CONSTRUCCIÓN DE INFRAESTRUCTURAS DE REDES SEGURAS MEDIANTE ENDIAN FIREWALL

MIGUEL ÁNGEL SANTA POLANCO
masantap@unadvirtual.edu.co
ARTHUR CHAVARRO COLLAZOS
achavarroC@unadvirtual.edu.co
JUAN CAMILO LÓPEZ PASTRANA
jclopezpa@unadvirtual.edu.co

RESUMEN: *En el presente artículo se documentarán diferentes procedimientos orientados a la configuración de servicios de red y seguridad utilizando el sistema GNU/Linux Endian Firewall, dentro de un entorno virtualizado en VirtualBox. Para ello, se iniciará con la configuración de la instancia en VirtualBox, incluyendo la asignación adecuada de tarjetas de red y la instalación efectiva de Endian Firewall como base para la implementación posterior de servicios. A continuación, se abordará la configuración de una Zona Desmilitarizada (DMZ), permitiendo servicios como HTTP y FTP desde el servidor ubicado en dicha zona hacia la red interna, al tiempo que se aplicarán restricciones como el bloqueo del protocolo ICMP, con el objetivo de proteger los recursos internos de accesos no autorizados. Finalmente, se procederá a la implementación de un proxy HTTP no transparente, incorporando políticas de autenticación de usuarios y el uso de listas negras, con el propósito de regular y controlar la navegación en Internet desde la red local.*

PALABRAS CLAVE: Endian, Firewall, Proxy, DMZ, Seguridad.

INTRODUCCIÓN

En un entorno digital cada vez más expuesto a amenazas cibernéticas y dependiente de infraestructuras de red robustas, la implementación de medidas de seguridad y segmentación eficiente se ha convertido en una necesidad crítica para organizaciones de todos los tamaños. La adecuada configuración de servicios de red no solo permite garantizar la continuidad operativa, sino también proteger los activos digitales frente a accesos no autorizados, vulnerabilidades o fugas de información.

En este contexto, el presente artículo explora el uso del sistema GNU/Linux Endian Firewall como herramienta para fortalecer la gestión de redes seguras dentro de entornos virtualizados. Se analizan aspectos clave como la segmentación mediante zonas de seguridad incluida la creación de una Zona Desmilitarizada (DMZ), la aplicación de reglas de firewall y proxy para denegar o permitir el acceso a puertos, servicios o sitios web. Estas configuraciones permiten establecer un entorno controlado, en el que es posible supervisar y limitar el acceso a los recursos según políticas definidas.

La experiencia presentada aquí busca no solo demostrar la viabilidad técnica del uso de Endian Firewall en entornos simulados, sino también evidenciar cómo estas prácticas pueden ser aplicadas en escenarios reales, donde la seguridad de la información y la correcta administración de servicios de red son pilares fundamentales para el funcionamiento confiable de cualquier organización.

1. CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX (TARJETAS DE RED) E INSTALACIÓN EFECTIVA DEL MISMO

Para la instalación se asignan los recursos de hardware para la máquina virtual de Endian, como se aprecia en la Figura 1.

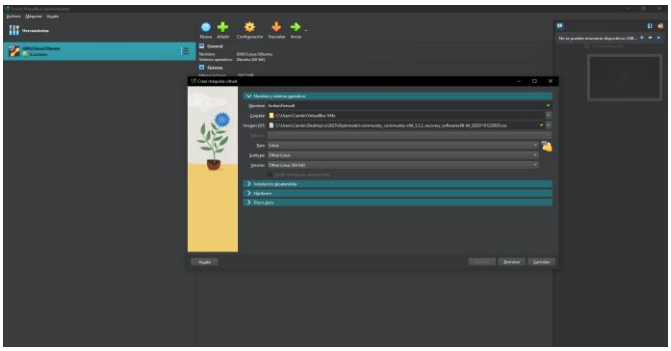

Figura 1. Creación de la máquina virtual de Endian.
Fuente: Elaboración propia. Juan Camilo López Pastrana (2025).

Una vez creada la máquina virtual se la inicia y se hace las configuraciones que van apareciendo en la instalación, (Figura 2).

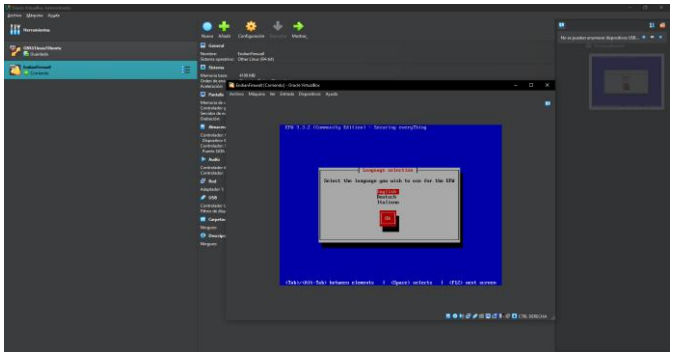

Figura 2. Configuraciones iniciales de la instalación, Fuente: Elaboración propia. Juan Camilo López Pastrana (2025).

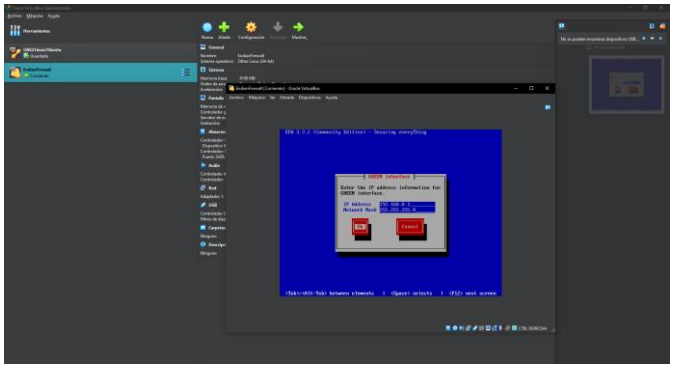

Figura 3. Configuración de la IP para la zona verde. Fuente: Elaboración propia. Juan Camilo López Pastrana (2025).

Al realizar todas las configuraciones se muestra el entorno inicial de Endian, donde se muestra la IP asignada y el puerto por el cual se puede acceder desde un navegador a Endian en la web (Figura 4).

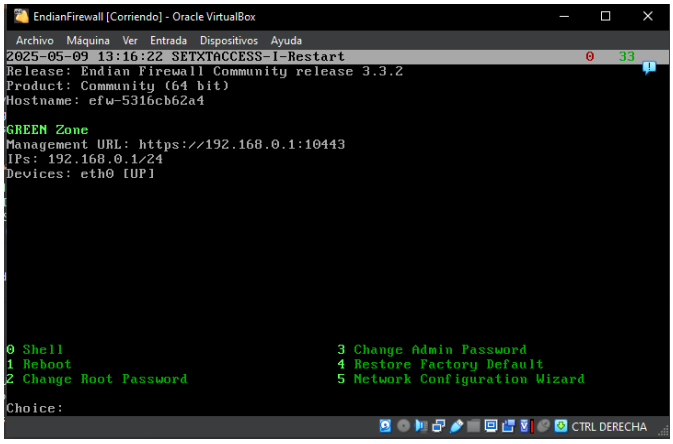

Figura 4. Entorno inicial de Endian., Fuente: Elaboración propia. Juan Camilo López Pastrana (2025).

Se configura el adpatador de red para la máquina de escritorio la cual estará en la zona verde, (Figura 5).

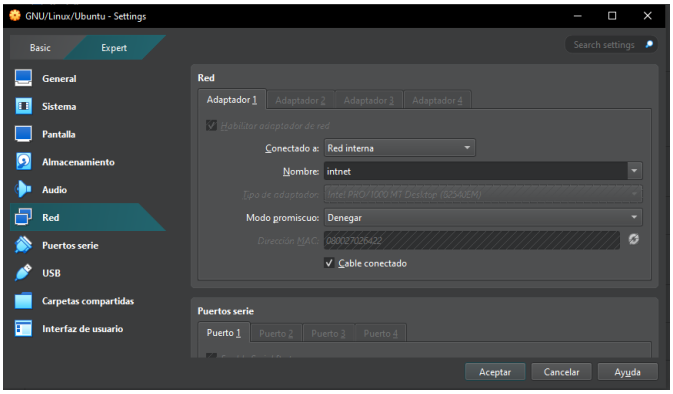

Figura 5. Configuración adpatador de red para máquina de escritorio. Fuente: Elaboración propia. Juan Camilo López Pastrana (2025).

Se configura la dirección IP para la máquina virtual de escritorio.

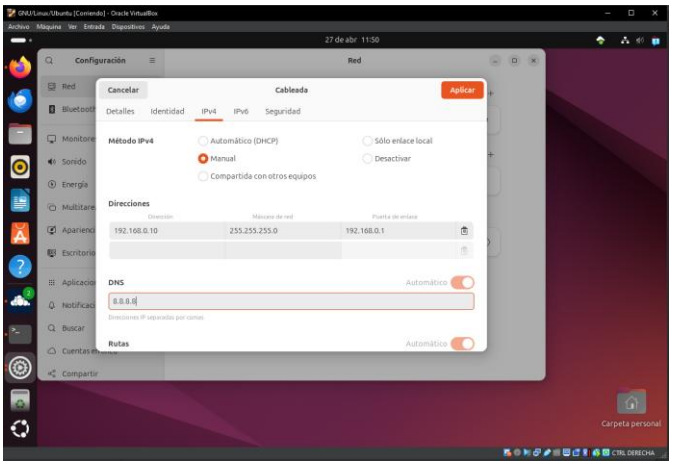

Figura 6. Dirección IPv4 de la máquina de escritorio. Fuente: Elaboración propia. Juan Camilo López Pastrana (2025).

