IMPLEMENTACIÓN Y CONFIGURACIÓN DE FIREWALL PERIMETRAL ENDIAN LINUX

GRUPO 202338299_33

Edisson Camilo Frasica Triana
e-mail: ecfrasicat@unadvirtual.edu.co

RESUMEN: *Este informe detalla el proceso de configuración e implementación de una solución de seguridad perimetral con el uso de la distribución Endian Firewall Community (EFW) basada en GNU/Linux Se abordó la instalación del sistema, la definición de zonas de red (LAN, WAN y DMZ), y el establecimiento de reglas de firewall, Direcciones de Red NAT y reglas de tráfico Inter-Zona. Adicionalmente, se implementó un servidor proxy HTTP no transparente con políticas de autenticación y filtrado de contenido. Las configuraciones y pruebas realizadas simularon un escenario de red segmentado, validando la efectividad de las políticas de seguridad aplicadas y demostrando la capacidad de EFW para la protección perimetral y el control del tráfico de red*

PALABRAS CLAVE: LAN, WAN, DMZ, Protocolo, NAT

1 INTRODUCCIÓN

Este informe técnico describe la implementación y configuración de Endian Firewall Community (EFW), una distribución de seguridad perimetral basada en GNU/Linux, como parte de un ejercicio práctico del Diplomado de Profundización en Linux. El proyecto integra los principios fundamentales de un firewall con múltiples interfaces para gestionar una red LAN, una WAN y una Zona Desmilitarizada (DMZ). Se configuraron reglas de firewall, Traducción de Direcciones de Red (NAT) para el acceso interno y externo, y un proxy HTTP no transparente con políticas de autenticación y filtrado de URL.

Con lo que busca demostrar la capacidad de configurar y administrar eficazmente los componentes de seguridad esenciales, controlando el tráfico de red y asegurando los servicios publicados y validando la funcionalidad de cada componente de seguridad y las políticas de control de tráfico implementadas. Se documentaron los pasos de instalación, configuración y las pruebas realizadas, con el fin de consolidar las habilidades técnicas y el conocimiento en la administración de sistemas de seguridad.

2 INSTALACION ENDIAN

Configuración de la instancia para GNU/Linux Endian en Virtualbox (tarjetas de red) e instalación efectiva del mismo

Lo primero que se debe hacer es descargar el ISO de endian desde su página principal https://www.endian.com/en/community/ y luego se debe instalar desde cualquier programa de virtualización que maneje como VirtualBox, se le deben asignar los recursos necesarios para la gestión 20 GB de espacio mínimo y 2 GB de Ram y 2 CPU

después de asignar los recursos se debe dirigir a la zona de configuración de red donde se debe configurar las zonas GREEN, ORANGE Y RED.

En el adaptador 1 que será eth0 en el Firewall se configurará en modo NAT y se destina a la Zona ROJA (WAN), lo que permitirá a Endian obtener una dirección IP y tener salida a Internet

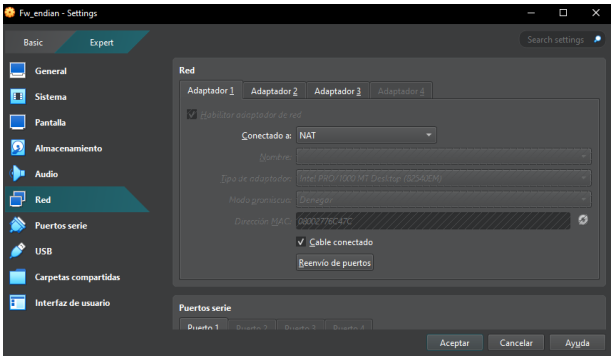

Imagen 1. Configuración de Tarjeta Zona RED

En el adaptador 2 que será eth1 en el Firewall se configurará como red interna LAN y esta se asigna a la Zona VERDE (LAN), la cual representará la red interna gestionada por el firewall

Imagen 2. Configuración de Tarjeta Zona GREEN

En el adaptador 3 que será eth2 en el Firewall se configurará como red interna DMZ y este se asigna a la Zona NARANJA (DMZ)

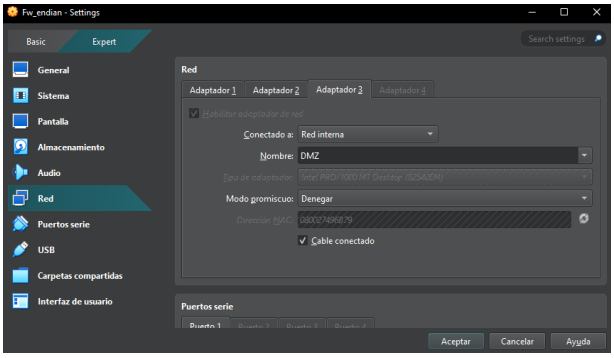

Imagen 3. Configuración de Tarjeta Zona ORANGE

Ahora debe proceder con la instalación, se debe proceder la selección del lenguaje deseado y se debe asignar una ip y Network mask con la cual representará la red interna (LAN) y será el punto de acceso para le gestión del firewall.

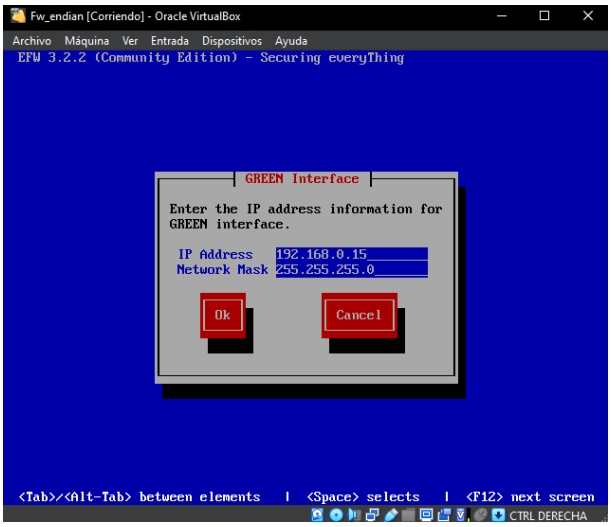

Imagen 4. Instalación Endian firewall.

Al finalizar la instalación desde la vm de endian debe ingresar el comando 5 para ingresar a la configuración de las interfaces de las zonas configuradas previamente donde se deberá configurar nombre del dominio y nombre del hostname para eth0 (Zona ROJA), usualmente se mantiene la configuración por defecto (DHCP). Para eth1 (Zona VERDE), se confirma la IP asignada durante la instalación.
Para eth2 (Zona NARANJA), se asigna una IP dentro del rango definido para la DMZ

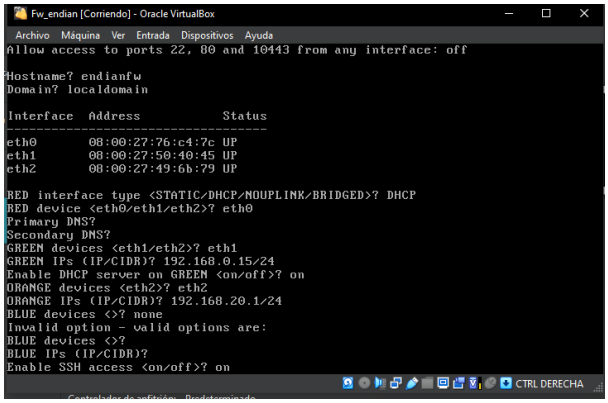

Imagen 5. Configuración Network Endian

después de finalizar la configuración de endian, se valida el estatus donde debe visualizar la dirección de gestión para el firewall y la ip y los devices configurados previamente

