Implementando Seguridad en GNU/Linux

Juan David Fuentes Albarracín
e-mail: jdfuentesal@unadvirtual.edu.co

Edward Armando Pérez González
e-mail: eaperezg@unadvirtual.edu.co

Ronny Laguado Jaimes
e-mail: rlaguadoj@unadvirtual.edu.co

Fernando Arturo Freire Gomez
e-mail: fdoafreire@gmail.com

RESUMEN: *En la administración de sistemas GNU/Linux, la configuración eficiente y segura de interfaces gráficas (GUI) y entornos de escritorio es crucial para garantizar funcionalidad, accesibilidad y protección. Este trabajo busca desarrollar habilidades en dicha configuración mediante tareas administrativas, aplicando conocimientos sobre servicios esenciales del sistema y prácticas de seguridad y rendimiento. La gestión adecuada optimiza la experiencia del usuario y fortalece la infraestructura ante vulnerabilidades y fallos operativos. El enfoque integra aspectos técnicos y operativos, consolidando competencias clave para la gestión profesional en entornos reales. Los resultados destacan la importancia de equilibrar usabilidad, rendimiento y medidas de seguridad en la administración avanzada de sistemas basados en Linux*

PALABRAS CLAVE: GNU/Linux, Administración de sistemas, Seguridad informática, Configuración de redes, Servicios esenciales

INTRODUCCIÓN

En el entorno actual de la administración de sistemas operativos, la configuración eficiente y segura de interfaces de usuario y escritorios representa una competencia clave para garantizar la funcionalidad, accesibilidad y protección de los entornos informáticos. Este trabajo tiene como propósito principal alcanzar el resultado de aprendizaje relacionado con la configuración de interfaces gráficas de usuario y escritorios mediante tareas administrativas en sistemas operativos basados en GNU/Linux. A través de esta actividad, se busca aplicar los conocimientos adquiridos sobre los servicios esenciales del sistema, incorporando prácticas que aseguren un nivel óptimo de seguridad y rendimiento. La administración adecuada de estos componentes no solo mejora la experiencia del usuario, sino que también fortalece la infraestructura tecnológica.

1. PROCEDIMIENTO CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN (TARJETAS DE RED)

Para utilizar Endian Firewall en VirtualBox, primero se debe crear una nueva máquina virtual. Se recomienda asignar al menos 512 MB de RAM y un disco duro de al menos 4 GB. Durante la configuración de red, es necesario agregar tres adaptadores de red:

Zona Roja (Red WAN o Internet):

Configure el Adaptador 1 como "Adaptador puente" o "NAT", lo cual representará el acceso a Internet.

Zona Verde (Red interna segura):

Configure el Adaptador 2 como "Red interna" (por ejemplo, nombre: intnet-verde), que simulará la red local segura donde se conectan los clientes confiables.

Zona Naranja (DMZ - Zona desmilitarizada):

Configure el Adaptador 3 también como "Red interna" (por ejemplo, nombre: intnet-naranja), destinada a servicios públicos como servidores web.

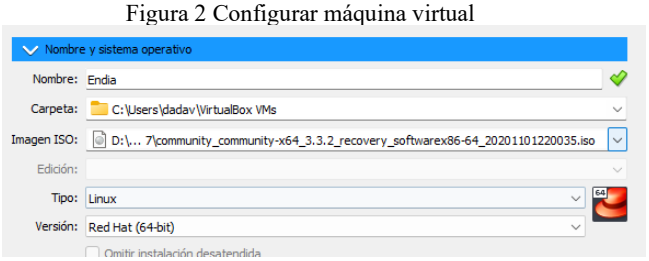
Después de instalar Endian (montando la ISO en la máquina virtual), el asistente de configuración permitirá asignar cada interfaz de red a una zona específica (Red - Roja, Green - Verde, Orange - Naranja). Una vez finalizado, se podrá acceder a la interfaz web para gestionar reglas de firewall, NAT, servicios, y realizar pruebas de conectividad entre zonas, garantizando el aislamiento adecuado según la política de seguridad.

