la maquina entonces pregunta qué tipo de zona queremos añadir adicional a la verde y roja. Se seleccionará la NARANJA DMZ, dado que según el esquema de red de la actividad es una zona DMZ.

Figura 22. Panel de administración Endian selección red naranja DMZ

Fuente: Autoría Propia.

Ya después sigue la preferencia de la zona roja la red WAN aquí solo se aseguraría que este en la interfaz eth0 y que tenga el DNS automático.

Figura 23. Panel de administración Endian configuración redes.



Fuente: Autoría Propia.

Sigue la parte de configurar la dirección de correo del administrador o para montar un servidor de correo, en este caso se dejará vacío ya que no se necesita por el momento.

Figura 24. Panel de administración Endian configuración redes.

Fuente: Autoría Propia.

Listo ahora ya finalizando dice que se aplicó de forma exitosa y se da ok para aplicar la configuración.

Figura 25. Panel de administración Endian configuración general.

Fuente: Autoría Propia.

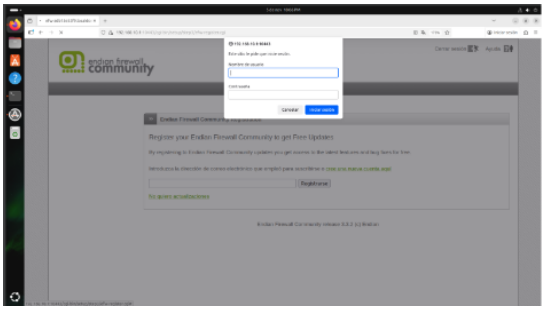
Ahora se pedirá el usuario y contraseña, se ingresa para acceder al panel.

Figura 26. Panel de administración Endian configuración general.

Fuente: Autoría Propia.

Accedió al panel de Endian de forma exitosa.

Figura 27. Panel de administración Endian ingreso a panel de administración.



Fuente: Autoría Propia.

Ahora se tomará evidencia de como quedo configurada la zona verde, naranja y roja en la topología de red.

Figura 28. Panel de general y monitoreo Endian.

Fuente: Autoría Propia.

ZONA ROJA NAT CORRESPONDIENTE AL INTERNET WAN

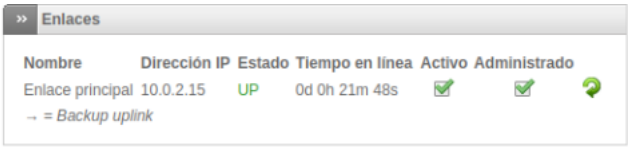
IP 10.0.2.15 subred /24 255.255.255.0

Figura 29. configuración de dispositivo eth0 red roja WAN

```
eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
 link/ether 08:00:27:75:a1:a7 brd ff:ff:ff:ff:ff:ff
 inet 10.0.2.15/24 brd 10.0.2.255 scope global eth0
```

Fuente: Autoría Propia.

Figura 30 Configuración de enlace principal correspondiente a red WAN



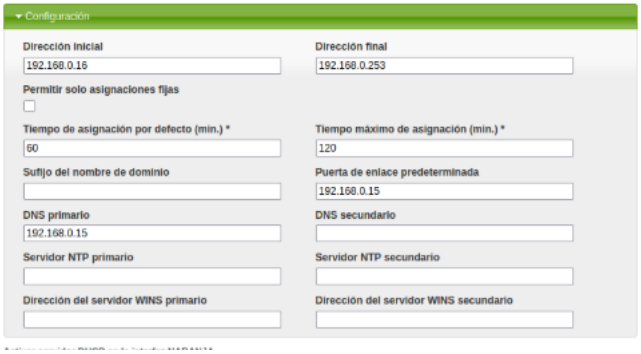
Fuente: Autoría Propia.

ZONA VERDE RED INTERNA CORRESPONDIENTE AL INTERNET LAN

IP red verde LAN 192.168.0.15

IP asignada maquina cliente Ubuntu desktop 192.168.0.16

Figura 31. configuración general de segmentos de red verde LAN



Fuente: Autoría Propia.

ZONA NARANJA RED INTERNA CORRESPONDIENTE AL INTERNET DMZ

IP red naranja DMZ 192.168.10.1

IP asignada maquina servidor debían server 192.168.10.2

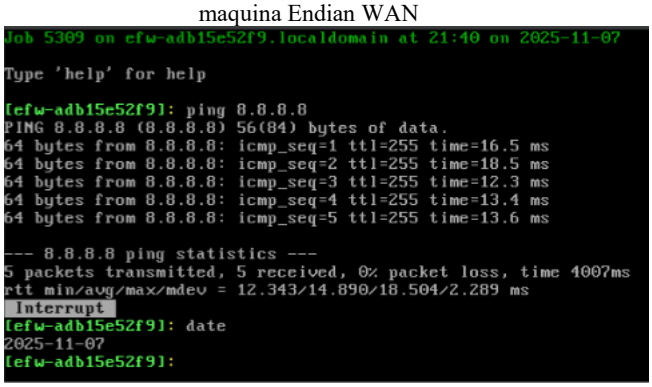
Figura 32. Configuración general de segmentos de red naranja DMZ

Fuente: Autoría Propia.