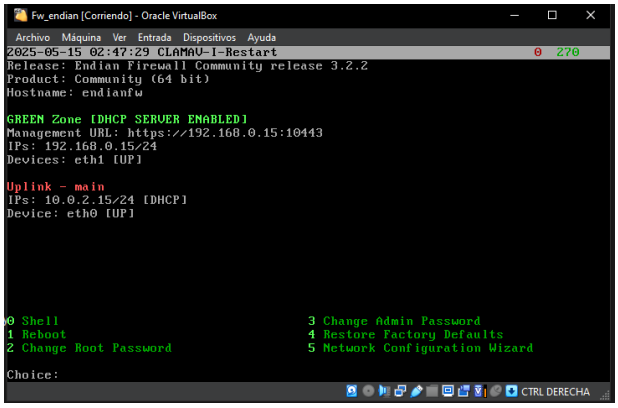

Imagen 6. Estatus de la configuración en Endian Firewall

Ahora se debe dirigir a la VM cliente LAN en la zona verde y se deben validar que tenga la interface asignada correctamente y la ip

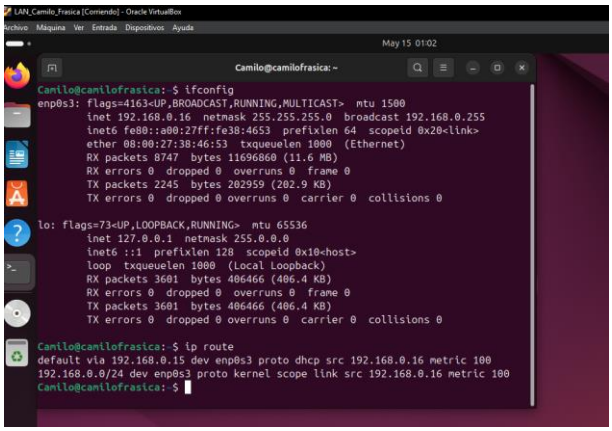

Imagen 7. Estatus zona verde

Debe ingresar a la dirección que se visualizó en endian para entrar a la gestión del firewall y validar el acceso

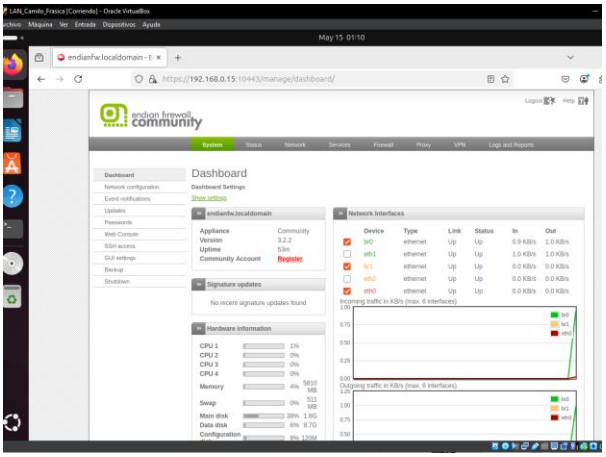

Imagen 8. Acceso a url de gestión del firewall endian

Se debe dirigir ahora a la url de gestión del firewall y configurar las dos zonas verde y naranja, para la zona verde debe verificar que el servidor DHCP esté habilitado para la interfaz green, luego debe asignar un rango de ips de inicio y una de finalización, y luego asignar la ip de gestión de endian a la puerta de enlace y dns

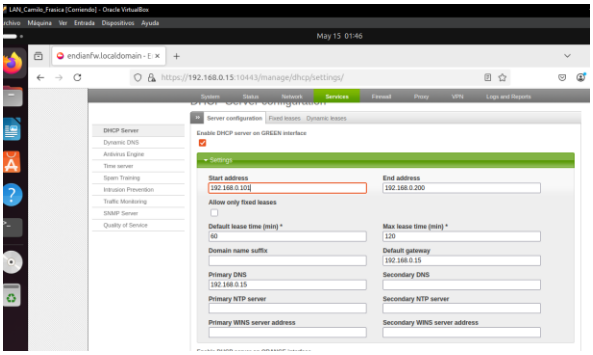

Imagen 9. configuración DHCP zona verde

Ahora debe dirigirse a la configuración de la zona naranja y habilitarla debe seleccionar un rango de ips nuevamente y como dns y puerta de enlace debe usar la ip que se configura en endian previamente para eth2

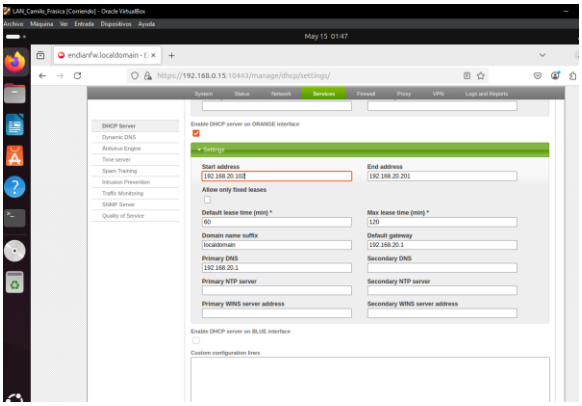

Imagen 10. configuración DHCP zona naranja

3 TEMATICA 2

Configuración de regla NAT para generar la comunicación desde la LAN y DMZ hacia la WAN, para luego establecer comunicación hacia internet.

Se debe dirigir a la interfaz web de administración de endian se debe dirigir a Firewall y a outgoing traffic para crear una nueva regla, debe asigar la zona verde y naranja como recurso y destino la zona roja (WAN) y habilitar el protocolo TCP-UDP y no asignar puertos para que permita cualquiera, luego deberá marcar enable asignarle el nombre a la regla y permitir allow ips para que permita cualquier ip

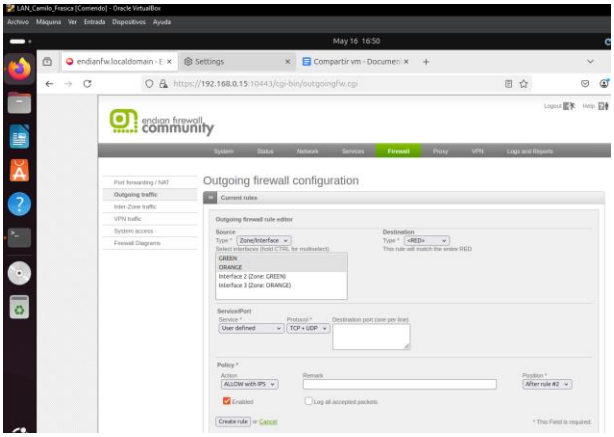

Imagen 11. configuración regla tráfico TCP-UDP

después de crea la regla necesaria debe ubicar la regla por prioridad para que esta tome control según el orden que requiera para su configuración.

