

PROYECTO DE TITULACIÓN

Carrera de Ingeniería en Tecnologías de la Información

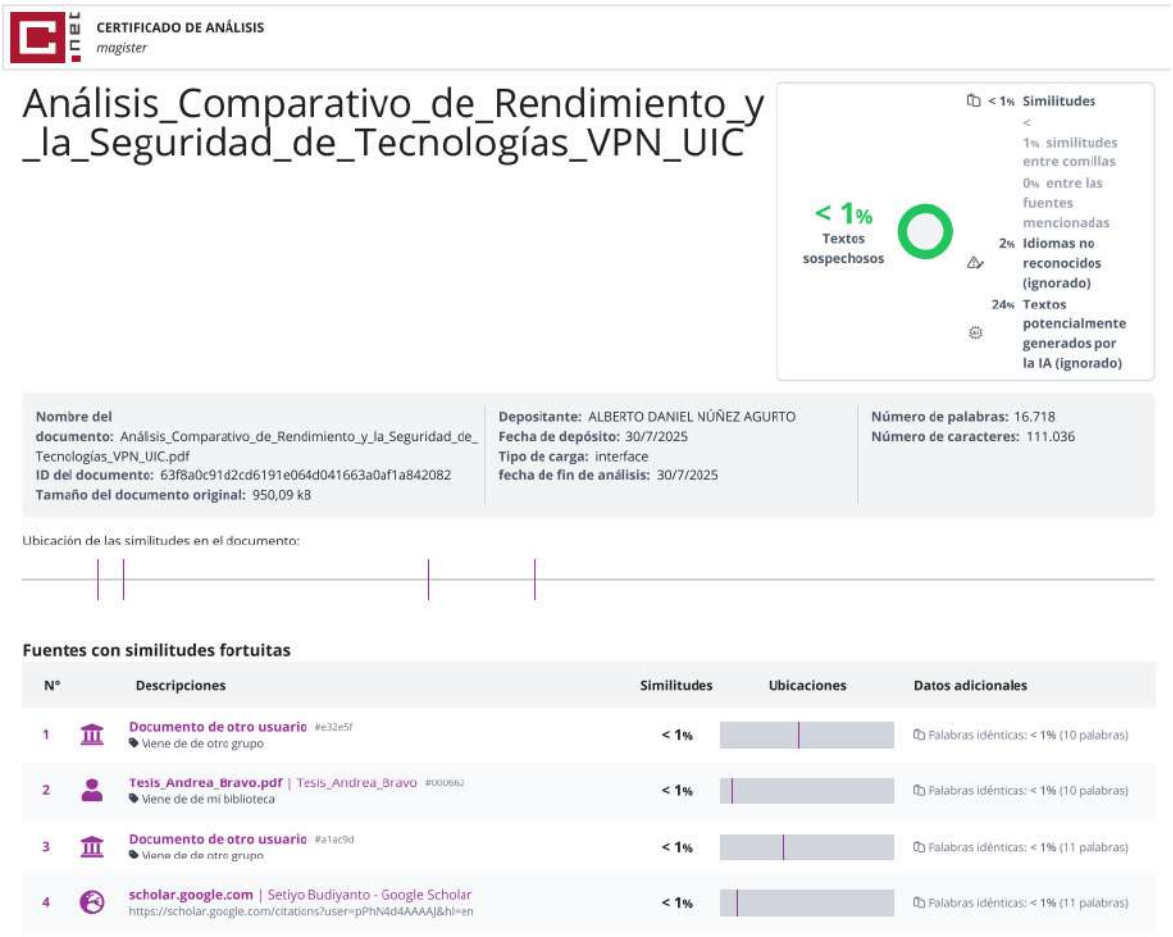
TEMA: Análisis Comparativo del Rendimiento y la Seguridad de Tecnologías VPN.

AUTOR: Floril Condemaita, Jonathan Steven

TUTOR: Ing. Núñez Agurto, Alberto Daniel, PhD.

Santo Domingo de los Tsáchilas, 14 de agosto del 2025

Reporte de verificación de contenido



CERTIFICADO DE ANÁLISIS
magister

Análisis_Comparativo_de_Rendimiento_y_la_Seguridad_de_Tecnologías_VPN_UIC

< 1% Similitudes
< 1% similitudes entre comillas
0% entre las fuentes mencionadas
2% Idiomas no reconocidos (ignorado)
24% Textos potencialmente generados por la IA (ignorado)

< 1% Textos sospechosos

Nombre del documento: Análisis_Comparativo_de_Rendimiento_y_la_Seguridad_de_Tecnologías_VPN_UIC.pdf
ID del documento: 63f8a0c91d2cd6191e064d041663a0af1a842082
Tamaño del documento original: 950,09 kB

Depositante: ALBERTO DANIEL NÚÑEZ AGURTO
Fecha de depósito: 30/7/2025
Tipo de carga: interface
fecha de fin de análisis: 30/7/2025

Número de palabras: 16.718
Número de caracteres: 111.036

Ubicación de las similitudes en el documento:

Fuentes con similitudes fortuitas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	Documento de otro usuario #e32e5f Viene de de otro grupo	< 1%		Palabras idénticas: < 1% (10 palabras)
2	Tesis_Andrea_Bravo.pdf | Tesis_Andrea_Bravo #000662 Viene de de mi biblioteca	< 1%		Palabras idénticas: < 1% (10 palabras)
3	Documento de otro usuario #a1ac9d Viene de de otro grupo	< 1%		Palabras idénticas: < 1% (11 palabras)
4	scholar.google.com | Setiyo Budiyanto - Google Scholar https://scholar.google.com/citations?user=pPhN4d4AAAAJ&hl=en	< 1%		Palabras idénticas: < 1% (11 palabras)

Firma

Firmado electrónicamente por:
ALBERTO DANIEL
NUNEZ AGURTO
Validar únicamente con FirmaEC

_____

Ing. Núñez Aguirre, Alberto Daniel, PhD.
C. C.: 1716527458

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Certificación

Certifico que el trabajo de integración curricular: **"Análisis comparativo del rendimiento y la seguridad de tecnologías VPN"** fue realizado por el señor **Floril Condemaita Jonathan Steven**, el mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE. Además, fue revisado y analizado en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se lo sustente públicamente.