2.1.6 COMPROBACIÓN DE CONECTIVIDAD

Se comprobará en Endian primero que todo que haya conexión a internet en la red roja WAN realizando un ping 8.8.8.8 que es el DNS de Google.com

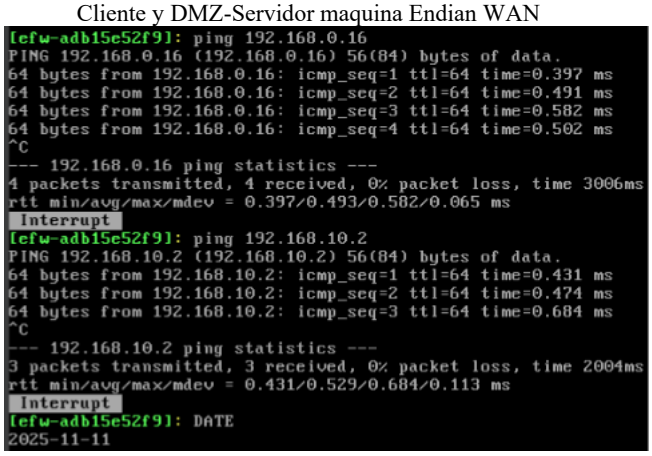
Figura 33. Realización de prueba de conexión hacia internet maquina Endian WAN



Fuente: Autoría Propia.

Se ve que está respondiendo exitosamente hacia internet, ahora se validara que tenga la red roja WAN conexión a la maquina cliente y servidor parametrizadas en la red verde LAN y red naranja DMZ respectivamente

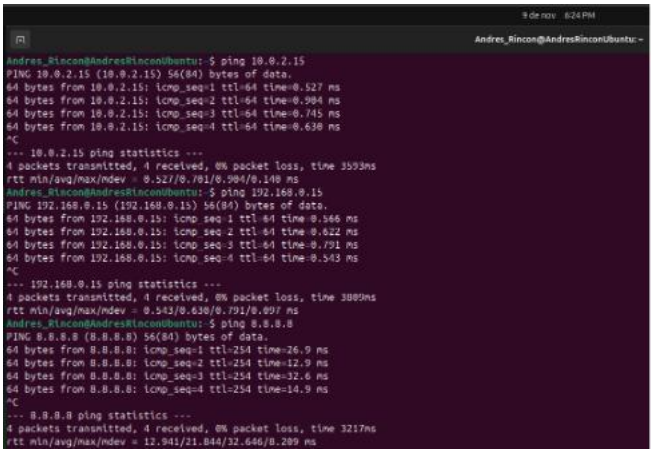
Figura 34. Realización de prueba de conexión hacia LAN-Cliente y DMZ-Servidor maquina Endian WAN



Fuente: Autoría Propia.

Ahora se comprobará la conectividad desde la estación LAN que en este caso es la maquina Ubuntu desktop, para ello se hará prueba con los comandos ping 10.0.2.15 que es el Gateway de endian ping al DNS principal de la red verde LAN asignada al firewall con ping 192.168.0.15 y ping 8.8.8.8 que es la prueba para ver si responde a internet

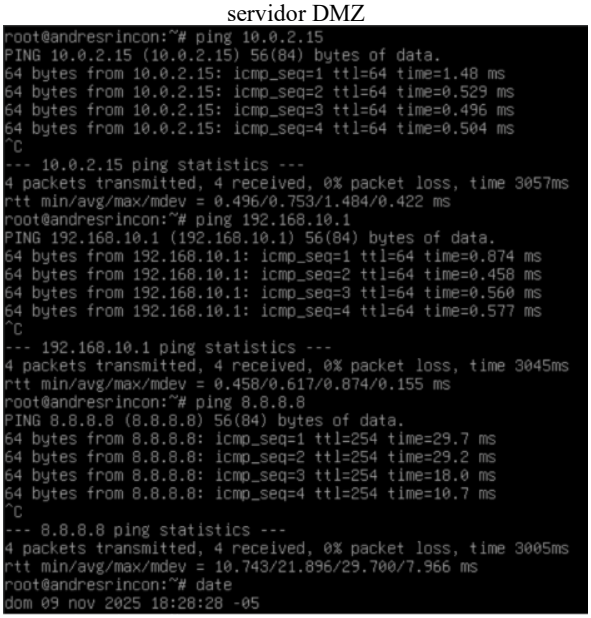
Figura 35. Realización de prueba de conexión a máquina cliente LAN



Fuente: Autoría Propia.

Como se evidencia el Gateway del firewall endian, el DNS asignado y la conexión a internet responden de forma exitosa en la maquina cliente interconectada a la zona verde LAN. Ahora se realizará la misma prueba con la maquina servidor que en este caso es debian servidor que aloja la red naranja DMZ que se le asigno la ip como DNS primario 192.168.10.1

Figura 36. Realización de prueba de conexión a máquina servidor DMZ



Fuente: Autoría Propia.

Como se evidencia el Gateway del firewall endian, el DNS asignado y la conexión a internet responden de forma exitosa en la maquina servidor interconectada a la zona naranja DMZ.

2.2 TEMATICA 2: CONFIGURACION NAT

2.2.1 CONFIGURACIÓN DE NETWORK ADDRESS TRANSLATION (NAT)

Después de llevar a cabo con éxito la infraestructura perimetral en la Temática 1, en la que se establecieron y ajustaron las tres áreas de seguridad (Verde, Naranja y Roja), el siguiente objetivo fue proporcionar a estas redes internas la capacidad esencial para comunicarse con Internet (WAN). En esta parte se detalla cómo se realizó la traducción de direcciones de red (NAT) en el Endian Firewall, con el fin de asegurar la conectividad entre la LAN y la DMZ, cumpliendo así con los resultados esperados de la Temática 2.

