OPTIMIZACIÓN DE LA SEGURIDAD EN REDES LINUX CON ENDIAN FIREWALL

Erly Tatiana Perez Joven
e-mail: etperezj@unadvirtual.edu.co
Brillyn Narváez Vargas
e-mail: bnarvaezv@unadvirtual.edu.co
Cristian Camilo Gómez Fajardo
e-mail: ccgomezfa@unadvirtual.edu.co
Liliana Andrea Paz Ferrer
e-mail: Lapazf@unadvirtual.edu.co
Marlon Stiven Rojas Moreno
e-mail: msrojasmo@unadvirtual.edu.co

RESUMEN: *El presente trabajo tiene como propósito la implementación y configuración del sistema GNU/Linux Endian Firewall (EFW) dentro de un entorno virtualizado con Oracle VM VirtualBox, orientado a simular un entorno empresarial seguro mediante la segmentación de redes y la aplicación de políticas de control y filtrado de tráfico. La propuesta inicia con la correcta configuración de las interfaces de red del firewall para establecer las zonas verdes (LAN), roja (WAN) y naranja (DMZ), asegurando así la estructura perimetral de la red. A continuación, se procede con la creación de reglas de NAT que permitan la comunicación de la red interna y la DMZ hacia Internet, validando el enrutamiento mediante el reenvío de puertos.*

Posteriormente, se habilitan servicios esenciales como HTTP y FTP desde un servidor ubicado en la zona DMZ, restringiendo simultáneamente protocolos como ICMP para fortalecer la seguridad. Se diseñan reglas específicas de acceso entre zonas, estableciendo permisos y denegaciones según los protocolos y orígenes de tráfico, las cuales son verificadas mediante pruebas funcionales desde navegadores web y terminales. Finalmente, se implementa un proxy HTTP no transparente con autenticación de usuarios, permitiendo establecer filtros de navegación mediante listas negras, con el objetivo de restringir el acceso a ciertos portales web desde la red LAN. Esta experiencia práctica integra conceptos clave de seguridad perimetral, administración de servicios en red y gestión de usuarios, consolidando un entorno virtual seguro y funcional para la gestión del tráfico interzonal y externo.

PALABRAS CLAVE: Endian Firewall, VirtualBox, DMZ, NAT y servicios HTTP y FTP

INTRODUCCIÓN

En el contexto actual de las redes informáticas, la implementación de soluciones de seguridad perimetral robustas es fundamental para garantizar la integridad y el control del tráfico de datos entre diferentes zonas de una organización. Por ello, este proyecto tiene como objetivo principal la instalación, configuración y puesta en marcha del sistema operativo GNU/Linux Endian Firewall (EFW), en su versión comunitaria, dentro de un entorno virtualizado con Oracle VM VirtualBox. Esta implementación permitirá comprender de forma práctica cómo segmentar y gestionar el tráfico de red entre diferentes zonas, así como aplicar políticas de seguridad, traducción de direcciones y control de servicios.

El diseño de red propuesto se representa en la Figura 1, donde se observa la segmentación en tres zonas: verde (LAN), roja (WAN) y naranja (DMZ), todas gestionadas por el firewall Endian.

Inicialmente, se procede con la configuración de la instancia de EFW, ajustando correctamente las interfaces de red en VirtualBox para representar tres zonas críticas: la zona verde (LAN), correspondiente a la red interna; la zona roja (WAN), simulando el acceso a Internet; y la zona naranja (DMZ), destinada a servidores expuestos al exterior. Una vez completada la instalación efectiva del sistema, se establece la conectividad entre las zonas mediante reglas de NAT (Network Address Translation), permitiendo así el acceso desde la LAN hacia la WAN y desde la DMZ hacia la red externa, mediante reglas de reenvío de puertos que facilitan la visibilidad del tráfico.

Posteriormente, se configuran servicios específicos en la zona DMZ, habilitando protocolos como HTTP (puerto 80) y FTP (puerto 21) desde un servidor Ubuntu Server, al tiempo que se aplican políticas de seguridad para bloquear el protocolo ICMP (puertos 8 y 30), evitando así respuestas al comando ping desde otras zonas de la red. Esto se complementa con la implementación de reglas de acceso que permiten o deniegan el tráfico entre zonas específicas, como la comunicación entre la zona verde y la zona naranja mediante los protocolos antes mencionados, así como la interacción entre la zona DMZ y la zona de Internet. Estas reglas son

validadas mediante pruebas de navegación y tráfico en tiempo real, verificando la correcta aplicación de políticas.

Se configura un Proxy HTTP no transparente con políticas de autenticación para navegación controlada desde la red interna. En este proceso, se crea un perfil de usuario asociado a una política que restringe el acceso a sitios específicos como *www.hotmail.com*, *www.youtube.com* y *www.elnuevodia.com.co*, garantizando así un control efectivo de contenidos. La autenticación se realiza mediante la creación de usuarios y grupos dentro del sistema, quienes serán sujetos a las restricciones establecidas. Las pruebas de navegación desde la LAN permiten verificar la efectividad de estas medidas, consolidando así una solución de firewall integral, segura y completamente funcional para entornos empresariales simulados.

INSTALACIÓN DE ENDIAN

1.1 REQUISITOS:

Mínimos:

- **CPU:** Procesador Intel/AMD de 64 bits (x86_64)
- **RAM:** 2 GB
- **Disco duro:** 40 GB de espacio libre mínimo
- **Tarjetas de red:** Al menos 2 interfaces de red (NIC) para configurar las zonas (roja, verde, naranja)
- **Unidad de CD/DVD o USB:** Para la instalación desde ISO
- **Monitor y teclado:** Para la instalación inicial (puede administrarse luego por interfaz web)

1.2 SOPORTE DE HARDWARE:

Endian se basa en Linux CentOS/RHEL, por lo que es compatible con una amplia gama de hardware compatible con Linux, incluyendo:

- Tarjetas de red Intel, Realtek, Broadcom (PCI/PCIe)
- Discos SATA, IDE, SCSI y SSD
- Virtualización completa en entornos como VirtualBox, VMware, Proxmox, KVM, entre otros
- Soporte para hardware estándar de servidores y PC

TEMÁTICA 1: CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX

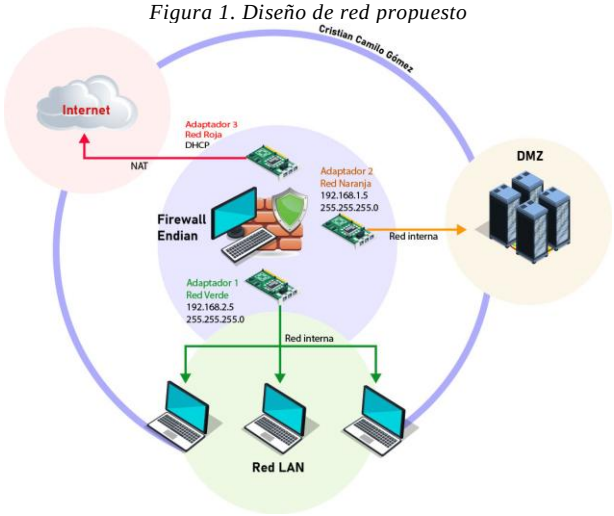
Antes de comenzar se debe considerar las direcciones que se van a utilizar para cada zona de la red.