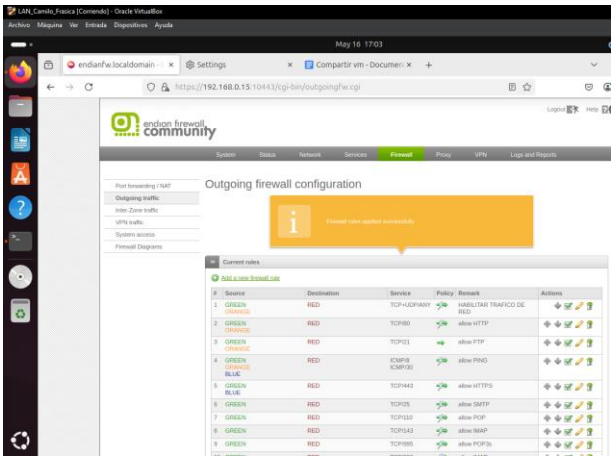

Imagen 12. Prioridad de reglas de Firewall

Ahora se debe configurar la IP estática definida para la interfaz naranja (DMZ), asegurándose de que esté dentro del segmento de red, pero gestionada estáticamente en el servidor, se debe dirigir a /etc/netplan/ y editar el archivo. yalm con la dirección estática, la puerta de enlace configurada para la zona naranja y los servidores DNS con ip de la zona naranja y un dns publico

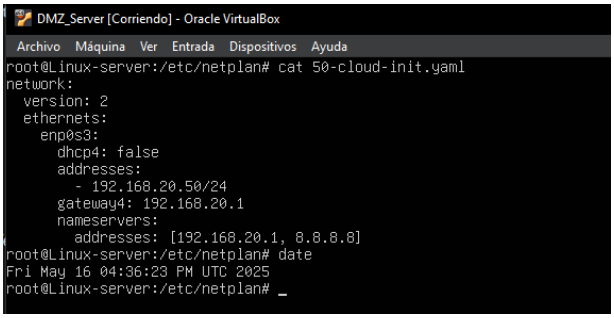

Imagen 13. Configuración ip estática DMZ

Para verificar que el tráfico de las Zonas VERDE (LAN) y NARANJA (DMZ) pueda salir a Internet, debe verificar la configuración del enlace principal Main uplink en Endian Firewall, en la opción de Network e Interfaces, donde deberá observar el Main uplink, asociado al dispositivo eth0 correspondiente a la Zona ROJA/WAN

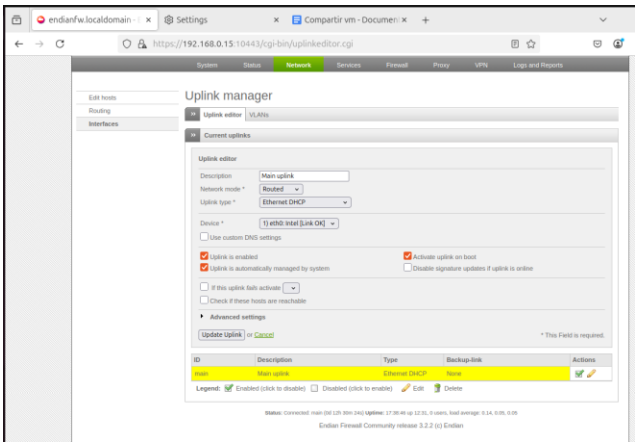

Imagen 14. Verificación Main uplink Zona ROJA

Una vez verificada la configuración para comprobar la comunicación desde la Zona VERDE (LAN) hacia la WAN debe realizar pruebas de conexión y verificar la salida a internet desde LAN

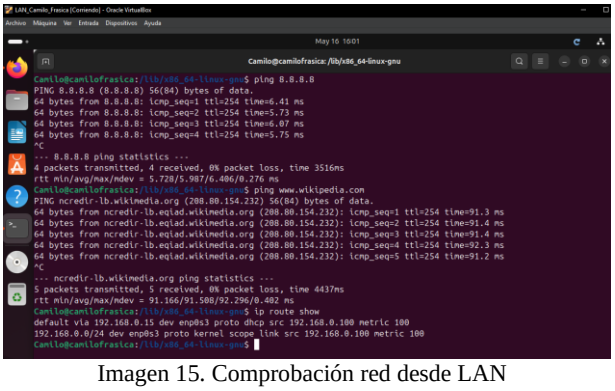

Imagen 15. Comprobación red desde LAN

Luego debe dirigirse y realizar las mismas pruebas desde su servidor de DMZ para comprobar la comunicación desde la Zona NARANJA (DMZ) hacia Internet.

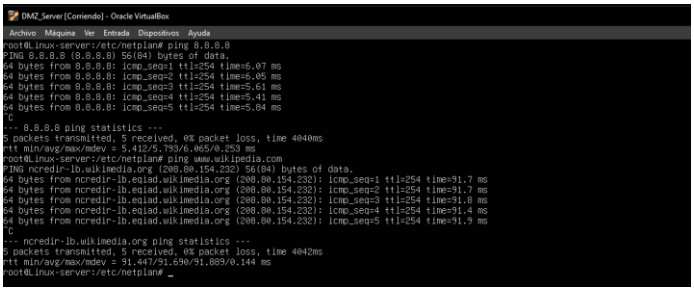

Imagen 16. Comprobación red desde DMZ

4 TEMATICA 3

Configuración de servicios en la zona DMZ, para permitir el tráfico HTTP, FTP y denegación de ICMP

Desde la interfaz web de administración de endian se debe dirigir inicialmente a Firewall y a outgoing traffic para crear las reglas de puertos.

Para la primera regla debe establecer el recurso en interface y seleccionar las zonas verde y naranja como origen y como destino la zona roja, luego selecciona el servicio como http y protocolo TCP con el puerto 80 y selecciona allow para todas las ips, debe seleccionar la casilla enable y aplicar la regla

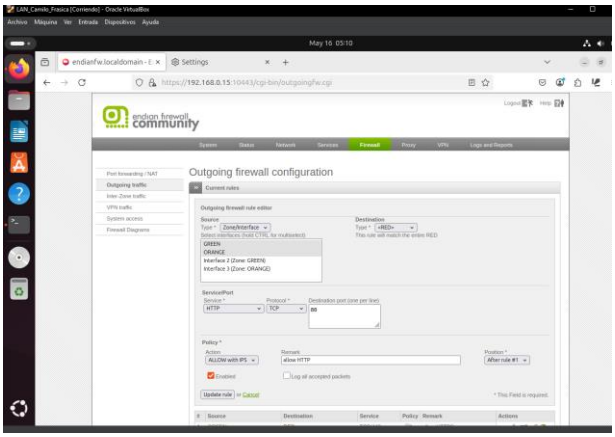

Imagen 17. Configuración para permitir el tráfico HTTP

Para la segunda regla debe seleccionar la zona verde y naranja y destino igualmente la zona roja. Ahora debe configurar para el servicio FTP y protocolo TCP con el puerto 21, y la política en allow