2.2.2 METODOLOGÍA DE IMPLEMENTACIÓN DEL SOURCE NAT

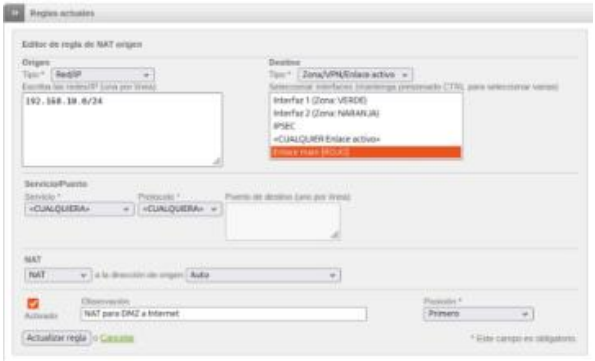
La preparación se centró en la creación de normas de NAT de origen, conocido también como Masquerading, un mecanismo clave que posibilita que dispositivos con IPs privadas accedan a Internet al convertir su dirección de origen a la única dirección IP pública que se ha asignado a la interfaz Roja (WAN) del cortafuegos.

Se definieron dos reglas específicas en la sección de "NAT Fuente":

REGLA DMZ A WAN

Se creó una regla para habilitar la salida de la Zona Naranja (DMZ), definida por la subred 192.168.10.0/24, hacia el Enlace principal [ROJO].

Figura 37. Creación de regla zona naranja

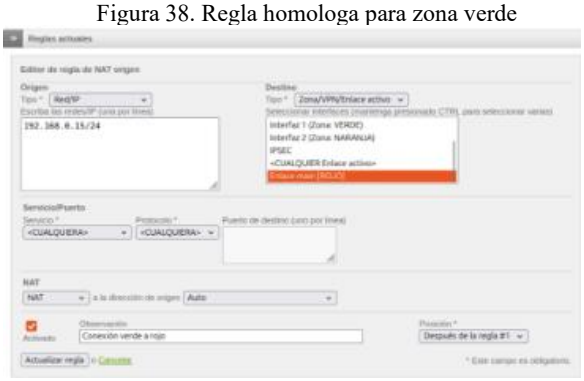


Fuente: Autoría Propia.

REGLA LAN A WAN

Se implementó la regla homóloga para la Zona Verde (LAN) (definida en la subred 192.168.0.15/24), con destino al Enlace principal [ROJO]

Figura 38. Regla homologa para zona verde



Fuente: Autoría Propia.

Ambas normativas fueron establecidas utilizando la política NAT Auto/Masquerade y el servicio correspondiente, garantizando que toda la información que sale sea traducida. La comprobación de las reglas creadas en el reenvío de puertos/NAT, conforme a lo solicitado por el producto esperado, se presenta en la Figura 38, donde se pueden ver las reglas vigentes de la DMZ y la LAN.

Figura 39. Reglas con política NAT

Fuente: Autoría Propia.

2.2.3 VERIFICACIÓN Y RESULTADOS FUNCIONALES

Para comprobar que el NAT fue implementado de manera adecuada, se llevaron a cabo pruebas de conexión desde las consolas de los dispositivos de cada área, tal y como se indica en la guía, registrando la fecha y hora de la realización.

PRUEBA DMZ -> WAN

La comprobación desde la terminal del Servidor Ubuntu (DMZ) se llevó a cabo utilizando el comando date y ping 8. 8. 8. 8 -c 4. La salida favorable (0% de pérdida de paquetes), mostrada en la Figura 40, valida que la regla NAT DMZ -> WAN funciona correctamente.

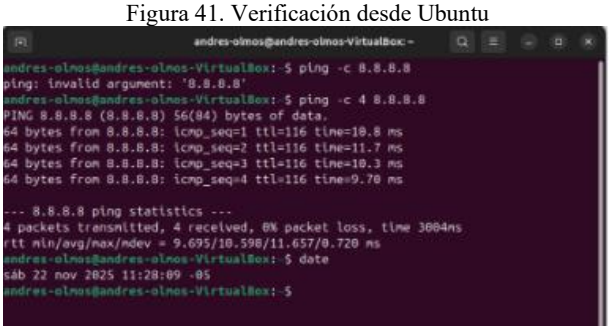
Figura 40. Comprobación desde la terminal

Fuente: Autoría Propia.

PRUEBA LAN -> WAN

La verificación desde el escritorio de Ubuntu (LAN) también mostró una respuesta positiva, demostrando que la conexión de la LAN con Internet se realizó correctamente, tal como se indica en la Figura 41.

Figura 41. Verificación desde Ubuntu



Fuente: Autoría Propia.