En el navegador web se ingresa a Endian y se realiza las configuraciones iniciales necesarias.

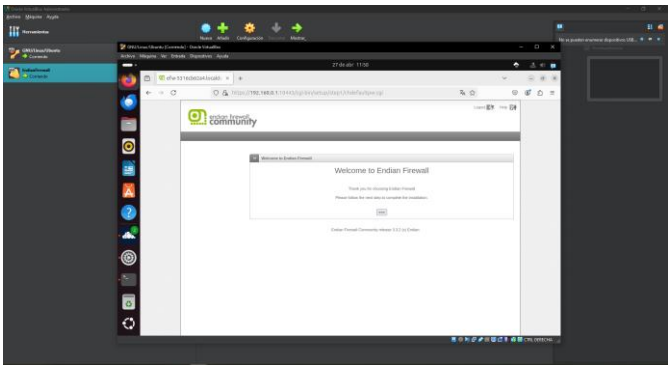

Figura 7. Entorno web inicial de Endian. Fuente: Elaboración propia. Juan Camilo López Pastrana (2025).

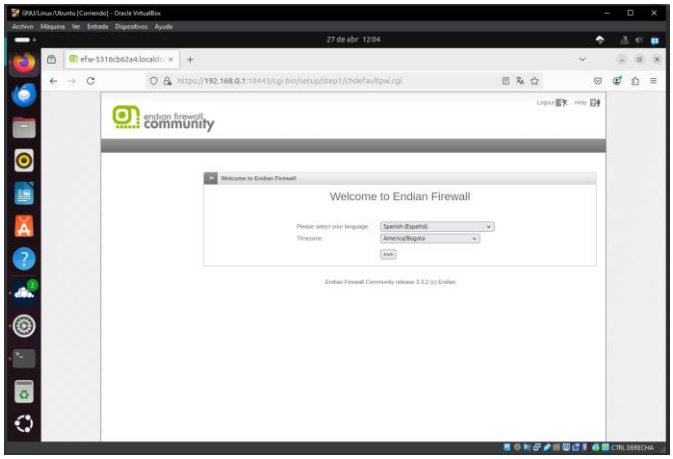

Figura 8. Configuración del idioma. Fuente: Elaboración propia. Juan Camilo López Pastrana (2025).

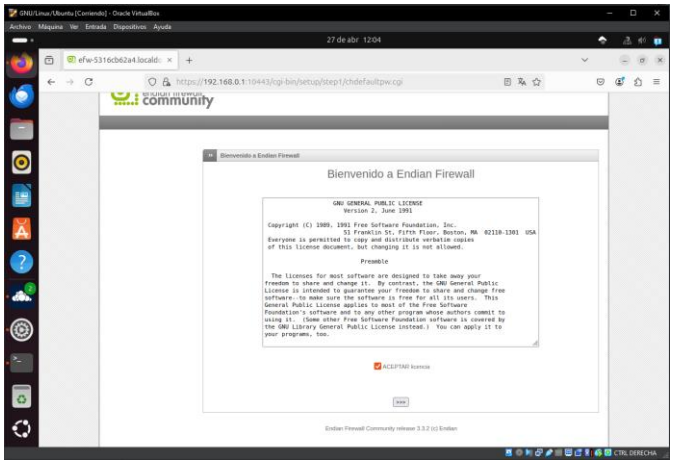

Figura 9. Aceptación de licencia. Fuente: Elaboración propia. Juan Camilo López Pastrana (2025).

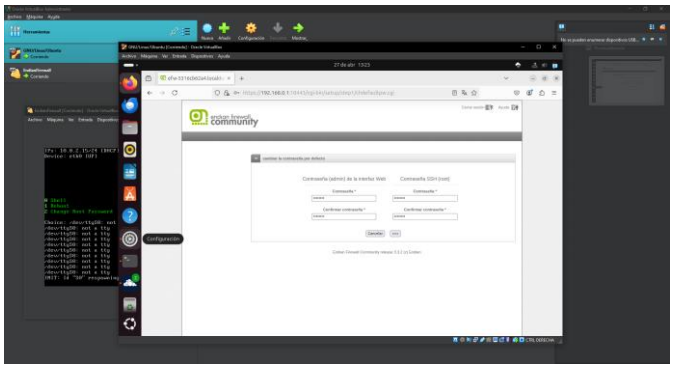

Figura 10. Asignación de contraseñas para el usuario admin y root. Fuente: Elaboración propia. Juan Camilo López Pastrana (2025).

Dentro de las configuraciones iniciales se configuras las tres zonas, la roja, la verde y la naranja.

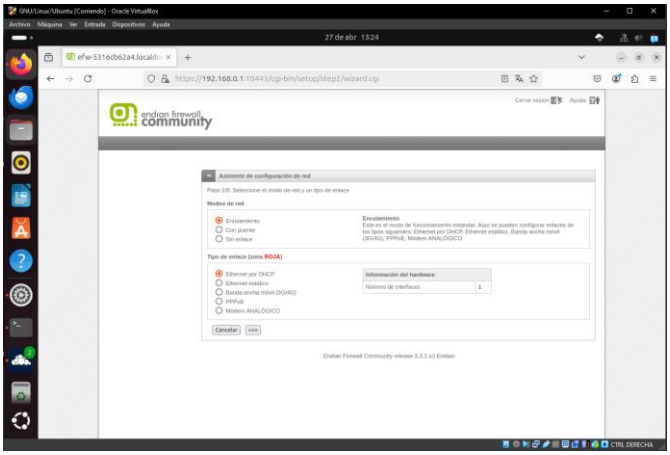

Figura 11. Configuración de la zona roja (Red WAN). Fuente: Elaboración propia. Juan Camilo López Pastrana (2025).

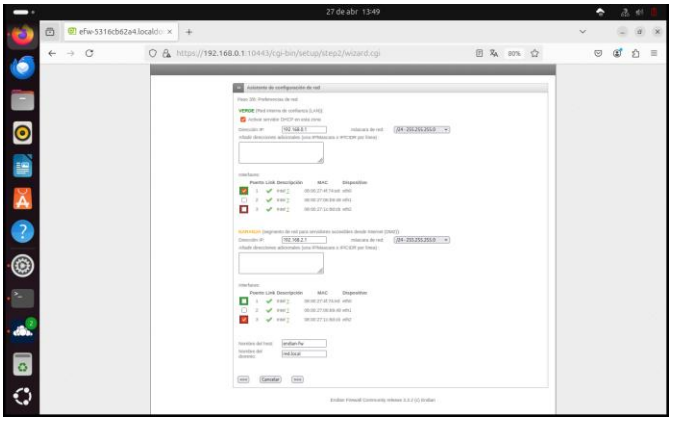

Figura 12. Configuración de la zona Verde y Naranja (DMZ). Fuente: Elaboración propia. Juan Camilo López Pastrana (2025).

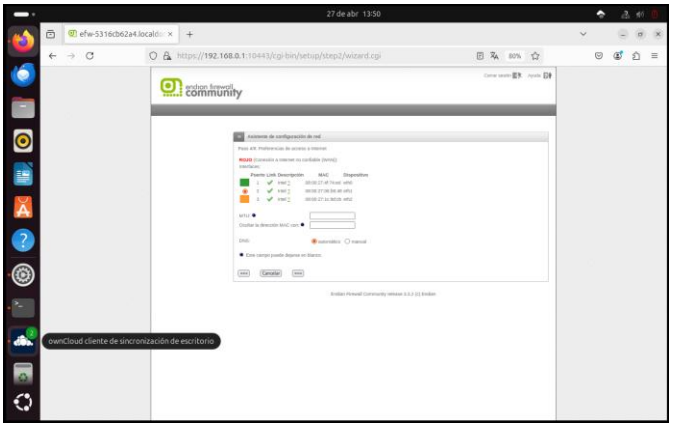

Figura 13. Selección de la zona roja para conectarse a internet. Fuente: Elaboración propia. Juan Camilo López Pastrana (2025).

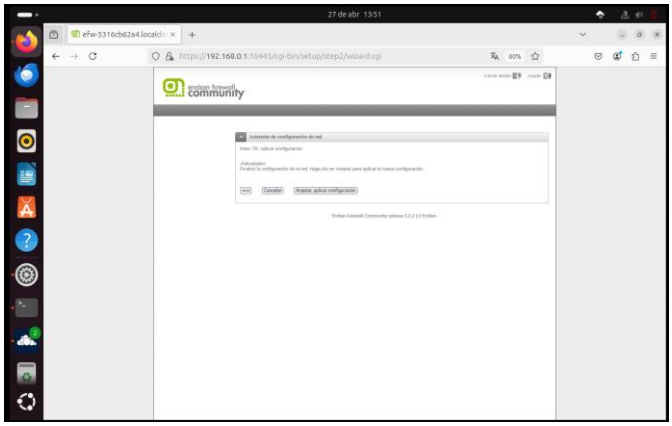

Figura 14. Se guardan las configuraciones. Fuente: Elaboración propia. Juan Camilo López Pastrana (2025).

