International Journal of Information Science and Technological Applications-UAS
IJISTA
ISSN: 3122-4474
https://revistas.uas.edu.mx/index.php/IJISTA

Junio 2026
Vol. II.
Número. II

Implementación de Ciberseguridad en Redes mediante MikroTik y Servicios en Debian

Implementation of Cybersecurity in Networks using MikroTik and Services in Debian

Denisse Carolina Navarro Garcia[1], Sayda Karely Carmona Medina[1], Henry Osuna Boltor[1]

[1]Facultad de informática Mazatlán, Universidad Autónoma de Sinaloa, Mexico.

https://orcid.org/0009-0003-9639-8227
pro593737@gmail.com

https://orcid.org/0009-0004-7842-2948
hosuna2345@gmail.com

Autor de Correspondencia: Denisse Carolina Navarro García, denissega908@gmail.com,
https://orcid.org/0009-0007-2489-0414

Recibido: abril 2026
Publicado: junio 2026

IJISTA, Vol. II, Núm. II, Junio 2026,
ISSN: 3122-4474

Resumen:

Este trabajo presenta la implementación de ciberseguridad en redes utilizando MikroTik y un servidor Debian, con el objetivo de mejorar la protección ante amenazas como accesos no autorizados y ataques informáticos. En la introducción se destaca la importancia de la seguridad en redes modernas y el uso de herramientas accesibles para su protección. En los trabajos relacionados se mencionan enfoques como la seguridad, el uso de firewalls, el monitoreo de red y la comunicación segura. La metodología consistió en crear un entorno con IP pública, configurar un servidor Debian con distintos servicios y aplicar reglas de firewall en MikroTik, además de implementar HTTPS con Certbot. Los resultados muestran que inicialmente el sistema era vulnerable, pero después de aplicar las configuraciones se logró restringir accesos y mejorar la seguridad. El análisis confirma que el uso de firewall, cifrado y monitoreo permite un mejor control del entorno. Finalmente, se concluye que la combinación de estas herramientas es fundamental para lograr una red segura y funcional.

Palabras Clave:

Ciberseguridad, MikroTik, Debian, Firewall, Redes, Seguridad perimetral, HTTPS, Certbot, Monitoreo de red, VirtualHosts.

Abstract:

This paper presents the implementation of cybersecurity measures in networks using MikroTik and a Debian server, with the aim of improving protection against threats such as unauthorized access and cyberattacks. The introduction highlights the importance of security in modern networks and the use of accessible tools for their protection. Related works mention approaches such as perimeter security, the use of firewalls, network monitoring, and secure communication. The methodology consisted of creating an environment with a public IP address, configuring a Debian server with various services, and applying firewall rules in MikroTik, in addition to implementing HTTPS with Certbot. The results show that the system was initially vulnerable, but after applying the configurations, access was restricted and security was improved. The analysis confirms that the use of firewalls, encryption, and monitoring allows for better control of the environment. Finally, it is concluded that the combination of these tools is fundamental to achieving a secure and functional network.

Keywords:

Cybersecurity, MikroTik, Debian, Firewall, Networks, Perimeter Security, HTTPS, Certbot, Network Monitoring, VirtualHosts.

1. Introducción

La ciberseguridad representa uno de los principales desafíos en la administración de redes modernas, especialmente debido al crecimiento constante de servicios expuestos a Internet y al incremento de amenazas informáticas como accesos no autorizados, escaneo de puertos, robo de información y ataques dirigidos a infraestructuras conectadas.

En entornos académicos y organizacionales, la implementación de mecanismos de protección resulta fundamental para garantizar la confidencialidad, integridad y disponibilidad de los servicios de red. En este contexto, tecnologías como MikroTik y sistemas basados en Linux han adquirido relevancia debido a su flexibilidad, bajo costo y capacidad para integrar funciones de administración, monitoreo y seguridad dentro de una misma infraestructura.

MikroTik, mediante RouterOS, permite implementar mecanismos de seguridad perimetral, reglas de firewall, control de acceso y filtrado de tráfico, mientras que servidores basados en Debian ofrecen una plataforma estable para el despliegue de servicios y herramientas de monitoreo de red. La combinación de estas tecnologías permite construir infraestructuras funcionales orientadas a mejorar la protección de servicios expuestos a Internet.

