CONFIGURACIÓN DE NAT Y PUBLICACIÓN DE SERVICIOS EN DMZ MEDIANTE ENDIAN FIREWALL
(Opción de Grado) Código: 202338299_72

Diana Paola Bohorquez Sánchez
e-mail: dpbohorquezsa@unadvirtual.edu.co
Jhon Alexánder Hincapié Zambrano
e-mail: jahincapieza@unadvirtual.edu.co
Daniel Alejandro Moreno
e-mail: damorenofr@unadvirtual.edu.co
Omar Alfredo Pacheco Yepez
e-mail: Oapachecoy@unadvirtual.edu.co

RESUMEN— *El presente artículo describe el proceso de instalación y configuración del firewall Endian en un entorno virtualizado a través de VirtualBox. enfocado en la implementación de traducción de direcciones de red (NAT) y el uso de una zona DMZ para la publicación de servicios. Se documenta la preparación de los adaptadores de red en la máquina virtual, la instalación del sistema Endian Firewall, la creación de reglas de firewall, la habilitación de NAT para permitir la salida de la LAN hacia la WAN y la configuración de reglas de redirección de puertos desde la DMZ hacia Internet. Cada captura de pantalla se acompaña de una breve explicación del paso realizado, con el fin de evidenciar el cumplimiento de los requerimientos planteados en la guía académica.*

PALABRAS CLAVE— *Endian, Firewall, IP.*

ABSTRACT-*This article describes the process of installing and configuring the Endian firewall in a virtualized environment using VirtualBox. focused on implementing network address translation (NAT) and using a DMZ zone for publishing services. The preparation of network adapters in the virtual machine, the installation of the Endian Firewall system, the creation of firewall rules, the enabling of NAT to allow LAN traffic to reach the WAN, and the configuration of port forwarding rules from the DMZ to the Internet are documented. Each screenshot is accompanied by a brief explanation of the step performed, in order to demonstrate compliance with the requirements outlined in the academic guid***e.**

Keywords— *Endian, Firewall, IP, Security, Networks.*

1. INTRODUCCIÓN

En entornos de red corporativos y académicos es fundamental comprender el funcionamiento de los firewalls perimetrales y la correcta aplicación de técnicas como la traducción de direcciones de red (NAT) y la segmentación mediante zonas seguras, como la DMZ. En este trabajo se implementa Endian Firewall como solución UTM sobre una máquina virtual, configurando las interfaces de red, las políticas de filtrado y las reglas de NAT para permitir la comunicación entre la red interna (LAN), la red desmilitarizada (DMZ) y la red externa (WAN). La seguridad perimetral (Firewalls o filtrado de tráfico) es esencial para proteger las infraestructuras tecnológicas ante amenazas cibernéticas cada vez más complejas.

Endian Firewall es una distribución GNU/Linux especializada que ofrece una solución de seguridad integral y económica, la cual incluye filtrado de paquetes, detección de intrusiones, VPN, proxy y control de ancho de banda.

El objetivo principal es demostrar, de forma práctica, la configuración de NAT desde la LAN hacia la WAN, así como la configuración de reglas de reenvío de puertos desde la DMZ hacia Internet, evidenciando la creación y el funcionamiento de dichas reglas mediante pruebas de conectividad y acceso a servicios.

La arquitectura de red con DMZ crea un segmento intermedio entre la red interna y la externa, permitiendo alojar servicios públicos sin poner en riesgo los sistemas críticos. En la DMZ se ubican servidores expuestos, aplicando controles de acceso estrictos.

1.1 ÁREAS DE CONOCIMIENTO INVOLUCRADAS

Este trabajo integra conocimientos de tres áreas fundamentales de las tecnologías de la información. En primer lugar, la Seguridad de la Información y Redes, que

abarca la implementación de firewalls perimetrales, la segmentación mediante zonas DMZ, y la aplicación de técnicas de traducción de direcciones (NAT, SNAT y DNAT) para proteger la infraestructura tecnológica contra amenazas cibernéticas.

En segundo lugar, la Administración de Sistemas y Virtualización, que comprende la configuración de entornos virtualizados mediante VirtualBox, la gestión de sistemas operativos basados en GNU/Linux, y la optimización de recursos computacionales para simular infraestructuras de red complejas sin necesidad de hardware físico dedicado.

Finalmente, la Arquitectura de Redes, que involucra el diseño de topologías multicapa, la configuración de enrutamiento entre diferentes segmentos de red, y la implementación de servicios fundamentales como DNS, HTTP y FTP. La integración de estas tres áreas permite construir una solución de seguridad perimetral completa y funcional, demostrando cómo convergen diferentes disciplinas para resolver problemas reales de infraestructura tecnológica.

2. MARCO TEÓRICO

La traducción de direcciones de red (NAT) permite que múltiples dispositivos de una red privada accedan a Internet utilizando una o pocas direcciones IP públicas, realizando el enmascaramiento de las direcciones internas. La DMZ (zona desmilitarizada) es un segmento de red intermedio donde se ubican servidores que deben ser expuestos a Internet, reduciendo el riesgo para la red interna. Endian Firewall es una distribución orientada a seguridad perimetral que integra funciones de cortafuegos, NAT, VPN, proxy y otras características de seguridad.

3. DESARROLLO

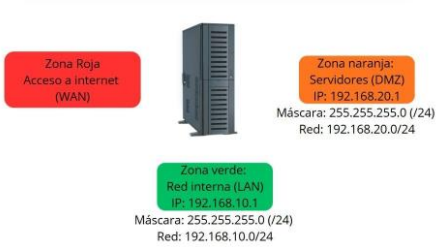
3.1 PREPARACIÓN DEL ENTORNO DE VIRTUALIZACIÓN

La implementación de Endian Firewall requiere una planificación cuidadosa de la arquitectura de red virtual. VirtualBox proporciona las capacidades necesarias para simular una infraestructura de red completa incluyendo múltiples segmentos aislados. Para esta implementación se configuró una máquina virtual con recursos suficientes para el correcto funcionamiento del firewall, estableciendo 2048 MB de memoria RAM y 20 GB de almacenamiento en disco.

El componente crítico de esta configuración consiste en la asignación de tres interfaces de red virtuales, cada una correspondiente a una zona de seguridad específica. La primera interfaz se configuró en modo NAT para simular la conexión a Internet, representando la zona roja o WAN. Esta interfaz permite que el firewall obtenga conectividad externa y actúe como gateway para los dispositivos de las redes internas. La segunda interfaz se estableció como red interna denominada LAN_interna, constituyendo la zona verde donde residen las estaciones de trabajo corporativas. La tercera interfaz se configuró también como red interna bajo el nombre DMZ_servidores, formando la zona naranja destinada a alojar servidores web y de aplicaciones accesibles públicamente.

Durante el proceso de instalación de Endian Firewall desde la imagen ISO oficial, el sistema solicita la identificación y asignación de las interfaces de red a las zonas de seguridad correspondientes. Se estableció el esquema de direccionamiento IP 192.168.10.0/24 para la zona verde con el firewall actuando como gateway en la dirección 192.168.10.1, mientras que para la zona naranja se asignó el rango 192.168.20.0/24 con gateway en 192.168.20.1. Esta segmentación IP facilita la implementación de políticas de enrutamiento y reglas de firewall específicas para cada zona, quedando de la siguiente manera:

Figura 1. *Resultado configuración de tarjetas de red a través de Endian Firewall:*



Fuente: autoría propia.

A continuación, se describe la configuración de cada adaptador a detalle.

TEMÁTICA NO. 1

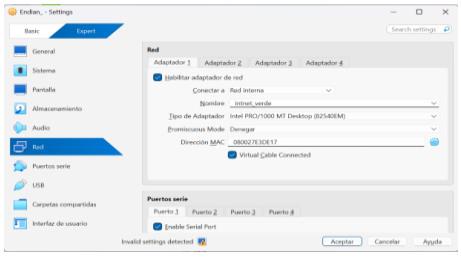
3.1.2 CONFIGURACIÓN DE ADAPTADORES DE RED EN LA MÁQUINA VIRTUAL

Para garantizar el correcto funcionamiento de las zonas de red en Endian se configuraron tres adaptadores en la máquina virtual: uno para la red externa (WAN), otro para la red interna (LAN/Verde) y un tercero para la zona DMZ (Naranja). A continuación, se describen las principales configuraciones realizadas.

3.1.3 Adaptador 1 (LAN/VERDE)

En esta etapa se configura el primer adaptador para la red interna, que será asociada a la zona verde (GREEN) de Endian. Desde esta red se conectarán los equipos de la LAN que saldrán a Internet mediante NAT. La Fig. 1 muestra la configuración del adaptador 1 de la máquina virtual Endian, habilitado y conectado a una red interna con el nombre intnet_verde, que corresponde a la red LAN.

Figura 2. *Configuración adaptador 1:*



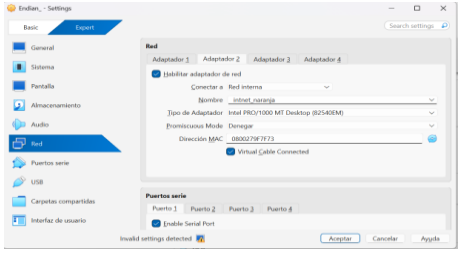
Fuente: autoría propia.

Configuración del adaptador 1 de la máquina virtual Endian. Lo habilito y lo conecto a una Red interna, asignándole el nombre internet verde, que corresponde a la red LAN (zona VERDE).

3.1.4 Adaptador 2 (DMZ/NARANJA)

El segundo adaptador se configura para la red desmilitarizada (DMZ), asociada a la zona naranja (ORANGE) de Endian, donde se ubicarán los servidores que serán publicados hacia Internet. La Fig. 3 presenta la configuración del adaptador 2, conectado a la red interna intnet_naranja asociada a la DMZ.