Santo Domingo, 14 de agosto de 2025

Firma

Firmado electrónicamente por:
ALBERTO DANIEL
NUNEZ AGURTO
Validar únicamente con FirmaEC

_____-

Ing. Núñez Aguirre, Alberto Daniel, PhD.
C. C.: 1716527458

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Responsabilidad de Autoría

Yo, **Floril Condemaita Jonathan Steven**, con cédula de ciudadanía n.° 1722919451, declaro que el contenido, ideas y criterios del trabajo de integración curricular: **Análisis comparativo del rendimiento y la seguridad de tecnologías** VPN es de mi autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Santo Domingo, 14 de agosto de 2025

Firma

Floril Condemaita Jonathan Steven
C. C.: 1722919451

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Autorización de Publicación

Yo, **Floril Condemaita Jonathan Steven**, con cédula de ciudadanía n.º 1722919451, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de integración curricular: **Análisis comparativo del rendimiento y la seguridad de tecnologías VPN** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Santo Domingo, 14 de agosto de 2025

Firma



Floril Condemaita Jonathan Steven
C. C.: 1722919451

DEDICATORIA

Este trabajo de integración curricular esta dedicado a mi esposa Melany, mis abuelos Humberto y Celia y mis padres Erika y Samuel, todos han sido un pilar indispensable de motivación y perseverancia en este camino. El amor y apoyo que me han dado en todo este tiempo me ha permitido formarme como profesional y lograr las metas y objetivos que he planteado en mi vida y les agradezco por permitirme vivir este momento y los que tendre gracias al esfuerzo constante que siempre me inculcaron.

Floril Condemaita, Jonathan Steven

AGRADECIMIENTO

Quiero empezar agradeciendo a mi Padre Celestial. Desde niño me guió hacia el mejor destino que tenía preparado para mí. Reconozco que cada uno de mis logros se los debo a Él, y me siento muy feliz de que me permita vivir esta experiencia. Todo se lo debo a Él y me siento muy honrado de poder servirle a lo largo de mi vida, como hijo de Dios y como profesional.

Agradezco a cada uno de los miembros de mi familia que me acompañaron en este camino, porque desde niño me inculcaron los valores de la perseverancia, el respeto y la diligencia, los cuales me han permitido formarme y establecer los pilares más importantes de mi vida.

A mi amada esposa, quien ha sido mi motivación constante para seguir preparándome y progresar continuamente y me siento muy agradecido por la familia que hemos formado y por las metas que juntos hemos podido cumplir, además de las que tenemos planeadas para el futuro. Es infinita la gratitud y el amor que tengo por acompañarme en este camino.

A mi tutor de tesis, el doctor Daniel Núñez, quien desde que tuve la oportunidad de ser instruido por él fue un ejemplo de admiración y dedicación constante. Como tutor, me ayudó continuamente a avanzar, y agradezco la paciencia que tuvo conmigo, ya que todo ese trayecto me permitió llegar a este momento.

A mis docentes en la universidad, ya que con sus enseñanzas y ejemplo me inspiraron a autoeducarme constantemente. Gracias a ellos me he preparado y he logrado tener una noción más clara de lo que es el mundo laboral. Estoy profundamente agradecido por sus enseñanzas.

Finalmente, agradezco a mi grupo de amigos: Mishell, Bryan, Stefany, Leonardo, Fabricio, Andrea y David, quienes me motivaron y apoyaron constantemente en cada uno de los ciclos y experiencias que viví en mi trayectoria universitaria.