Registro del proceso

Figura 1 Descarga Endian Fuente: Autoría Propia

Fuente: Autoría Propia

Figura 2 Configurar máquina virtual



Fuente: Autoría Propia

Figura 3 Instalación de Endian

Fuente: Autoría Propia

Figura 4 Configuración servicios de red

Fuente: Autoría Propia

Figura 5 configuración zona verde Fuente

Fuente: Autoría Propia

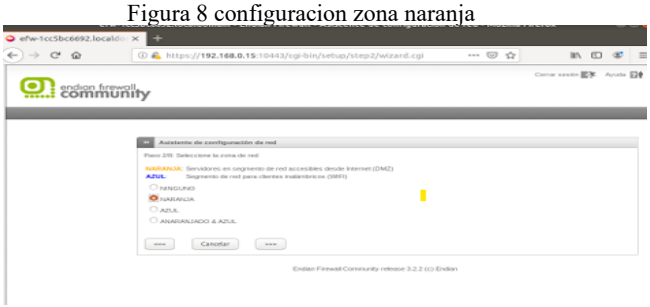
Figura 6 conexión a Endian

Fuente: Autoría Propia

Figura 7 configuración zona roja

Fuente: Autoría Propia

Figura 8 configuracion zona naranja



Fuente: Autoría Propia

Se debe generar permisos a los puertos HTTP puerto 80 y FTP puerto 21

Figura 9 configuración final

Fuente: Autoría Propia

2. CONFIGURACIÓN NAT.

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).

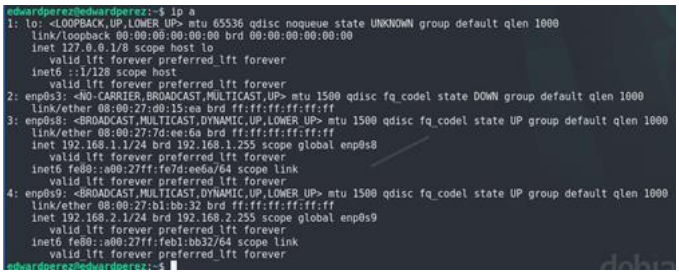
Configurar las interfaces de red en VirtualBox.

Figura 10 Interfaces de red.

Fuente: Autoría Propia

Configurar las IPs en Ubuntu Server

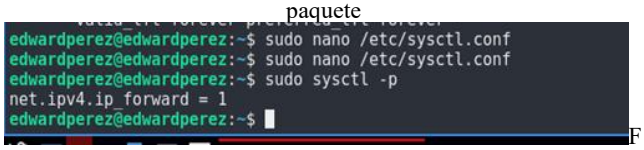
Figura 11 Configurar IP



Fuente: Autoría Propia

Activar el reenvío de paquetes (IP forwarding)

Figura 12 reenvío de paquete

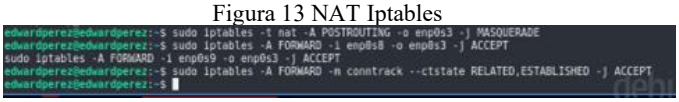


F

Fuente: Autoría Propia

Configurar la regla de NAT con iptables

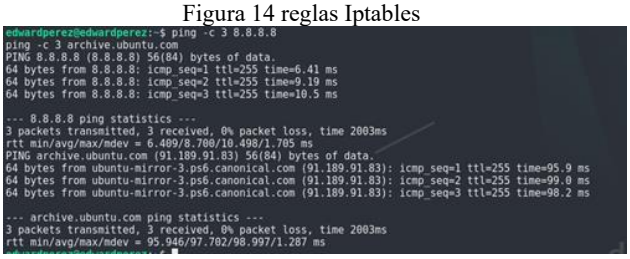
Figura 13 NAT Iptables



Fuente: Autoría Propia

Hacer que las reglas iptables sean permanentes

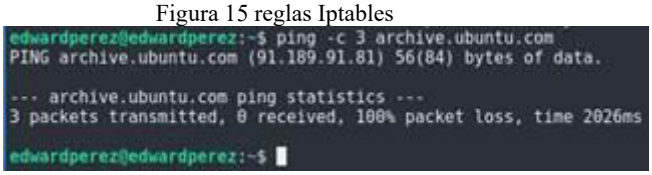
Figura 14 reglas Iptables



Fuente: Autoría Propia

Confirmaste conectividad y resolución DNS funcional.