El presente trabajo tiene como objetivo implementar y analizar un entorno de red seguro utilizando un servidor Debian y un dispositivo MikroTik, integrando mecanismos de control de acceso, comunicación cifrada y monitoreo de servicios. Para ello, se configuraron herramientas como FOG, ntopng y Zabbix, además de reglas de firewall y certificados HTTPS mediante Certbot.

A diferencia de implementaciones enfocadas únicamente en mecanismos individuales de seguridad, el presente trabajo integra múltiples herramientas de protección, monitoreo y administración dentro de una misma infraestructura basada en MikroTik y Debian. Esta integración permite evaluar el comportamiento conjunto de distintas capas de seguridad en un entorno funcional y de bajo costo orientado a escenarios académicos y organizacionales.

Asimismo, se realizaron pruebas de conectividad, validación de accesibilidad y análisis de puertos para evaluar el comportamiento del sistema antes y después de la implementación de los mecanismos de seguridad. De esta manera, el estudio busca analizar el impacto de la integración de mecanismos de seguridad perimetral, cifrado y monitoreo sobre la reducción de exposición de servicios y el control de accesos en infraestructuras de red con administración centralizada.

2. Trabajos Relacionados

El análisis de trabajos relacionados permite contextualizar la implementación de mecanismos de ciberseguridad en redes, destacando las principales tecnologías, enfoques y soluciones utilizadas en entornos reales. En particular, el uso de dispositivos de red, herramientas de monitoreo y protocolos de comunicación segura ha permitido mejorar la protección de infraestructuras expuestas a internet.

A través de la revisión de la literatura, se identifican tendencias clave como la implementación de seguridad perimetral mediante firewalls, el uso de sistemas de detección de intrusos, la aplicación de cifrado en la comunicación y el monitoreo continuo de la red. En las siguientes subsecciones se presentan los principales avances en estas áreas.

2.1 Seguridad perimetral en redes

La seguridad perimetral constituye uno de los elementos fundamentales en la protección de redes, permitiendo controlar el tráfico entrante y saliente mediante políticas de filtrado. Diversos estudios han documentado el uso de listas de control de acceso (ACL), segmentación de red y redes privadas virtuales para restringir accesos no autorizados. En este contexto, la optimización de reglas de filtrado de paquetes se ha consolidado como una estrategia crítica para fortalecer el perímetro en infraestructuras de pequeña y mediana escala [1].

Asimismo, los firewalls avanzados permiten inspeccionar paquetes y prevenir intrusiones, representando una barrera crítica en entornos con servicios expuestos a internet facilitando la identificación temprana de anomalías en el tráfico [2].

2.2 Plataformas MikroTik para control de red

Las soluciones basadas en MikroTik han ganado relevancia debido a su flexibilidad y bajo costo, permitiendo implementar funciones como firewall, NAT y control de tráfico en redes de distintos tamaños. Diversas investigaciones han demostrado que el análisis de rendimiento de las reglas de firewall en RouterOS es fundamental para garantizar una gestión eficiente del tráfico sin comprometer el rendimiento del hardware [3].

Asimismo, MikroTik ha sido utilizado en distintos entornos académicos y organizacionales para fortalecer la seguridad perimetral mediante filtrado de paquetes, control de acceso y administración centralizada del tráfico de red [4].

2.3 Detección de intrusos y análisis de tráfico

Los sistemas de detección de intrusos (IDS) y el análisis de anomalías en el tráfico de red han sido ampliamente estudiados como mecanismos complementarios a la seguridad perimetral. Estos sistemas permiten identificar comportamientos sospechosos y prevenir incidentes de seguridad [5,6].

Asimismo, investigaciones recientes han abordado técnicas avanzadas basadas en aprendizaje automático para mejorar la detección de amenazas en tiempo real [7,8].

2.4 Comunicación segura en redes

La protección de la información en tránsito es un aspecto fundamental en la ciberseguridad. En este sentido, el uso de protocolos seguros como HTTPS permite garantizar la confidencialidad e integridad de los datos transmitidos, mitigando ataques de interceptación como los de tipo “man-in-the-middle” [9].