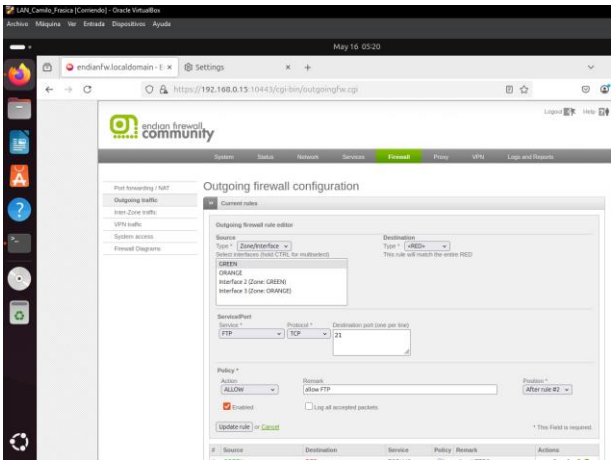

Imagen 18. Configuración para permitir el tráfico FTP

Para la tercera regla en la que deberá configurar para la zona verde y naranja y destino a la zona rojas (WAN), debe seleccionar el protocolo ICMP con los puertos 8 y 30, después en action seleccionar Deny, con esta regla deberá de bloquear las solicitudes de ping originadas desde las redes internas hacia la WAN

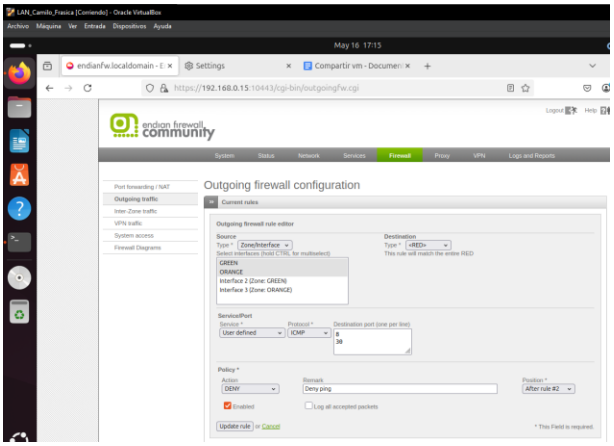

Imagen 19. Configuración para denegar ICMP, ports 8,30

después de crear las reglas necesarias debe ubicar las reglas por prioridad nuevamente.

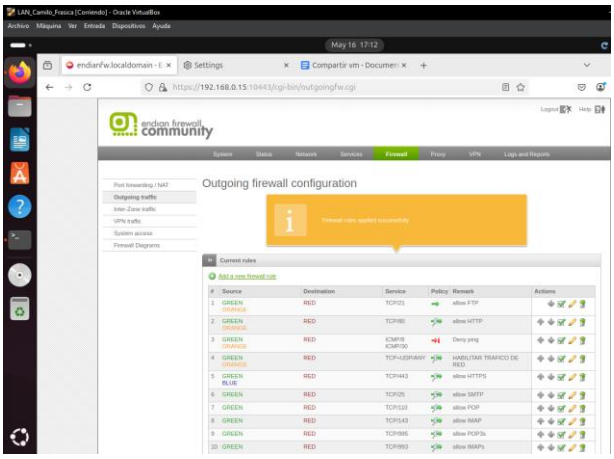

Imagen 20. Prioridad de reglas de Firewall

Puede hacer validación también de que los puertos configurados estén escuchando el puerto 21 (FTP) y 80 (HTTP).

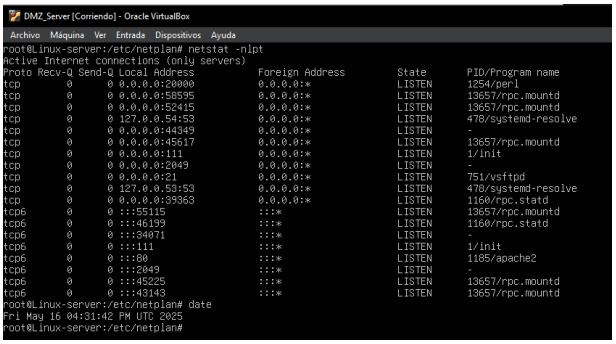

Imagen 21. Validación netstat

Ahora debera comprobar que las reglas tengan el comportamiento esperado desde la consola se deben ralizar pruebas de ping y/o telnet al dns y a urls estas deberán fallar desde la zona naranja (DMZ) y verde (LAN)

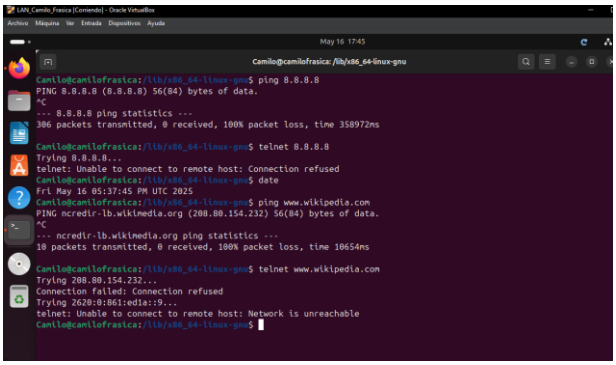

Imagen 22. Validación regla deny zona verde

Para probar la conexión a los puertos allow como el 80 HTTP debería poder ingresar a alguna url desde el navegador

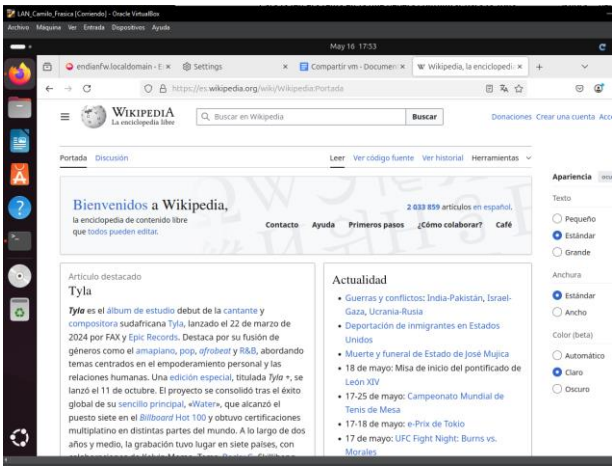

Imagen 23. Validación regla puerto 80 HTTP zona verde

Para la dmz al usar ping y telnet deberán ser denegados y al realizar curl -v a una url esta deberia ser permitida ya que se esta conectara por el puerto 80 el cual esta permitido en las reglas configuradas previamente.

Imagen 24. Validación reglas zona naranja

5 TEMATICA 4

Se verifica que están activas y estén las dos reglas configuradas previamente para el puerto 80 HTTP y 21 FTP

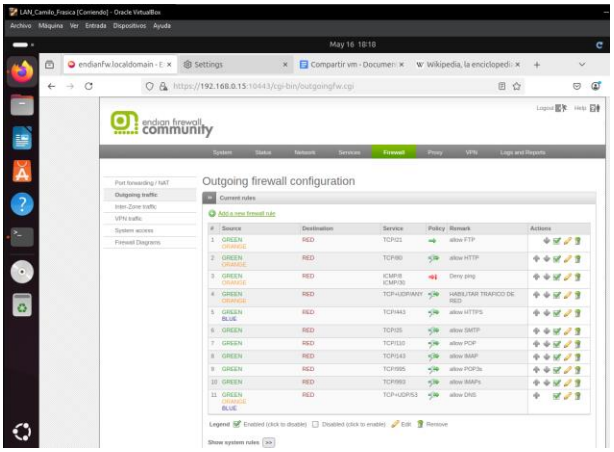

Imagen 25. Validación reglas para FTP Y HTTP activas

Ahora debe dirigirse a Inter-Zone traffic, donde se configurará la comunicación de la zona verde con la zona naranja para HTTP Y FTP.