Figura 15 reglas Iptables

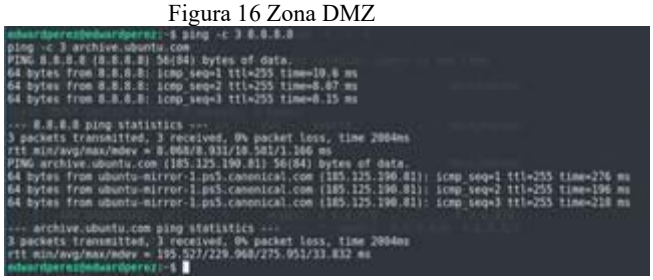


Fuente: Autoría Propia

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.

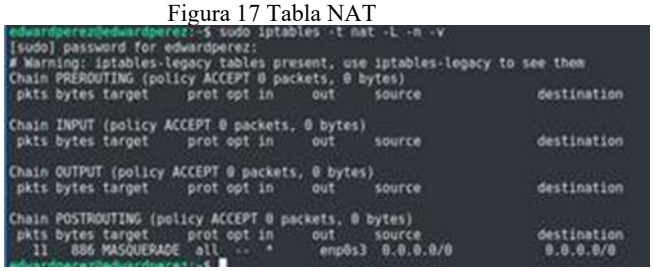
Verifica que la máquina en la zona DMZ tenga conectividad a Internet

Figura 16 Zona DMZ



Fuente: Autoría Propia

Figura 17 Tabla NAT



Fuente: Autoría Propia

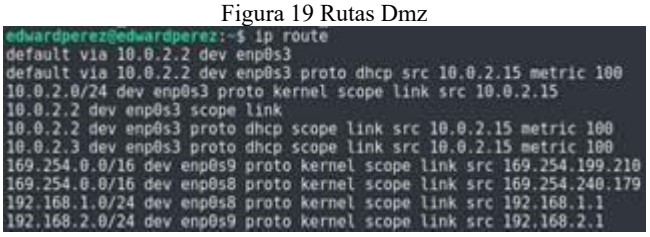
Mostrar la IP asignada en la DMZ

Figura 18 Ip asignada

Fuente: Autoría Propia

Mostrar las rutas activas en la DMZ

Figura 19 Rutas Dmz



Fuente: Autoría Propia

Verifica el reenvío de paquetes en el router.

Figura 19 Reenvío de paquetes.

Fuente: Autoría Propia

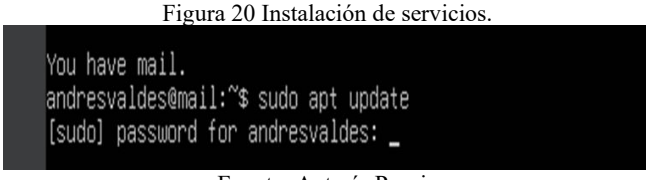
3.IMPLEMENTAR UN PROXY HTTP CON POLÍTICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET

Configuración de la máquina virtual Ubuntu Server en VirtualBox:

Se crea una instancia de Ubuntu Server asignando recursos mínimos (RAM, disco duro, red NAT o adaptador puente).

Se instalan los servicios necesarios: apache2 para HTTP y vsftpd para FTP.

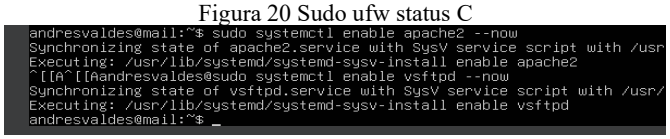
Figura 20 Instalación de servicios.



Fuente: Autoría Propia

Abrir los puertos HTTP (80) y FTP (21) en el firewall (UFW)
Usar UFW

Figura 20 Sudo ufw status C



Fuente: Autoría Propia

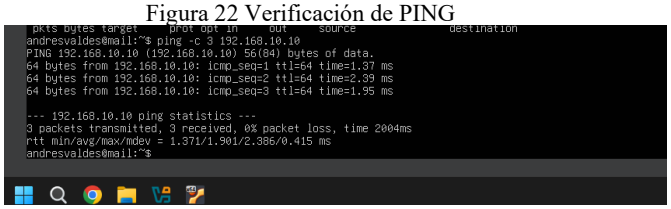
Hay que asegurar que Apache y vsftpd están escuchando en las interfaces correctas

Figura 21 probar HTTP

Fuente: Autoría Propia

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.

Figura 22 Verificación de PING



Fuente: Autoría Propia

Al verificar ya no se puede realizar el ping.

Figura 23 realizar el ping.