En este caso los segmentos estarán dispuestos de la siguiente manera:

- Zona verde: 192.168.2.5
- Cliente conectado: 192.168.2.10
- Zona naranja (DMZ): 192.168.1.5
- Server conectado: 192.168.1.10
- Zona roja: DHCP

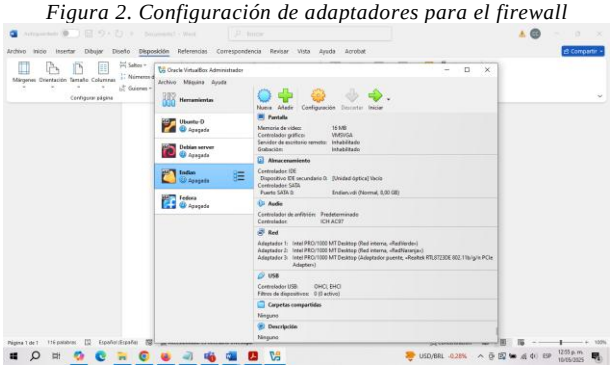
De esta manera se asegura que las maquinas puedan comunicarse entre sí ya que se busca crear una red que se ajuste al siguiente diagrama.

Figura 1. Diseño de red propuesto



Fuente: Cristian Camilo Gómez Fajardo

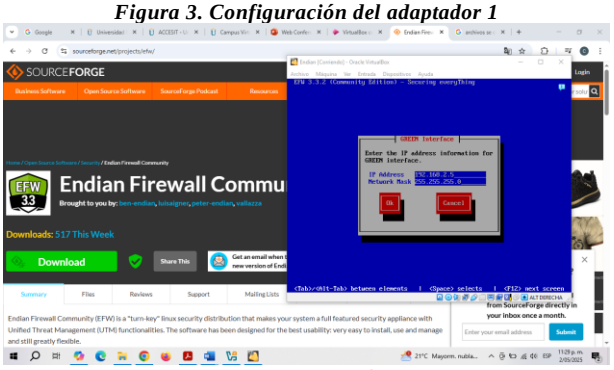
Figura 2. Configuración de adaptadores para el firewall



Fuente: Cristian Camilo Gómez Fajardo

Siguiendo la configuración planteada se crean y asignan las redes para cada adaptador en la configuración de la maquina desde VirtualBox.

Figura 3. Configuración del adaptador 1



Fuente: Cristian Camilo Gómez Fajardo

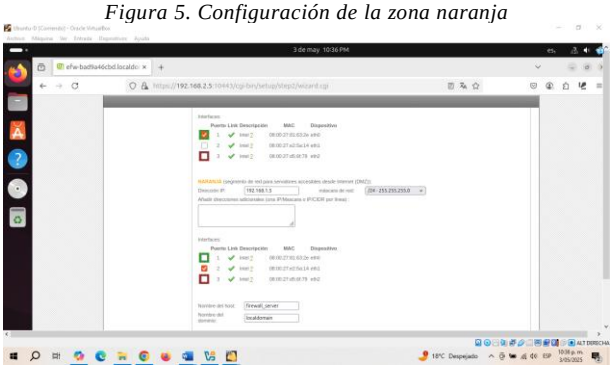
Se comienza con la asignación de la ip para zona verde ya que corresponde al adaptador 1 de la máquina virtual durante la instalación de Endian.

Figura 4. Iniciando el Firewall

Fuente: Cristian Camilo Gómez Fajardo

Una vez completada la instalación de Endian se puede apreciar la asignación de direcciones para los adaptadores 1 y 3 ya que el primero se asignó en la instalación y el tercero es asignado automáticamente por el rúter mediante DHCP, en este caso haría falta configurar el adaptador 2 que corresponde a la zona naranja.

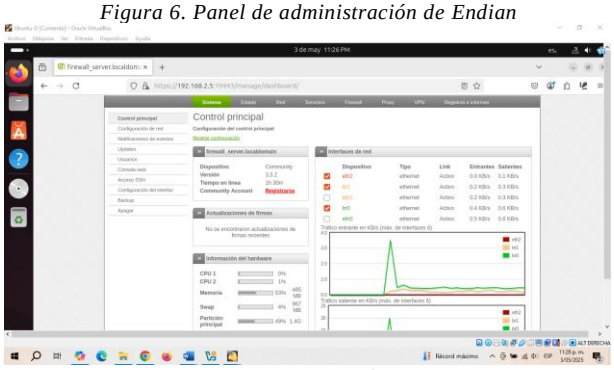
Figura 5. Configuración de la zona naranja



Fuente: Cristian Camilo Gómez Fajardo

Desde la interfaz accedida desde el cliente es posible asignar la dirección que hace falta, de esta manera se habilita la comunicación con la DMZ y por tanto al server conectado a la misma.

Figura 6. Panel de administración de Endian

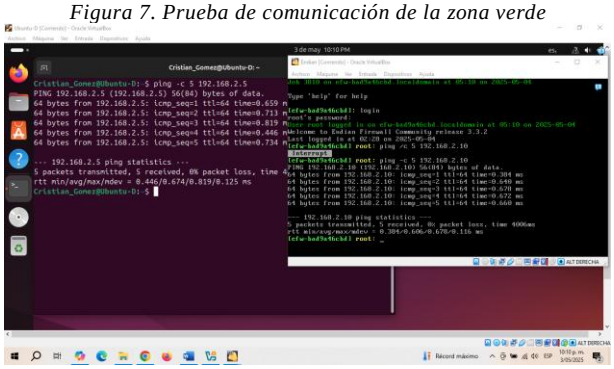


Fuente: Cristian Camilo Gómez Fajardo

Una vez que la configuración esta completa al 100% se puede acceder al panel de administración de Endian desde la zona verde, si todo ha salido bien se podrá visualizar el tráfico de red de cada zona.