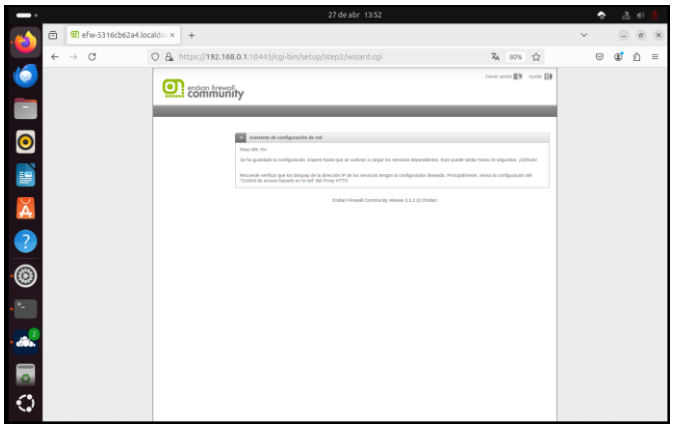

Figura 15. Se cargan las configuraciones realizadas. Fuente: Elaboración propia. Juan Camilo López Pastrana (2025).

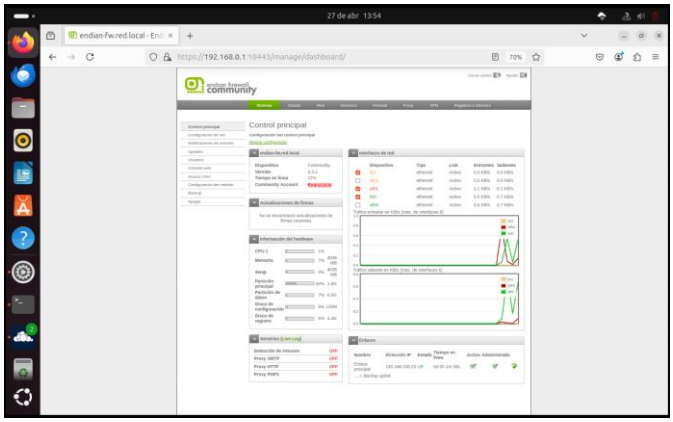

Figura 16. Resumen del sistema de las configuraciones de las diferentes zonas. Fuente: Elaboración propia. Juan Camilo López Pastrana (2025).

Realizadas las configuraciones se verifica la conectividad desde la zona verde mediante ping.

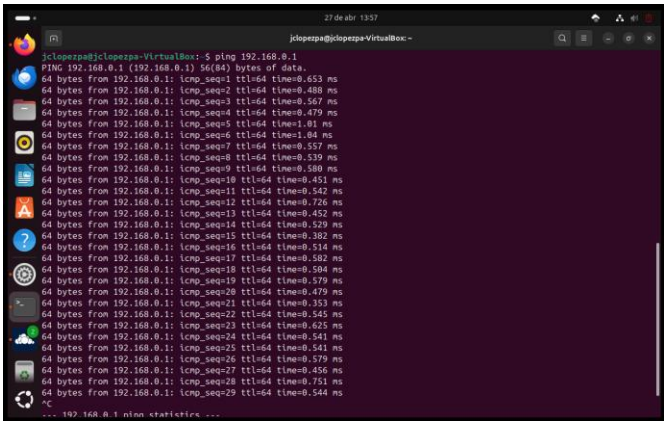

Figura 17. Ping desde la máquina de escritorio a la IP 192.168.0.1 Fuente: Elaboración propia. Juan Camilo López Pastrana (2025).

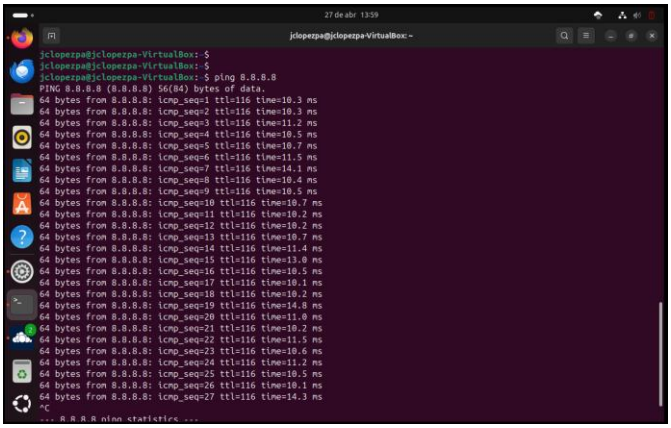

Figura 18. Ping al DNS de google para verificar la conectividad a internet. Fuente: Elaboración propia. Juan Camilo López Pastrana (2025).

Se documenta la configuraciones de los adpatadores para las diferentes zonas.

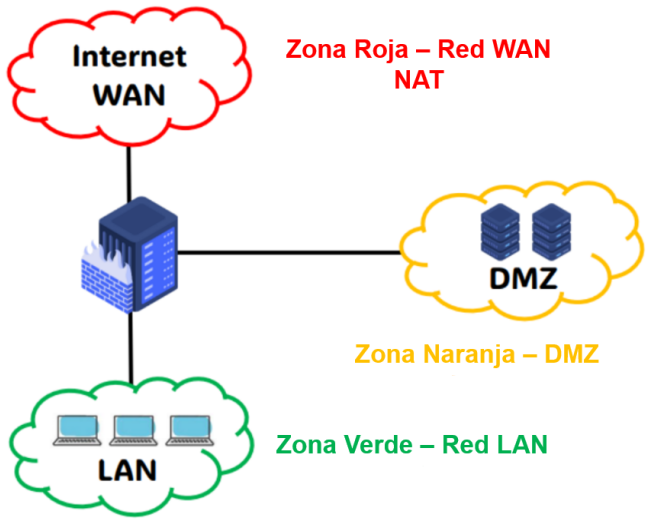

Figura 19. Representación gráfica de las 3 zonas. Fuente: Elaboración propia. Juan Camilo López Pastrana (2025).

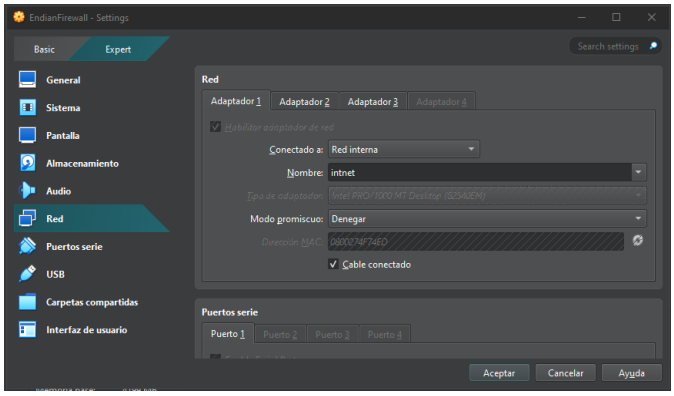

Figura 20. Configiración del adpatador 1. Fuente: Elaboración propia. Juan Camilo López Pastrana (2025).

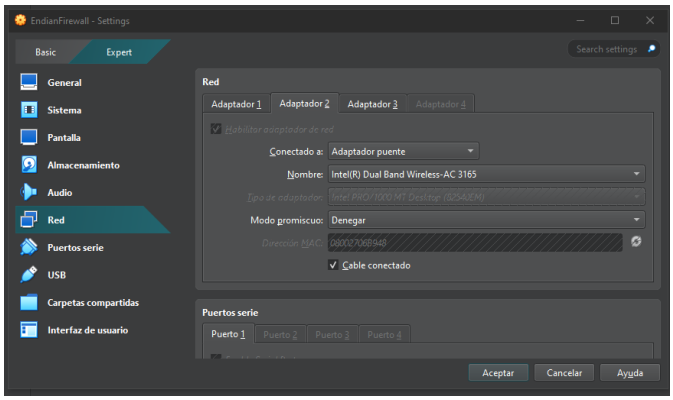

Figura 21. Configuración del adaptador 2. Fuente: Elaboración propia. Juan Camilo López Pastrana (2025).

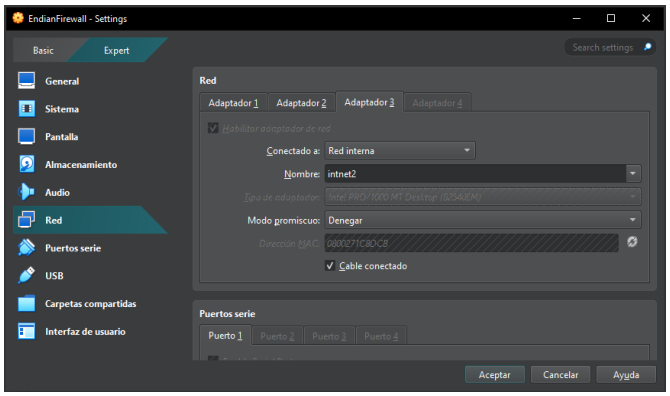

Figura 22. Configuración del adaptador 3. Fuente: Elaboración propia. Juan Camilo López Pastrana (2025).