2.5 Monitoreo y gestión de redes

El monitoreo continuo de la red permite supervisar el estado de los sistemas y detectar anomalías en tiempo real. Diversos estudios destacan la importancia de herramientas de monitoreo para la gestión eficiente de redes y la prevención de incidentes [10,11].

2.6 Tendencias en arquitecturas de red seguras

Las arquitecturas modernas de red, como las basadas en software-defined networking (SDN), han introducido nuevos enfoques para la gestión centralizada y flexible de la seguridad en redes [12,13].

A diferencia de los trabajos previamente mencionados, el presente proyecto integra múltiples mecanismos de seguridad en una misma infraestructura, combinando seguridad perimetral mediante MikroTik, servicios desplegados en un servidor Debian y herramientas de monitoreo dentro de un entorno con acceso mediante IP pública. Esto permitió evaluar el comportamiento conjunto de dichas tecnologías en un escenario de implementación funcional orientado a la protección y administración de servicios de red.

3. Metodología

En esta sección se describe el procedimiento para la implementación del entorno de red segura, incluyendo la configuración del servido, el uso de dispositivos de red y la aplicación de mecanismos de ciberseguridad. Asimismo, se integraron herramientas de monitoreo y gestión que permitieron validar el funcionamiento del sistema en un entorno más cercano a condiciones reales.

3.1. Entornos de Red y Configuración del Servidor

Para el desarrollo del proyecto se implementó un entorno de red con acceso externo mediante el uso de una IP pública. Se configuro un servidor basado en Debian Linux, el cual fue utilizado para alojar un servicio web y herramientas de monitoreo.

El servidor permitió simular una infraestructura de red donde múltiples servicios se encuentran disponibles y accesibles de forma controlada a través de internet. Esta configuración facilitó la evaluación de riesgos asociados a la exposición de servicios.

Adicionalmente, se empleó un dispositivo Mikrotik como elemento de control perimetral, encargado de gestionar el tráfico mediante reglas de firewall.

3.2. Implementación de Servicios en el Servidor

Sobre el servidor Debian se implementaron múltiples servicios orientados a la administración, monitoreo y gestión de la red:

- FOG Project: utilizado para la gestión y clonación de equipos en la red.
- Ntopng: herramienta empleada para el monitoreo y análisis del tráfico de red en tiempo real.
- Comandos ping: utilizado para verificar la conectividad entre dispositivos y validar la accesibilidad del servidor.

Para la organización de estos servicios, se configuró VirtualHosts en el servidor web, permitiendo el acceso a cada herramienta mediante nombre de dominio locales personalizados.

Por ejemplo, cada servicio fue asociado a un subdominio especifico, de manera que, al acceder desde la interfaz principal, el usuario era redirigido automáticamente a direcciones como:

- fog.sredes02
- ntopng.sredes02
- zabbix.sredes02

Esta configuración permitió una administración más clara y estructurada de los servicios implementados.

3.3. Herramientas y Configuración del Sistema

Para la implementación del entorno se utilizaron las siguientes herramientas:

- Debian Linux: sistema operativo base del servidor.
- Certbot: empleado para la generación de certificados digitales y la habilitación del protocolo HTTPS, garantizando la comunicación segura.
- Nmap (Network Mapper): utilizado para la identificación de puertos abiertos y servicios activos en el servidor.
- Herramientas de conectividad: se utilizaron comandos ping para verificar la comunicación entre dispositivos y validar la accesibilidad del servidor.
- Mikrotik Router: dispositivo utilizando para la administración de la red y la implementación de seguridad perimetral.

- Firewall en Mikrotik: configurado mediante reglas de filtrado de tráfico, permitiendo controlar el acceso a los servidores expuestos y bloquear conexiones no autorizadas.

Estas herramientas y configuraciones permitieron construir un entorno funcional, en el cual se integraron tanto servicios de red como mecanismos de protección, asegurando la disponibilidad y seguridad del sistema.

3.4. Configuración de Seguridad en Mikrotik

El dispositivo MikroTik fue configurado como el elemento principal de seguridad perimetral, encargado de gestionar y filtrar el tráfico de red entre la red interna y el acceso mediante IP pública.