Floril Condemaita, Jonathan Steven

ÍNDICE

Dedicatoria I

Agradecimiento II

Resumen 1

Abstract 2

I Introducción y estado del arte 3

A Introducción 3

B Estado del arte 4

C Objetivos 9

D Alcance 10

II Marco teórico 11

A Red Privada Virtual 11

B Entorno Emulado 17

C Calidad de Servicio 19

D Métricas de Calidad de Servicio 21

E Seguridad en VPNs 23

F Herramientas de Medición 25

G Metodología PPDIOO 26

III Metodología 28

A Preparar 28

B Planificar 29

C Diseñar 30

D Implementar 31

E Operar 41

F Optimizar 44

IV Resultados 47

A Metodología de Evaluación de Rendimiento 47

B Documentación de Resultados de Pruebas - WireGuard 48

C Documentación de Resultados de Pruebas - PPTP 51

D Documentación de Resultados de Pruebas - IPsec 53

E Documentación de Resultados de Pruebas - SSTP 56

F Análisis Comparativo Integral de Rendimiento y Seguridad 59

V Conclusiones y recomendaciones 63

A Conclusiones 63

B Recomendaciones 63

C Trabajos futuros 64

Referencias bibliográficas 66

ÍNDICE DE TABLAS

I Características principales de las VPN 12

II Características técnicas de WireGuard 13

III Componentes principales de IPsec 14

IV Características operativas de SSTP 15

V Especificaciones técnicas de PPTP 17

VI Características de los entornos emulados 18

VII Mecanismos principales de QoS 20

VIII Componentes de la latencia en redes 22

IX Causas principales de pérdida de paquetes 23

X Tipos y causas del jitter en redes 24

XI Factores que afectan la gestión del bandwidth 24

XII Métricas de rendimiento medidas por iperf 26

XIII Evaluación de riesgos del proyecto 29

XIV Planificación general del proyecto 30

XV Configuración de direccionamiento IP del laboratorio 31

XVI Configuración BGP de routers en la nube 32

XVII Resultados de latencia para WireGuard 48

XVIII Resultados de ancho de banda para WireGuard 49

XIX Resultados de jitter y pérdida de paquetes para WireGuard 50

XX Resultados de latencia para PPTP 51

XXI Resultados de ancho de banda para PPTP 52

XXII Resultados de jitter y pérdida de paquetes para PPTP 52

XXIII Resultados de latencia para IPSec 54

XXIV Resultados de ancho de banda para IPSec 55

XXV Resultados de jitter y pérdida de paquetes para IPSec 55

XXVI Resultados de latencia para SSTP 57

XXVII Resultados de ancho de banda para SSTP 57

XXVIII Resultados de jitter y pérdida de paquetes para SSTP 58

XXIX Comparación de latencia entre tecnologías VPN 60

XXX Comparación de ancho de banda entre tecnologías VPN 60

XXXI Comparación de jitter y pérdida de paquetes entre tecnologías VPN 61

XXXII Ranking general de rendimiento por tecnología VPN 61

XXXIII Ranking general de seguridad por tecnología VPN 62

ÍNDICE DE FIGURAS

1 Estructura de tunelización VPN [11] 11

2 Arquitectura de WireGuard como protocolo VPN moderno [14] 13

3 Arquitectura de red SSTP 16

4 Ilustración conceptual de la protección en túneles VPN con el protocolo PPTP [21] 16

5 Ejemplo de entorno emulado utilizando GNS3 para pruebas de red [25] 19

6 Representación conceptual de Calidad de Servicio en redes [30] 21

7 Arquitectura cliente-servidor de iperf para medición de ancho de banda [40] 25

8 Metodología PPDIOO para gestión del ciclo de vida de redes [42] 27

9 Topología de red para el análisis comparativo de tecnologías VPN 31

10 Configuración BGP del router R1 32

11 Configuración de WireGuar ddel MikroTik-7 34

12 Configuración consolidada del servidor PPTP en MikroTik-7 35

13 Configuración del cliente PPTP en MikroTik-8 36

14 Configuración de servidor IPsec en MikroTik-7 38

15 Configuración del cliente IPsec en MikroTik-8 39

16 Configuración del servidor SSTP en MikroTik-7 40

17 Configuración del cliente SSTP en MikroTik-8: interfaz sstp-out1, autenticación y enrutamiento 41

18 Verificación de operación del túnel SSTP 42

19 Verificación de túnel IPsec en MikroTik-8 43

20 Verificación de túnel PPTP 44

21 Verificación de túnel WireGuard: tráfico en interfaz wg1 y respuesta al ping desde MikroTik-7 45

RESUMEN

En un contexto global donde la conectividad remota y la privacidad de los datos son pilares fundamentales para la continuidad operativa de las organizaciones, las Redes Privadas Virtuales (VPN) se posicionan como una solución tecnológica clave para establecer canales de comunicación seguros sobre redes públicas. A pesar de su extendida adopción, persiste una falta de directrices empíricas claras que orienten a los profesionales en la selección del protocolo más adecuado según las condiciones específicas de la red y los requerimientos de seguridad y rendimiento de las aplicaciones. Este estudio tuvo como objetivo principal realizar un análisis comparativo exhaustivo del rendimiento y la seguridad de cuatro tecnologías VPN ampliamente utilizadas: WireGuard, IPsec, PPTP y SSTP. Para cumplir con este propósito, se diseñó e implementó un entorno de emulación controlado y replicable utilizando la plataforma GNS3 y el sistema operativo MikroTik RouterOS. En este escenario, se configuraron túneles sitio a sitio para cada protocolo, sobre los cuales se ejecutaron pruebas estandarizadas para evaluar métricas de rendimiento como la latencia, el jitter, la pérdida de paquetes y el ancho de banda efectivo. Para la recolección de datos se emplearon herramientas especializadas como ping e iperf3, mientras que el análisis de seguridad se centró en la robustez de los algoritmos de cifrado, los mecanismos de autenticación y la integridad de los datos de cada tecnología. Los resultados cuantitativos revelaron diferencias significativas de rendimiento. IPsec demostró ser la tecnología más fiable para aplicaciones sensibles al tiempo, como VoIP y videoconferencias, al presentar la menor latencia y el jitter más bajo. WireGuard destacó por su notable eficiencia y simplicidad, ofreciendo un rendimiento sólido con una menor sobrecarga y empleando criptografía de última generación. Por su parte, SSTP, aunque capaz de alcanzar un alto ancho de banda, lo hizo a costa de una mayor latencia. Se confirmó, además, que PPTP no solo presenta el rendimiento más bajo, sino también vulnerabilidades de seguridad documentadas que lo hacen inadecuado para entornos modernos. Este trabajo constituye una guía de referencia técnica para administradores de red y responsables de seguridad, demostrando que la elección de una VPN debe ser una decisión estratégica. Se recomienda priorizar IPsec para la máxima fiabilidad en tiempo real y WireGuard para un balance óptimo de eficiencia y seguridad, mientras se desaconseja categóricamente el uso de PPTP.