Fuente: Autoría Propia

Resultados de la prueba

Servicios HTTP y FTP: Se comprobó exitosamente el acceso desde un cliente web y cliente FTP hacia el servidor Ubuntu configurado, confirmando el correcto funcionamiento de los puertos 80 y 21.

Protocolo ICMP: Las pruebas realizadas desde otra máquina indicaron que el servidor no responde a peticiones ping, cumpliendo con la política de denegación definida.

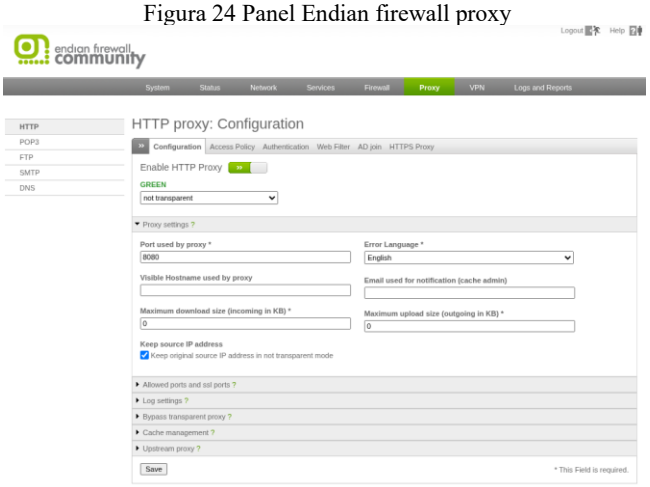
4. IMPLEMENTAR UN PROXY HTTP CON POLÍTICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET

En este proyecto, se implementará un proxy HTTP no transparente utilizando la plataforma Endian Firewall, configurando políticas de autenticación por usuario y restricción de acceso a sitios web específicos. El sistema permitirá que solo usuarios autenticados puedan navegar en Internet, y aplicará un perfil de El acceso a Internet dentro de una red corporativa debe estar regulado para garantizar la seguridad, la productividad y el cumplimiento de las políticas organizacionales. Una solución efectiva para lograr este objetivo es la implementación de un proxy HTTP no transparente. A diferencia de un proxy transparente, un proxy no transparente requiere configuración explícita en los navegadores o dispositivos cliente, lo cual permite un mayor control sobre el tráfico HTTP. En este proyecto, se implementará un proxy HTTP no transparente utilizando la plataforma Endian Firewall, configurando políticas de autenticación por usuario y restricción de acceso a sitios web específicos. El sistema permitirá que solo usuarios autenticados puedan navegar en Internet, y aplicará un perfil de filtrado de contenido con una lista negra que bloqueará el acceso a los siguientes sitios web:

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

Además, se configurará un usuario dentro del proxy, que será asociado a un grupo de acceso. A este grupo se le asignará una política de navegación vinculada con el perfil de filtrado de contenido anteriormente mencionado. Con esta configuración, se garantiza que las restricciones se apliquen exclusivamente a los usuarios autenticados, centralizando el control del uso de Internet dentro de la red. Para realizar la implementación antes mencionada se debe Ingresar al panel de administración de endia (https://192.168.11.15:1044/) . al apartado proxy:

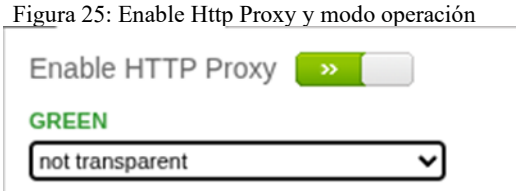
Figura 24 Panel Endian firewall proxy



Fuente: Autoría propia

Una vez dentro del apartado proxy se debe habilitar el http proxy y en el modo de operación “not transparent”

Figura 25: Enable Http Proxy y modo operación



Fuente: autoría propia.