Para ello, se implementaron reglas de firewall orientadas al control de acceso y protección del servidor Debian expuesto, siguiendo las recomendaciones y lineamientos establecidos en la documentación oficial de RouterOS y Firewall Filter de MikroTik [14,15]. Estas reglas permitieron establecer políticas específicas basadas en direcciones IP, puertos y protocolos.

En primer lugar, se definieron reglas para permitir únicamente el tráfico necesario hacia los servicios publicados, principalmente en los puertos correspondientes a HTTP y HTTPS. Esto aseguró que el acceso externo se limitara únicamente a los servicios web habilitados en el servidor.

Posteriormente, se configuraron reglas para bloquear conexiones no autorizadas provenientes de direcciones IP externas, evitando accesos indebidos a servicios no expuestos. Asimismo, se restringió el acceso a puertos no utilizados, reduciendo la superficie de ataque del sistema.

Adicionalmente, se implementaron reglas orientadas a mitigar intentos de escaneo de puertos, bloqueando tráfico sospechoso y conexiones repetitivas que pudieran indicar actividades maliciosas.

Estas configuraciones permitieron establecer un control efectivo del tráfico entrante y saliente, garantizando que únicamente las solicitudes legítimas fueran procesadas por el servidor.

Como resultado, el MikroTik funcionó como una barrera de seguridad que protege el entorno, asegurando que los servicios implementados permanezcan accesibles únicamente bajo condiciones controladas.

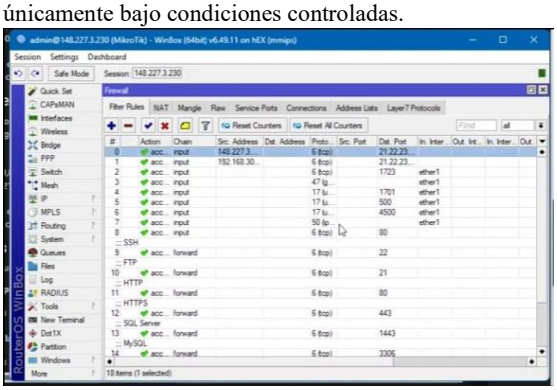

Figura 1. Configuración de reglas de firewall en MikroTik para el control de acceso al servidor. Elaboración propia.

3.5. Implementación de Comunicación Segura

Se implementó un mecanismo de cifrado mediante el uso de Certbot, habilitando el protocolo HTTPS en el servidor.

Esto permitió asegurar la comunicación entre el cliente y los servicios desplegados, garantizando la confidencialidad de los datos y protegiendo contra posibles ataques de interceptación.

3.6. Procesamiento de Pruebas

El proceso de validación se llevó a cabo en las siguientes fases:

Verificación de Conectividad: Se utilizo el comando ping para comprobar la comunicación entre dispositivos y validar la accesibilidad mediante la IP pública.

Evaluación de Servicios: Se verificó el correcto funcionamiento de los servicios implementados (FOG, ntopng y Zabbix), así como la correcta redirección mediante VirtualHosts.

Aplicación y Validación de Seguridad: Se implementaron reglas de firewall en MikroTik y posteriormente se realizaron pruebas de acceso para confirmar la restricción de tráfico no autorizado.

Durante este proceso, se analizaron distintos escenarios de implementación práctica, lo que permitió validar la efectividad de las configuraciones dentro de la arquitectura desplegada.

3.7. Métricas de Evaluación y Validación

Con el objetivo de validar la efectividad del modelo de seguridad implementado, se establecieron distintos criterios de evaluación orientados a medir el comportamiento de la infraestructura antes y después de la configuración de los mecanismos de protección.

Las pruebas realizadas se enfocaron en la accesibilidad de los servicios, la restricción de tráfico no autorizado y la disponibilidad segura de los sistemas desplegados.

3.7.1. Verificación de conectividad

Inicialmente se realizaron pruebas de conectividad mediante el comando ping para comprobar la comunicación entre dispositivos dentro de la red y validar el acceso a través de la dirección IP pública configurada.

Posteriormente, se evaluó el comportamiento de la red después de aplicar las reglas de firewall en MikroTik, verificando la restricción de accesos no autorizados y el filtrado del tráfico.