Palabras clave: VPN, Mikrotik, seguridad de redes, rendimiento de redes.

ABSTRACT

In a global context where remote connectivity and data privacy are fundamental pillars for business continuity, Virtual Private Networks (VPNs) serve as a critical technology to establish secure communication channels over public networks. Despite their widespread adoption, there remains a notable lack of clear empirical guidelines to direct professionals in selecting the most suitable protocol based on specific network conditions and application-level security and performance requirements. The primary objective of this study was to conduct a comprehensive comparative analysis of the performance and security of four widely used VPN technologies: WireGuard, IPsec, PPTP, and SSTP. To this end, a controlled and replicable emulation environment was designed and implemented using the GNS3 platform and the MikroTik RouterOS. In this scenario, site-to-site tunnels were configured for each protocol, upon which standardized tests were conducted to evaluate performance metrics such as latency, jitter, packet loss, and effective bandwidth. Specialized tools, including ping and iperf3, were used for data collection, while the security analysis focused on the robustness of each technology's encryption algorithms, authentication mechanisms, and data integrity. The quantitative results revealed significant performance differences. IPsec proved to be the most reliable technology for time-sensitive applications, such as VoIP and video conferencing, by exhibiting the lowest latency and minimal jitter. WireGuard was distinguished by its notable efficiency and simplicity, offering solid performance with lower overhead while employing state-of-the-art cryptography. Conversely, SSTP, while capable of achieving high bandwidth, did so at the cost of higher latency. Furthermore, it was confirmed that PPTP not only exhibits the lowest performance but also possesses documented security vulnerabilities, rendering it unsuitable for modern environments. This work serves as a technical reference guide for network administrators and security officers, demonstrating that VPN selection must be a strategic decision. It is recommended to prioritize IPsec for maximum real-time reliability and WireGuard for an optimal balance of efficiency and security, while the use of PPTP is a categorically discouraged.

Keywords: VPN, Mikrotik, network security, network performance.

I. Introducción y estado del arte

A. *Introducción*

La conectividad y el intercambio de información han pasado a formar parte de los elementos esenciales para el buen funcionamiento de las empresas en la actualidad. Con la llegada del trabajo a distancia y la necesidad de la conexión entre las distintas oficinas, las organizaciones se han visto obligadas a sustituir sistemas de comunicación convencionales tipo punto a punto por sistemas más versátiles, escalables y seguros[1]. Las VPN son una de las tecnologías pioneras que permiten realizar conexiones fiables a través de redes públicas como la Internet, garantizando la confidencialidad, integridad y disponibilidad de los datos transmitidos.

A medida que las amenazas cibernéticas se hacen más complejas y la demanda de rendimiento en las comunicaciones aumenta, las organizaciones tienen que enfrentarse como reto a la selección de la tecnología VPN más idónea, la cuál permite satisfacer adecuadamente las necesarias en base a sus requerimientos para su propio servicio. Las diferentes implementaciones como son IPSec (Internet Protocol Security), SSL/TLS (Secure Sockets Layer / Transport Layer Security), L2TP (Layer 2 Tunneling Protocol) y OpenVPN (una aplicación de código abierto que implementa técnicas VPN con soporte para múltiples protocolos) ofrecen diferentes propiedades de acuerdo a sus propias características de seguridad, rendimiento, facilidad de implementación y compatibilidad con diversas plataformas. Sin embargo, la mayoría de ellas presenta un comportamiento variante bajo diferentes condiciones de red, tipos de tráfico y escenarios de uso. [2]

La selección de una inapropiada tecnología VPN puede producir las vulnerabilidades relativas a la seguridad, la degradación del rendimiento de las aplicaciones de misión crítica o las dificultades operativas que afectan la productividad de los usuarios; de ahí que sean imprescindibles las pruebas comparativas que analicen el comportamiento de las diferentes tecnologías en condiciones controladas y representativas de las realidades que representan los posibles entornos de producción. Estas pruebas tienen que tener en cuenta el comportamiento en términos no solo de seguridad, sino también el comportamiento en términos de rendimiento (latencia, ancho de banda, consumo de recursos y eficiencia de la transmisión de información).

Este estudio busca realizar un análisis comparativo sistemático de las principales tecno-

logías VPN disponibles, para esto se utiliza entornos de emulación controlados que permitan medir los parámetros de rendimiento y seguridad mediante métricas precisas. Los resultados de este trabajo irán orientados a proporcionar la información suficiente para que las organizaciones elijan la solución VPN más adecuada en base a sus requerimientos y conseguir así optimizar las infraestructuras de las comunicaciones, proteger los activos de información en un contexto en el que no paran de ir en aumento las amenazas cibernéticas.

B. Estado del arte

Es de vital importancia establecer la necesidad de llevar a cabo la revisión, siendo el principal hecho que requiere de la identificación de la problemática del proyecto relacionada con el análisis comparativo de rendimiento y seguridad de las tecnologías VPN, para tener acceso a toda la bibliografía dedicada y subrayar de esta forma determinados aspectos que cobran relevancia para el proyecto.