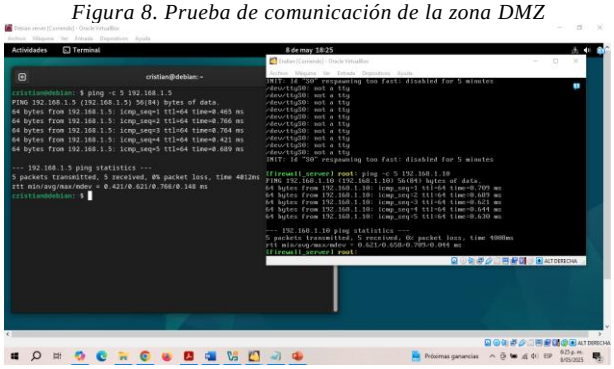
Antes de realizar las pruebas es necesario recordar que la configuración de las direcciones para las máquinas de cada zona debe estar previamente configuradas.

Figura 7. Prueba de comunicación de la zona verde



Fuente: Cristian Camilo Gómez Fajardo

Figura 8. Prueba de comunicación de la zona DMZ

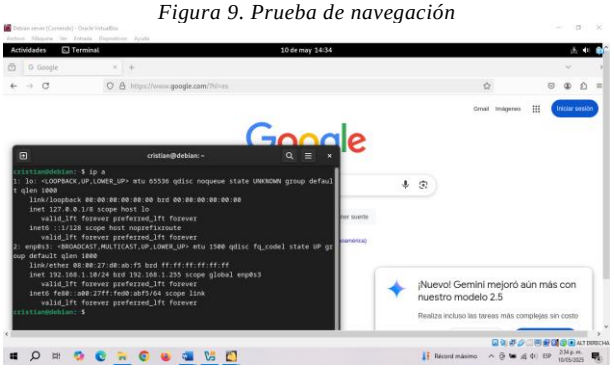


Fuente: Cristian Camilo Gómez Fajardo

Hasta este punto ya es posible evidenciar que la configuración de la red está funcionando correctamente y el envío de paquetes entre máquinas y entre zonas se realiza correctamente.

Adicionalmente se ha configurado el acceso a internet para las zonas, aunque no se va a detallar aquí ya que es tema para la segunda temática.

Figura 9. Prueba de navegación



Fuente: Cristian Camilo Gómez Fajardo

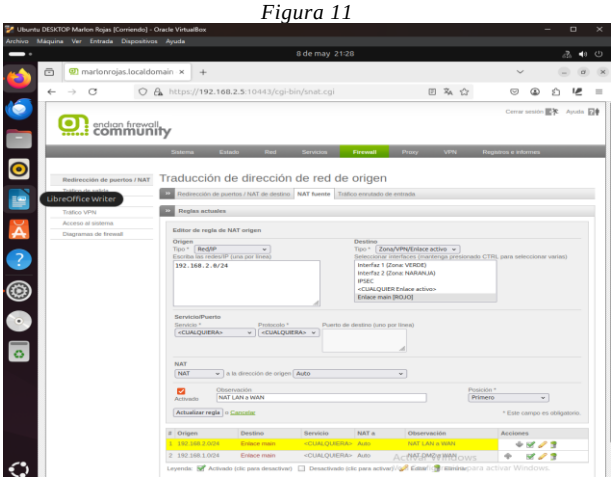
TEMÁTICA 2: CONFIGURACIÓN NAT.

Figura 10. visualizamos que las creaciones fueron exitosas y están guardadas

Fuente: Marlon Stiven Rojas Moreno

Configurar la regla de NAT (Network Address Translation / Traducción de Direcciones de Red), demostrando el establecimiento de la comunicación desde la LAN hacia la WAN (Red simulada de Internet).

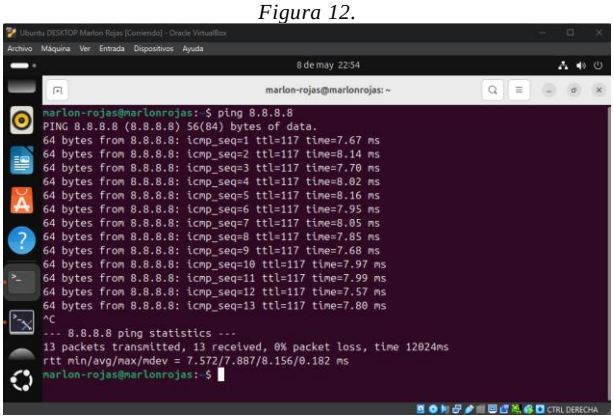
Figura 11



Fuente: Marlon Stiven Rojas Moreno

Se configuró una regla de Source NAT para permitir que el tráfico de la red VERDE (LAN) acceda a Internet a través de la red ROJA (WAN).

Figura 12.



Fuente: Marlon Stiven Rojas Moreno

En la imagen podemos ver que ejecutamos un comando ping hacia la dirección pública 8.8.8.8, que es un servidor DNS de Google. La respuesta es positiva: todos los paquetes fueron enviados y recibidos correctamente, con un tiempo de respuesta bajo, lo que confirma que tenemos acceso a Internet.

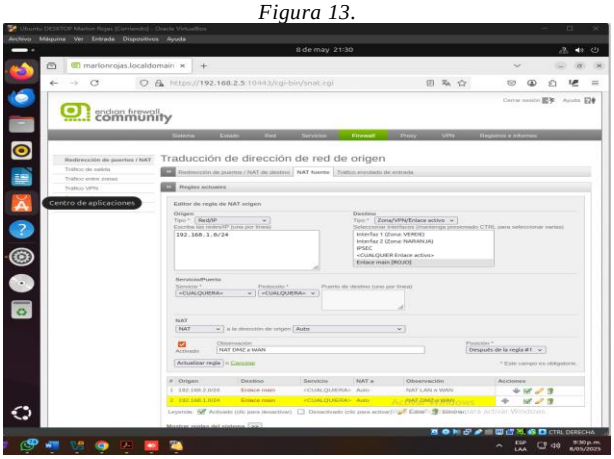
Esto demuestra que la regla de NAT configurada para la red VERDE está operando de forma correcta, permitiendo que los dispositivos de la LAN puedan salir a Internet a través de la red WAN.