Se crea una nueva regla para HTTP la cual debe seleccionar como recurso la zona verde y destino la zona naranja, con el servicio HTTP por TCP y el puerto 80

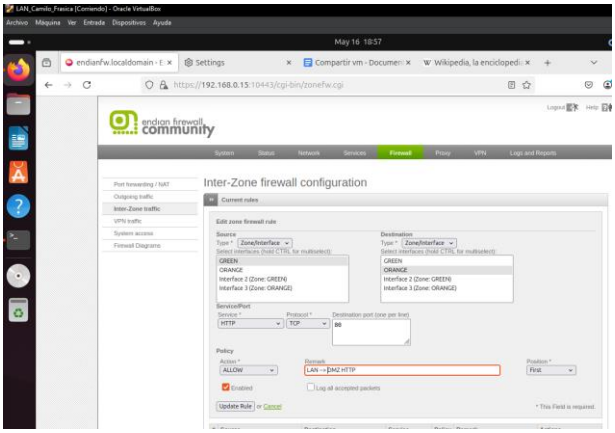

Imagen 26. Configuración HTTP de zona verde a naranja

Se crea una nueva regla para FTP la cual debe seleccionar como recurso la zona verde y destino la zona naranja, con el servicio FTP por TCP y el puerto 21

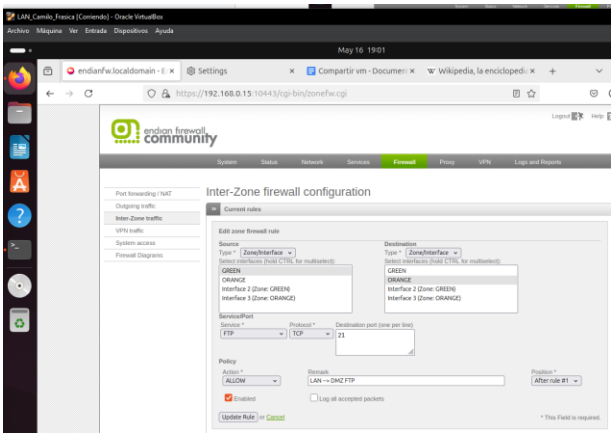

Imagen 27. Configuración FTP de zona verde a naranja

Ahora deberá dirigirse a la opción de port forwarding / destination NAT y deberá crear dos forwarding para permitir el direccionamiento de la (WAN) hacia la DMZ

Para el primer forwarding se configurará para el direccionamiento de FTP, debe elegir en incoming ip sea el uplink main IP all, y en el servicio deberá ser FTP y TCP por el puerto 21, y en translate to se deberá usar la ip estática de su dmz asignada y el puerto 21 con NAT la cual se configuro para la zona naranja

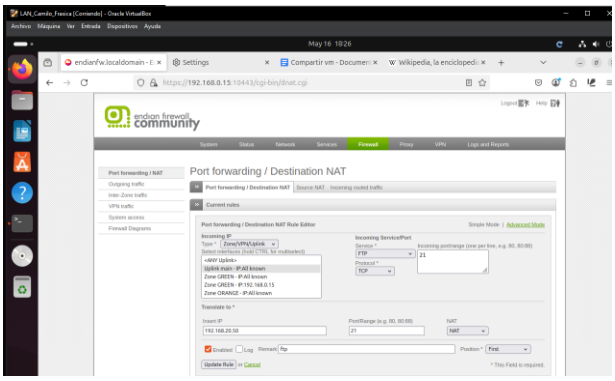

Imagen 28. Configuración forwarding para FTP

Para el segundo forwarding se configurará para el direccionamiento de HTTP, debe elegir en incoming ip sea el uplink main IP all, y en el servicio deberá ser HTTP y TCP por el puerto 80, y en translate to se deberá usar la ip estática de su dmz asignada y el puerto 80 con NAT la cual se configuro para la zona naranja

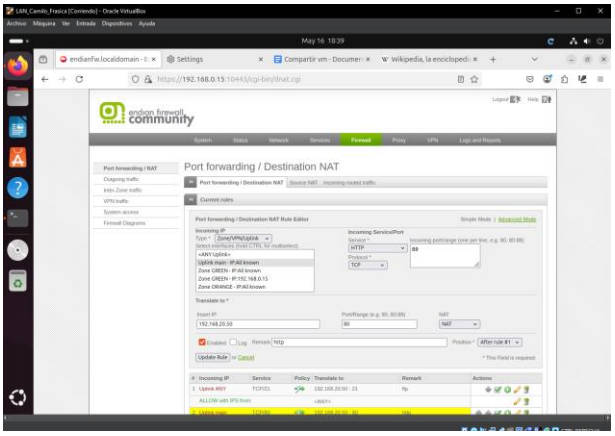

Imagen 29. Configuración forwarding para HTTP

Deberá comprobar las reglas creadas y que estén en la prioridad necesaria

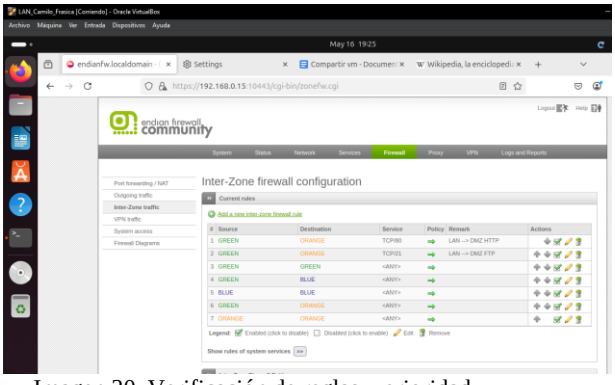

Imagen 30. Verificación de reglas y prioridad

Para realizar pruebas de conexión con las reglas configuradas se recomienda instalar servicios para FTP y HTTP

Desde su dmz debe usar el comando sudo apt install apache2 vsftpd, para instalar los servicios luego debe usar sudo systemctl enable y sudo systemctl start para apache y vsftpd, comprobamos que los servicios estén running desde dmz con systemctl estatus apache2 y systemctl estatus vsftpd

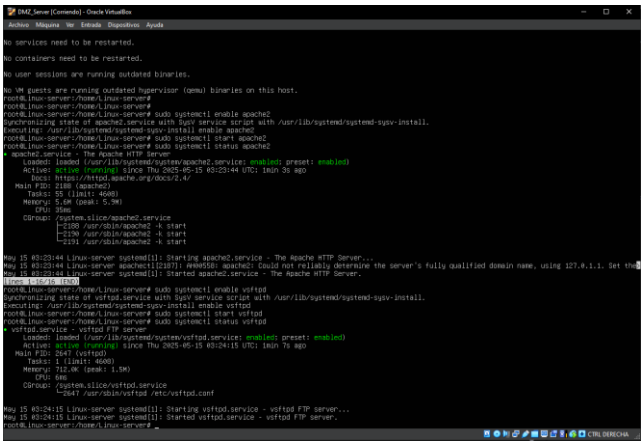

Imagen 31. Comprobación servicios apache y vsftpd

Se debe configurar el vsftpd desde la ruta /etc/ vsftpd.conf donde es recomendado para operar detrás de dispositivos NAT, mediante la directiva pasv_enable=YES activar el modo pasivo y asignar un rango de puertos para conectar desde la WAN externa hacia dmz