Los criterios de inclusión utilizados para la búsqueda de artículos relacionados con la investigación son los siguientes::

- Trabajos relacionados con análisis comparativos de tecnologías VPN
- Investigaciones que evalúen parámetros de rendimiento y/o seguridad en protocolos VPN
- Investigaciones publicadas de hasta 5 años de antiguedad

Por otro lado, los criterios de exclusión propuestos son:

- Artículos que se enfoquen únicamente en aspectos comerciales de soluciones VPN
- Estudios que no proporcionen datos cuantitativos sobre el rendimiento o seguridad
- Investigaciones que no esten escritas en inglés.

Para la búsqueda de toda la información relacionada con nuestra investigación se revisaron documentos, revistas científicas, actas de congresos, tesis doctorales y de máster. Para ello se emplearon bases de datos como: IEEE Xplore y Scopus y teniendo la siguiente cadena de búsqueda:

((VPN OR virtual private network OR OpenVPN OR IPSec OR WireGuard OR L2TP OR SSL VPN OR GRE) AND (performance OR security OR calidad de servicio OR QoS OR benchmark OR comparative OR comparison OR analysis OR evaluation) AND (throughput

OR latency OR jitter OR packet loss OR bandwidth OR encryption OR authentication OR vulnerability))

A la hora de aplicar dichas estrategias de búsqueda se detectaron de forma inicial 37 estudios potencialmente relevantes que acabaron reduciéndose a 8 artículos que llegaron a cumplir con los criterios de inclusión y exclusión consideración. Los artículos seleccionados fueron de idiomas inglés, español y polaco, además, estos estudios comparativos entre diversos protocolos de VPN mediante el uso de diferentes métricas de evaluación son la base para el estado del arte de la presente investigación.

1. Elaboración del estado del arte

EP1. "Comparative Analysis of Site-to-Site Layer 2 Virtual Private Networks" En su investigación, Aung y Thein [1] utilizaron un entorno emulado con RouterOS para comparar diferentes tecnologías VPN de capa dos a través de la comparación de PPTP, L2TP, OpenVPN, EoIP y MPLS/VPLS, a esto se le añadió un exhaustivo control a través como *iPerf* y *Wireshark*, y mediante diferentes pruebas como retardos, jitter o pérdidas llegaron a las conclusiones de que el protocolo tiene influencia tanto en la eficacia del transporte como en la seguridad, aunque su revisión estaba centrada en la capa dos, la idea de fondo les sirvió para situar los valores de tecnologías más actuales como pueden ser IPsec, OpenVPN y WireGuard. Siguiendo la misma línea de trabajo, el presente artículo da continuidad a dicho enfoque, que si bien toma de referencia otra topología emitida a partir de routers MikroTik, también expone situaciones de trabajo supervisadas a partir de las diferentes tecnologías VPN de capa tres, para la supervisión de la latencia, el ancho de banda o la eficiencia del tráfico se combinará *iPerf* y *Wireshark*, todo ello como fundamento para unir el rendimiento, el cifrado o la privacidad correspondiente.

EP2. "Comparative Analysis of VPN Protocols at Layer 2 Focusing on Voice Over Internet Protocol" Budiyanto y Gunawan [2] llevaron a cabo una investigación que consistía en una comparativa de protocolos VPN en la capa dos que se podía aplicar directamente a la tecnología VoIP, para ello realizaron un diseño de laboratorio en el que se incluyeron 1 servidor VoIP, 3 routers, 3 switches y algunos host además de 4 tipos de tunelización diferentes: GRE+IPSec, IPIP-SIP based, L2TP+IPSec y por último SSL VPN. Y por otro lado, para verificar el rendimiento se tomaron en consideración los valores a nivel de calidad del servicio como latencia, jitter, tasa de pérdida de paquetes y throughput, incluyendo herramientas como *Wireshark*

para la captura de información correspondiente. Los resultados mostraron que el protocolo SSL VPN presentaba el mejor rendimiento global en comparación de todos los protocolos, marcando una latencia media de 9.574 ms, 9.671 ms de jitter, 154.61 Kbps de throughput y 0% de tasa de pérdida de paquetes, teniendo en cuenta así la estandarización de ITU-T G.1010, y similar a nuestro trabajo investigativo nos deja como principal principio la importancia de la elección del protocolo VPN con respecto a la implementación que se vaya a llevar a cabo y como dato final, indicando que la seguridad que habilita IPSec puede dañar el rendimiento debido a la carga adicional que se requiere en la encriptación.

EP3.“Comparison of VPN Protocols at Network Layer Focusing on Wire Guard Protocol” Abdulazeez et al. [3] se ocuparon del análisis llevándose a cabo un importante trabajo de revisión sobre los protocolos VPN descritos dentro de los más utilizados a nivel de los de la capa de red, utilizando cada uno de los protocolos VPN conocidos como IPsec, GRE o WireGuard, realizando una comparación basada tanto en el rendimiento, en la seguridad y las características operacionales o de funcionamiento de cada uno de ellos. El resultado fue el establecimiento de WireGuard como un protocolo VPN superior, con un menor rendimiento para menos líneas de código (4.000 líneas para WireGuard frente a las 70.000 líneas necesarias para IPsec), mejor rendimiento y menor complejidad de su puesta en marcha. De esta forma, los autores también presentaron las desventajas que presenta IPsec como el obtener excelente seguridad a partir de sus protocolos AH o ESP, pero con penalizaciones importantes en el rendimiento frente a la menor complejidad por su puesta en marcha. Este trabajo sitúa a GRE como un protocolo rápido, pero que presenta notables carencias de características de seguridad como el cifrado nativo; mientras que WireGuard se alza como el protocolo más equilibrado, con un buen diseño que presenta un bajo coste computacional, cifrado fuerte y caracterizado por su elevada velocidad (ChaCha20/Poly1305). En este trabajo, el excelente resultado hace necesario definir cómo evaluar no sólo la seguridad sino el rendimiento, además de la seguridad de las distintas tecnologías VPN utilizadas dentro de entornos controlados, utilizando así toda la información como un marco de referencia para llevar a cabo las comparaciones entre distintas tecnologías, tal y como es en el caso del presente trabajo, donde se determinarían los niveles de eficiencia de cada una de las tecnologías VPN analizadas desde el punto de vista del uso.