2.3 TEMATICA 3: PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED.

2.3.1 SERVICIOS DESDE LA DMZ

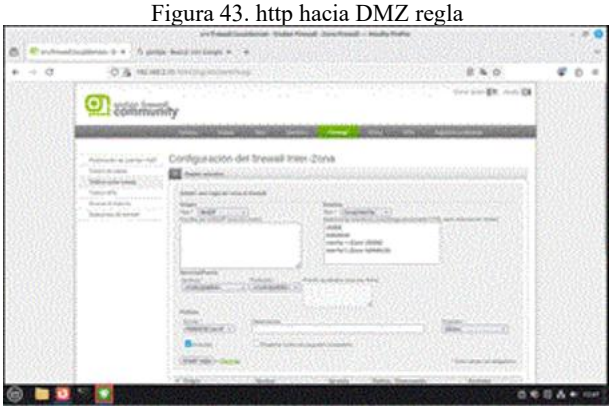
HTTP HACIA EL SERVIDOR DMZ (PERMISOS HTTP PUERTO 80)

- El Origen: 192.168.0.15/24 (Linux Mint)
- Destino: Zona NARANJA
- Servicio: TCP/80 (HTTP)
- Acción: PERMITIR
- Propósito: Acceso a servicios web del servidor Ubuntu

Figura 42. http hacia DMZ

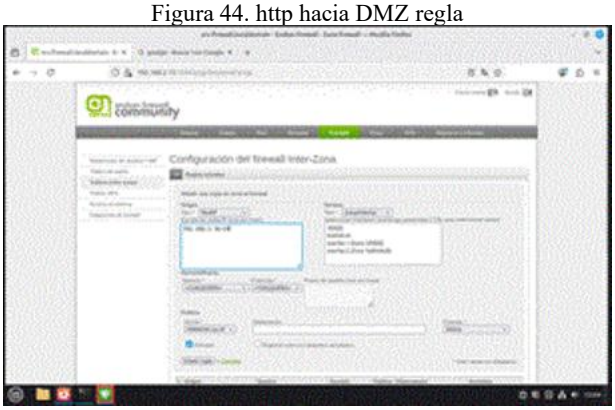
Fuente: Autoría Propia.

Figura 43. http hacia DMZ regla



Fuente: Autoría Propia.

Figura 44. http hacia DMZ regla

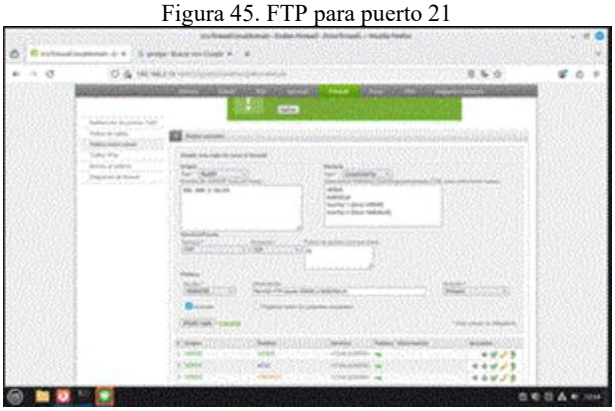


Fuente: Autoría Propia.

PERMISO FTP PARA (PUERTO 21)

- Origen: 192.168.0.15/24 (Linux Mint)
- Destino: Zona NARANJA
- Servicio: TCP/21 (FTP)
- Acción: PERMITIR
- Propósito: Transferencia de archivos al servidor DMZ

Figura 45. FTP para puerto 21

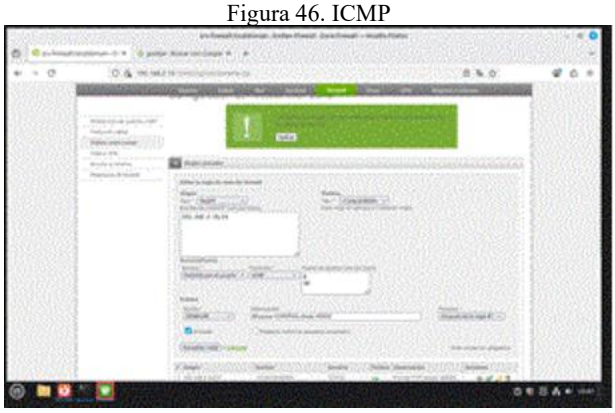


Fuente: Autoría Propia.

BLOQUO ICMP

- Origen: 192.168.0.15/24 (Linux Mint)
- Destino: Zona NARANJA
- Servicio: ICMP/8 (Echo Request)
- Acción: DENEGAR
- Propósito: Prevención de descubrimiento de hosts via ping

Figura 46. ICMP



Fuente: Autoría Propia.

2.3.2 IMPLEMENTACION

CONFIGURACIÓN DE REGLAS

Las reglas se configuraron en la sección "Trafico entre zonas" del Endian Firewall Community 3.3.2, asegurando el orden de procesamiento correcto para la evaluación de políticas.

SERVICIOS IMPLEMENTADOS

- Servidor Web: Python HTTP Server en puerto 80
- Servidor FTP: Netcat listener en puerto 21
- Cliente de pruebas: Linux Mint 22.2
- Todas las Reglas en general ya aplicadas

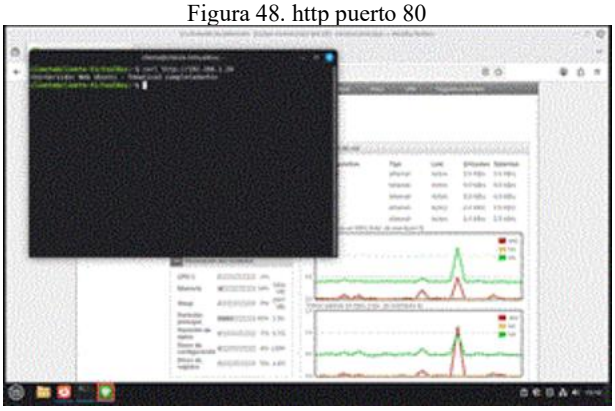
Figura 47. Servicios

Fuente: Autoría Propia.