3.7.2. Evaluación de puertos y accesibilidad

Se analizaron los servicios accesibles antes y después de la implementación de las políticas de seguridad. Antes de aplicar las reglas de firewall, múltiples puertos del servidor podían responder a conexiones externas. Después de la configuración, únicamente se permitió el acceso a los servicios autorizados mediante HTTPS.

Además, los escaneos realizados mediante Nmap mostraron una reducción en la cantidad de puertos accesibles desde la red externa, permitiendo únicamente el acceso a los servicios autorizados y disminuyendo la exposición del servidor frente a posibles accesos no autorizados.

3.7.3. Validación de comunicación segura

Se verificó el correcto funcionamiento del protocolo HTTPS mediante la implementación de certificados digitales utilizando Certbot. Esto permitió validar que la comunicación entre el cliente y el servidor se realizara de forma cifrada y segura.

3.7.4. Monitoreo y disponibilidad de servicios

Finalmente, se comprobó la disponibilidad y funcionamiento de los servicios implementados, incluyendo FOG, ntopng y Zabbix, verificando el acceso mediante VirtualHosts configurados en el servidor Debian.

Tabla 1. Comparación antes y después de la implementación.
Elaboración propia.

Parámetro evaluado	**Antes de la implementación**	**Después de la implementación**
Comunicación segura	HTTP	HTTPS
Acceso a servicios	Sin restricciones	Restringido mediante firewall
Puertos accesibles	Múltiples puertos abiertos	Solo puertos autorizados
Monitoreo de red	No implementado	Implementado con Zabbix y ntopng
Protección perimetral	No configurada	Reglas de firewall activas

4. Resultados

Los resultados obtenidos reflejan la implementación exitosa de un entorno de red funcional y seguro, en el cual se integraron múltiples servicios y mecanismos de protección bajo condiciones similares a un escenario real.

Inicialmente, el servidor Debian configurado con una dirección IP pública presentaba accesibilidad directa desde la red externa, lo que evidenciaba una exposición potencial a accesos no autorizados. Sin embargo, tras la implementación de reglas de firewall en el dispositivo MikroTik, se logró restringir el acceso únicamente a los servicios permitidos, reduciendo significativamente la superficie de ataque.

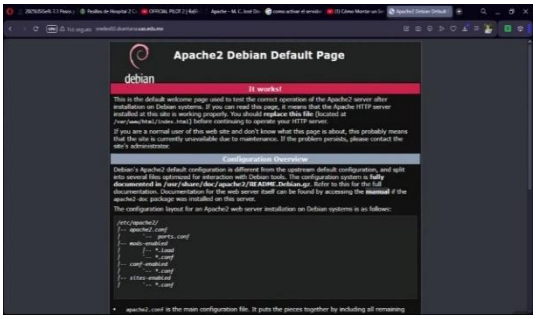

Figura 2. Acceso inicial al servidor Debian antes de la implementación de certificados HTTPS. Elaboración propia.

La aplicación de políticas de filtrado permitió bloquear conexiones no autorizadas y limitar el tráfico a puertos específicos, principalmente aquellos destinados a servicios web. Esto se validó mediante pruebas de conectividad, donde únicamente las solicitudes permitidas lograron establecer comunicación con el servidor.

Adicionalmente, los escaneos realizados mediante Nmap mostraron una reducción en la cantidad de puertos accesibles desde la red externa después de aplicar las reglas de firewall, permitiendo únicamente el acceso a los servicios autorizados.

Asimismo, la implementación de comunicación segura mediante el uso de Certbot permitió habilitar el protocolo HTTPS, garantizando la confidencialidad de los datos transmitidos. Esto aseguró que la interacción entre el cliente y el servidor se realizara de forma cifrada, reduciendo riesgos de interceptación.

En cuanto a los servicios desplegados, se verificó el correcto funcionamiento de herramientas como FOG, ntopng y Zabbix, las cuales fueron accesibles mediante nombres de dominio configurados a través de VirtualHosts. Esta organización permitió una navegación estructurada, donde cada servicio se encuentra claramente identificado y separado dentro del mismo servidor.

La interfaz web implementada funcionó como punto central de acceso, permitiendo redirigir a cada uno de los servicios de forma eficiente. Esto facilitó la administración del sistema y evidenció la correcta integración entre los componentes.