EP4. “Virtual Private Networks (VPN): A Conceptual Review of Security Protocols and Their Application in Modern Networks” Akinsanya, Ekechi, y Okeke [4] hacen un

exhaustivo análisis de los protocolos de seguridad de las VPNs y su utilización en las redes de hoy. El estudio se extiende desde el planteamiento clásico de IPSec y SSL/TLS hasta las aproximaciones modernas de WireGuard e QUIC. Los autores desarrollan un análisis de cada protocolo siguiendo diversas dimensiones como las propiedades de seguridad, el rendimiento o la adecuación de cada protocolo a diferentes tipos de uso, lo que establece unas bases adecuadas para entender las tecnologías VPN actuales. Aunque el enfoque es más bien conceptual y teórico, se convierte en un primer punto de apoyo para entender cómo los diferentes protocolos de seguridad afectan al rendimiento y la seguridad de las implementaciones VPNs, planteando en este sentido una perspectiva complementaria a las visiones más empíricas que tratan de realizar comparativas entre estas tecnologías. En el trabajo se pone de manifiesto también lo importante que es elegir el protocolo correcto en función de las necesidades de cada implementación, un aspecto clave en toda comparación del rendimiento de las VPNs.

EP5. "A Comparative Study on Virtual Private Networks for Future Industrial Communication Systems" En su investigación, Lackorzynski et al. [5] llevaron a cabo una exhaustiva experiencia comparativa de determinadas tecnologías VPN (OpenVPN, IPsec, Tinc, Freelan, SSH VPN, MACsec y WireGuard) centrada en los futuros escenarios industriales. A través de cinco plataformas de hardware diferentes, desde dispositivos embebidos con recursos reducidos hasta servidores potentes, realizaron una medición exhaustiva del rendimiento en términos de calidad de servicio, a través de las métricas throughput y latencia, utilizando herramientas como iperf3 y ping. Los resultados demostraron que las soluciones más actuales como MACsec y WireGuard superan ampliamente a las tecnologías VPN establecidas como OpenVPN e IPsec. Mientras que MACsec demostró viable consistentemente la latencia más baja, WireGuard alcanzó el mayor throughput en la mayoría de las plataformas. Esta investigación es de particular interés para la investigación, ya que sigue una metodología similar para medir rendimiento y seguridad en situaciones controladas, aunque en la presente investigación nos concentramos exclusivamente en OpenVPN, IPsec y WireGuard bajo determinados patrones de tráfico y configuraciones de red.

EP6. "Performance Comparison of VPN Solutions" En su trabajo, Osswald, Haeberle y Menth [6] efectúan un análisis exhaustivo del rendimiento de OpenVPN, IPsec y WireGuard, las tres soluciones de VPN por ellos estudiadas. En la configuración experimental de los autores, se utilizaban dos servidores virtuales conectados por un interfaz de 10 Gb/s, en ejecución de Ubuntu 18.04 (kernel Linux 5.3.5). En su trabajo, los autores midieron el rendimiento de la

red y el tiempo de ping, el conteo de retransmisiones del tráfico TCP con fijación de CPU y sin fijación de CPU. En lo que respecta a IPsec se són analizadas todas las combinaciones de protocolos y modos, acompañadas de una selección de algoritmos criptográficos, mientras que la solución OpenVPN es evaluada a partir de la selección de diferentes suites de cifrado y diversos métodos de optimización.En particular, los resultados mostraron que las versiones de IPsec con cifrado AES acelerado por hardware fueron significativamente superiores a WireGuard sin fijación de CPU. De este modo, IPsec alcanzó aproximadamente 3.7 Gb/s en comparación con los 3.2 Gb/s de WireGuard. Sin embargo, WireGuard, en el caso de fijación de CPU, también había logrado incrementar su rendimiento aproximadamente un 40% hasta 4.5 Gb/s. Por otro lado, IPsec, así como OpenVPN vieron disminuida su capacidad con la fijación de CPU debido a que el turbo boost estaba desactivado. OpenVPN mostró la peor capacidad en todas las configuraciones probadas, no llegando a los 0.9 Gb/s ni aun con optimizaciones. El trabajo concluye que IPsec con cifrado AES es una maravillosa opción para entornos virtualizados sin fijación de CPU, mientras que WireGuard llegaba a superar el rendimiento de IPsec aproximadamente un 30% en entornos que no están virtualizados. Este trabajo legitima la metodología de nuestro estudio al demostrar la importancia que tiene evaluar las soluciones VPNs en entornos controlados o estandarizados y medir métricas específicas del rendimiento, además de brindar valores de referencia para realizar comparaciones entre tecnologías VPNs modernas.