Con esta validación, aseguramos que nuestra red local tiene conectividad externa gracias a la traducción de direcciones configurada en Endian, cumpliendo así con los objetivos de La temática 2."

se cumplió. En la prueba desde Desktop, se configuró la regla de NAT que permite la salida desde la red LAN hacia la WAN. Esto quedó demostrado con éxito cuando la máquina realizó el ping a 8.8.8.8, confirmando que la comunicación desde la LAN hacia la red simulada de Internet está funcionando correctamente.

Configurar la regla de NAT, demostrando el establecimiento de la comunicación de la Zona DMZ hacia la Internet. Verificar en el re-envió de puertos / NAT, la creación de las reglas.

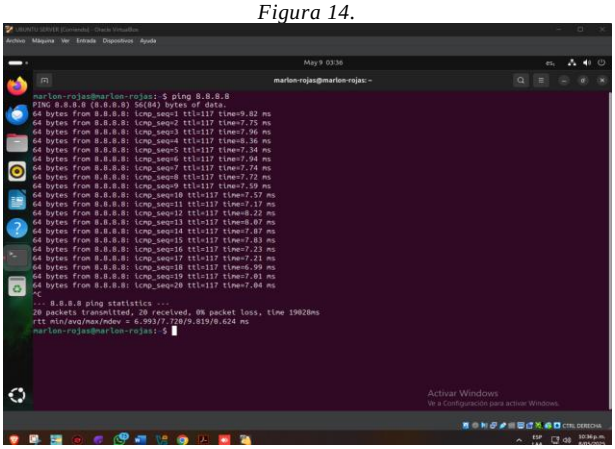
Figura 13.



Fuente: Marlon Stiven Rojas Moreno

regla de SNAT para la red ORANGE (DMZ), permitiendo que el tráfico de la red 192.168.1.0/24 se enmascare y salga hacia la interfaz RED (WAN). Esto habilita que la red DMZ tenga acceso a Internet a través de la red externa.

Figura 14.



Fuente: Marlon Stiven Rojas Moreno

Server también ha realizado con éxito la prueba, En la imagen podemos observar que el servidor ejecutó un ping exitoso a la dirección pública 8.8.8.8, lo que confirma que también tiene acceso a Internet. Todos los paquetes fueron transmitidos y recibidos sin pérdida, con tiempos de respuesta estables.

Esto demuestra que la configuración de red y NAT en el firewall Endian está funcionando correctamente, no solo para las estaciones de trabajo, sino también para los servidores, permitiendo la comunicación fluida con el exterior.

Con este resultado, confirmamos que toda la infraestructura de red tiene conectividad plena, validando el éxito de las reglas NAT configuradas Enel entorno.

se cumplió lo solicitado. Se configuró correctamente la regla de NAT en Endian, permitiendo la salida de la red DMZ hacia Internet. Esto se comprobó con los pings exitosos desde el Desktop y el servidor a 8.8.8.8, demostrando la conectividad. Además, las capturas muestran que las reglas de NAT fueron creadas y están activas en la sección de reenvío de puertos/NAT.

TEMÁTICA 3: PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED.

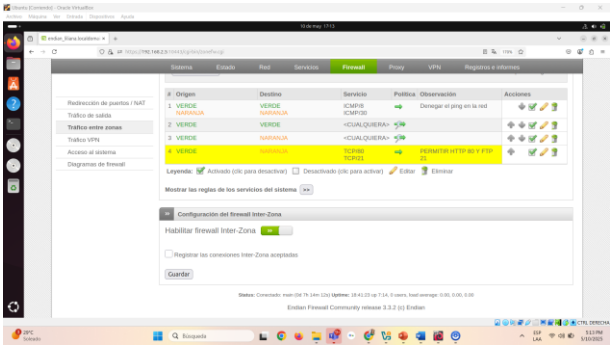
Permitir los servicios HTTP (Puerto 80) y FTP (Puerto 21) desde el servidor Web bajo Ubuntu Server.

Figura 15. Creación de regla para permitir servicios HTTP y FTP en Endian

Fuente: Liliana Andrea Paz Ferrer

La imagen muestra la configuración de una nueva regla en el firewall Endian, permitiendo el tráfico desde la red VERDE hacia la zona NARANJA. Se habilitan los servicios HTTP (puerto 80) y FTP (puerto 21), ambos bajo el protocolo TCP. Esta regla garantiza que los usuarios de la red interna puedan acceder al servidor Ubuntu ubicado en la DMZ.

Figura 16. Verificación de reglas activas para servicios HTTP y FTP en Endian



Fuente: Liliana Andrea Paz Ferrer

En esta captura se observa la lista de reglas activas del firewall. Se destaca la cuarta regla, la cual permite el tráfico desde la red VERDE hacia la zona NARANJA mediante los puertos TCP 80 y 21. Esta regla está correctamente etiquetada como "PERMITIR HTTP 80 Y FTP 21" y garantiza el acceso a los servicios web y de transferencia de archivos del servidor Ubuntu.

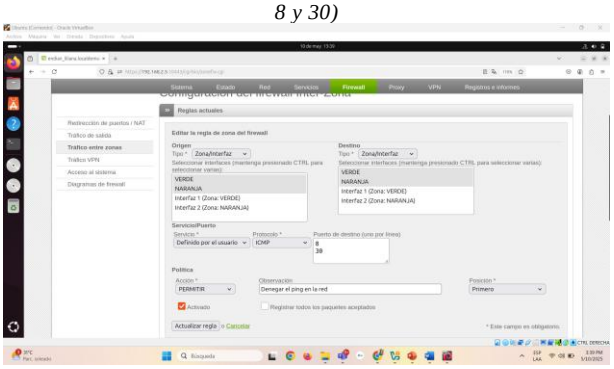
Figura 17. Reglas del firewall hacia el servidor Ubuntu para permitir servicios y bloquear ICMP

Fuente: Liliana Andrea Paz Ferrer

Esta imagen muestra reglas precisas configuradas en Endian: se permite el tráfico HTTP y FTP hacia el servidor Ubuntu (IP: 192.168.1.10) y se bloquea el protocolo ICMP (tipos 8 - Echo Request y 30 - Traceroute), impidiendo solicitudes de ping.

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.

Figura 18. Configuración de la regla para bloquear ICMP (tipos 8 y 30)



Fuente: Liliana Andrea Paz Ferrer

En esta imagen se observa la creación de una regla en el firewall Endian para denegar el tráfico ICMP desde la zona VERDE hacia la NARANJA. Se especifican los tipos 8 y 30, que son utilizados comúnmente por el comando ping y herramientas de diagnóstico. Aunque en el campo de "Acción" aparece configurado como PERMITIR, para cumplir con el objetivo de la temática es necesario que esta opción se modifique a DENEGAR, ya que el propósito es bloquear las solicitudes de eco en la red.