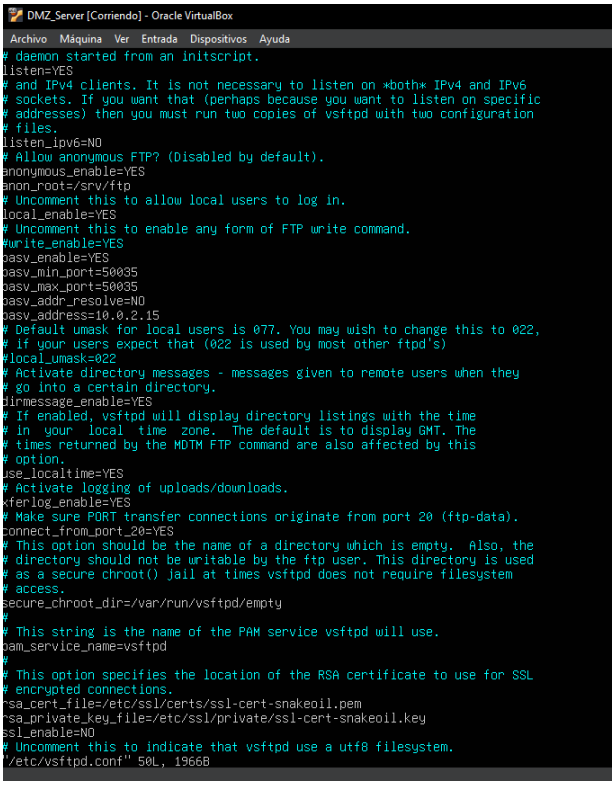

Imagen 32. Configuración de servicio vsftpd

Para el funcionamiento del servicio FTP a través de NAT también se debe crear un forwarding con el rango de puertos configurados por ejemplo el 50035, el puerto configurado para las conexiones de datos pasivas en el servidor vsftpd, y asignando la ip estática del dmz y el puerto 50035 nuevamente, esta regla junto con la correspondiente al puerto 21, permite el establecimiento de sesiones FTP en modo pasivo desde la WAN externa hacia el servidor en la DMZ

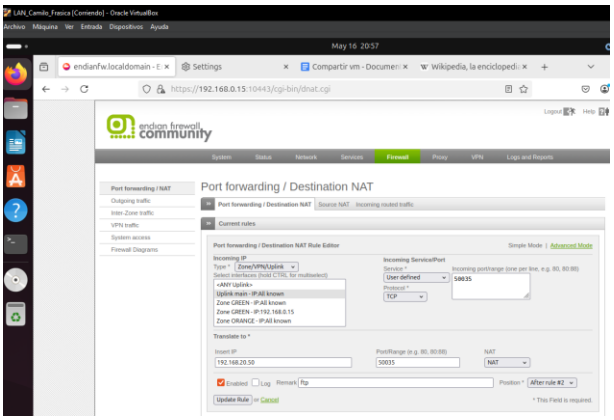

Imagen 33. Forwarding para servicio vsftpd wan externa

Ahora se debe exponer los puertos configurados en las reglas forwarding para que puedan ser usados desde la WAN externa, se debe dirigir al adaptador1 de endian y en la opción de reenvío de puertos debe crear tres reglas para cada puerto configurado 21,80,50035 como puertos de invitado y en puerto anfitrión debe seleccionar puertos que no estén en uso para establecer la conexión desde wan externa a dmz

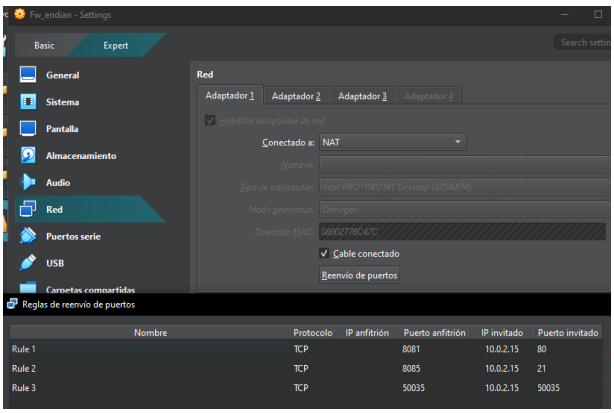

Imagen 34. puertos invitados para wan externa

Ahora se debe comprobar la conexión desde LAN y WAN hacia dmz

Se debe dirigir a LAN zona verde y probar la conexión a la url de apache con la ip estática de dmz y el puerto 80

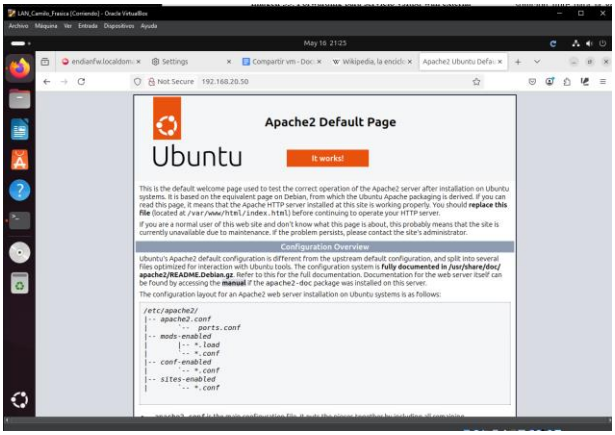

Imagen 35. Conexión HTTP LAN hacia DMZ

Ahora debe validar el ingreso desde la LAN hacia FTP de dmz Con ftp y su ip estática y a un ftp publico para validara la conexión hacia su DMZ y hacia WAN

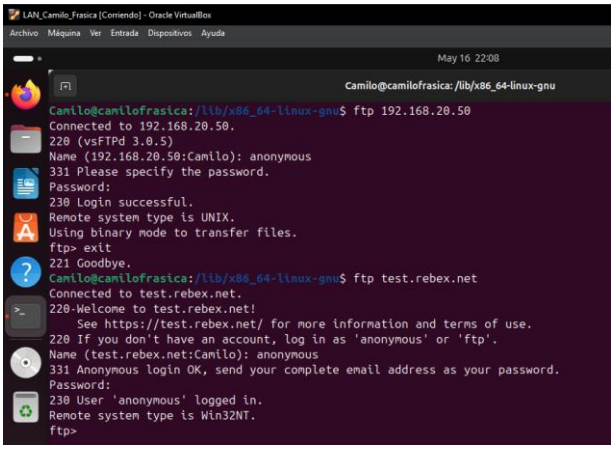

Imagen 36. Conexión FTP LAN hacia DMZ y WAN

Ahora se debe comprobar la conexión desde WAN externa hacia dmz, fuera de su red interna ingresar al localhost: y el puerto anfitrión

Para HTTP se abre la url con su puerto estatic configurado de dmz y el puerto 80, y se debera evidencia el despliegue de apache instalado en dmz

Imagen 37. Conexión HTTP WAN externa hacia DMZ

Y para Para FTP desde cualquier programa de gestion para FTP deberá poder establecer conexión hacia dmz y se debera evidencia conexión hacia FTP instalado en su dmz solo por ipv4 la cual fue la configurara previamente