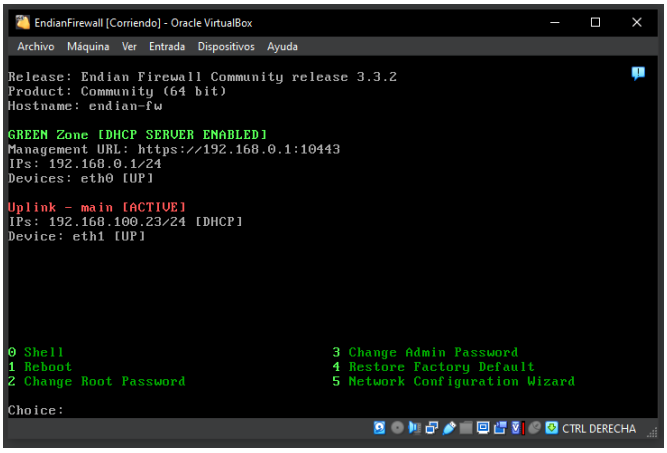

Figura 23. Zonas activadas. Fuente: Elaboración propia. Juan Camilo López Pastrana (2025).

2. CONFIGURACIÓN NAT

Se configura NAT en Endian Firewall, para ello se accede a la sección de FireWall y luego en Source NAT se agrega una nueva Regla Especificando la dirección IP de origen.

Figura 24. Opción para crear una regla NAT. Fuente: Elaboración propia. Miguel Ángel Santa (2025).

Se deja por defecto y se asigna la IP de la LAN **192.168.0.15.**

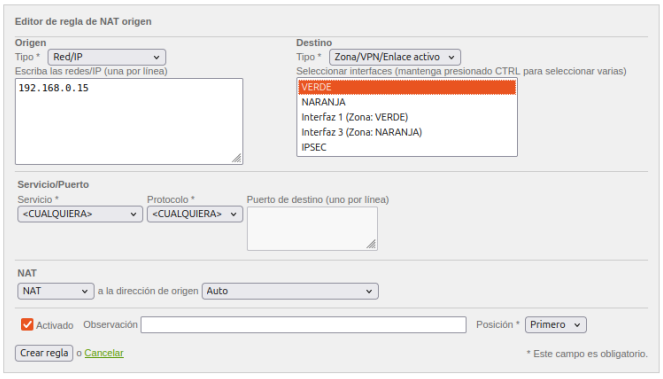

Figura 25. Regla NAT para la zona verde. Fuente: Elaboración propia. Miguel Ángel Santa (2025).

Ahora ajustamos la Zona Naranja para tener acesso con DMZ recordemos que la Ip es 192.168.40.15

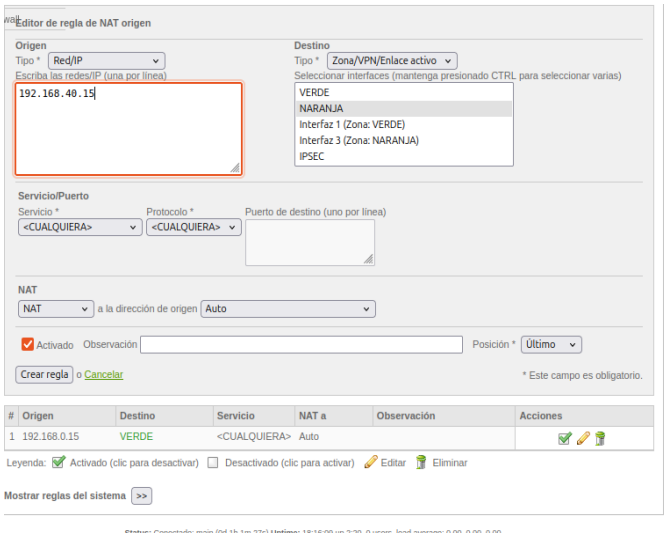

Figura 26. Regla NAT para la zona DMZ. Fuente: Elaboración propia. Miguel Ángel Santa (2025).

Se revisa que ambas reglas se hayan creado adecuadamente.

Figura 27. Visualización de las 2 reglas creadas. Fuente: Elaboración propia. Miguel Ángel Santa (2025).

Se accede desde la máquina configurada al ping de la Zona Naranja (DMZ) y al internet (WAN) para comprobar que da respuesta en la red.

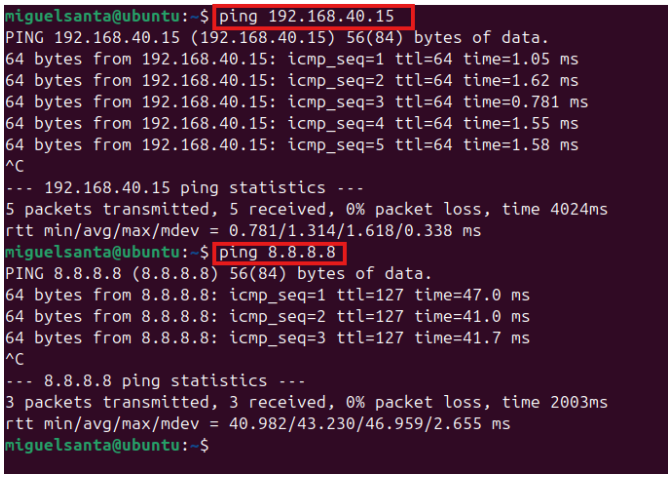

Figura 28. Ping desde la zona verde a la zona naranja y roja. Fuente: Elaboración propia. Miguel Ángel Santa (2025).

De igual forma usamos el navegador y accedemos a twitter
Y así comprobar el acceso al navegador.

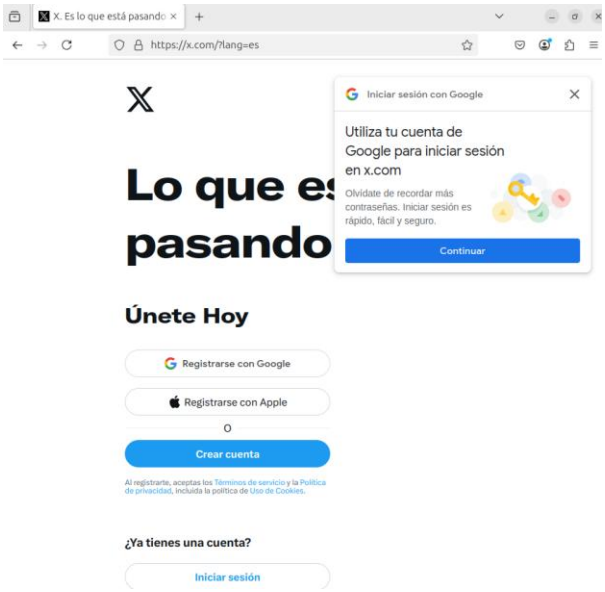

Figura 29. Verificación de la conectividad a internet. Fuente: Elaboración propia. Miguel Ángel Santa (2025).

3. PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

Estando en la interfaz web de Endian se crea una nueva regla de firewall en este caso para HTTP.

En la sección de firewall nueva regla se busca y se selecciona el servicio "HTTP (TCP/80)" y se le da añadir para incluirlo en la regla.

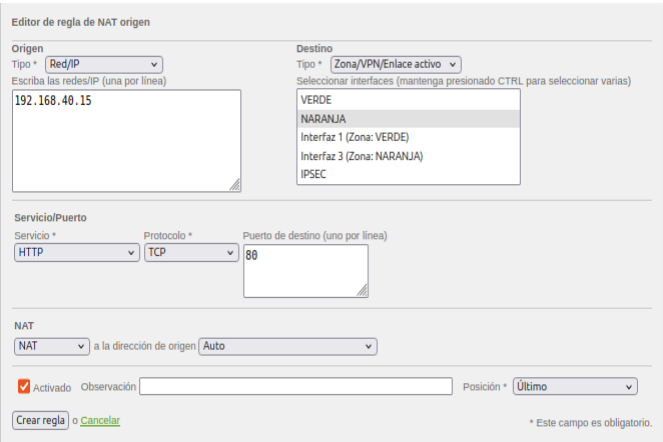

Figura 30. Regla para el servicio HTTP. Fuente: Elaboración propia. Miguel Ángel Santa (2025).

Para permitir tráfico FTP (Puerto 21) desde la DMZ hacia la Red se sigue los mismos pasos que para HTTP, pero en la configuración de la regla, se realiza los cambios en el servicio "FTP (TCP/21)".

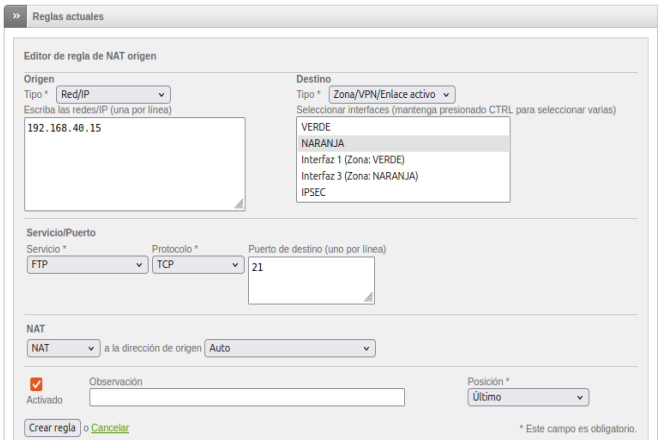

Figura 31. Regla para el servicio FTP. Fuente: Elaboración propia. Miguel Ángel Santa (2025).

Se deniega el protocolo ICMP (Ping) en la Red, para ello se crea una regla en el área de Tráfico en rutado de entrada que bloquee el tráfico ICMP entrante y saliente en las interfaces relevantes.