Figura 3. *Configuración adaptador 2:*



Fuente: autoría propia.

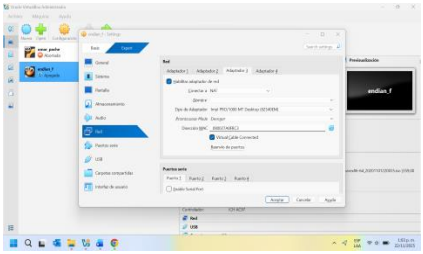
Configuración del adaptador 2 y lo conecto también a una Red interna, pero esta vez con el nombre intnet_naranja, asociado a la DMZ dentro de la topología de Endian.

Mantengo el mismo tipo de adaptador y parámetros de conexión. Esta red permitirá aislar servicios públicos como servidores web o FTP antes de exponerlos mediante reglas NAT.

3.1.5 Adaptador 3 (WAN/ROJO)

El tercer adaptador representa la zona WAN, es decir, la conexión hacia Internet. Su función principal es permitir que el firewall tenga salida a la red externa y reciba el tráfico entrante proveniente de Internet para ser filtrado y procesado según las reglas de seguridad. La Fig. 4 detalla la configuración de este adaptador en modo NAT, con cable conectado y modo promiscuo deshabilitado.

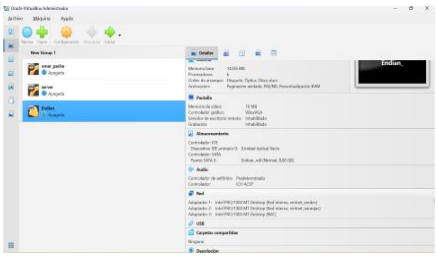
Figura 4. *Configuración adaptador 3:*



Fuente: autoría propia.

Configuración del adaptador 3 de la máquina virtual endian_f, definido en modo NAT para proporcionar acceso a Internet desde el firewall., con el modo promiscuo deshabilitado y el cable virtual conectado. Esta interfaz corresponde a la red ROJA (WAN), permitiendo que Endian tenga salida hacia la red externa durante la instalación y operación.

Figura 5. *Configuración máquina Endian:*



Fuente: autoría propia.

En esta imagen se observa la máquina Endian completamente configurada, con los adaptadores asignados y lista para iniciar el proceso de instalación.

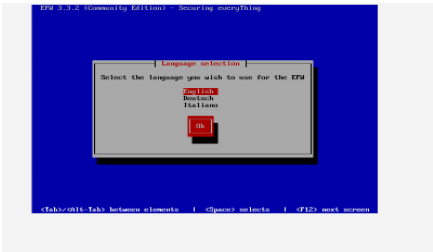
Este resumen me permite validar que la topología lógica coincide con el diseño requerido para aplicar

posteriormente reglas de NAT, filtrado y publicación de servicios.

3.2 Instalación de Endian Firewall

Una vez configurados los adaptadores de red en la máquina virtual, se procede a la instalación de Endian Firewall. Durante el asistente de instalación se seleccionan parámetros como el idioma, las interfaces de red y las credenciales de administración. Las Fig. 5 a 12 muestran las principales pantallas del proceso, desde la selección del idioma y el inicio del instalador, hasta la asignación de la dirección IP de la zona GREEN y la confirmación de que el sistema fue instalado correctamente.

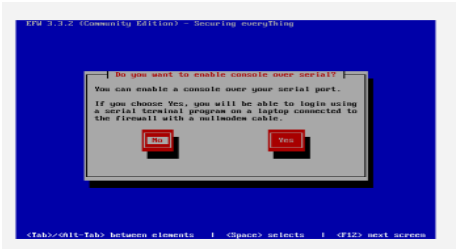
Figura 6. *Inicio instalador Endian:*



Fuente: autoría propia.

Esta pantalla corresponde al inicio del instalador, donde selecciono el idioma del sistema. Aquí elijo English, que será el idioma de la interfaz durante toda la instalación. Este paso solo define la visualización y no afecta la configuración de red.

Figura 7. *Configuración Endian.*



Fuente: autoría propia.

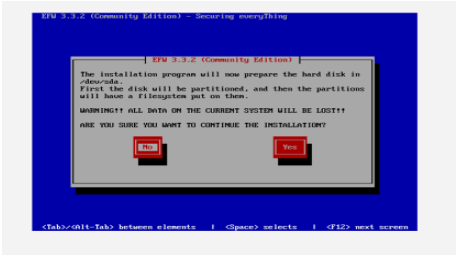
Imagen 7. El sistema pregunta si deseo habilitar el acceso por consola serial. Selecciono No, dado que no utilizaré un cable null-modem ni una terminal serial para administrar el firewall. Esta opción es útil solo en entornos industriales o de hardware específico.

Figura 8. *Configuración Endian.*

Fuente: autoría propia.

En este punto el asistente confirma que estoy entrando al proceso de instalación de Endian Firewall. Al seleccionar Ok, avanzo hacia las configuraciones de disco y red. Cancelar en este punto reiniciaría el sistema.

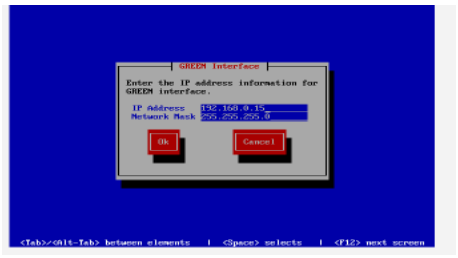
Figura 9. *Configuración Endian:*



Fuente: autoría propia.

El instalador advierte que se formateará por completo el disco /dev/sda. Seleccione Yes, autorizando que Endian cree las particiones necesarias y prepare el sistema de archivos. Esto es obligatorio para instalar el firewall como sistema operativo principal.

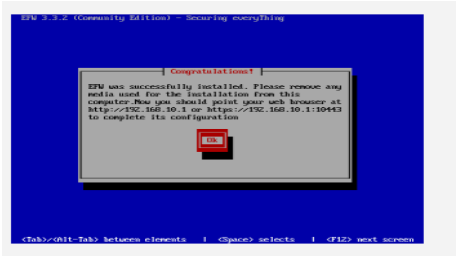
Figura 10. *Configuración Endian.*



Fuente: autoría propia.

En esta pantalla ingresar manualmente la dirección IP de la zona GREEN, asignando la IP 192.168.0.15 con máscara 255.255.255.0. Esta será la interfaz de administración inicial del firewall antes de configurar las demás zonas dentro del entorno web.

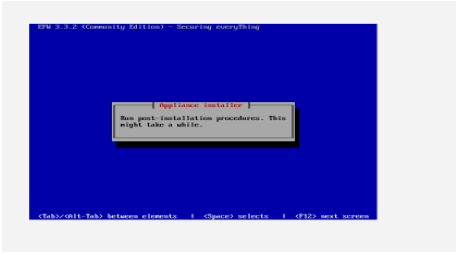
Figura 11. *Configuración Endian.*



Fuente: autoría propia.

El instalador confirma que Endian fue instalado correctamente. Aquí se me indica que retire los medios de instalación y acceda a la interfaz web mediante: http://192.168.10.1 - https://192.168.10.1:10443 Desde ahí continuaré con el asistente de configuración avanzada

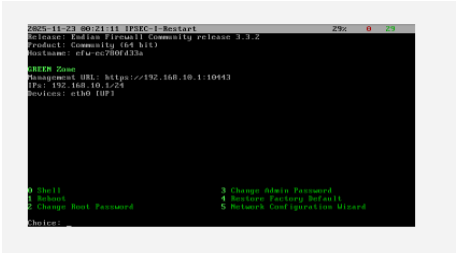
Figura 12. *Configuración Endian.*



Fuente: autoría propia.

Esta pantalla corresponde al proceso automático de inicialización posterior, donde Endian ejecuta tareas internas como creación de servicios, configuración de módulos y preparación del sistema. Es normal que tome algunos minutos.

Figura 13. *Inicio máquina Endian:*



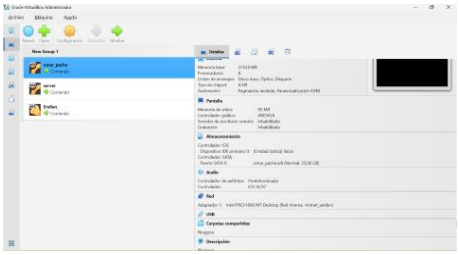
Fuente: autoría propia.

Una vez que el sistema inicia por completo, se muestra el menú de administración local. Aquí puedo: Abrir una Shell - Reiniciar el sistema - Cambiar la contraseña de root - Lanzar el Network configuración Wizard - Restaurar valores de fábrica. También confirma que la interfaz GREEN está activa en 192.168.10.1/24, lo que valida que puedo acceder a la interfaz web para continuar con la configuración.

3.3 CONFIGURACIÓN DE ENDIAN FIREWALL Y ZONAS DE RED

Con el sistema instalado, se accede a la interfaz web de administración para configurar las interfaces VERDE, NARANJA y ROJO, asignando direcciones IP adecuadas a cada segmento y ajustando las políticas básicas del cortafuegos. Las imágenes de la 14 a la 26 muestran la configuración de la máquina cliente en la LAN, la verificación de conectividad, la aceptación de la licencia, la definición del modo de funcionamiento enrutado, la activación de la zona NARANJA, la asignación de direcciones IP y DNS, el registro de correos de administración, la aplicación de la configuración y el panel de control de Endian una vez operativo. La Fig. 27 presenta una prueba de ping hacia la interfaz GREEN que confirma la conectividad desde la LAN.