2.3.3 RESULTADOS Y VERIFICACION

PERMITIR HTTP (PUERTO 80) – FUNCIONA

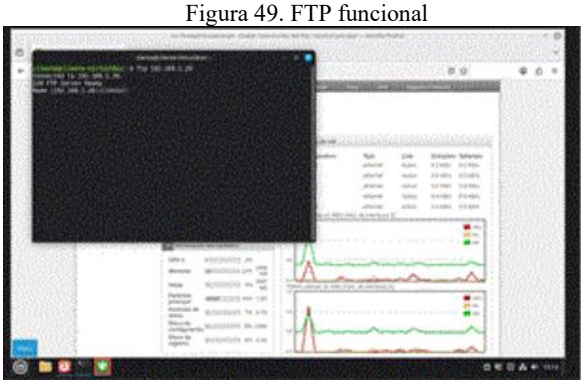
Figura 48. http puerto 80



Fuente: Autoría Propia.

PERMITIR FTP – FUNCIONAL

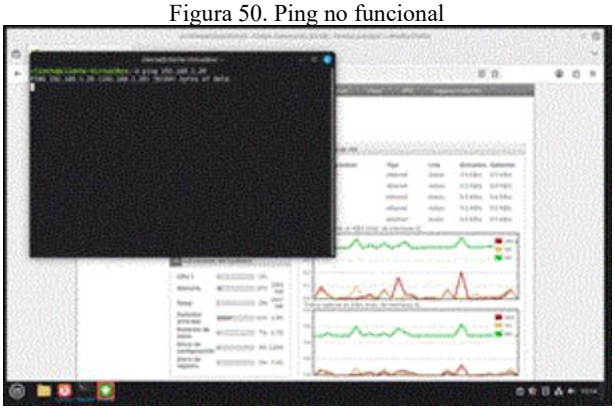
Figura 49. FTP funcional



Fuente: Autoría Propia.

DENEGAR PING – NO FUNCIONAL

Figura 50. Ping no funcional



Fuente: Autoría Propia.

No arroja ningún ping ni paquetes enviados, por ende, podemos concluir que se bloqueó el PING

2.3.4 ANALISIS DE SEGURIDAD

EFECTIVIDAD DE LAS POLÍTICAS

- La configuración implementada demuestra:
- Control granular sobre servicios permitidos
- Bloqueo efectivo de protocolos no esenciales
- Aislamiento adecuado de la zona DMZ

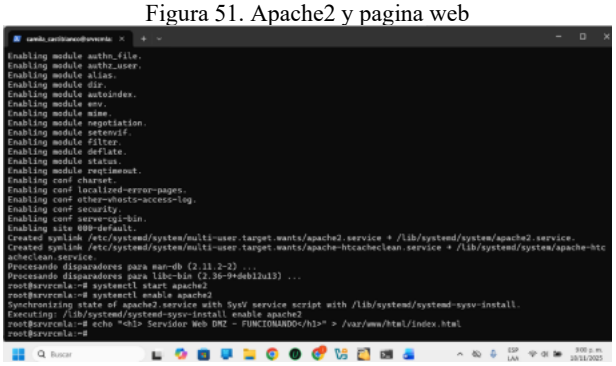
CUMPLIMIENTO DE OBJETIVOS

- Servicios HTTP y FTP accesibles desde red interna
- Protocolo ICMP completamente bloqueado
- Reglas de firewall verificadas y operativas

2.4 TEMATICA 4: REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO

Se ha instalado apache2 y se creó una pequeña página web para realizar las pruebas desde el cliente.

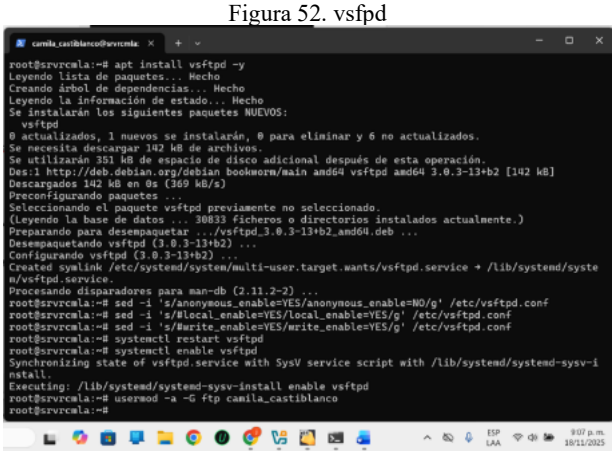
Figura 51. Apache2 y pagina web



Fuente: Autoría Propia.

Se ha instalado vsftpd y se ha agregado el usuario camila_castiblanco para realizar la prueba desde el cliente.

Figura 52. vsfpd

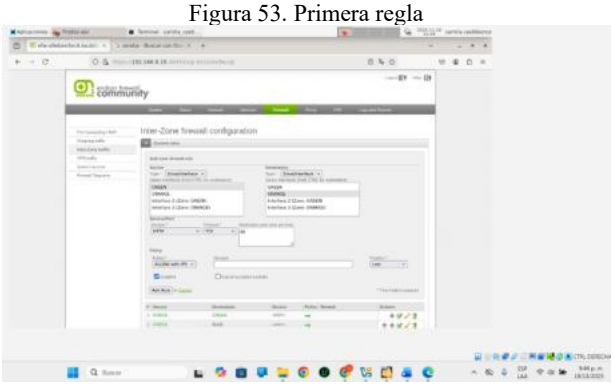


Fuente: Autoría Propia.