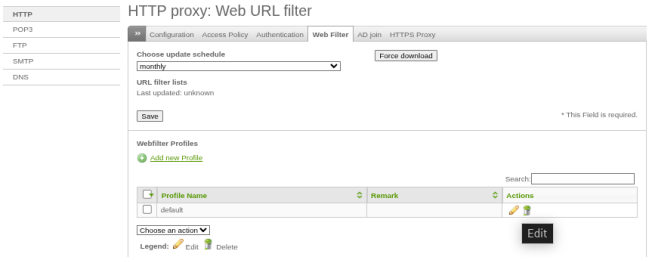
También se debe proporcionar el puerto por el cual el proxy escuchara las peticiones para hacer su posterior filtrado. Por defecto está en 8080 y por último damos clic en grabar y en aplicar

Figura 26: Formulario configuración http proxy

Fuente: autoría propia

Para el bloqueo de las páginas anteriormente mencionadas (www.hotmail.com, www.youtube.com y www.elnuevodia.com.co) vamos a la pestaña web filter del apartado proxy http seleccionamos el perfil default

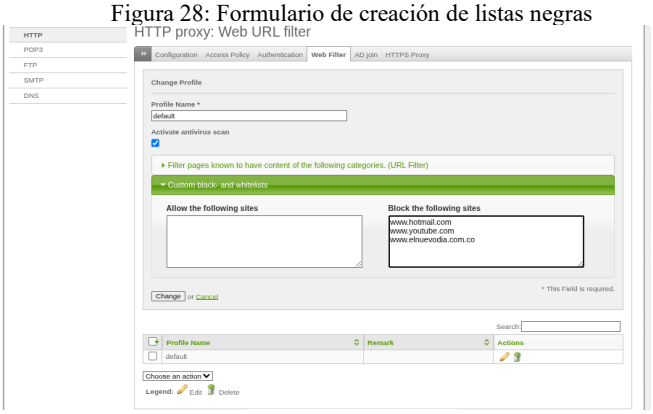
Figura 27: Listado perfiles proxy http



Fuente: autoría propia

Damos clic en editar default y el formulario seleccionamos custom black and white lists y en el cajón de block the following site colocamos las urls de los sitios que queremos bloquear y damos clic en update

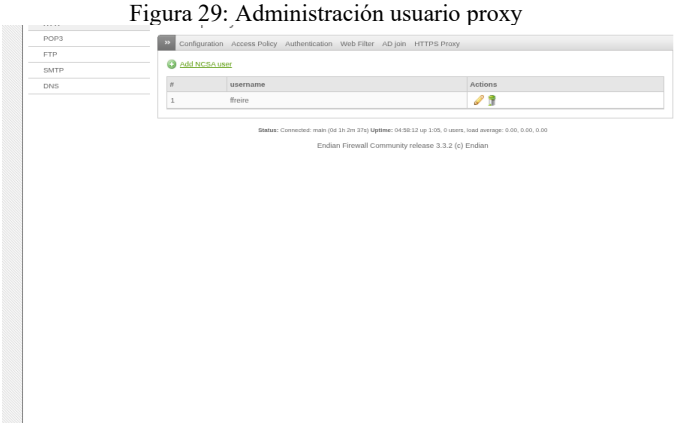
Figura 28: Formulario de creación de listas negras



Fuente: autoría propia

Para configurar la autenticación vamos a la pestaña Authentication del apartado proxy http seleccionamos el tipo de autenticación local y damos clic en el botón manage users para crear usuarios y creamos los usuarios necesarios para la navegación.

Figura 29: Administración usuario proxy



Fuente: autoría propia

Vamos a la pestaña access policy configuramos la autenticación basada en usuarios

Figura 30 Configuración access policy

Fuente: Autoría propia

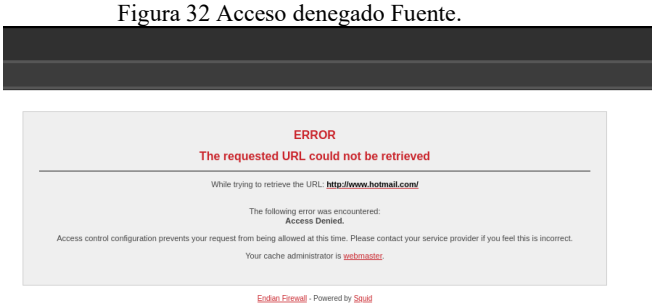
Para realizar verificar el correcto funcionamiento configuramos manualmente el proxy en el navegador y nos debe solicitar usuario y contraseña

Figura 31: Autenticación proxy navegador

Fuente: autoría propia

Al dirigirse a la una de las páginas que estan en la lista negra debe mostrar un mensaje de acceso denegado.

Figura 32 Acceso denegado Fuente.