Figura 19. Reglas activas del firewall inter-zona en Endian

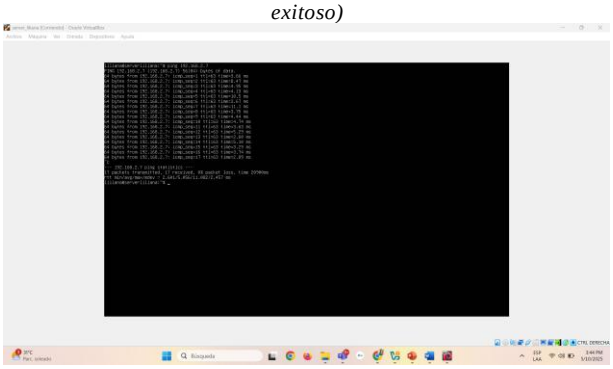
Fuente: Liliana Andrea Paz Ferrer

La imagen muestra la lista de reglas activas en el firewall de Endian. Se puede observar lo siguiente:

- La primera regla bloquea correctamente el protocolo ICMP, específicamente los tipos 8 (Echo Request) y 30 (Traceroute), desde las zonas VERDE y NARANJA hacia sus destinos. La política aplicada es de denegación, como indica la observación: “Denegar el ping en la red”.
- La cuarta regla permite el tráfico desde la red VERDE hacia la zona NARANJA a través de los servicios HTTP (puerto 80) y FTP (puerto 21) bajo el protocolo TCP. Esta regla está claramente etiquetada como: “PERMITIR HTTP 80 Y FTP 21”, cumpliendo con el requerimiento de habilitar servicios desde la red interna hacia el servidor ubicado en la DMZ.

Esta evidencia confirma que tanto las reglas de permitir servicios web y FTP, como la de bloquear ICMP, han sido aplicadas y están activas en el sistema de firewall de Endian.

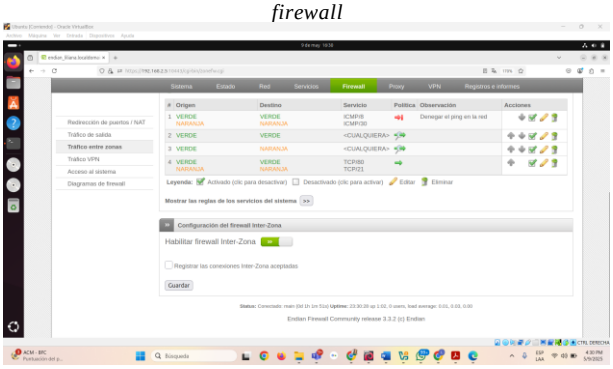
Figura 20. Prueba fallida de bloqueo del protocolo ICMP (ping exitoso)



Fuente: Liliana Andrea Paz Ferrer

En esta imagen se muestra la ejecución del comando ping 192.168.2.7 desde el servidor Ubuntu. Como se observa en la salida del terminal, se reciben múltiples respuestas del host de destino, lo cual indica que el protocolo ICMP tipo 8 (Echo Request) no está siendo bloqueado, a pesar de haber configurado la regla de denegación en el firewall.

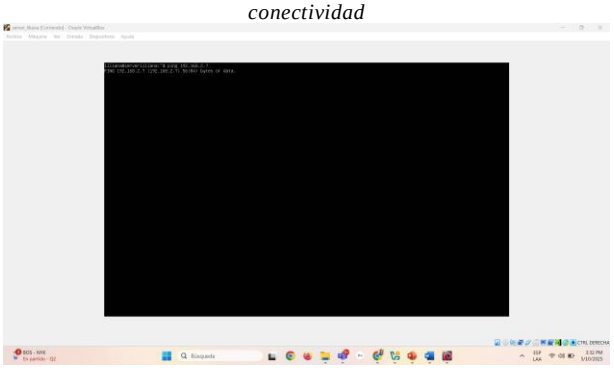
Figura 21. Verificación de tráfico bloqueado en la interfaz del firewall



Fuente: Liliana Andrea Paz Ferrer

En esta imagen se puede observar la interfaz de monitoreo del firewall Endian, donde se verifica que los paquetes ICMP están siendo bloqueados correctamente. La herramienta gráfica muestra en tiempo real el tráfico rechazado, lo cual permite confirmar que las reglas de denegación del protocolo ICMP (tipos 8 y 30) están funcionando de manera efectiva.

Figura 22. Verificación del bloqueo de ICMP mediante prueba de conectividad



Fuente: Liliana Andrea Paz Ferrer

En esta figura se muestra la ejecución del comando ping desde el servidor Ubuntu hacia la IP 192.168.2.7. La prueba resulta fallida, con 100% de pérdida de paquetes, lo que confirma que el firewall Endian ha bloqueado correctamente el protocolo ICMP. Esta validación evidencia que las reglas de seguridad configuradas para impedir respuestas a solicitudes de eco están funcionando como se esperaba.

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

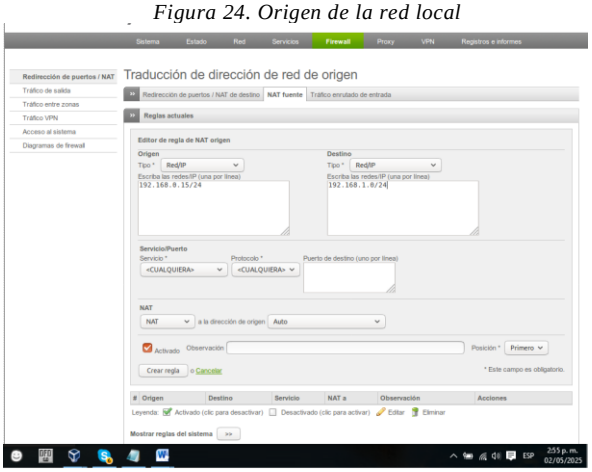
El primer paso consiste en establecer la regla de NAT, que permitirá la traducción del tráfico desde la red LAN hacia la red WAN. Para ello, se debe acceder al apartado de "Cortafuegos", seleccionar "NAT fuente" y proceder a añadir una nueva regla de NAT de tipo fuente.

Figura 23. Configuración de NAT

Fuente: Erly Tatiana Perez Joven

Indicamos como origen la red local (LAN) y como destino la red que representa nuestra conexión simulada a Internet (WAN).