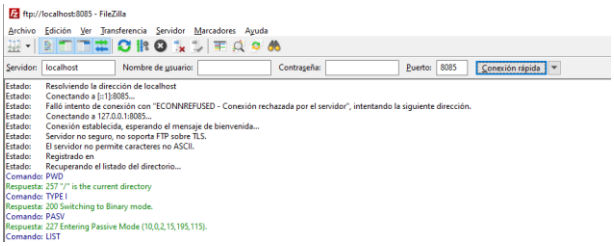

Imagen 38. Conexión FTP WAN externa hacia dmz

Verificar que aun pueda acceder a HTTP desde su LAN hacia la WAN, con cualquier URL

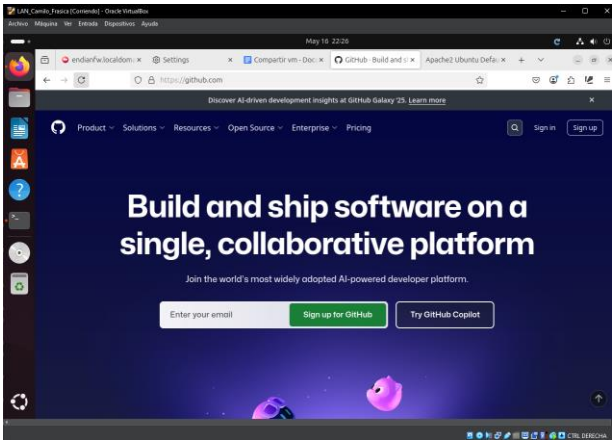

Imagen 39. Conexión HTTP LAN hacia WAN

6 TEMATICA 5

Implementar un Proxy HTTP (No transparente)
con políticas de autenticación para navegación en Internet.

Se debe ir a HTTP proxy y se debe habilitar HTTP proxy y se debe colocar not trasparent tanto para la zona GREEN Y zona ORANGE, luego debe asignar un puerto o se deja el default que es 8080 y aplicamos la configuración

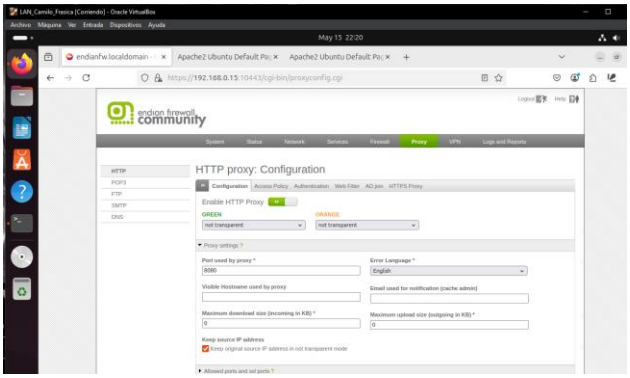

Imagen 40. configuración HTTP Proxy

Ahora Se debe dirigir ahora a web filtrer, y se debe crear un nuevo perfil el cual se le deben asignar las urls a la lista negra y blanca según sea el caso

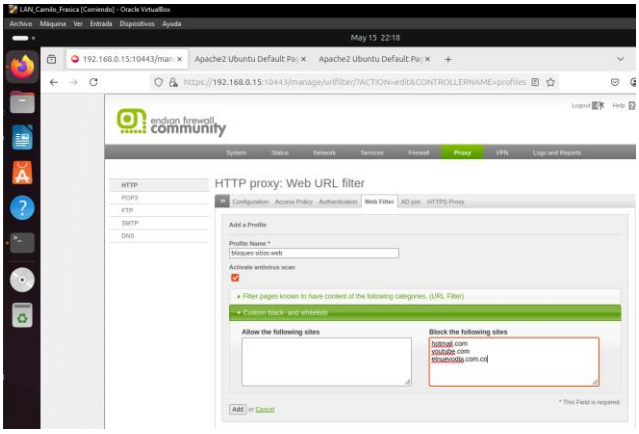

Imagen 41. configuración lista negra para proxy

Crear Grupo y Usuario: ahora se debe ir a authentication y vamos a manage user y se debe crear un nuevo usuario y asignarle un password

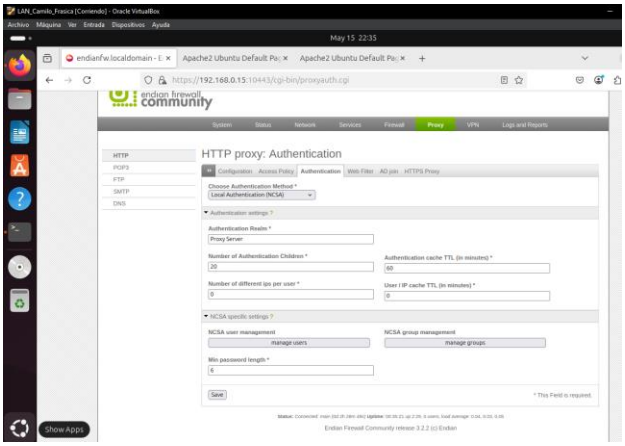

Imagen 42. Menú de creación usuario y grupo

luego se dirige a manage grupo y se crea el grupo nuevo este debe asociarse el usuario creado previamente y se debe visualizar la Asociación

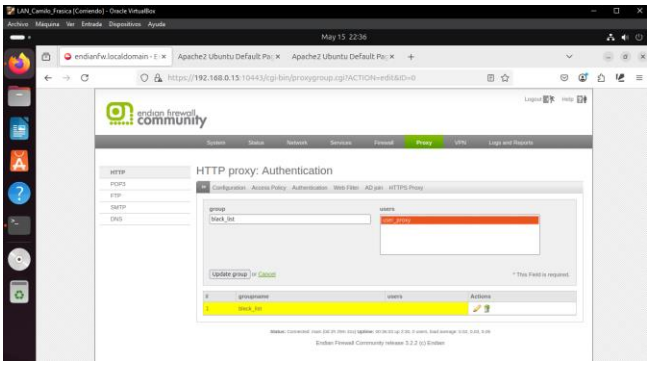

Imagen 43. Asociación grupo y usuario creado

Ahora se debe crear la política de acceso, se debe dirigir a policy access y crear nueva politica aca se debe seleccionar la zona GREEN como origen ya que es la LAN, se debe seleccionar como destino ANY o la zona RED, como autenticacion el grupo y usuario creado previamente allow access ya que se configurará una lista creada, y ahora debe seleccionar el profile creado previamente con el contenido de la lista negra o blanca

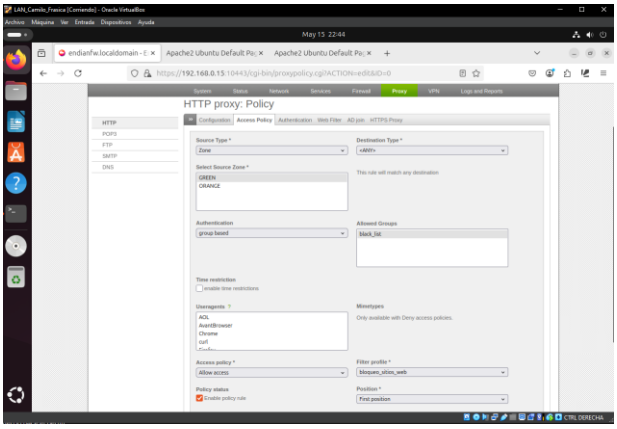

Imagen 44. Configuración política de acceso HTTP

Ahora se debe dirigir al navegador y configurar el proxy con la dirección ip de su fw endian y el puerto configurado de su proxy, y se debe seleccionar usar este proxy