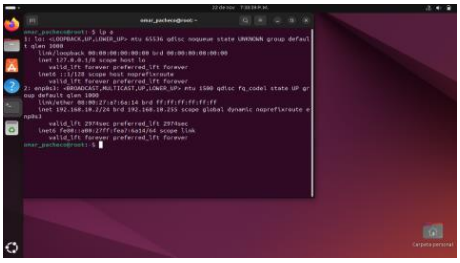
Figura 14. *Detalle máquina cliente.*



Fuente: autoría propia.

Esta imagen muestra los detalles de la máquina virtual destinada a integrarse en la red (LAN/Verde). El adaptador de red está configurado en la red interna “internet_verde”, adecuada para la LAN en Endian Firewall. Al estar corriendo, esta máquina sirve como host de pruebas para validar conectividad, asignación de direcciones y funcionamiento general del firewall.

Figura 15. *Comprobación ping desde máquina cliente.*

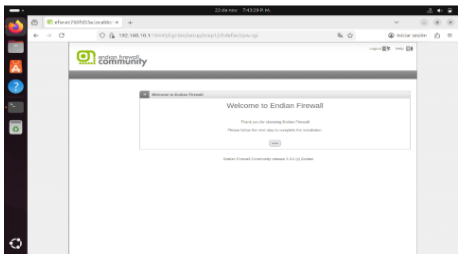


Fuente: autoría propia.

Con el comando IP a verifico las interfaces activas del host conectado a la LAN. Se observa la interfaz enp0s3 con la dirección 192.168.10.2/24, asignada por el segmento VERDE del firewall. Esto confirma que la máquina cliente

está correctamente enlazada a la infraestructura de Endian y lista para pruebas de conectividad.

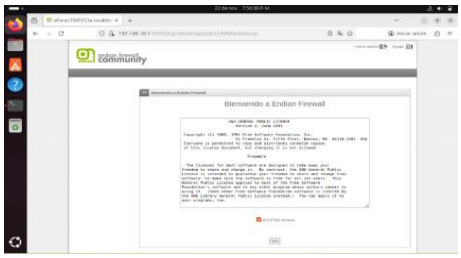
Figura 16. *Acceso a Endian Firewall*



Fuente: autoría propia.

Esta imagen presenta la interfaz inicial del asistente de instalación, donde el sistema solicita iniciar la configuración básica del firewall. Desde aquí comienza el proceso de definición de modos de red, interfaces, zonas y parámetros fundamentales del sistema.

Figura 17. *Aceptar la licencia GNU GPL Endian.*



Fuente: autoría propia.

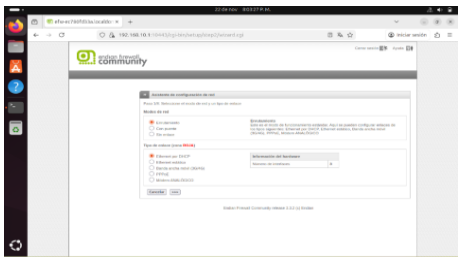
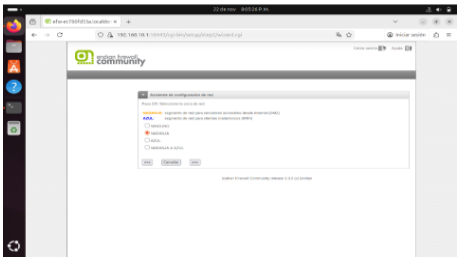


Imagen 18. Aquí selecciono el modo de funcionamiento del firewall en Enrutamiento, y además elijo el tipo de enlace para la zona ROJA (WAN), en este caso Ethernet estático/DHCP, permitiendo que la interfaz externa se conecte al router o modem del proveedor.

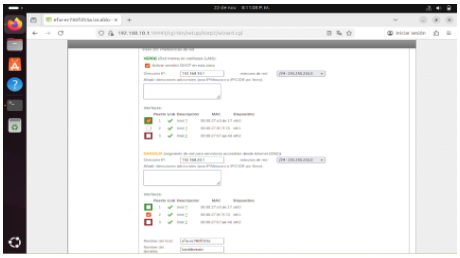
Figura 18. Interfaz gráfica Endian desde máquina cliente



Fuente: autoría propia.

Imagen 19. En este paso el asistente me permite activar zonas adicionales. Se habilita la zona NARANJA (DMZ) para alojar servicios públicos aislados.

Figura 19. *Asignación zona naranja (DMZ).*



Fuente: autoría propia.

Imagen 20. La imagen muestra la asignación de direcciones para las zonas principales: GREEN: 192.168.10.1/24 - ORANGE (DMZ): 192.168.20.1/24 También selecciono los adaptadores de red correspondientes para cada zona, garantizando su separación lógica y física dentro del firewall.

Figura 20. *Asignación de direcciones zona verde, naranja y roja.*

Fuente: autoría propia.

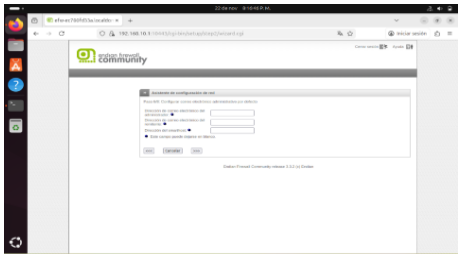
Imagen 21. Aquí se configura la interfaz ROJO seleccionando la tarjeta de red que se conectará a la WAN. Este paso define la conexión externa que usará el firewall como puerta de enlace hacia Internet.

Imagen 21. *Configuración interfaz ROJO.*

Fuente: autoría propia.

Imagen 22. En este paso asigno manualmente servidores DNS públicos: DNS 1: 8.8.8.8 - DNS 2: 8.8.4.4 Esto asegura que el firewall y las zonas internas resuelvan nombres hacia Internet correctamente.

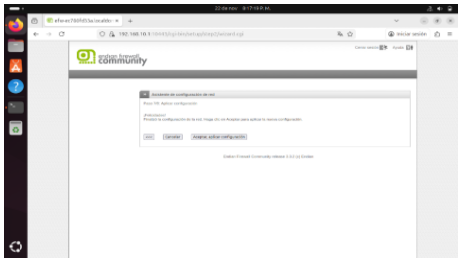
Figura 22. *Asignación servidores DNS:*



Fuente: autoría propia.

Imagen 23. se muestra la pantalla para registrar correos de administración del sistema. Este paso es opcional y permite que Endian envíe alertas o notificaciones al administrador mediante correo electrónico.

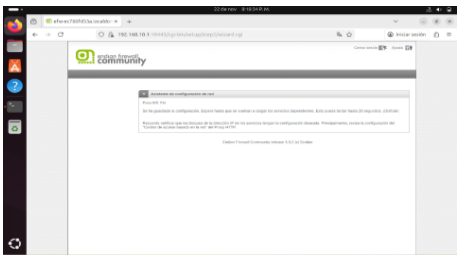
Figura 23. *Registro correos administración del sistema*



Fuente: autoría propia.

Imagen 24. Esta imagen corresponde al paso final del asistente, donde Endian confirma que la configuración de red fue completada. Aquí hago clic en “Aceptar, aplicar configuración” para que el firewall aplique las nuevas direcciones, zonas e interfaces asignadas en los pasos anteriores. Este punto marca el cierre del proceso de inicialización.

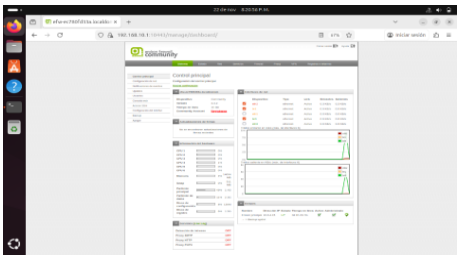
Figura 24. *Confirmación configuración de Endian completa desde máquina cliente.*



Fuente: autoría propia.

Imagen 25. En esta pantalla el asistente indica que la configuración ha sido guardada exitosamente y que los servicios dependientes se reiniciarán. Se menciona que el proceso puede tardar unos segundos, lo cual es normal mientras se levantan los servicios del firewall y las interfaces adoptan sus configuraciones definitivas.

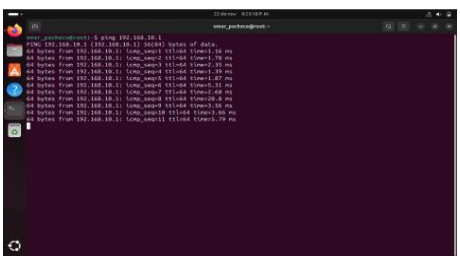
Figura 25. *Configuración completa de Endian desde máquina cliente:.*



Fuente: autoría propia.

Imagen 26. Aquí se muestra el panel de control (dashboard) de Endian una vez aplicada toda la configuración. Se observan estadísticas del sistema, carga de CPU, uso de memoria, estado de servicios y las tres interfaces de red: ROJO (WAN) - VERDE (LAN) - NARANJA (DMZ). Este panel confirma que el firewall está operativo y gestionando tráfico en cada una de sus zonas

Figura 26. *Ping desde máquina virtual cliente a red verde.*



Fuente: autoría propia.

Imagen 27. En esta imagen se observa un ping hacia 192.168.10.1, dirección correspondiente a la interfaz GREEN del firewall, el cual nos comunica que la configuración quedó correcta.

TEMÁTICA 2.
3.4 CONFIGURACIÓN DE NAT DESDE LA LAN HACIA LA WAN

La configuración de NAT de origen (Source NAT) en Endian Firewall permite que los equipos de la red interna (zona VERDE) accedan a recursos externos mediante el enmascaramiento de sus direcciones privadas. Para ello se define una regla SNAT que aplica masquerading a todo el tráfico con destino a redes externas. En la imagen 27 se observa el apartado de administración de reglas de NAT de origen; en la imagen. 28 se define la regla SNAT para la red 192.168.10.0/24; y en la imagen. 29 se aprecia la regla aplicada y operativa.