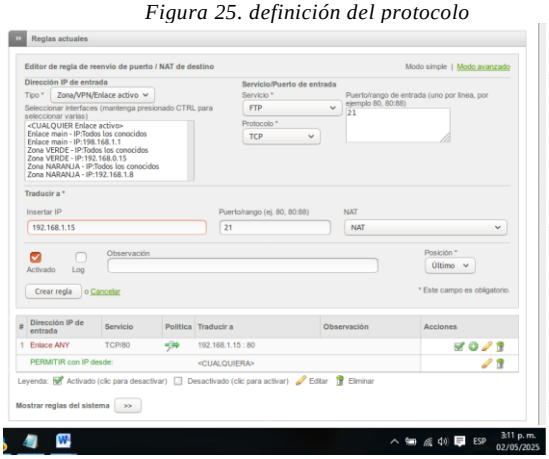
Figura 24. Origen de la red local



Fuente: Erly Tatiana Perez Joven

Es importante asegurarnos de definir correctamente el protocolo que deseamos publicar, al igual que los servicios que queremos hacer accesibles desde la zona DMZ hacia Internet.

Figura 25. definición del protocolo



Fuente: Erly Tatiana Perez Joven

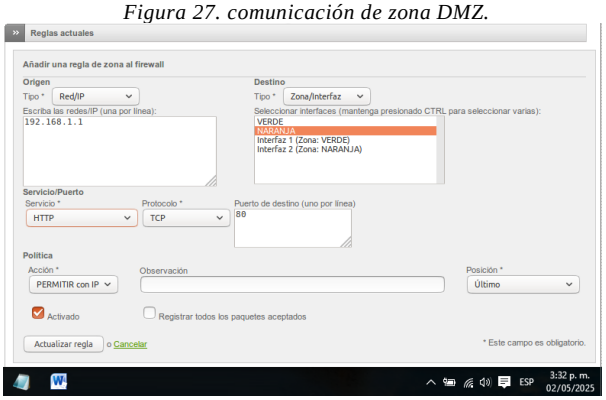
REGLAS ENTRE ZONAS: A continuación, procedemos a incorporar las reglas necesarias para permitir la comunicación entre las distintas zonas de la red.

Figura 26. configuración del firewall.

Fuente: Erly Tatiana Perez Joven

Comunicar la zona Internet con la zona DMZ.

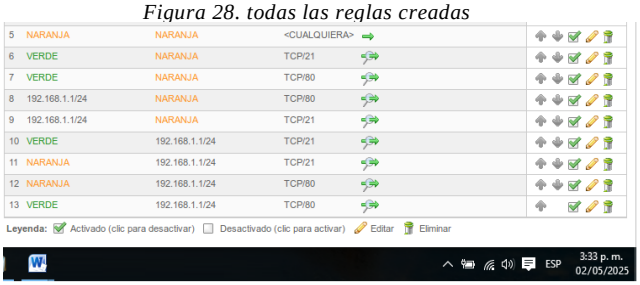
Figura 27. comunicación de zona DMZ.



Fuente: Erly Tatiana Perez Joven

Aquí vemos todas las reglas ya creadas en el tráfico Inter zonas.

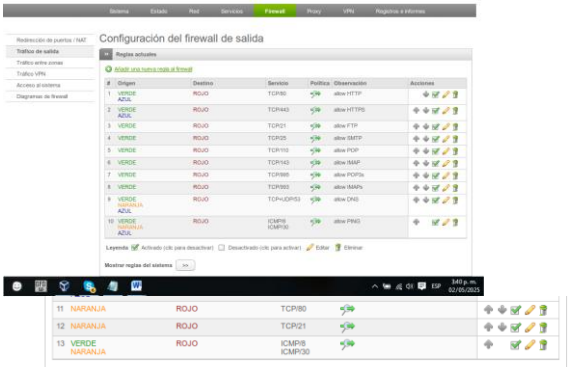
Figura 28. todas las reglas creadas



Fuente: Erly Tatiana Perez Joven

En el tráfico de salida se crearon tres reglas.

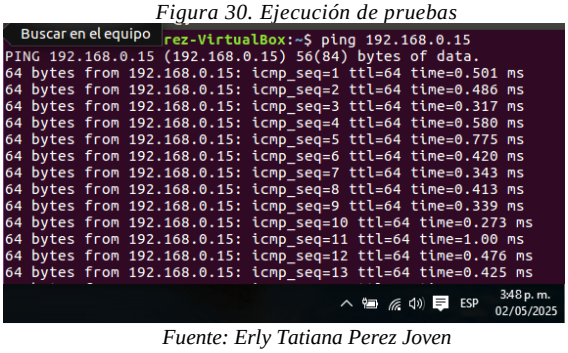
Figura 29. gráfico de reglas de salidas.



Fuente: Erly Tatiana Perez Joven

Procedemos a hacer pruebas.

Figura 30. Ejecución de pruebas



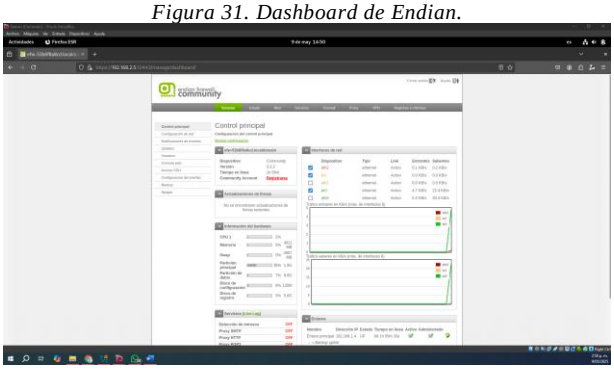
Fuente: Erly Tatiana Perez Joven

TEMÁTICA 5: IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE)

Para cumplir con los objetivos de esta temática, se realizó la implementación de un servidor Endian Firewall Community configurado como un proxy HTTP no transparente, con el propósito de controlar el acceso a la navegación mediante políticas de autenticación y listas de restricción.

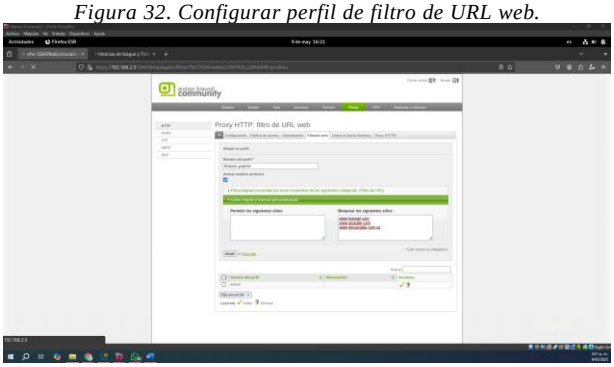
Inicialmente, se accedió al panel de administración del Endian a través de su interfaz web (192.168.2.5:10443), donde se procedió a crear un nuevo perfil de filtro web. En este perfil se definió una lista negra personalizada, en la cual se incluyeron las siguientes URL: www.hotmail.com, www.youtube.com y www.elnuevodia.com.co. Estas páginas fueron bloqueadas como parte del control de contenido de navegación.