EP7. “Comparative calidad de servicio Analysis of VPN Protocols on IPv6” En su trabajo de investigacion, Oktavia et al. [7] llevaron a cabo un análisis comparativo del rendimiento de los protocolos VPN WireGuard y L2TP/IPSec sobre IPv6 y los parámetros de calidad de servicio (QoS) característicos como la latencia, jitter, cantidad de paquetes perdidos, el rendimiento y el Mean Opinion Score (MOS): ejecutaron tres pruebas de rendimiento distintas (ipPerf3, transferencia de archivos FTP y escritorio remoto) en un entorno de emulación controlada usando routers Mikrotik y un túnel 6to4. Los resultados mostraron que el protocolo L2TP/IPSec es superior al de WireGuard para las pruebas de FTP y el escritorio remoto, partiendo de conclusiones que indicaban dicha circunstancia, así como también el protocolo WireGuard sólo mostraba ventajas para la transferencia de documentos. Sus resultados son una evidencia valiosa para la selección del protocolo VPN en función del rendimiento, desde la base de esta referencia, en esta investigación actual deseamos analizar estos protocolos de VPN junto al protocolo OpenVPN en condiciones de red diferentes con el fin de generar recomendaciones

más completas sobre configuraciones óptimas.

EP8. "Full-mesh VPN performance evaluation for a secure edge-cloud continuum" Kjorveziroski et al. [8] hacen una revisión completa del rendimiento de tres soluciones VPN de malla completa (Headscale, Netbird y ZeroTier) para su posible uso como red de infraestructura en clústeres de Kubernetes distribuidos. Para ello, los autores definieron un marco de criterios esenciales y opcionales que deberán cumplir las soluciones de VPN antes de ser usadas para interconectar nodos de cómputo geográficamente dispersos. El análisis consisitió en exhaustivas pruebas de rendimiento de throughput TCP y UDP site-to-site, así como de los tiempos de respuesta de la API de Kubernetes, bajo diferentes escenarios, incluso uno en el que la red era adversa (pérdidas de paquetes 1%, 5%, 10% o retardos de paquetes 50m, 250s, 350ms). Los resultados indicaron que Netbird, concretamente su implementación en el kernel de Wireguard, fue el que mejor rendimiento aportó con red estable: alcanzó los 707.45 Mbps en las pruebas TCP, mientras que Headscale y ZeroTier alcanzaron los 304.01 Mbps y 303.01 Mbps, respectivamente. Sin embargo, con la introducción de la pérdida de paquetes, tanto Headscale como ZeroTier superan en gran medido a Netbird, gracias a sus capacidades de retransmisión de TCP, muy marcado en escenarios con 10% de pérdida, donde Headscale y ZeroTier consiguieron rendimientos de 8.84 y 8.26 Mbps, respectivamente, comparado con los 2.49 Mbps de Netbird. Este trabajo presenta una evaluación práctica y sistemática de modernas tecnologías de VPN en entornos de orquestación de contenedores estableciendo un precedente metodológico útil para nuestra investigaciones en el análisis comparativo del rendimiento y la seguridad de las tecnologías de VPN.

C. Objetivos

1. Objetivo General

Realizar un análisis comparativo del rendimiento y la seguridad de tecnologías VPN.

2. Objetivos Específicos

- Determinar los principales tecnologías de VPNs y los trabajos relacionados en protocolos de encapsulación en el ámbito corporativo.
- Diseñar y configurar escenarios de red utilizando VPN en un entorno de emulación controlado, midiendo parámetros clave de rendimiento bajo distintas condiciones.

- Analizar y comparar los resultados obtenidos en términos de latencia, ancho de banda, tasa de transferencia y eficiencia del tráfico.

D. Alcance

El presente estudio se centra en la comparación del rendimiento y la seguridad de cuatro tecnologías de redes privadas virtuales: WireGuard, SSTP (Secure Socket Tunneling Protocol), PPTP (Point-to-Point Tunneling Protocol) e IPsec, aplicadas en un escenario de emulación controlado diseñado para simular túneles site-to-site con enlaces punto a punto. La investigación se limita a pruebas realizadas bajo condiciones de red definidas, utilizando herramientas estándar como ping e iperf3. Las métricas evaluadas incluyen latencia, jitter, pérdida de paquetes, ancho de banda y eficiencia del tráfico para el análisis de rendimiento, así como métodos de cifrado, autenticación e integridad de datos para el análisis de seguridad. Este trabajo se restringe a un entorno concreto determinado por los recursos disponibles en el escenario de pruebas, sin extenderse a entornos de producción reales ni a otros tipos de dispositivos como móviles o servidores físicos.

II. MARCO TEÓRICO

A. *Red Privada Virtual*

Una Red Privada Virtual es la tecnología de la red que establece la vinculación mediante un acceso automatizado y cifrado trabajando por medio de una infraestructura de red pública como el Internet, permitiendo a usuarios remotos o bien a sitios distantes un acceso seguro a la red privada de una determinada entidad [9]. Esta tecnología amplía la funcionalidad de una red privada utilizando conexiones virtuales enrutadas a través de Internet, de manera que los usuarios puedan conectarse a los recursos corporativos como si estuviesen directamente conectados a la red local de la empresa.

El concepto fundamental de una VPN radica en el establecimiento de un túnel virtual cifrado entre el dispositivo del usuario y el servidor VPN de destino. Las VPN operan mediante protocolos de tunelización que encapsulan los datos originales dentro de paquetes cifrados, los transmiten a través de la red pública y los descifran en el punto de destino [10].

1. *Características Principales de las VPN*

En la Tabla I se presentan las características fundamentales que definen el funcionamiento y los beneficios de las tecnologías VPN:

En la Fig. 1 se muestra la estructura básica de tunelización VPN, donde se puede observar cómo dos redes LAN remotas se conectan de forma segura a través de Internet mediante routers VPN que establecen un túnel cifrado entre las ubicaciones.