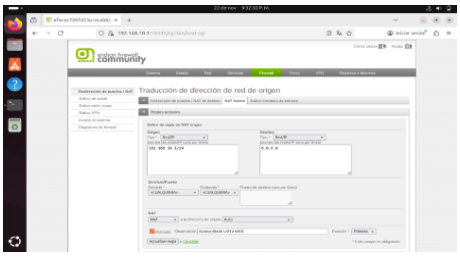
Las imágenes. 31 a 33 muestran las pruebas de conectividad realizadas desde un host de la LAN hacia 8.8.8.8, google.com y unad.edu.co, donde se valida la correcta resolución DNS y el acceso a servicios externos mediante la regla de NAT configurada.

Figura 27. *Configuración red NAT*

Fuente: autoría propia.

Imagen 28. Se visualiza el apartado Firewall → NAT fuente, donde se administran las reglas de Source NAT en Endian. En este punto no existe ninguna regla configurada, lo que indica que la LAN aún no tiene habilitada la salida hacia la WAN. Desde este menú se inicia el proceso de creación de la regla de enmascaramiento.

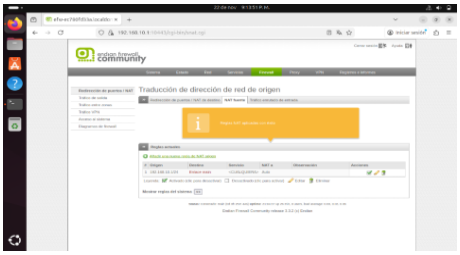
Figura 28. *Configuración red NAT*



Fuente: autoría propia.

Imagen 29. Se define una regla de Source NAT (SNAT) aplicando masquerading para permitir que la red interna 192.168.10.1/24 (verde) utilice la dirección de la interfaz RED como origen al generar tráfico hacia cualquier red externa (0.0.0.0). Esta configuración habilita el acceso a Internet para todos los hosts de la LAN.

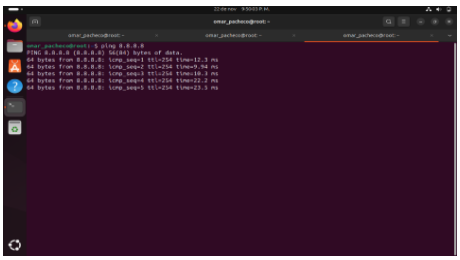
Figura 29. *Definición regla de Source NAT*



Fuente: autoría propia.

Imagen 30. Aquí se muestra la regla SNAT ya aplicada y operativa. La interfaz confirma que el enmascaramiento está activo para la red interna, lo cual autoriza la traducción de direcciones para el tráfico saliente hacia la WAN, permitiendo la comunicación con redes externas.

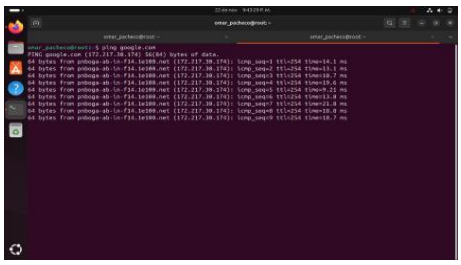
Figura 30. *Máquina cliente haciendo ping a red interna:*



Fuente: autoría propia.

Imagen 31. La prueba ICMP enviada desde un host de la LAN hacia el DNS público 8.8.8.8 responde correctamente, validando que el tráfico es enmascarado por la interfaz RED mediante la regla SNAT, y confirmando conectividad hacia Internet sin restricciones.

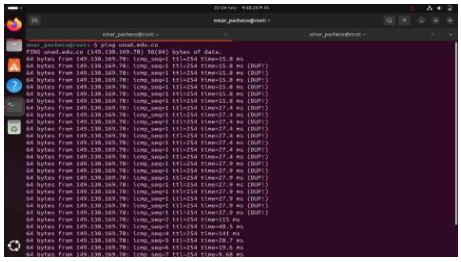
Figura 31. *Prueba desde el host de LAN al DNS público*



Fuente: autoría propia.

Imagen 32. El ping a google.com evidencia correcta resolución DNS y comunicación con servidores externos. Esto demuestra que la LAN no solo tiene salida vía NAT, sino que también puede resolver nombres mediante DNS, completando así la verificación funcional del servicio.

Figura 32. *Imagen de ping en funcionamiento.*



Fuente: autoría propia.

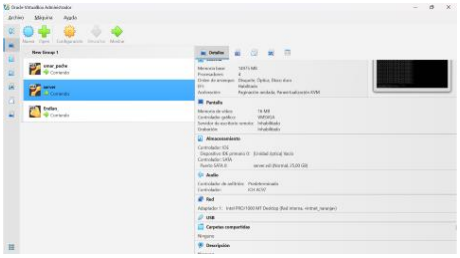
Imagen 33. El ping hacia unad.edu.co muestra respuesta desde el dominio institucional, verificando conectividad completa a redes académicas externas. La presencia de algunos paquetes duplicados (DUP) es un comportamiento común en rutas balanceadas y no afecta la verificación de NAT.

3.5 CONFIGURACIÓN DE DMZ HACIA LA INTERNET

La redirección de puertos (Destination NAT o DNAT) permite que un servicio alojado en la zona DMZ/Naranja sea accesible desde la red externa. Para lograrlo se crea una regla DNAT indicando que las conexiones entrantes a un puerto específico de la interfaz RED se traduzcan hacia la dirección IP del servidor en la DMZ. La imagen. 33 muestra la configuración de la máquina virtual utilizada como servidor en la DMZ; las Fig. 34 y 35 ilustran la creación de la regla DNAT para publicar un servicio FTP sobre el puerto 21.

Finalmente, las imágenes. 36 a 38 presentan las pruebas de conectividad realizadas desde la DMZ hacia la WAN, confirmando que la DMZ tiene acceso a dominios públicos y que el firewall permite el tráfico necesario para la operación de los servicios expuestos.

Figura 33. *Configuración máquina virtual en Virtualbox:.*



Fuente: autoría propia.

Imagen 34. En esta imagen se observa la configuración de mi máquina virtual “server”, la cual utilizo como servidor dentro de la zona DMZ de mi arquitectura con Endian Firewall. Este equipo es el que yo destino para alojar el servicio que publicaré mediante la regla DNAT.

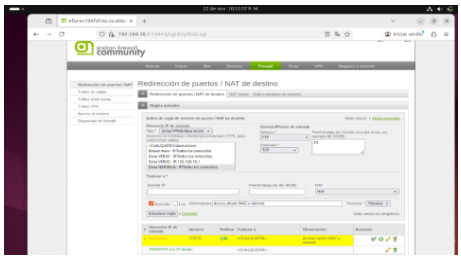
Puedo ver que el Adaptador de red 1 está configurado como Red interna, asociado a la red “intnet_naranja”, que corresponde directamente a la DMZ (ORANGE). Esto garantiza que el tráfico redirigido desde la WAN llegue correctamente a este servidor.

Figura 34. *Comprobación zona DMZ (Naranja):*

Fuente: autoría propia.

Imagen 35. La captura muestra la creación de una regla DNAT donde el tráfico entrante al puerto 21/TCP (FTP) es redirigido hacia un servidor ubicado en la DMZ (zona NARANJA). La interfaz de entrada seleccionada es NARANJA, y la traducción se realiza hacia la IP interna del servidor FTP en la DMZ. La regla está activa y permite el acceso externo, tal como se evidencia en la tabla inferior, donde se muestra una política de permitir para el servicio TCP/21 con su correspondiente dirección traducida.

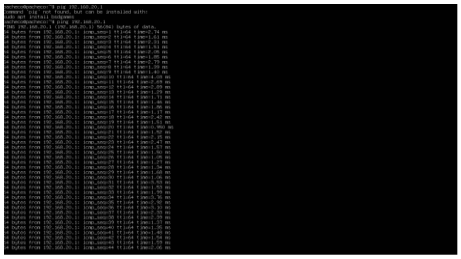
Figura 35. *Creación regla DNAT desde máquina cliente:*



Fuente: autoría propia.

Imagen 36. La configuración completa de una regla DNAT que expone un servicio FTP alojado en la DMZ hacia Internet, permitiendo que clientes externos accedan al puerto 21 mediante la traducción de direcciones desde la interfaz RED hacia el servidor interno en la zona ORANGE.

Figura 36. *Configuración completa regla DNAT haciendo ping:.*



Fuente: autoría propia.

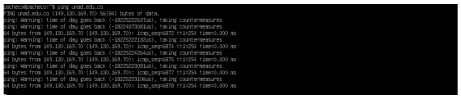
Imagen 37 esto confirma que la red DMZ está funcionando adecuadamente, que existe comunicación entre el servidor y la puerta de enlace de DMZ, y que la topología está correctamente configurada para permitir el DNAT.

Figura 37. Funcionamiento red DMZ

Fuente: autoría propia.

Figura 38. Las respuestas ICMP validan que el tráfico de la DMZ puede salir a la WAN, lo cual es indispensable para que los servicios expuestos operen correctamente y puedan resolver DNS o responder conexiones externas

Figura 38. *Respuesta ICPM.*



Fuente: autoría propia.

Figura 39. Confirma que la DMZ tiene acceso a dominios públicos y que el firewall está permitiendo el tráfico originado en la DMZ hacia la WAN con normalidad. La salida funcional es evidencia de que la política aplicada en Endian permite la comunicación DMZ → Internet.