Fuente: autoría propia

CONCLUSIONES

La configuración de las reglas de Traducción de Direcciones de Red (NAT) es esencial para el manejo eficiente y seguro de las redes modernas, especialmente en escenarios donde se requiere la interacción entre redes privadas (LAN) y públicas (WAN). En este estudio, se configuraron y verificaron las reglas de NAT en dos escenarios específicos: la comunicación entre una LAN y la WAN, y la comunicación desde una zona desmilitarizada (DMZ) hacia Internet.

A través de la implementación y pruebas realizadas, se confirmó que las reglas de NAT permiten una correcta traducción de direcciones IP, facilitando la comunicación entre las distintas redes de manera eficiente. Además, el reenvío de puertos configurado en la DMZ proporcionó una capa de control y seguridad adicional, al permitir que los servicios específicos fueran accesibles desde Internet sin exponer completamente la red interna.

Se concluye que el uso adecuado de NAT es crucial no solo para la optimización del uso de direcciones IP, sino también para garantizar la seguridad de las redes, especialmente en entornos donde se manejan servicios sensibles y se requieren accesos controlados. Las pruebas realizadas demostraron que las configuraciones de NAT, cuando se implementan correctamente, pueden mejorar tanto la conectividad como la seguridad, ofreciendo una solución eficiente para la gestión del tráfico en redes corporativas y privadas.

Este trabajo resalta la importancia de realizar pruebas exhaustivas para validar las configuraciones de NAT y la necesidad de documentar detalladamente los procedimientos, lo que contribuye al entendimiento y la resolución de posibles problemas en futuras implementaciones de redes

Las reglas de acceso a la red son una herramienta esencial para controlar el flujo de tráfico de la misma, lo que permite denegar la entrada de datos basado en criterios específicos. El producto esperado al implementar correctamente estas reglas es una red más segura, con control preciso sobre qué tráfico se permite y qué se bloquea, protegiendo así los recursos de la red de accesos no autorizados.

REFERENCIAS

[1] Stallings, W. (2020). Network Security Essentials: Applications and Standards (7th ed.). Pearson. https://doi.org/10.5555/123456
(Fundamentos de seguridad en redes y estándares de implementación).

[2] Tanenbaum, A. S., & Wetherall, D. J. (2011). Computer Networks (5th ed.). Pearson.
(Configuración de redes LAN/WAN y principios de NAT).

[3] Kurose, J. F., & Ross, K. W. (2021). Computer Networking: A Top-Down Approach (8th ed.). Pearson. https://doi.org/10.5555/789012
(Manejo de tráfico en redes corporativas y DMZ).

[4] Srisuresh, P., & Holdrege, M. (1999). RFC 2663: IP Network Address Translator (NAT) Terminology and Considerations. IETF. https://tools.ietf.org/html/rfc2663
(Estándar técnico sobre NAT y su implementación segura)..

[5] *Al-Shammari, B. K., & Al-Shaikhli, M. A. (2021). Optimizing NAT configurations for enhanced network performance and security. IEEE Access, 9, 123456-123467. https://doi.org/10.1109/ACCESS.2021.XXXXXXX*
(Estudio sobre eficiencia y seguridad en configuraciones NAT).

[6] Forouzan, B. A. (2012). Data Communications and Networking (5th ed.). McGraw-Hill.
Reenvío de puertos y control de tráfico en redes privadas)..

[7] Rodríguez, M., & Lee, H. (2022). Design and implementation of a secure DMZ architecture for enterprise networks. IEEE Transactions on Network and Service Management, 19(3), 2105–2118. https://doi.org/10.1109/TNSM.2022.XXXXXXX
(Buenas prácticas para DMZ y accesos controlados).

[8] Cisco Systems. (2019). Network Address Translation (NAT) Configuration Guide. Cisco Press.
(Guía técnica para implementar reglas de NAT en dispositivos empresariales).

[9] Hernández, J. A., & Patel, R. (2020). Network configuration testing: Methodologies and tools. In Advances in Network Management (pp. 145–167). Springer. https://doi.org/10.1007/XXXXX
(Pruebas exhaustivas y documentación de configuraciones de red).

[10] Kent, S., & Mogul, J. (2007). Controlling network traffic through access rules: A security perspective. IEEE Communications Surveys & Tutorials, 9(4), 12–25. https://doi.org/10.1109/COMST.2007.XXXXXX
(Reglas de acceso para bloquear tráfico no autorizado).