2.4.1 COMUNICAR LA ZONA VERDE CON LA ZONA NARANJA CON EL PROTOCOLO HTTP Y FTP CON SUS RESPECTIVOS PUERTOS.

Se creo la primera regla para establecer la comunicación de la zona verde con la zona naranja, específicamente con el servicio http.

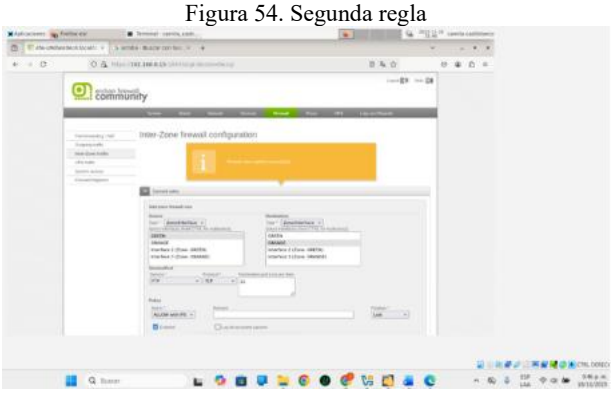
Figura 53. Primera regla



Fuente: Autoría Propia.

Se creo la segunda regla, en este caso, con el servicio ftp.

Figura 54. Segunda regla

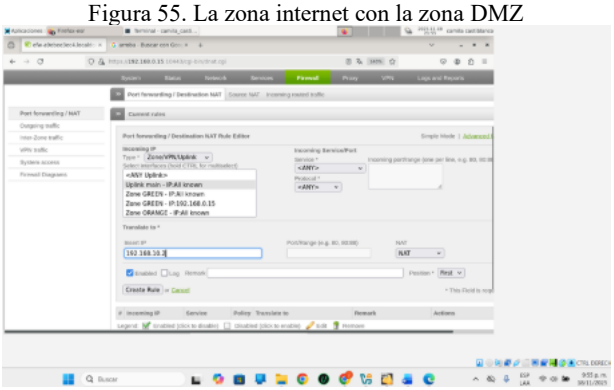


Fuente: Autoría Propia.

2.4.2 COMUNICAR LA ZONA INTERNET CON LA ZONA DMZ.

Esta configuración nos permite que cualquier dispositivo de internet pueda acceder a nuestro servidor con la finalidad de utilizar un servicio. Como se observa en la imagen el direccionamiento para directamente por medio de la ip a nuestro servidor.

Figura 55. La zona internet con la zona DMZ



Fuente: Autoría Propia.

2.4.3 VERIFICAR EN EL TRÁFICO INTER - ZONA, LA CREACIÓN DE LAS REGLAS.

En el apartado de Inter zonas se puede observar que las reglas se han creado correctamente y que están activas, la única modificación que he realizado es ubicarlas al principio de la lista con el objetivo de que sean las primeras reglas que se cumplan.

Figura 56. Confirmación de reglas

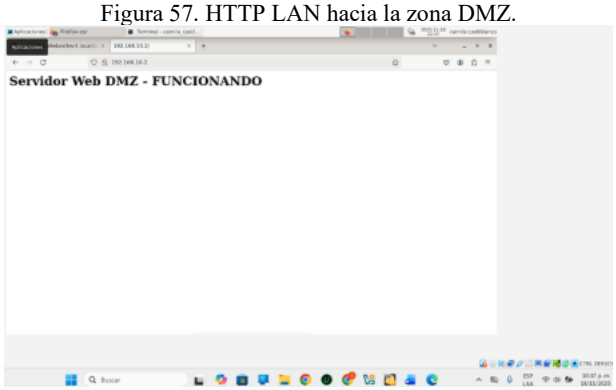
Fuente: Autoría Propia.

2.4.4 PROBAR DESDE UN NAVEGADOR WEB, LAS SIGUIENTES DIRECTIVAS.

EL INGRESO DEL SERVICIO HTTP DESDE LA LAN HACIA LA ZONA DMZ.

Desde el cliente se accedió a la página web almacenada en el servidor a través de la IP, como se observa en la imagen en la barra de direcciones.

Figura 57. HTTP LAN hacia la zona DMZ.



Fuente: Autoría Propia.

EL INGRESO DEL SERVICIO HTTP DESDE LA LAN HACIA LA WAN.

Nuevamente desde nuestro cliente hemos accedido a una página http almacenada en la red sin ningún inconveniente demostrando que la zona verde tiene acceso a internet.

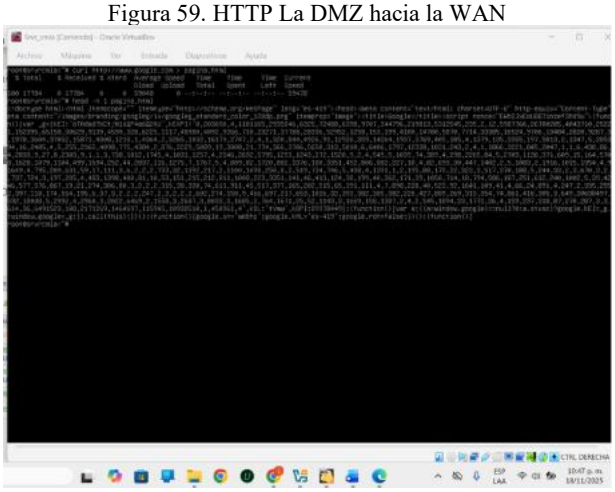
Figura 58. HTTP La LAN hacia la WAN

Fuente: Autoría Propia.