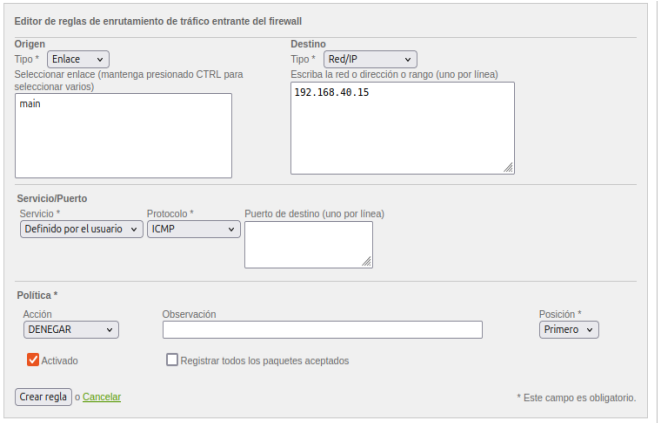

Figura 32. Denegar el protocolo ICMP. Fuente: Elaboración propia. Miguel Ángel Santa (2025).

Se verifica la no respuesta al comando ping, para ello se abre Ubuntu Server, y se hace ping a la máquina que se encuentra dentro de la red local (que no sea el servidor web en la DMZ).

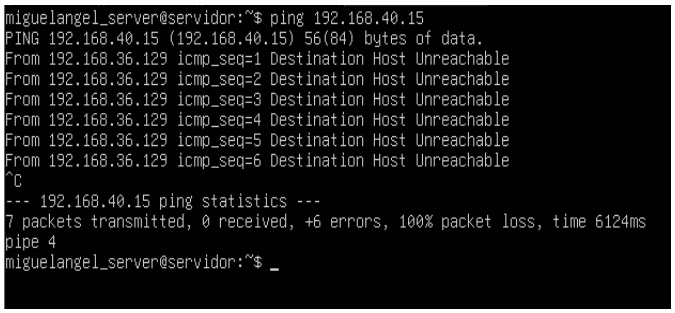

Figura 33. Ping desde el servidor a la máquina de escritorio. Fuente: Elaboración propia. Miguel Ángel Santa (2025).

Como no se pudo conectar indica que el protocolo ICMP está siendo bloqueade do.

Se verifica la creación de las reglas en el tráfico de salida.

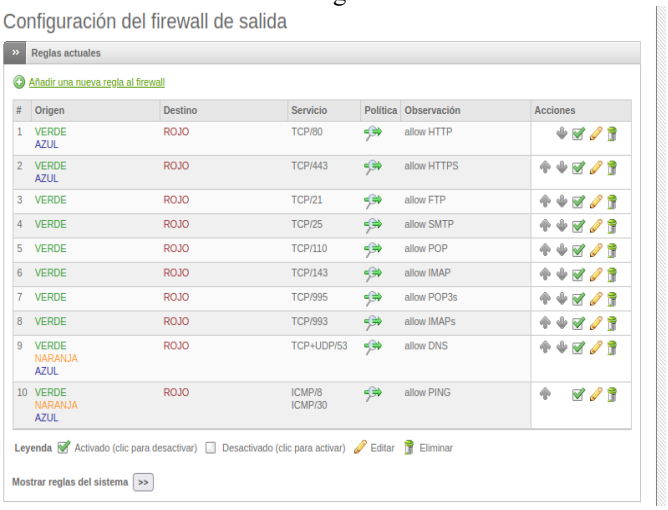

Figura 34. Visualización de las reglas creadas en el firewall. Fuente: Elaboración propia. Miguel Ángel Santa (2025).

Se debería observar entradas que indiquen que el tráfico HTTP y FTP desde la dirección IP del servidor web en la DMZ está siendo permitido hacia la red. Por otro lado, no se ve ningún tráfico ICMP exitoso hacia ninguna dirección de la red. Las reglas de denegación de ICMP deberían estar evitando cualquier comunicación de este tipo.

4. REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO

Creamos las reglas que permitan la comunicación entre Los dispositivos de la red local (Zona Verde) y los servidores ubicados en la DMZ (Zona Naranja) utilizando los protocolos HTTP (puerto TCP 80) y FTP (puerto TCP 21).

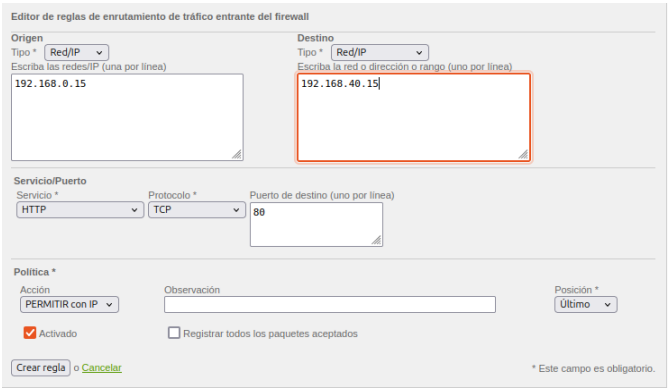

Figura 35. Regla para el servicio HTTP puerto 80. Fuente: Elaboración propia. Miguel Ángel Santa (2025).

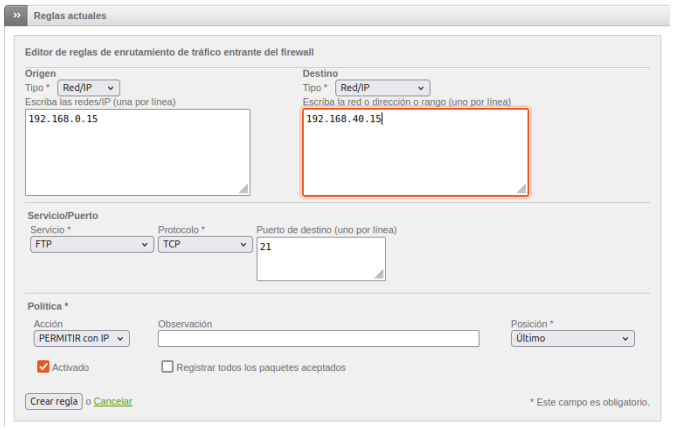

Figura 35. Regla para el servicio FTP puerto 21. Fuente: Elaboración propia. Miguel Ángel Santa (2025).

Se prueba la conexión de los servicios desde una maquina configurada con DMZ.

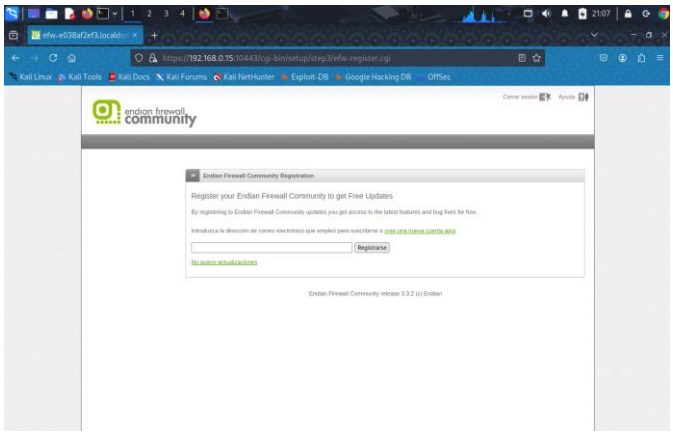

Figura 36. Comunicar la zona internet con la zona DMZ. Fuente: Elaboración propia. Miguel Ángel Santa (2025).

Dentro del área Redirección de puertos / NAT de destino se configura la regla de redirección para HTTP puerto(80) donde se accede a internet, posterior a ello se crea la regla de firewall que permitrá la entrada del trafico a la DMZ.

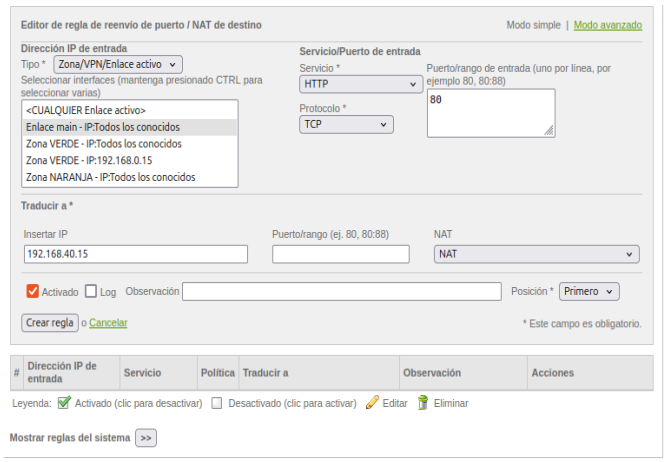

Figura 37. Configuración de regla NAT puerto 80. Fuente: Elaboración propia. Miguel Ángel Santa (2025).

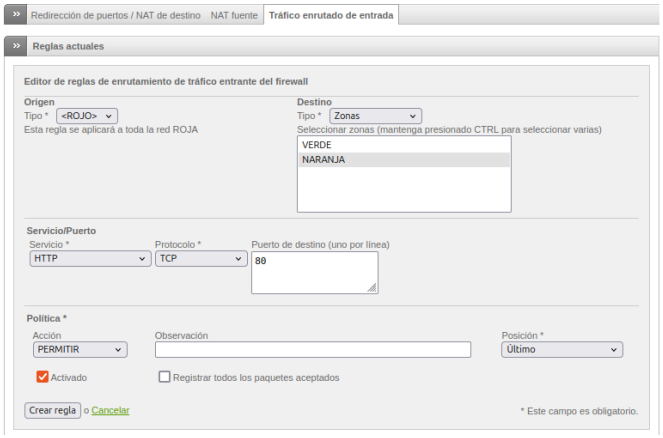

Figura 38. Regla de enrutamiento de firewall puerto 80. Fuente: Elaboración propia. Miguel Ángel Santa (2025).