TEMÁTICA 3

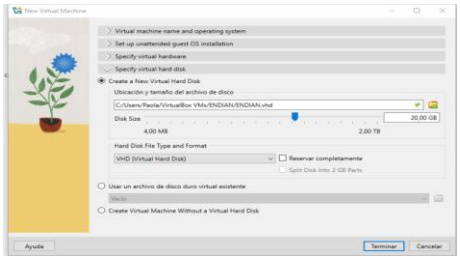
Permitir servicios de la Zona DMZ para la red. Producto esperado: 1. Permitir los servicios HTTP (Puerto 80) y FTP (Puerto 21) desde el servidor Web bajo Ubuntu Server. 2. Denegar el protocolo ICMP (Puerto 8 y puerto 30) para no permitir hacer ping en la red. Probar a través de una consola o terminal la no respuesta del comando ping hacia una IP de la red. Verificar en el tráfico de salida, la creación de las reglas.

Para dar solución a la actividad, Lo primero que realice fue instalar 3 máquinas virtuales en virtual box: Primero instalé y configuré Endian Firewall (EFW) como la plataforma principal de seguridad de la red se creó con tres adaptadores 1 adaptador verde 2 adaptador Naranja 3 adaptador Nat.

Figura 40 *Configuraciòn primera maquina virtual Endian memoria y núcleos.*

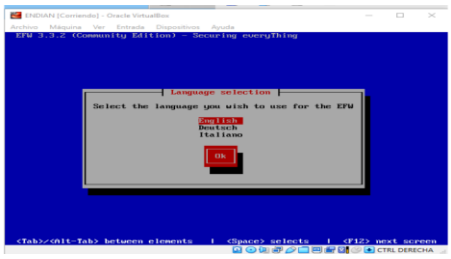
Fuente: autoría propia.

Figura 41. *Configuraciòn primera maquina virtual Endian*



Fuente: autoría propia.

Figura 42. *Se inicia instalación máquina virtual Endian*

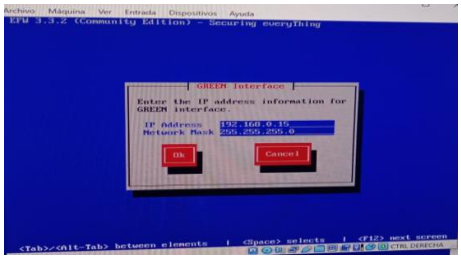


Fuente: autoría propia.

Figura 43. *Instalación máquina virtual Endian*

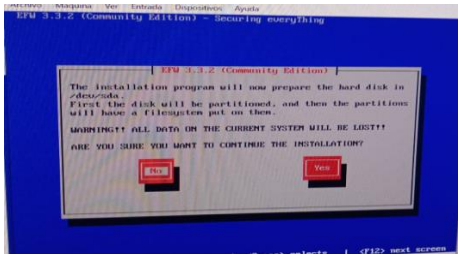
Fuente: autoría propia.

Figura 44. *Instalación máquina virtual Endian*



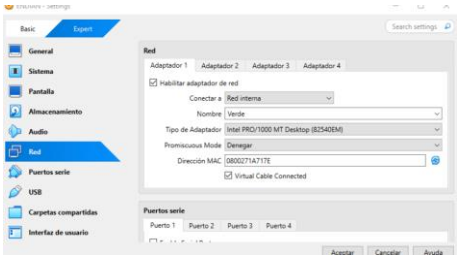
Fuente: autoría propia.

Figura 45. *Instalación máquina virtual Endian*



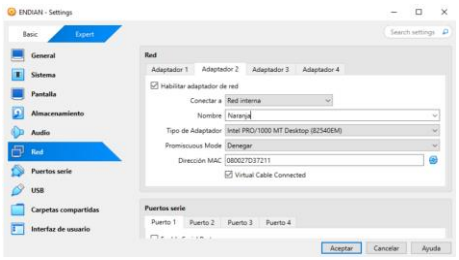
Fuente: autoría propia.

Figura 46. *Selección adaptador 1 verde*



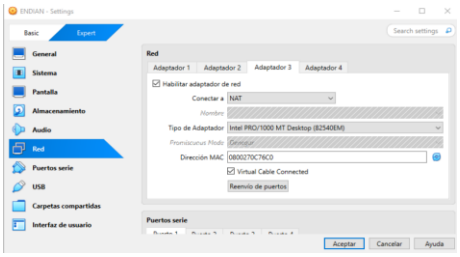
Fuente: autoría propia.

Figura 47. *Selección adaptador 2 Naranja*



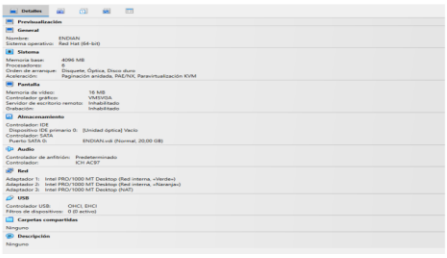
Fuente: autoría propia.

Figura 48. *Selección adaptador 3 Nat*



Fuente: autoría propia.

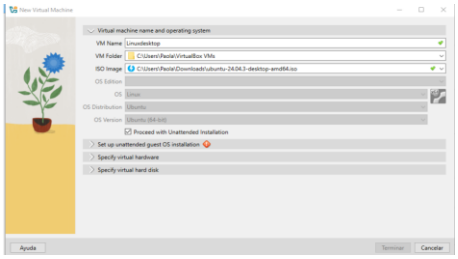
Figura 49. *Configuràon de los 3 adaptadores*



Fuente: autoría propia.

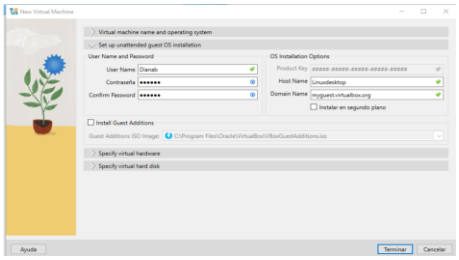
Lo que realicé fue que instalé y configuré Endian Firewall (EFW) como la plataforma principal de seguridad de la red, asignando los tres adaptadores uno para la red verde (LAN), otro para la red naranja (DMZ) y un adaptador NAT para simular la salida a internet.

Figura 50. *Configuraciòn segunda máquina virtual desktop*



Fuente: autoría propia.

Figura 51. *Configuraciòn segunda máquina virtual desktop*

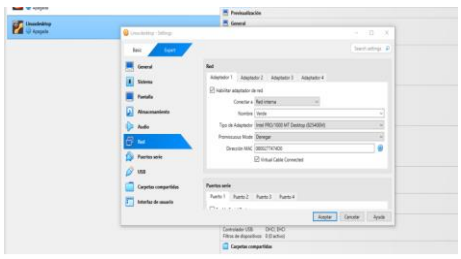


Fuente: autoría propia.

Figura 52. *Configuraciòn segunda máquina virtual desktop*

Fuente: autoría propia.

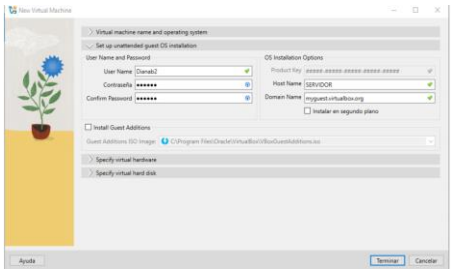
Figura 53. *Configuración para que utilice la misma red(red verde) de Endian.*



Fuente: autoría propia.

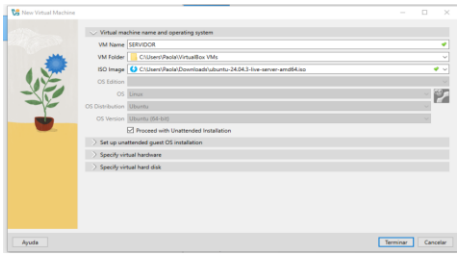
En resumen, Le coloqué un adaptador en la red verde, ya con esto tendré que configurar una IP del segmento LAN y usé como gateway la interfaz verde del Endian para permitir la comunicación.

Figura 54 . *Configuración tercera máquina virtual server*



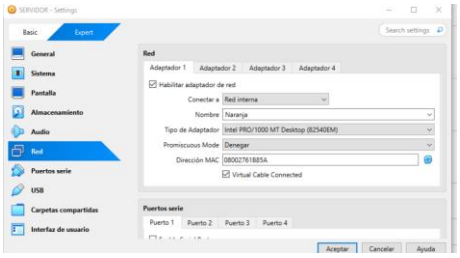
Fuente: autoría propia.

Figura 55 . *Configuraciòn tercera máquina virtual server*



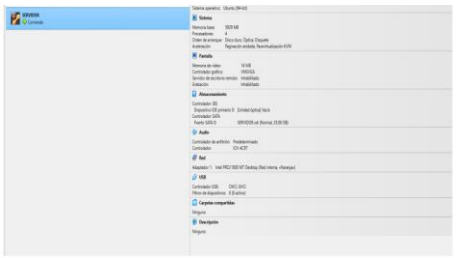
Fuente: autoría propia.

Figura 56. *Configuración para que utilice la misma red(red naranja) de Endian.*



Fuente: autoría propia.

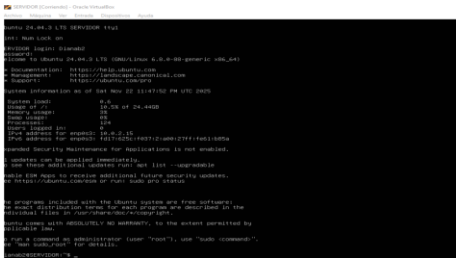
Figura 57. *Evidencia configuración para que utilice la misma red(red naranja) de Endian.*



Fuente: autoría propia.