Figura 31. Dashboard de Endian.



Fuente: Brillyn Narváez Vargas

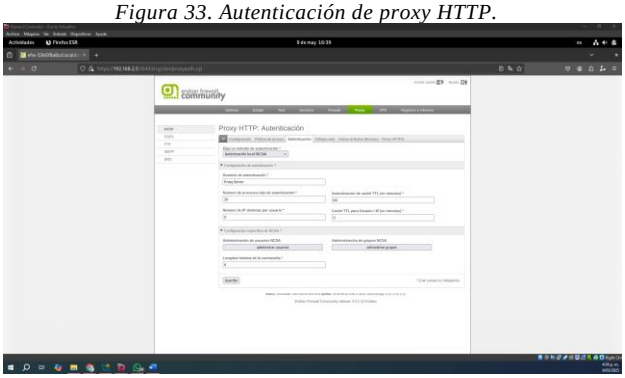
Figura 32. Configurar perfil de filtro de URL web.



Fuente: Brillyn Narváez Vargas

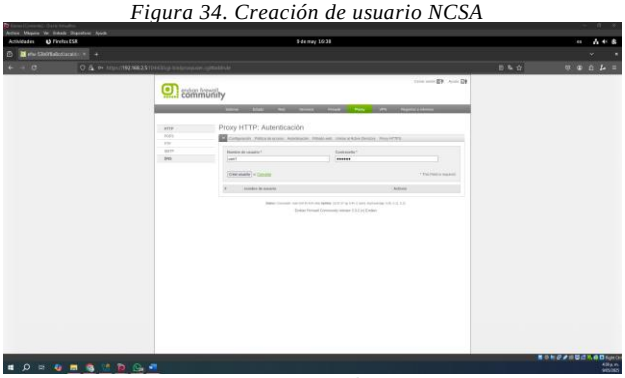
Posteriormente, se configuró la autenticación mediante el módulo NCSA del proxy HTTP. Se creó un usuario con nombre de usuario y contraseña, y se asoció a un nuevo grupo. Esta asociación fue necesaria para definir reglas de acceso basadas en identidad de usuario.

Figura 33. Autenticación de proxy HTTP.



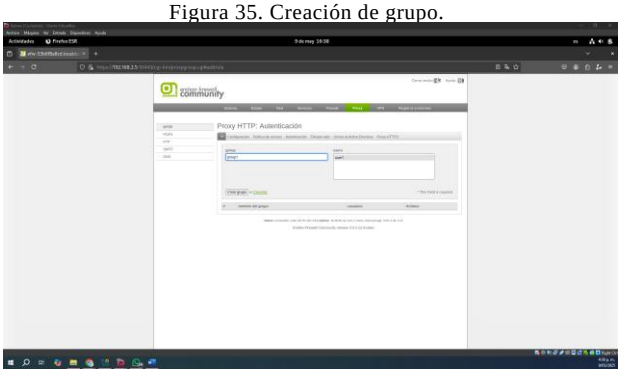
Fuente: Brillyn Narváez Vargas

Figura 34. Creación de usuario NCSA



Fuente: Brillyn Narváez Vargas

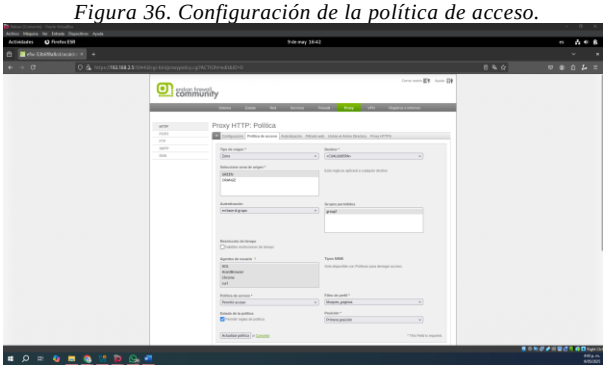
Figura 35. Creación de grupo.



Fuente: Brillyn Narváez Vargas

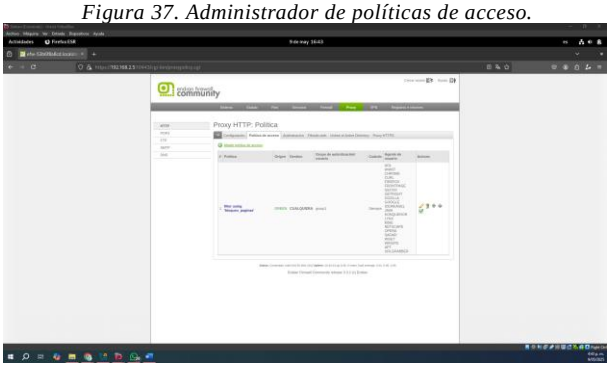
Una vez definidos el perfil de filtrado y los parámetros de autenticación, se procedió a establecer una política de acceso. Esta política vinculó el perfil de filtrado anteriormente creado, especificando como origen la red interna (zona verde) y habilitando la autenticación por usuario. Con esto, se logró un control detallado sobre el tráfico HTTP saliente.

Figura 36. Configuración de la política de acceso.



Fuente: Brillyn Narváez Vargas

Figura 37. Administrador de políticas de acceso.



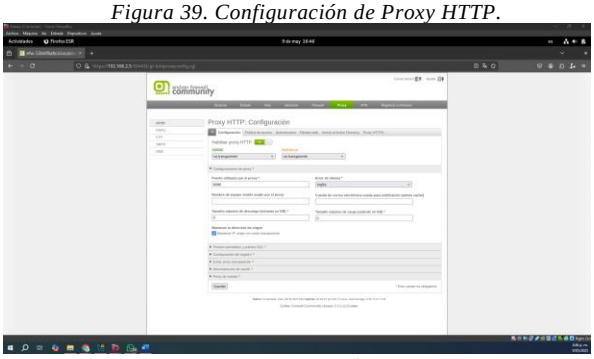
Fuente: Brillyn Narváez Vargas

Finalmente, se habilitó el proxy en modo no transparente, y se configuró manualmente el navegador cliente para utilizar la IP del Endian (192.168.2.5) y el puerto 8080. Al acceder a Internet, el navegador solicitó las credenciales del usuario previamente creado, demostrando que la autenticación estaba activa. Al intentar acceder a cualquiera de los sitios incluidos en la lista negra, el proxy respondió con un mensaje de "acceso denegado", confirmando la efectividad de la configuración.