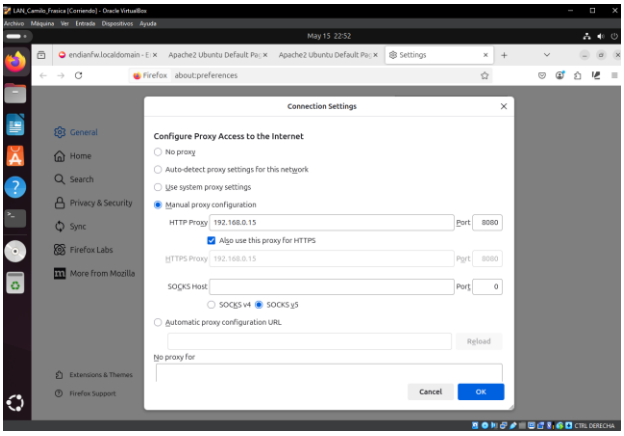

Imagen 45. Configuración proxy navegador

Debe realizar pruebas al cargar una url se le pedirá ingresar las credenciales del usuario creado y contraseña asignada y deberá poder navegar correctamente exceptuando las añadidas en la lista negra

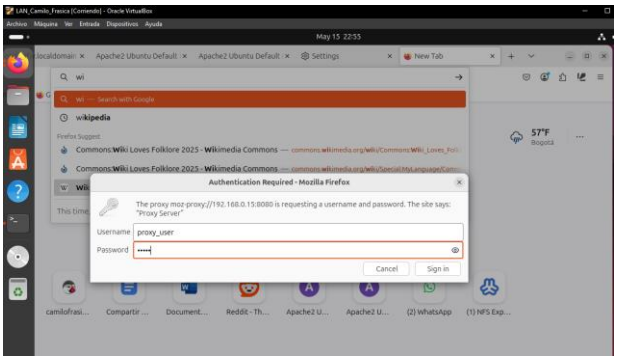

Imagen 46. Ingreso de credenciales proxy

después de ingresar las credenciales debería poder navegar correctamente por internet.

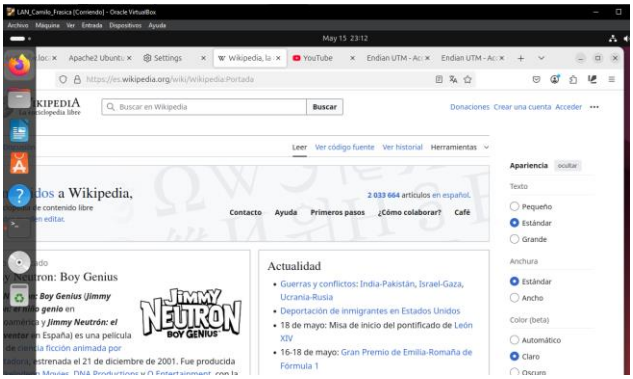

Imagen 47. Ingreso HTTP

Y deberá comprobar que las páginas ingresadas en la lista negra estén bloqueadas y no pueda ingresar a estas

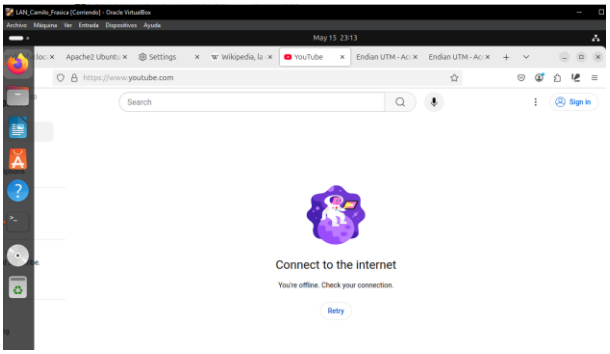

Imagen 48. Ingreso a YouTube sin conexión

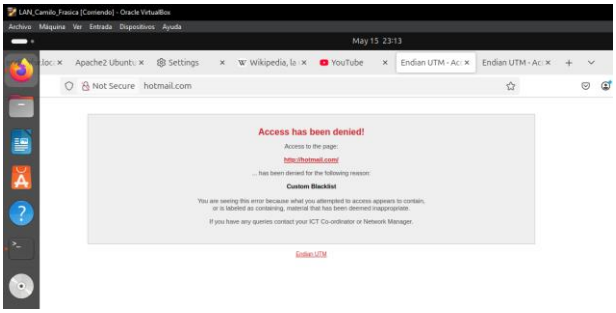

Imagen 49. Ingreso a Hotmail rechazado

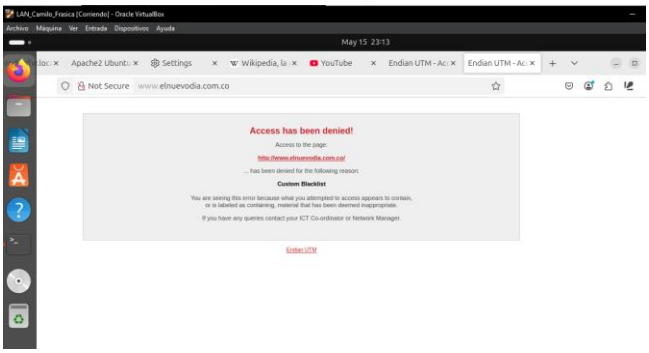

Imagen 50. Ingreso a elnuevodia rechazado

7 CONCLUSIONES

La virtualización de Endian Firewall Community mediante VirtualBox facilitó la creación de un entorno de red segmentado con zonas VERDE (LAN), ROJA (WAN) y NARANJA (DMZ). Este proceso práctico fue esencial para comprender la configuración inicial de un firewall y la delimitación de perímetros de seguridad.

La implementación de NAT en Endian Firewall resultaron fundamentales para establecer una comunicación segura y controlada entre la zona roja y la zona verde y naranja. Esta configuración es vital para proteger la red interna de amenazas externas y gestionar cómo los recursos internos acceden a Internet, minimizando así los riesgos.

Se logro aplicar la aplicación de restricciones de tráfico, como la denegación de ICMP, y el de filtrado inherente a Endian Firewall, demostrando la importancia de estas herramientas para mantener la integridad y confidencialidad de la información y los sistemas. El monitoreo del tráfico a través de las distintas zonas proporciona datos valiosos que permiten a los administradores mantener y optimizar un entorno de red seguro y eficiente.

Se logra implementar la configuración y verificación de reglas de acceso Inter-Zona y de Port Forwarding en Endian Firewall se demostró el control de la comunicación entre los diferentes segmentos de red LAN, DMZ y la WAN. Se validó exitosamente el acceso a servicios HTTP y FTP alojados en la DMZ tanto desde la red interna LAN como desde la red externa WAN, así como la conectividad de estas zonas hacia Internet. asegurando una comunicación controlada y segura a través de los parámetros definidos.

La implementación de un proxy HTTP no transparente con autenticación y filtrado de URL en Endian Firewall para la gestión del acceso a Internet. Usando la configuración de perfiles, listas negras y grupos, se denegó el acceso a sitios web específicos, evidencian como reforzar la seguridad y aplicar políticas de acceso a la red.

8 REFERENCIAS

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

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

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

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

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