Le configuré un único adaptador conectado a la red naranja, para después asignarle una IP dentro del rango de la DMZ y configurando como puerta de enlace la interfaz naranja del Endian.

Figura 58. *Instalación 3 máquina virtual server*



Fuente: autoría propia.

Resumen servidor Ubuntu Server será el encargado de los servicios web y FTP

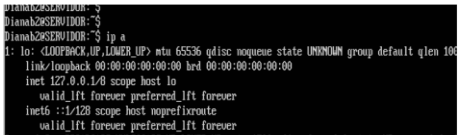
A continuación, tenemos un cuadro donde describimos los resultados de la configuración de las tres máquinas con Endian

Figura 59. *Cuadro de configuración de las tres máquinas con ed*ian

Máquina	Adaptador	Zona / Tipo	Modo (VirtualBox)	IP asignada
Endian Firewall	Adaptador 1	Verde (LAN)	Red Interna: green	192.168.10.1
	Adaptador 2	Naranja (DMZ)	Red Interna: dmz	192.168.20.1
	Adaptador 3	WAN (Internet)	NAT	Automática (DHCP)
Servidor	Adaptador 1	DMZ (Naranja)	Red Interna: dmz	192.168.20.10
Desktop / Cliente	Adaptador 1	LAN (Verde)	Red Interna: green	192.168.10.10

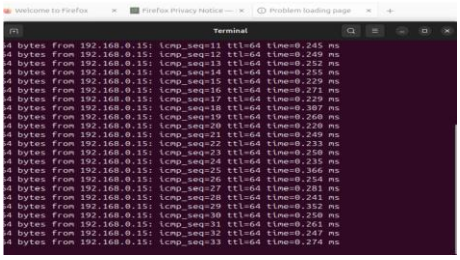
Fuente: autoría propia.

Figura 60. *Asignacion de ip manual IP 192.168.1.20 a la máquina Ubuntu*



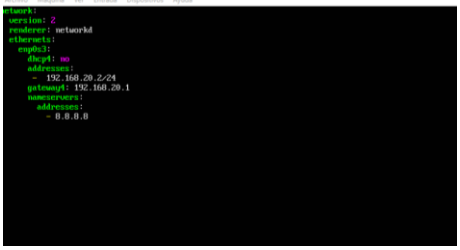
Fuente: autoría propia.

Figura 61. Validación ping verde en desktop y funciona:



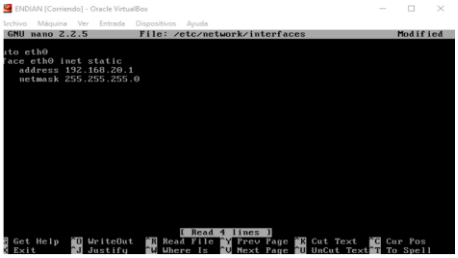
Fuente: autoría propia.

Figura 62. *Configuraciòn server para la conexiones*



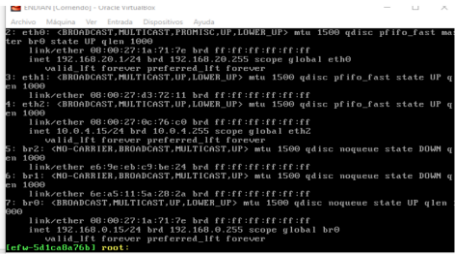
Fuente: autoría propia.

Figura 63. *Configuraciòn Endian para la conexiones*



Fuente: autoría propia.

Figura 64. *Verificación con adaptador naranja está configurado en endian:*

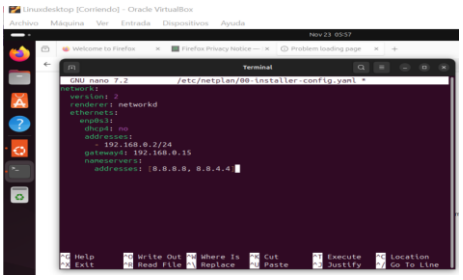


Fuente: autoría propia.

Figura 65. *Configuraciòn para conectar el adaptador naranja configurando la ip estática en server:*

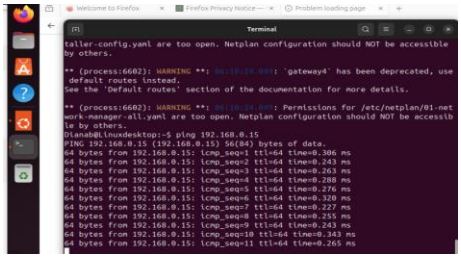
Fuente: autoría propia.

Figura 66. *Configuración de la interfaz de la red en desktop:*



Fuente: autoría propia.

Figura 67. *Evidencia de desktop está conectada correctamente a endian:*



Fuente: autoría propia.

Lo que realice es que a cada máquina le asigné su dirección IP correspondiente y configuré la puerta de enlace apuntando a la interfaz adecuada del Endian. Después verifiqué la comunicación entre las redes, asegurándome de que el desktop pudiera salir por el firewall y que el servidor en la DMZ respondiera según las reglas configuradas

Además de la configuración de IP y puertas de enlace, realicé pruebas de conectividad entre las máquinas para asegurar que todo estuviera funcionando correctamente, por lo cual utilicé comandos de **ping** desde el desktop hacia el firewall y hacia el servidor, y también desde el servidor hacia el Endian de esta manera verifique que cada red respondiera como debía.

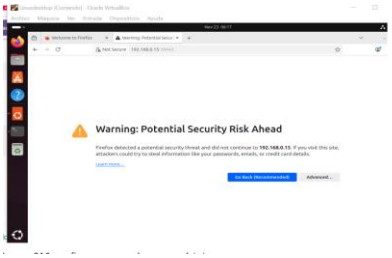
De esta forma las pruebas realizadas permitieron confirmar que las interfaces estaban bien configuradas, que las rutas eran correctas y que la comunicación entre la red verde.

Figura 68. *Ingreso al panel web de endian:*

Imagen 24 Ahora se intenta ingresar desde el navegador de desktop al panel web de endian

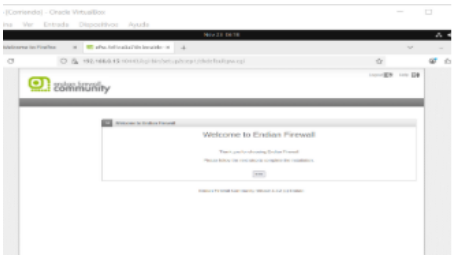
Fuente: autoría propia.

Figura 69: *Ingreso al panel web de endian*



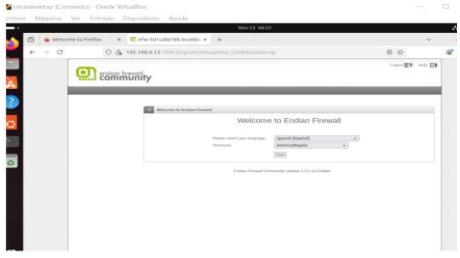
Fuente: autoría propia.

Figura 70. *Conexión correcta al panel de endian*



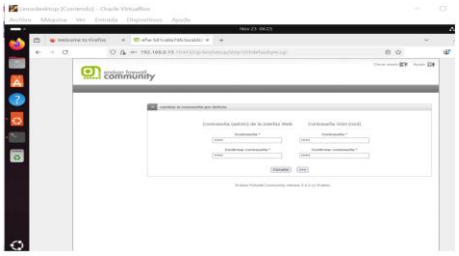
Fuente: autoría propia.

Figura 71. *Conexión correcta al panel de endian*



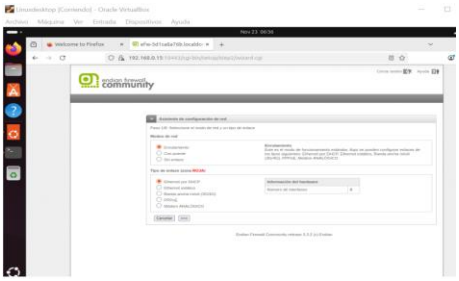
Fuente: autoría propia.

Figura 72. *Ingreso al panel web de endian*



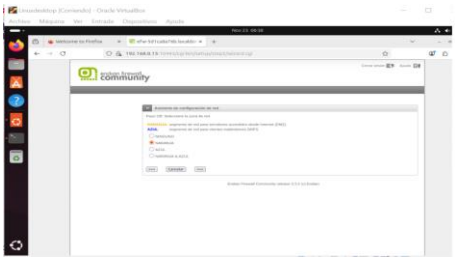
Fuente: autoría propia.

Figura 73. *En la opción configuraciòn Red se valida el número de tarjetas (3):*



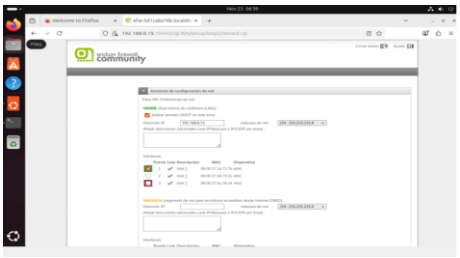
Fuente: autoría propia.

Figura 74. *Elección de la red que se va a configurar (Naranja)*



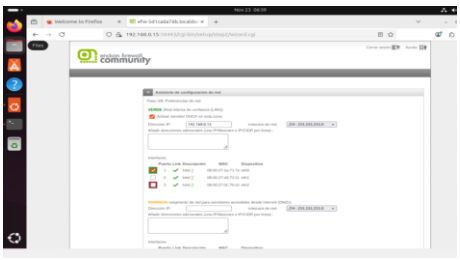
Fuente: autoría propia.