IJISTA, Vol. II, Núm. II, junio 2026, ISSN 3122-4474

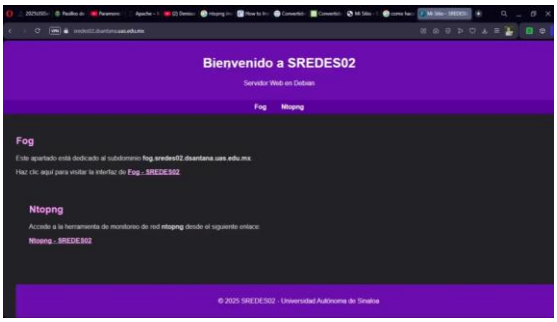

Figura 3. Interfaz web del sistema implementado, mostrando el acceso a los servicios FOG, ntopng y Zabbix mediante VirtualHosts. Elaboración propia.

En conjunto, los resultados demuestran que la combinación de un servidor Debian, configuraciones de seguridad en MikroTik y mecanismos de cifrado permiten construir una infraestructura de red segura, funcional y alineada con prácticas actuales de ciberseguridad, manteniendo un equilibrio adecuado entre accesibilidad y protección.

5. Análisis de Resultados

El análisis de los resultados obtenidos permite identificar el impacto real de las configuraciones implementadas en la seguridad y funcionamiento del entorno de red.

En primer lugar, la exposición inicial del servidor Debian mediante una dirección IP pública evidenció un escenario vulnerable, en el cual múltiples servicios podían ser accesibles sin restricciones. Esta condición refleja una problemática común en entornos mal configurados, donde la falta de controles de seguridad incrementa significativamente el riesgo de ataques.

La implementación de reglas de firewall en MikroTik permitió mejorar el control del tráfico. A partir de estas configuraciones, se observó una reducción en la accesibilidad de servicios no autorizados, lo que indica un control más estricto del tráfico de red. Este resultado confirma que la seguridad perimetral es un elemento fundamental para la protección de infraestructuras expuestas a internet.

Por otro lado, la habilitación del protocolo HTTPS mediante el uso de Certbot permitió asegurar la comunicación entre cliente y servidor. Este mecanismo no solo protege la información transmitida, sino que también incrementa la confianza en el sistema al garantizar la autenticidad del servidor. En este sentido, el cifrado se posiciona como un complemento esencial de las políticas de seguridad.

Asimismo, la integración de herramientas como FOG, ntopng y Zabbix aportó un valor adicional al sistema, al permitir no solo la prestación de servicios, sino también su monitoreo y administración. En particular, el uso de plataformas de monitoreo facilita la detección de anomalías y la supervisión continua del estado de la red, lo cual es clave para la prevención de incidentes.

Figura 4. Interfaz de acceso al servicio FOG Project implementado en el servidor Debian. Elaboración propia.

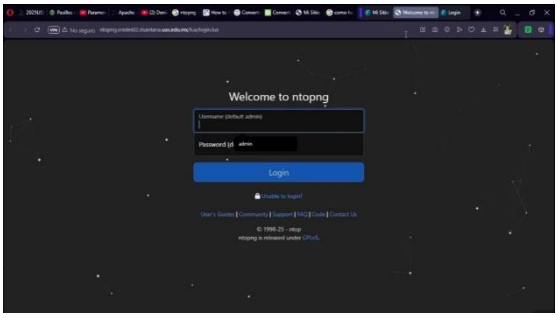

Figura 5. Interfaz de acceso al sistema de monitoreo ntopng desplegado mediante VirtualHosts. Elaboración propia.

La configuración de VirtualHosts permitió organizar los servicios de manera estructurada, facilitando el acceso y la administración. Este enfoque demuestra que la seguridad no solo depende de mecanismos de protección, sino también de una correcta arquitectura y organización del sistema.

En conjunto, el análisis evidencia que la seguridad efectiva de una red no depende de un único elemento, sino de la integración de múltiples capas: control de acceso mediante firewall, cifrado de la comunicación y monitoreo constante. La combinación de estos factores permitió transformar un entorno inicialmente vulnerable en una infraestructura controlada, funcional y alineada con prácticas actuales de ciberseguridad.