Ya configurado el puerto 80 se habilita el enrutamiento al puerto 21, es un poco parecido pero con el protocolo TCP es decir un servicio FTP.

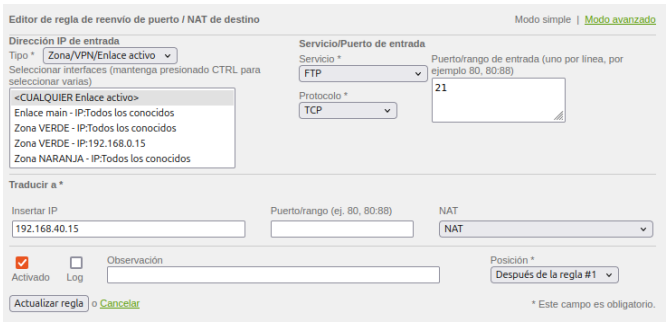

Figura 39. Regla NAT para el puerto 21. Fuente: Elaboración propia. Miguel Ángel Santa (2025).

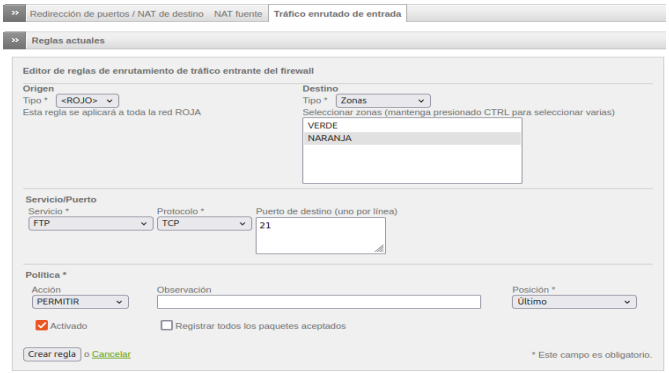

Figura 40. Regla de enrutamiento de firewall puerto 21. Fuente: Elaboración propia. Miguel Ángel Santa (2025).

Se verifica en el tráfico Inter - Zona, la creación de las reglas, para ello se accede a la sección de Registro y informes en la sección del Firewall para verificar el trafico.

Figura 41. Visualización de reglas en el tráfico de enrutado. Fuente: Elaboración propia. Miguel Ángel Santa (2025).

Se prueba desde un navegador Web, las siguientes directivas. El ingreso del servicio HTTP desde la LAN hacia la zona DMZ para ingresar al servidor web de apache2.

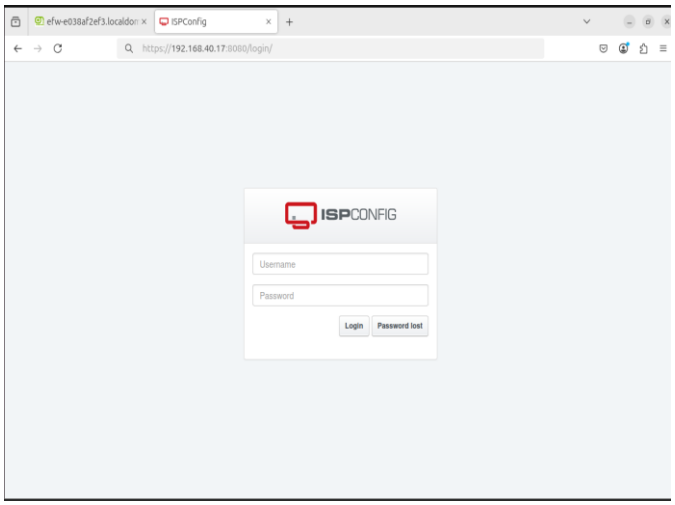

Figura 42. Ingreso a la página ISPConfig. Fuente: Elaboración propia. Miguel Ángel Santa (2025).

Se verifica que los protocolos corren perfectamente.

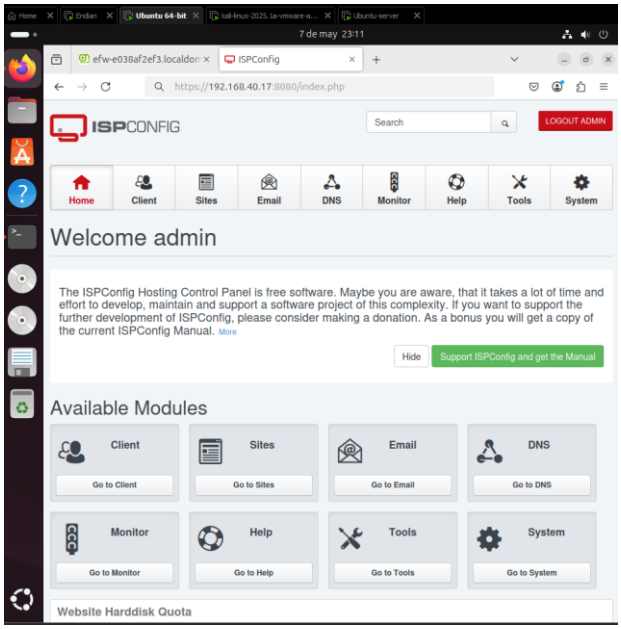

Figura 43. Verificación del acceso de los protocolos. Fuente: Elaboración propia. Miguel Ángel Santa (2025).

Del igual forma hay respuesta de la WAN

Figura 44. Descarga de archivos de Google. Fuente: Elaboración propia. Miguel Ángel Santa (2025).

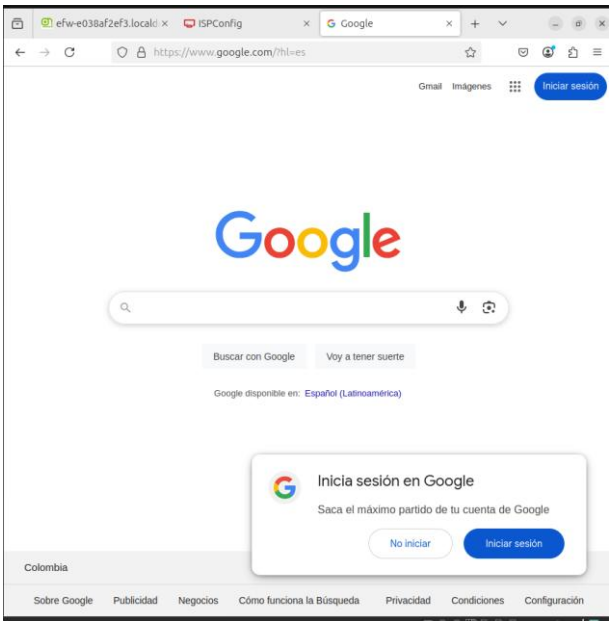

Figura 45. Ingreso a internet (Google). Fuente: Elaboración propia. Miguel Ángel Santa (2025).

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

Teniendo configurado Endian Firewall como se ha visto anteriormente se ingresa a la web se activa el Proxy HTTP para posteriormente crear una lista negra para denegar el permiso a ciertos sitios web.

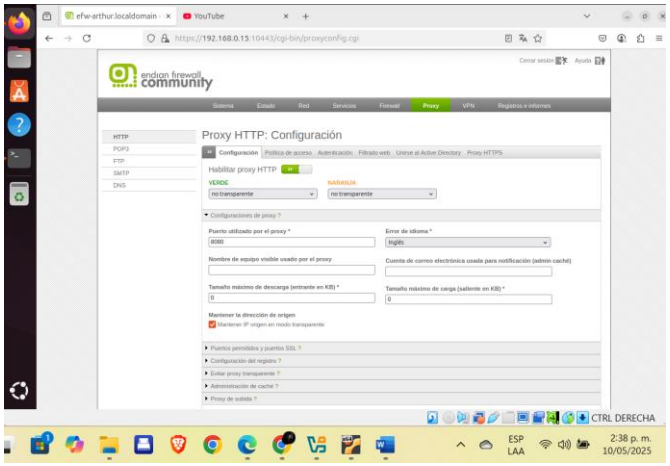

Figura 46. Activación del Proxy. Fuente: Elaboración propia. Arthur Chavarro (2025).

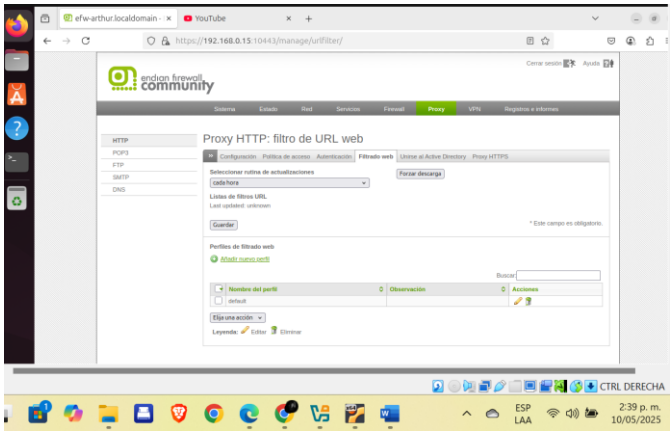

Figura 47. Configuración del periodo de tiempo en que se realiza las actualizaciones. Fuente: Elaboración propia. Arthur Chavarro (2025).