Figura 75. *Configuración red Naranja (Naranja)*



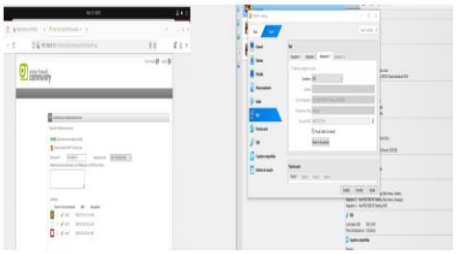
Fuente: autoría propia.

Figura 76. *Validación de que la ip esta en el mismo servidor (192.168.0.15):*



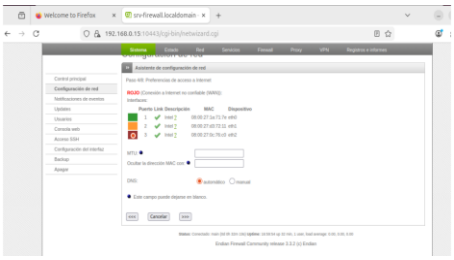
Fuente: autoría propia.

Figura 77. *Evidencia de conexión de endian mirando en virtual box las configuración de red Mac son la misma:*



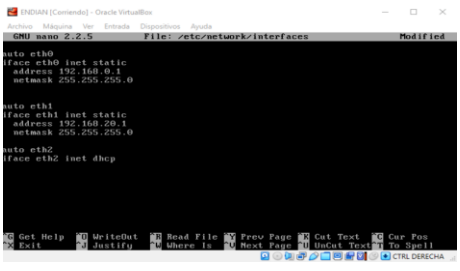
Fuente: autoría propia.

Figura 78. *Configuración red naranja:*



Fuente: autoría propia.

Figura 79: *Ajuste de la ip en endian:*

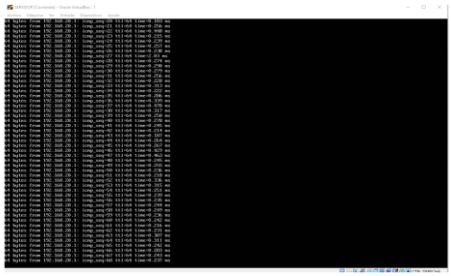


Fuente: autoría propia.

Figura 80. Evidencia *conexión server:*

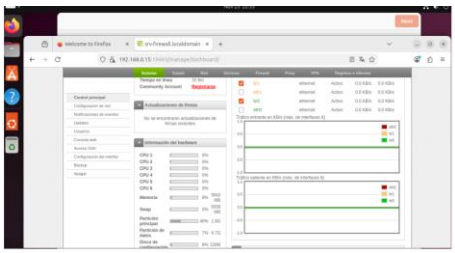
Fuente: autoría propia.

Figura 80. *Conexion server:*



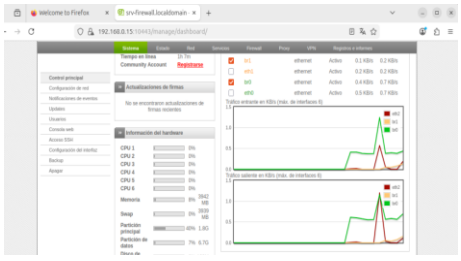
Fuente: autoría propia.

Figura 81. *Funcionamiento firewall endian:*



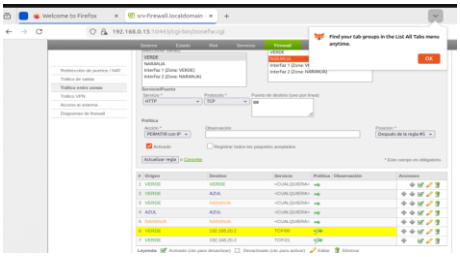
Fuente: autoría propia.

Figura 82. *Funcionamiento firewall endian*



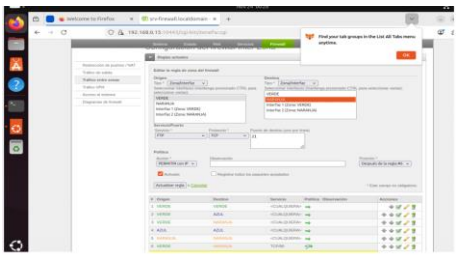
Fuente: autoría propia.

Figura 83. Aplicación reglas temática 3 -creación regla HTTP:



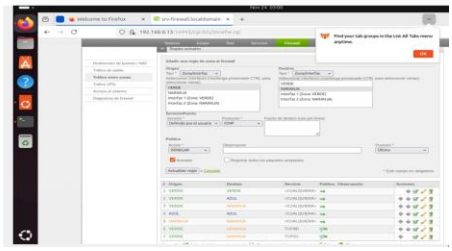
Fuente: autoría propia.

Figura 84. Creaciòn Regla fpt



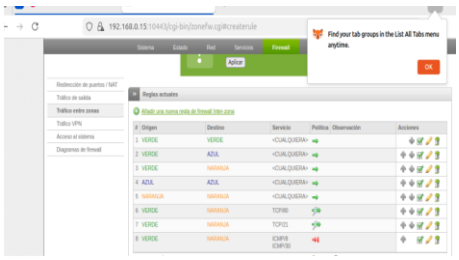
Fuente: autoría propia.

Figura 85. Creación regla ICMP:



Fuente: autoría propia.

Figura 86. Evidencia creaciòn de reglas (las dos verdes hppt y fpt y la icmp que bloquea es la de flecha roja):



Fuente: autoría propia.

Figura 87. La prueba con curl http://192.168.2.10 confirmó que el servicio HTTP en la DMZ. Demostración que el http hacia el dmz está navegando correctamente con el uso de curl http://192.168.2.10 server:

Fuente: autoría propia.

Figura 88. La prueba desde el servidor con ftp 192.168.2.10 confirmó que el acceso FTP. Esto es desde el servidor Demostración que el FTP hacia el dmz está navegando correctamente con el uso de ftp 192.168.2.10:

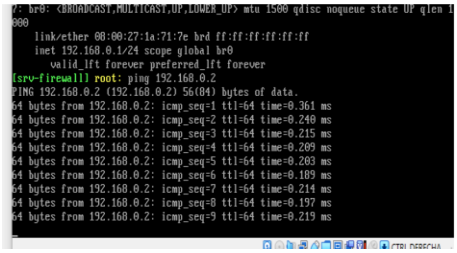
Fuente: autoría propia.

Figura 89. Evidencia que el ping falla sin recibir paquetes, indicando que el bloqueo funciona.

Fuente: autoría propia.

Figura 90. El ping desde Endian al desktop responde correctamente, confirmando la conectividad.

Fuente: autoría propia.



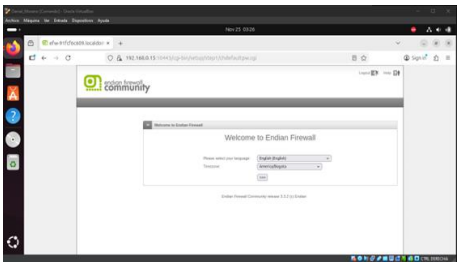
Cuando finalice la configuración de la infraestructura, pasé a la solución puntual de la temática 3 que fue la que elegí, En Endian habilité únicamente los servicios necesarios desde la 32 DMZ hacia la red: HTTP (puerto 80) y FTP (puerto 21) para que el servidor web pudiera ofrecer sus aplicaciones y permitir transferencias. Luego configuré las reglas de firewall para bloquear completamente el protocolo ICMP, de manera que los equipos de la red no pudieran hacer ping hacia direcciones internas. Probé el bloqueo desde la consola intentando hacer ping a una IP de la red y verifiqué que no había respuesta. Finalmente, revisé el tráfico y confirmé las reglas. En lo posible coloque al detalle todo lo que hice. y me enfoqué en dar solución a la creación de las reglas configurándose en endian para permitir únicamente HTTP y FTP desde la DMZ, y bloqueé el ICMP para impedir pings entre redes, verificando que solo el tráfico *autorizado pasará.*

TEMÁTICA 5.

En la siguiente se implementará un Proxy HTTP (No transparente) con políticas de autenticación para navegación en Internet, con el fin de restringir el acceso a diferentes direcciones web, esto con el objetivo de generar políticas de acceso sobre recursos externos.

Una vez concluido el proceso de instalación procedemos a ingresar a nuestra máquina virtual Linux que nos servirá como el cliente de nuestro Proxi, para lo cual se debe ingresar a la siguiente dirección: https://192.168.0.15:10443

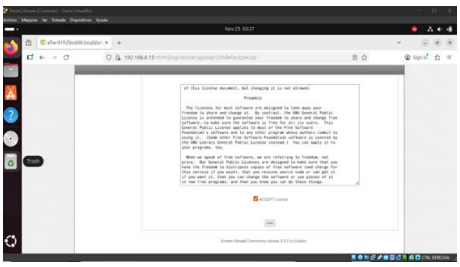
Figura 91. *Ingreso a Endian (Interfaz gráfica Endian desde máquina cliente):*



Fuente: autoría propia.

Se realiza la aceptación de términos y condiciones, esto con el fin poder continuar con la configuración.

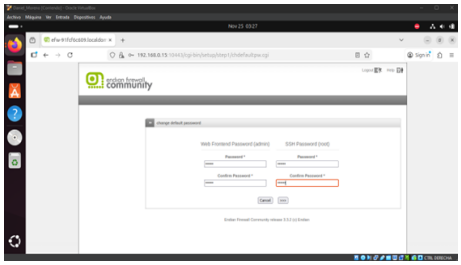
Figura 92. *Términos y Condiciones Endian (Interfaz gráfica Endian desde máquina cliente):*



Fuente: autoría propia.