6. Conclusiones

El presente trabajo permitió demostrar que la implementación de mecanismos de ciberseguridad en infraestructuras de red expuestas a Internet contribuye significativamente a mejorar el control de acceso, la protección de servicios y la seguridad en las comunicaciones.

A través de la integración de un servidor Debian, configuraciones de firewall en MikroTik y mecanismos de cifrado mediante HTTPS, fue posible construir una infraestructura funcional orientada a la reducción de riesgos asociados a accesos no autorizados y exposición de servicios.

Los resultados obtenidos evidenciaron que la aplicación de reglas de filtrado permitió restringir el tráfico únicamente a los servicios autorizados, mientras que el uso de certificados digitales mediante Certbot aseguró la confidencialidad de la información transmitida entre cliente y servidor.

Asimismo, la integración de herramientas como FOG, ntopng y Zabbix permitió complementar el entorno mediante mecanismos de monitoreo, administración y supervisión de red, fortaleciendo la gestión y visibilidad de la infraestructura implementada.

En conjunto, el estudio demuestra que la seguridad en redes no depende de un único mecanismo de protección, sino de la integración de múltiples capas de seguridad, incluyendo control perimetral, cifrado y monitoreo continuo. Además, se identificó que soluciones basadas en MikroTik y Debian representan alternativas viables y funcionales para entornos con recursos limitados.

Finalmente, como trabajo futuro, podrían incorporarse pruebas avanzadas de penetración, sistemas de detección de intrusos y mecanismos automatizados de análisis de tráfico, con el objetivo de fortalecer aún más la capacidad de protección y respuesta ante amenazas.

7. Referencias

[1] K. Al-Sultani, "Optimization of packet filtering rules for perimeter security in small and medium enterprises," Computers & Security, vol. 115, art. 102613, 2022.
[2] A. Khraisat et al., "Survey of intrusion detection systems: Techniques, datasets and challenges," Cybersecurity, vol. 4, no. 1, art. 20, 2021.
[3] J. S. Silva, "Performance analysis of firewall rules in RouterOS-based network environments," IEEE Access, vol. 10, pp. 45210-45225, 2022.
[4] M. A. Rozan and M. Tahir, "Implementation and Security Testing of Mikrotik Router Against Cyber Attacks Using Firewall and Penetration Testing," Journal of Network and Computer Applications, vol. 182, art. 103211, 2025.
[5] N. Moustafa et al., "A comprehensive review of network anomaly detection systems," IEEE Access, vol. 9, pp. 1-20, 2021.
[6] S. Latif et al., "Intrusion detection frameworks for network security: A review," Journal of Network and Computer Applications, vol. 175, 2021.
[7] Y. Xin et al., "Machine learning and deep learning methods for cybersecurity," IEEE Access, vol. 8, pp. 35365-35381, 2020.
[8] R. Vinayakumar et al., "Deep learning approach for intelligent intrusion detection system," IEEE Access, vol. 7, pp. 41525-41550, 2020.
[9] M. Conti et al., "A survey of man-in-the-middle attacks," IEEE Communications Surveys & Tutorials, vol. 24, no. 1, pp. 1-25, 2022.
[10] S. Ahmed et al., "A survey on network anomaly detection techniques," Journal of Information Security and Applications, vol. 58, 2021.
[11] M. Usman et al., "A survey of distributed denial-of-service attacks," IEEE Access, vol. 9, pp. 1-15, 2021.
[12] D. Kreutz et al., "Software-defined networking: A comprehensive survey," Proceedings of the IEEE, vol. 103, no. 1, 2020.
[13] N. Zarca et al., "Security management architecture for NFV/SDN-aware IoT systems," IEEE Internet of Things Journal, vol. 7, no. 10, pp. 1-12, 2020.
[14] MikroTik, "RouterOS: Firewall Filter," MikroTik Documentation, 2024. [En línea]. Disponible en: https://help.mikrotik.com/docs/display/ROS/Filter [Accedido: 11-mayo-2026].
[15] MikroTik, "Firewall and NAT," MikroTik Documentation, 2023. [En línea]. Disponible en: https://help.mikrotik.com/docs/display/ROS/NAT [Accedido: 11-mayo-2026].