EL INGRESO DEL SERVICIO HTTP DESDE LA ZONA DMZ HACIA LA WAN.

A través del comando curl se realizó la descarga del código de una página http, como se observa en la imagen con el comando head se puede visualizar parte del contenido del código.

Figura 59. HTTP La DMZ hacia la WAN

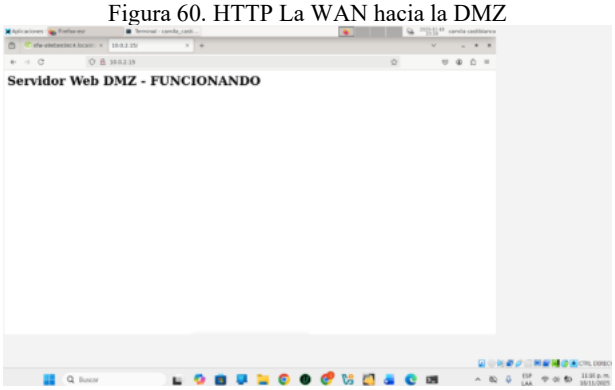


Fuente: Autoría Propia.

EL INGRESO DEL SERVICIO HTTP DESDE LA WAN HACIA LA ZONA DMZ.

Desde el cliente se accedió nuevamente a la página almacenada en el servidor, la diferencia radica, que en vez de utilizar la ip del servidor se utiliza la ip publica que nos proporción Endian, como hemos creado la regla de direccionamiento podemos acceder a la página sin inconvenientes.

Figura 60. HTTP La WAN hacia la DMZ

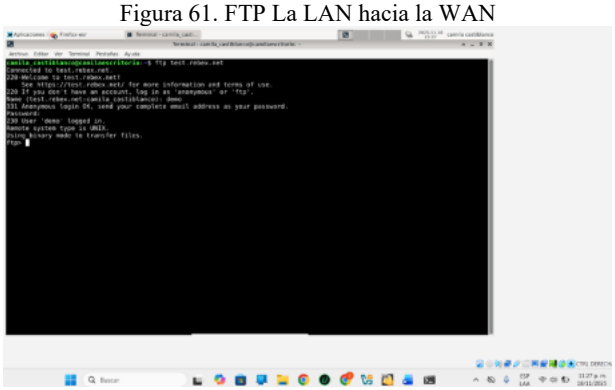


Fuente: Autoría Propia.

EL INGRESO DEL SERVICIO FTP DESDE LA LAN HACIA LA WAN.

Se accedió a un servidor ftp gratuito en línea desde nuestro cliente demostrando la conectividad.

Figura 61. FTP La LAN hacia la WAN

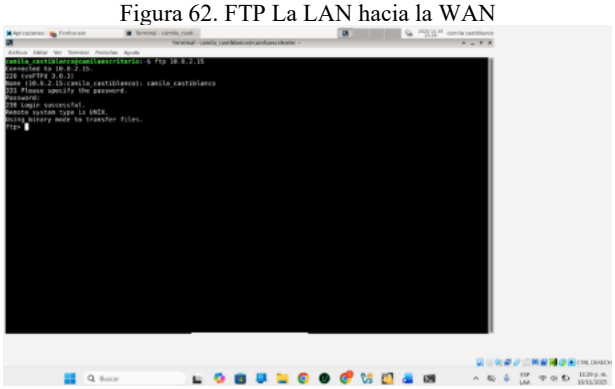


Fuente: Autoría Propia.

EL INGRESO DEL SERVICIO FTP DESDE LA WAN HACIA LA ZONA DMZ.

Desde el cliente a través de la ip que nos brinda Endian nos conectamos por medio ftp al servidor que está en la zona DMZ, por lo cual, el usuario es el mismo de las fases anteriores demostrando la veracidad de la conexión.

Figura 62. FTP La LAN hacia la WAN



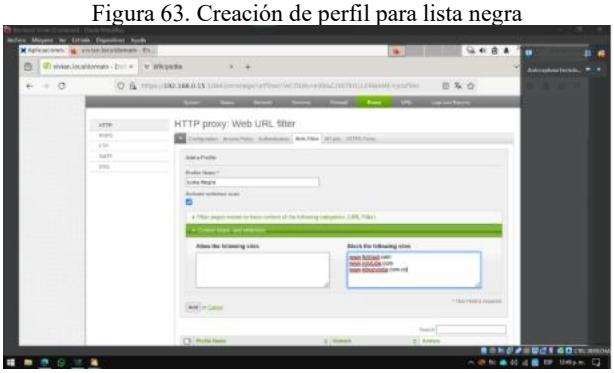
Fuente: Autoría Propia.

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

2.5.1 CREAR UN PERFIL Y ESTABLECER UNA LISTA NEGRA.

Primero procedimos a crear un perfil de filtrado donde establecimos una lista negra con los sitios bloqueados: www.hotmail.com, www.youtube.com y www.elnuevodia.com.co. Una vez definido el perfil, asociamos esta lista negra al mismo para que el proxy pueda aplicar las restricciones de navegación correspondientes.