Paso siguiente se establecen las contraseñas de los usuarios, Admin y Root

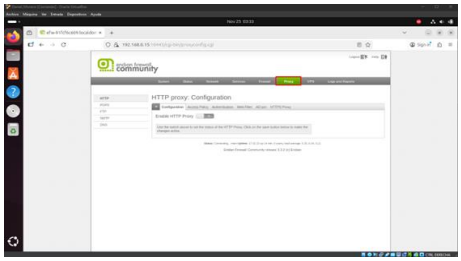
Figura 93. *Configuración usuarios:*



Fuente: autoría propia.

Una vez culminada esta configuración se procede con la configuración, para esto se ingresa a la opción Proxy como se ve a continuación:

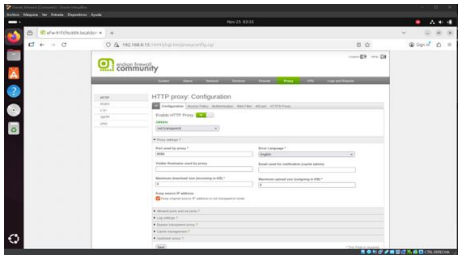
Figura 94. *Configuración Proxy*



Fuente: autoría propia.

Paso siguiente se realiza la habilitación de la opción "Enable HTTP Proxy", esta es para que se pueda configurar la lista negra así como los perfiles de usuario.

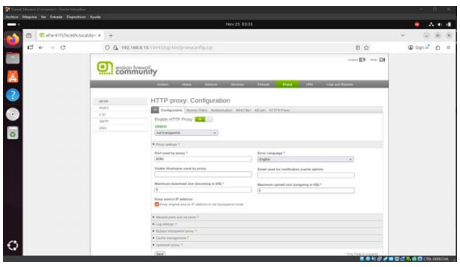
Figura 95. *Configuración Proxy HTTP*



Fuente: autoría propia.

En esta interfaz se realiza la configuración de la red verde (Green), donde se va a indicar que es transparente, así como el puerto a usar.

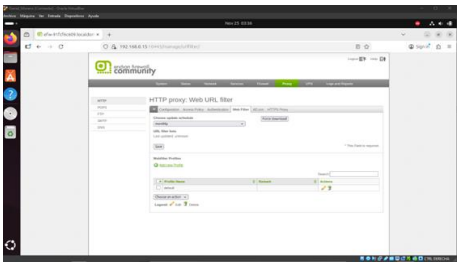
Figura 96. *Configuración Proxy HTTP*



Fuente: autoría propia.

Una vez culminada esta opción, paso siguiente ingresamos a Web Filter, esto para ya comenzar con todo el tema de parametría.

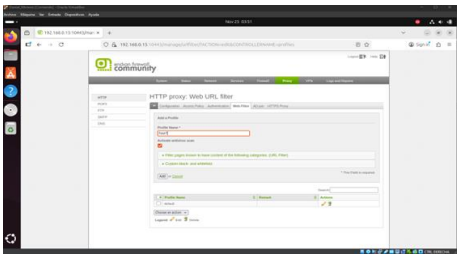
Figura 97. *Configuración Proxy HTTP*



Fuente: autoría propia.

Se realiza la creación del perfil, que se usará para la realización de la lista negra, con los diversos sitios web que se quieren registrar.

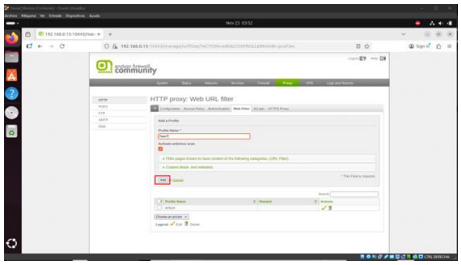
Figura 98. *Creación Perfil*



Fuente: autoría propia.

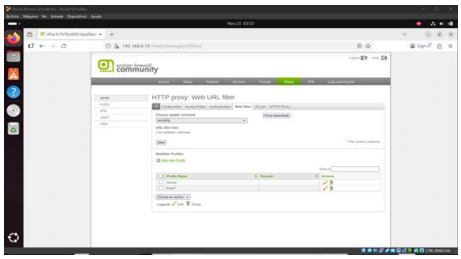
Le damos en la opción de ADD, esto para confirmar los cambios y que se vea reflejado el usuario.

Figura 99. *Adiciòn del usuario*



Fuente: autoría propia.

Figura 100. *Adición de usuario correcto*

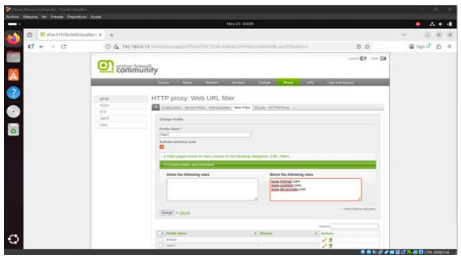


Fuente: autoría propia.

Una vez finalizada esta configuración del perfil, se continúa con la creación de lista negra para no permitir el acceso las páginas que nos indica la guía de aprendizaje, para ello se añadirán las siguientes URL`S

- www.hotmail.com
- www.youtube.com
- www.elnuevodia.com.co

Figura 101. *Configuración Lista negra:*



Fuente: autoría propia.

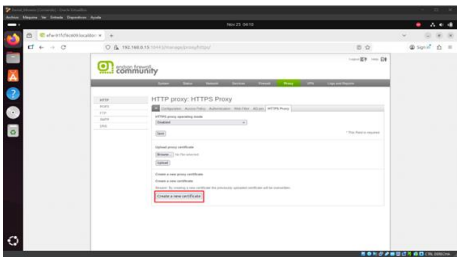
Una vez ingresadas las páginas, se procede con la aplicación de cambios.

Figura 102. *Confirmación lista negra:*

Fuente: autoría propia.

Para fines de instalación y configuración a otros equipos o exploradores se realiza la descarga del certificado

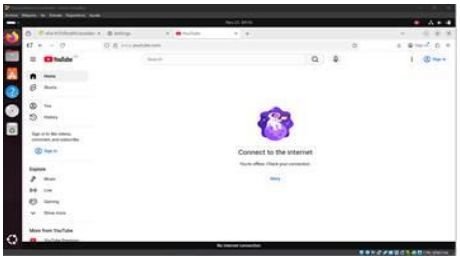
Figura 102. *Descarga del certificado:*



Fuente: autoría propia.

Una vez se realiza toda la configuración anteriormente descrita se realiza al ingreso de una de las páginas de la lista negra, la cual no se debe permitir el acceso o evitar la carga de esta, para ello se intenta ingresar a YouTube

Figura 103. *Ingreso a Youtube:*



Fuente: autoría propia.

Como se evidencia y resultado de la práctica se puede concluir que Endian Firewall, es una herramienta útil al momento que se quiera realizar restricción y seguridad de los sitios Web, y tratar de aislar al máximo la navegación por temas de políticas de seguridad en alguna empresa o por nuestra misma protección como usuarios finales.

Link de videos explicativos:

Jhon Hincapié:
https://youtu.be/1ZjfLa2bIwQ

Omar Alfredo Pacheco Yepez:
https://youtu.be/t5GbodIhNZk?si=Um1x6dVT6gZMCVu4

Diana Paola Bohorquez
https://youtu.be/1FEK2audhVk

Daniel Moreno
https://www.youtube.com/watch?v=bnz-08TFTho
https://youtu.be/_rFkIwd4wI4

4 CONCLUSIONES

La implementación de Endian Firewall permitió comprender de manera práctica la configuración de zonas de red y la aplicación de técnicas de seguridad perimetral. A través de la correcta definición de las interfaces VERDE, NARANJA y ROJO, así como de las reglas de firewall y NAT, se habilitó la salida de la LAN hacia Internet y la publicación controlada de servicios en la DMZ mediante Port Forwarding.

Las pruebas realizadas desde las estaciones de trabajo de la LAN y desde clientes externos demuestran el correcto funcionamiento de las reglas definidas, cumpliendo con los objetivos planteados en la guía de la temática 2 relacionados con NAT y DMZ. Este ejercicio refuerza la importancia de diseñar adecuadamente la topología de red y las políticas de acceso para proteger los recursos internos de la organización.

5 ANEXOS:

Total, figuras: 103.

6 REFERENCIAS

[1] Canonical, “Guía del Ubuntu Desktop 20.04 LTS”, *Help Ubuntu*. [En línea]. Disponible en: https://help.ubuntu.com/20.04/ubuntu-help/index.html. Año 2023.

[2] J. Conejos, “Instala tu servidor Zentyal en Ubuntu Server”, *Blog de José Conejos*. [En línea]. Disponible en: https://joseconejos.wordpress.com/2018/03/06/instala-tu-servidor-zentyal-en-ubuntu-server/. Oct. 2019.

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

[4] Endian, “Endian UTM 3.2 Manual de referencia”. [En línea]. Disponible en: http://docs.endian.com/3.2/utm/index.html. Año 2016.

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

[6] F. Muhammad, A. Mutiara and I. Ismail, “Implementation of Management and Network Security Using Endian UTM Firewall”, pp. 1–9, ebscohost. [En línea]. Disponible en: http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.C2217DDD&lang=es&site=eds-live&scope=site. Año 2017.

[7] Oracle, “Manual de usuario VirtualBox”. [En línea]. Disponible en: https://www.virtualbox.org/manual/. Año 2020.

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

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

[10] P. F. Hernández and J. Sánchez, “Monitoreo y administración de sistemas Linux”, Objeto virtual de información (OVI), Repositorio Institucional UNAD. [En línea]. Disponible en: https://repository.unad.edu.co/handle/10596/53211. Año 2022.