Figura 38. Imagen de unos de los sitios boleados antes de activar el proxy.

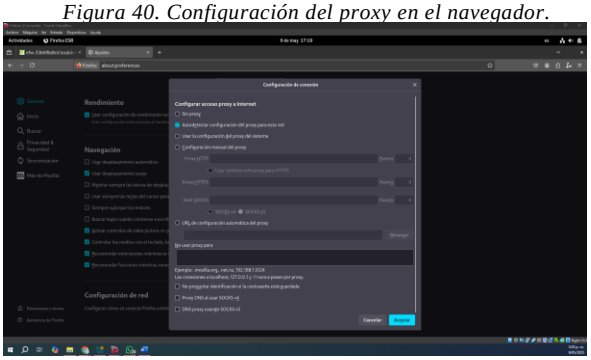
Fuente: Brillyn Narváez Vargas

Figura 39. Configuración de Proxy HTTP.



Fuente: Brillyn Narváez Vargas

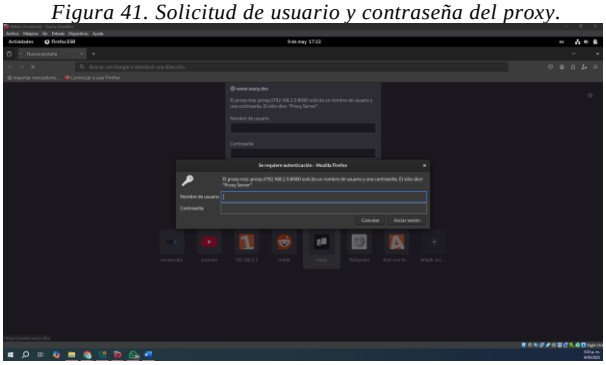
Figura 40. Configuración del proxy en el navegador.



Fuente: Brillyn Narváez Vargas

Estos resultados validan la correcta implementación del proxy HTTP no transparente con autenticación y filtrado de contenido, cumpliendo satisfactoriamente con los requerimientos establecidos en la temática.

Figura 41. Solicitud de usuario y contraseña del proxy.



Fuente: Brillyn Narváez Vargas

Figura 42. Pagina bloqueada por el proxy.

Fuente: Brillyn Narváez Vargas

CONCLUSIONES.

La implementación de GNU/Linux Endian como cortafuegos y servidor de seguridad en un entorno virtualizado con VirtualBox permitió comprender de manera práctica la segmentación de redes en zonas diferenciadas (Verde, Roja y Naranja), facilitando la administración y control del tráfico de red. La configuración adecuada de las interfaces de red fue fundamental para asegurar el aislamiento y la comunicación específica entre las zonas LAN, WAN y DMZ, garantizando así una arquitectura segura y funcional.

La configuración de reglas de NAT (Network Address Translation) resultó esencial para permitir la comunicación desde redes internas hacia la red externa simulada. Se evidenció la importancia de una correcta definición de origen, destino y protocolos involucrados para establecer conexiones seguras y eficientes, tanto desde la zona LAN como desde la DMZ hacia Internet.

En cuanto al manejo de servicios en la DMZ, se logró habilitar exitosamente los protocolos HTTP y FTP, asegurando la disponibilidad controlada de estos servicios desde distintas zonas, mientras que la restricción del protocolo ICMP demostró una capa adicional de seguridad, al evitar respuestas a peticiones de ping no deseadas. Las reglas de tráfico entre zonas permitieron validar el control granular del acceso entre segmentos de red, probando el acceso tanto desde navegadores como mediante herramientas de análisis.

Por último, la implementación de un servidor proxy HTTP no transparente con autenticación por usuario permitió establecer políticas de navegación seguras, restringiendo el acceso a sitios específicos mediante listas negras. Esta funcionalidad resalta el valor del control de contenido en redes corporativas, donde la seguridad y el cumplimiento de políticas de acceso a Internet son críticos.

El ejercicio práctico fortaleció los conocimientos sobre administración de redes, configuración de seguridad perimetral y gestión de servicios mediante herramientas Open Source, aportando habilidades fundamentales para entornos reales de TI con alta demanda de protección de datos y comunicaciones seguras.

REFERENCIAS

[1] "Oracle VirtualBox", *Virtualbox.org*. [En línea]. Disponible en: https://www.virtualbox.org/. [Consultado: 21-may-2025].

[2] "Endian Firewall Community – free open source security for home users", *Endian.com*. [En línea]. Disponible en: https://www.endian.com/en/community/. [Consultado: 21-may-2025].

[3] "Ubuntu Server documentation", *Ubuntu Server*. [En línea]. Disponible en: https://documentation.ubuntu.com/server/. [Consultado: 21-may-2025].

[4] *Redeszone.net*. [En línea]. Disponible en: https://www.redeszone.net/. [Consultado: 21-may-2025].

[5] *Techtarget.com*. [En línea]. Disponible en: https://www.techtarget.com/searchnetworking/definition/NAT. [Consultado: 21-may-2025].

[6] *Edu.co*. [En línea]. Disponible en:

https://repository.ucc.edu.co/entities/publication/3363776b-580b-4307-a644-bdb1b73d0654. [Consultado: 21-may-2025].

[7] "Endian UTM 3.2 Reference Manual — Endian UTM 3.2 Reference Manual", *Endian.com*. [En línea]. Disponible en: https://docs.endian.com/3.2/utm/index.html. [Consultado: 21-may-2025].

[8] Wikipedia contributors, "Endian Firewall", *Wikipedia, The Free Encyclopedia*. [En línea]. Disponible en: https://en.m.wikipedia.org/wiki/Endian_Firewall.

[9] J. S. Giraldo, "VirtualBox con Endian 3.3.2, 3 Zonas: Verde, Naranjada y Roja". [En línea]. Disponible en: https://www.youtube.com/watch?v=Dvht5wCPIrI. [Consultado: 21-may-2025].

[10] InfoRed, "Cómo configurar endian firewall Paso a Paso Parte 1". [En línea]. Disponible en: https://www.youtube.com/watch?v=zOa1q1n7kU0. [Consultado: 21-may-2025].