Los sitios web que se encontrarán en la lista negra a donde los usuarios no podrán ingresar a menos que sean autorizados mediante credenciales son: YouTube, Hotmail y El Nuevo Día.

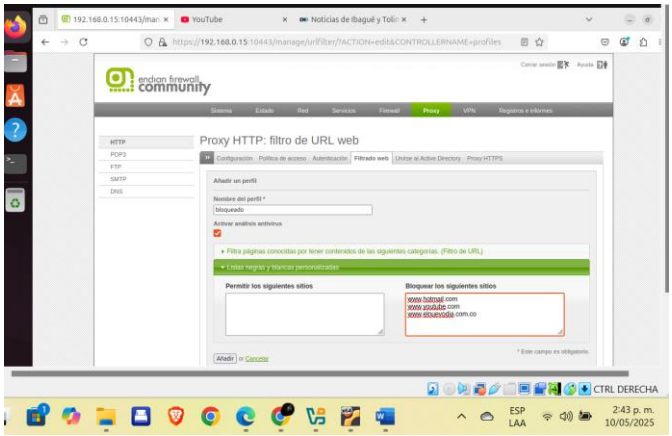

Figura 48. Creación de la lista negra. Fuente: Elaboración propia. Arthur Chavarro (2025).

Se crea el usuario y se lo añade al grupo, con dicho usuario se podrá acceder a los sitios bloqueados por el proxy.

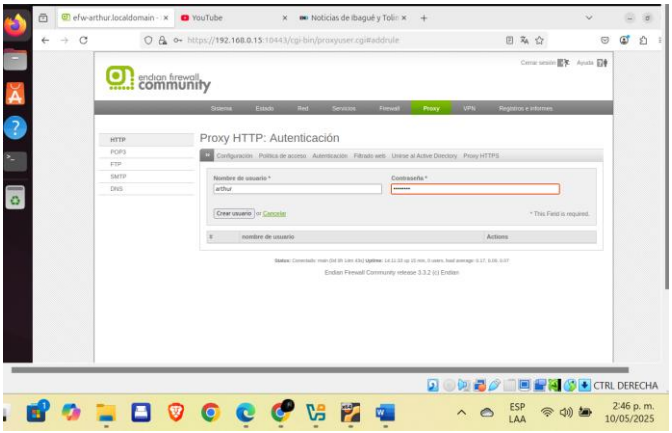

Figura 49. Creación de usuario. Fuente: Elaboración propia. Arthur Chavarro (2025).

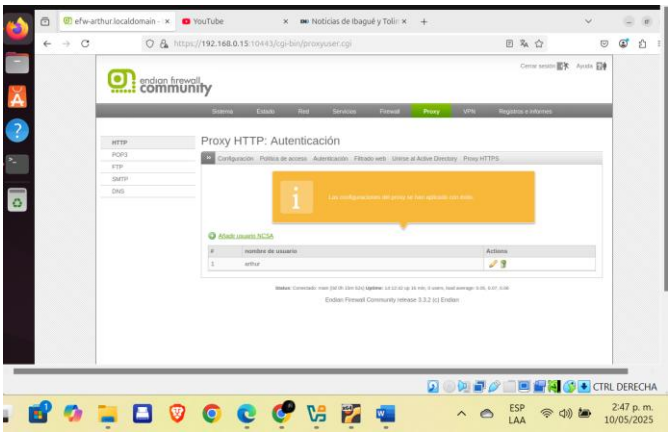

Figura 50. Verificación de la creación del usuario. Fuente: Elaboración propia. Arthur Chavarro (2025).

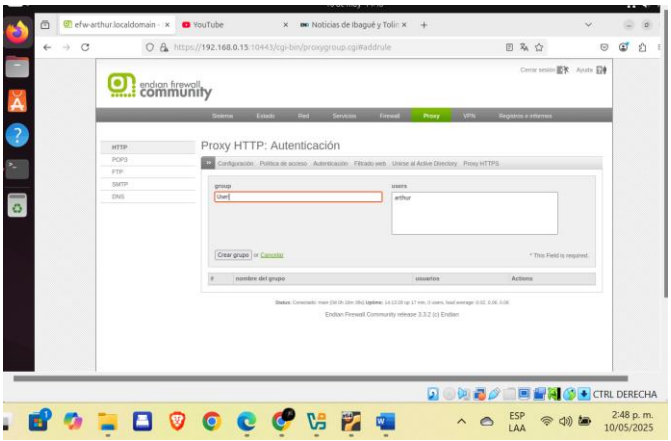

Figura 51. Creación del grupo. Fuente: Elaboración propia. Arthur Chavarro (2025).

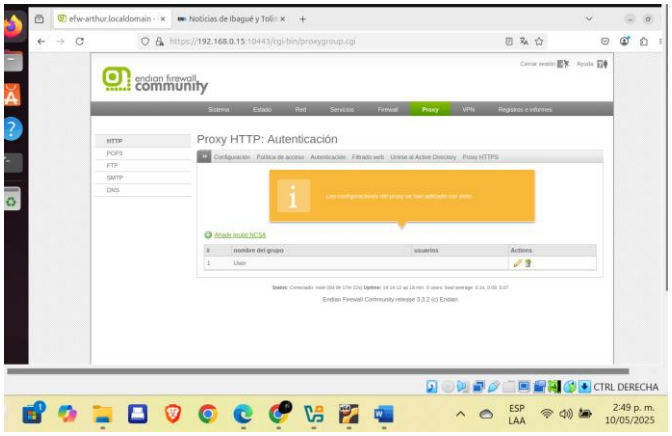

Figura 52. Verificación de la creación del grupo. Fuente: Elaboración propia. Arthur Chavarro (2025).

Se crea una política en el Proxy en base al usuario para que pueda acceder a cualquier sitio web.

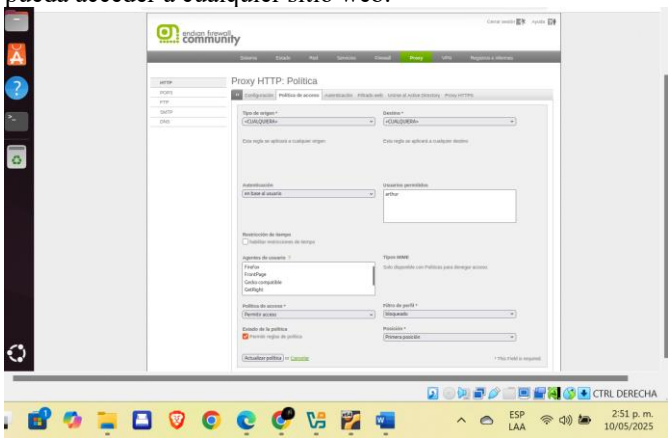

Figura 53. Politica del proxy. Fuente: Elaboración propia. Arthur Chavarro (2025).

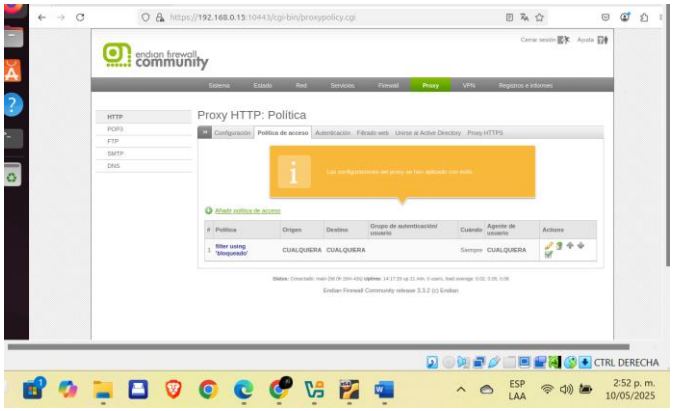

Figura 54. Activación de la regla del proxy. Fuente: Elaboración propia. Arthur Chavarro (2025).

Realizadas las configuraciones se activa el proxy en la máquina de escritorio, despues se ingresa a los sitios ded la lista negra, para acceder se solicitará credenciales.

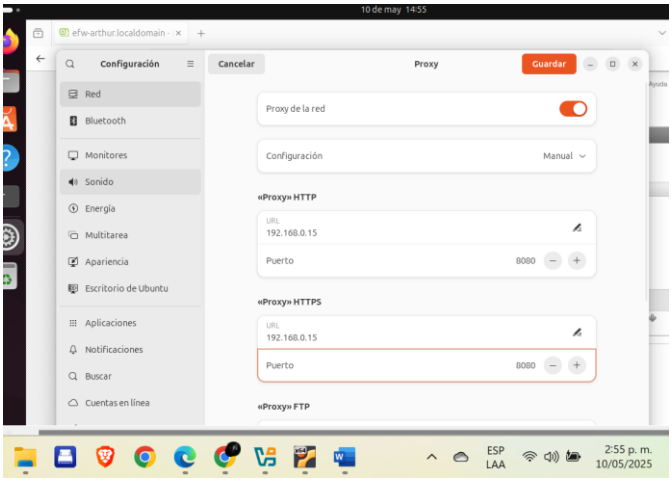

Figura 55. Activación del proxy en la máquina de escritorio. Fuente: Elaboración propia. Arthur Chavarro (2025).