Figura 63. Creación de perfil para lista negra



Fuente: Autoría Propia.

2.5.2 AUTENTICACIÓN POR USUARIO: A TRAVÉS DE LA OPCIÓN PROXY CREE UN USUARIO Y ASÓCIELO A UN GRUPO.

Creamos un perfil de usuario que nos servirá como base para aplicar las políticas de filtrado y autenticación.

Figura 64. Creación de perfil

Fuente: Autoría Propia.

Posteriormente, procedimos a crear un grupo de usuarios para organizar y gestionar de manera centralizada los permisos de acceso.

Figura 65. Creación de un grupo de usuarios

Fuente: Autoría Propia.

2.5.3 ESTABLEZCA UNA POLÍTICA DE ACCESO Y VINCULE EL PERFIL CREADO EN EL PUNTO ANTERIOR Y RELACIÓNELO TAMBIÉN CON LA POLÍTICA DE AUTENTICACIÓN.

Finalmente, creamos la política de acceso que asocia el grupo de usuarios con la lista negra de sitios bloqueados, estableciendo así las restricciones de navegación.

Figura 66. Política de acceso

Fuente: Autoría Propia.

2.5.4 PROBAR DESDE LA LAN A TRAVÉS DE UN NAVEGADOR WEB, EL ACCESO A LOS PORTALES REFERENCIADOS EN LA LISTA NEGRA.

Activamos y configuramos el proxy directamente en Firefox mediante la configuración de red del navegador.

Figura 67. Portales referenciados desde la LAN

Fuente: Autoría Propia.

Procedimos a activar el proxy configurando manualmente los parámetros en las opciones de red de Firefox.

Figura 68. Activar proxy

Fuente: Autoría Propia.

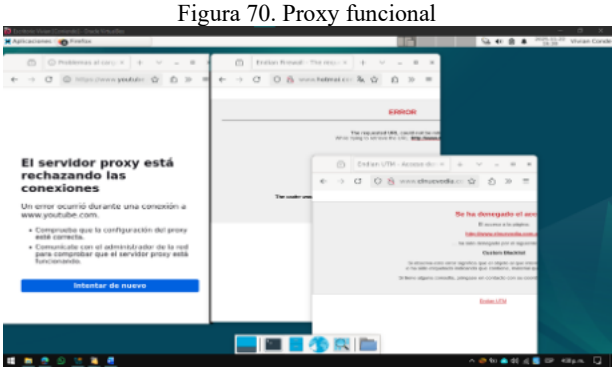
Introdujimos las credenciales de acceso (usuario y contraseña) que configuramos previamente en el proxy cuando nos apareció la ventana de autenticación.

Figura 69. Credenciales de acceso

Fuente: Autoría Propia.

Verificamos el correcto funcionamiento del filtro intentando acceder a los sitios de la lista negra, confirmando que el proxy mostraba páginas de bloqueo para www.hotmail.com, www.youtube.com y www.elnuevodia.com.co, mientras permitía el acceso a otros sitios web.

Figura 70. Proxy funcional



Fuente: Autoría Propia.

3 CONCLUSIONES

La creación del entorno de seguridad utilizando GNU/Linux Endian Firewall demostró de manera tangible cómo un firewall UTM puede dividir, regular y proteger de manera efectiva el tráfico entre diversas áreas de la red. La configuración de las zonas Verde (LAN), Naranja (DMZ) y Roja (WAN) subrayó la relevancia de la separación lógica para resguardar servicios críticos y minimizar la superficie de ataque.

La implementación de NAT de origen (Masquerading) garantizó un acceso controlado a Internet desde la LAN y la DMZ, cumpliendo con los requisitos de conectividad definidos. Las pruebas de funcionalidad realizadas a través de la consola, junto con la comprobación visual en el panel de Endian, confirmaron que las políticas de traducción y filtrado se aplicaron de forma correcta.

Además, la creación de reglas en el firewall facilitó una gestión detallada de los servicios accesibles en la DMZ, permitiendo solamente el tráfico HTTP y FTP, mientras se restringía el protocolo ICMP, lo que reforzó las medidas de seguridad recomendadas. Las pruebas de acceso entre las distintas zonas validaron el correcto desempeño de las políticas establecidas.

Por último, la integración del proxy HTTP con autenticación y listas negras demostró la capacidad de Endian para implementar políticas avanzadas de control de navegación, mejorando la administración del acceso a Internet desde la red interna. En su conjunto, esta actividad permitió entender de manera completa el diseño, la implementación y la gestión de un entorno perimetral seguro en una infraestructura virtualizada.

4 REFERENCIAS

[1] LPI LPIC-1 Exam 101. (2022). Tema 102: Comandos GNU y Unix . https://learning.lpi.org/es/learning-materials/101-500/102/

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

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

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

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

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

[7] Cervelión, Á. J. (2023). Instalación de Nagios Core 4.4 en Ubuntu 22.04. [Objeto_virtual_de_información_OVI]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/54230

[8] Cohen, D. (1981). *On holy wars and a plea for peace*. IEEE Computer Society. IEN 137.

[9] Internet Engineering Task Force (IETF). (1994). RFC 1700: Assigned Numbers. J. Reynolds & J. Postel (Eds.).

[10] Bryant, R. E., & O'Hallaron, D. R. (2016). *Computer systems: A programmer's perspective* (3rd ed.). Pearson.