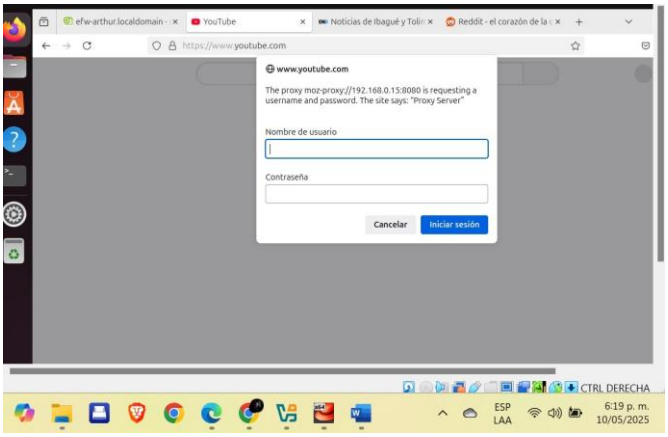

Figura 56. Intento de ingreso a YouTube. Fuente: Elaboración propia. Arthur Chavarro (2025).

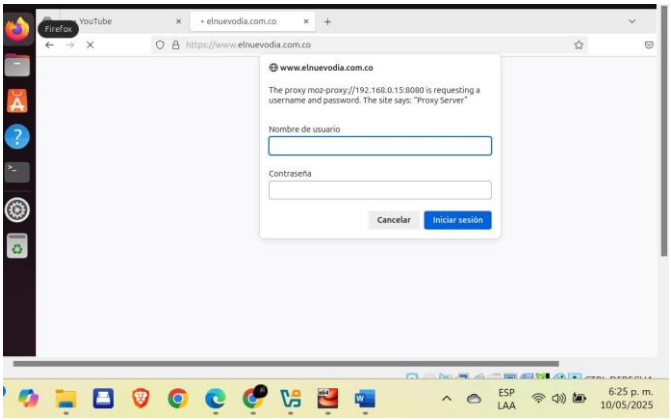

Figura 57. Intento de ingreso a El Nuevo Día. Fuente: Elaboración propia. Arthur Chavarro (2025).

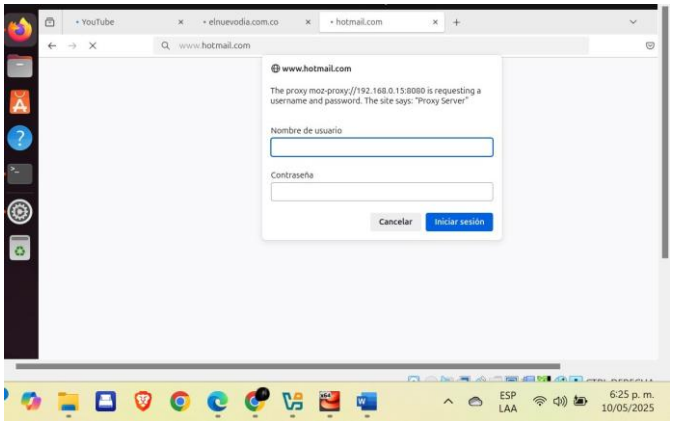

Figura 58. Intento de ingreso a Hotmail. Fuente: Elaboración propia. Arthur Chavarro (2025).

Como se puede observar se requiere ser usuario autenticado para acceder, en este caso se ingresará con el usuario creado y poder acceder al sitio web.

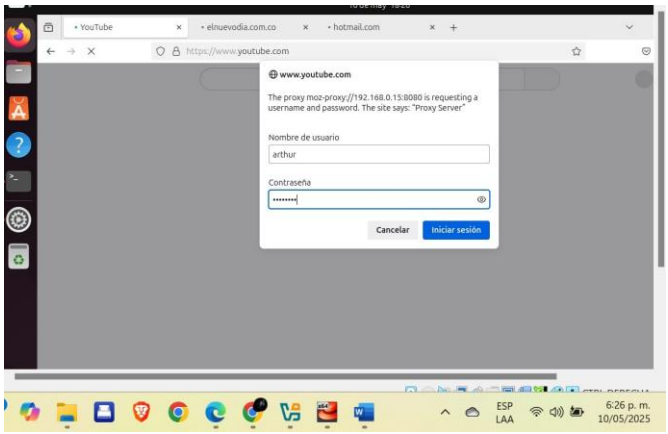

Figura 59. Digtación de credenciales del usuario autorizado. Fuente: Elaboración propia. Arthur Chavarro (2025).

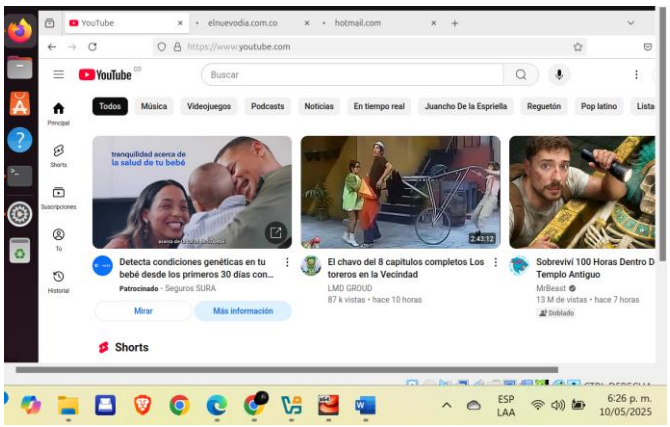

Figura 60. Ingreso del usuario autenticado a YouTube. Fuente: Elaboración propia. Arthur Chavarro (2025).

Figura 61. Ingreso del usuario autenticado a El Nuevo Día. Fuente: Elaboración propia. Arthur Chavarro (2025).

6. SUSTENTACIÓN

Estudiante: Miguel Angel Santa Polanco
Link: https://youtu.be/FdFYtpcf68o

Estudiante: Juan Camilo Lopez
Link: https://youtu.be/-umFNx3An8E

Estudiante: Arthur Chavarro Collazos
Link: https://youtu.be/IPSia4j9GEs

7. CONCLUSIONES

A lo largo del proceso de implementación, se comprendió que una Zona Desmilitarizada (DMZ) no constituye únicamente un segmento aislado dentro de la red, sino un puente cuidadosamente gestionado entre la red interna y el entorno exterior. Esta configuración evidenció la importancia de exponer únicamente los servicios estrictamente necesarios como HTTP y FTP, lo cual permite reducir de manera significativa los riesgos de seguridad. La denegación del protocolo ICMP se identificó como una táctica sutil pero eficaz para disminuir la visibilidad de la red frente a posibles escaneos, reforzando el enfoque de seguridad en capas y la necesidad de limitar la información innecesariamente expuesta.

Durante el desarrollo de la actividad, se reconoció la complejidad y el alcance funcional de un firewall como herramienta para la gestión del tráfico entre zonas con distintos niveles de confianza. La configuración de reglas precisas que habilitan servicios específicos entre la LAN y la DMZ, así como la implementación del acceso controlado desde Internet hacia la DMZ a través de mecanismos como NAT, permitió adquirir una visión más clara sobre cómo se administra la seguridad en entornos segmentados. La verificación de estas reglas, además, destacó la importancia de validar el funcionamiento efectivo de cada configuración aplicada.

Por otro lado, la implementación de un proxy HTTP no transparente permitió comprender cómo las políticas de seguridad también pueden aplicarse a nivel de la capa de aplicación. La configuración de autenticación de usuarios facilitó el control sobre quién puede acceder a Internet desde la red interna, mientras que la creación y aplicación de listas negras proporcionó una estrategia práctica para restringir contenidos específicos, con efectos tanto en la seguridad como en la productividad. En conjunto, estos aprendizajes evidenciaron el valor del proxy como una herramienta versátil para la supervisión y el control del tráfico web.

8. REFERENCIAS

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

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

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

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

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

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

[7] Configuración básica de SNAT en Endian Firewall
Endian. (s.f.). SNAT (Source NAT) - Basic Setup. Endian Help Center. Recuperado de https://help.endian.com/hc/en-us/articles/218144248-SNAT-Source-NAT-Basic-Setup .

[8] Implementando seguridad en GNU/Linux: Configuración de NAT
YouTube. (2025). Implementando Seguridad en Linux: Configuración de NAT utilizando la distribución Endian Firewall. Recuperado de https://www.youtube.com/watch?v=YPDKuFOeR-U

[9] Implementación de servicios en la zona DMZ con Endian Firewall
Scribd. (s.f.). Paso 6 - Implementando Seguridad en GNU-Linux - Sandra Salazar. Recuperado de https://de.scribd.com/document/435436372/Paso-6-Implementando-Seguridad-en-GNU-Linux-Sandra-Salazar-Colaborativo

[10] Configuración de reglas de tráfico inter-zona en Endian Firewall
YouTube. (2019). Cómo Configurar Reglas de Tráfico Inter-Zona en Endian Firewall. Recuperado de https://www.youtube.com/watch?v=XK0QdHYk6pg

[11] Configuración de un proxy HTTP no transparente en Endian FirewallEndian. (s.f.). Transparent HTTP Proxy Basic Setup. Endian Help Center. Recuperado de https://help.endian.com/hc/en-us/articles/115012758208-Transparent-HTTP-Proxy-Basic-Setup