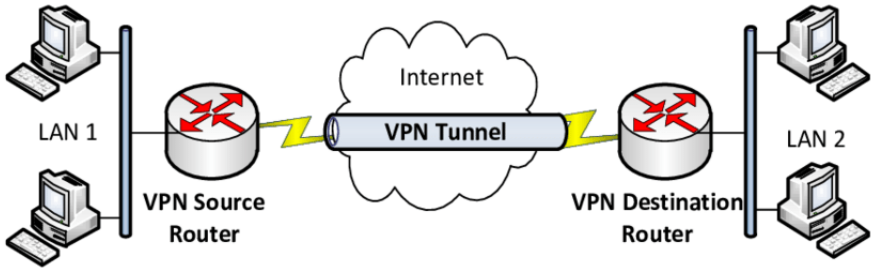


Fig. 1. Estructura de tunelización VPN [11]

2. *WireGuard*

WireGuard es un protocolo VPN moderno desarrollado por Jason A. Donenfeld que representa una nueva generación de tecnologías de túnel de red, diseñado con el objetivo de

TABLA I
CARACTERÍSTICAS PRINCIPALES DE LAS VPN

Característica	**Descripción**
Confidencialidad	Protege la información mediante cifrado robusto, impidiendo que terceros no autorizados puedan acceder o interpretar los datos transmitidos, incluso si logran interceptar el tráfico de red.
Integridad de datos	Implementa mecanismos de verificación que detectan y rechazan cualquier modificación no autorizada en los datos durante la transmisión, garantizando que la información llegue íntegra a su destino.
Autenticación	Verifica la identidad de usuarios y dispositivos antes de permitir el acceso a la red privada, utilizando credenciales, certificados digitales o autenticación multifactor.
Tunelización	Establece un canal virtual seguro que encapsula y enruta el tráfico de datos a través de redes públicas, creando una conexión punto a punto confiable.
Flexibilidad geográfica	Permite el acceso a recursos de red desde cualquier ubicación con conectividad a Internet, facilitando el trabajo remoto y la movilidad empresarial.

ser más simple, rápido y seguro que los protocolos VPN tradicionales [12]. Su desarrollo se fundamentó en principios de simplicidad y eficiencia, resultando en una implementación que utiliza aproximadamente 4,000 líneas de código.

La arquitectura criptográfica de WireGuard se fundamenta en el protocolo Noise, utilizando Curve25519 para el intercambio de claves Diffie-Hellman, ChaCha20 para cifrado simétrico y Poly1305 para autenticación de mensajes. La implementación de WireGuard en el espacio del kernel de Linux contribuye significativamente a su rendimiento superior [13].

La Figura 2 presenta la identidad visual oficial de WireGuard, destacando su posicionamiento como una solución VPN moderna, rápida y segura que representa la evolución hacia protocolos de nueva generación con arquitecturas simplificadas y criptografía de vanguardia.

TABLA II
CARACTERÍSTICAS TÉCNICAS DE WIREGUARD

Característica	Descripción
Implementación	Aproximadamente 4,000 líneas de código, significativamente menor que protocolos alternativos, facilitando auditorías de seguridad y mantenimiento.
Criptografía	Utiliza algoritmos modernos como Curve25519 para intercambio de claves, ChaCha20 para cifrado simétrico, Poly1305 para autenticación de mensajes, y BLAKE2 para funciones hash.
Rendimiento	Opera a nivel de kernel de Linux, minimizando la latencia y maximizando el throughput mediante la eliminación de transiciones innecesarias entre espacios de memoria.
Enrutamiento criptográfico	Asocia directamente claves públicas con direcciones IP específicas, simplificando la configuración y eliminando la necesidad de infraestructura compleja de gestión de direcciones.
Roaming IP	Soporta cambios transparentes de dirección IP, permitiendo que las conexiones se mantengan activas cuando los dispositivos se mueven entre diferentes redes sin requerir reconfiguración.



Fig. 2. Arquitectura de WireGuard como protocolo VPN moderno [14]

3. IPsec

IPsec representa un conjunto integral de protocolos de comunicación desarrollados por el Internet Engineering Task Force (IETF) para establecer conexiones seguras sobre redes IP [15]. El framework IPsec proporciona servicios de seguridad a nivel de capa de red, incluyendo

confidencialidad mediante cifrado, integridad y autenticación de datos, y protección contra ataques de repetición.

La arquitectura de seguridad de IPsec se basa en el concepto de Asociaciones de Seguridad (SA), que constituyen contratos de seguridad unidireccionales entre entidades comunicantes. IPsec implementa dos protocolos principales: Authentication Header (AH) que proporciona integridad y autenticación sin confidencialidad, y Encapsulating Security Payload (ESP) que ofrece confidencialidad, integridad y autenticación [16].

TABLA III
COMPONENTES PRINCIPALES DE IPSEC

Componente	**Función**
Authentication Header (AH)	Proporciona integridad de datos, autenticación del origen y protección contra ataques de repetición, sin ofrecer confidencialidad mediante cifrado.
Encapsulating Security Payload (ESP)	Ofrece confidencialidad mediante cifrado de la carga útil, además de integridad, autenticación y protección contra repetición, siendo el protocolo más utilizado en implementaciones modernas.
Internet Key Exchange (IKE)	Protocolo de gestión de claves que utiliza algoritmos Diffie-Hellman para establecer asociaciones de seguridad y negociar parámetros criptográficos entre los peers IPsec.
Security Association (SA)	Base de datos que mantiene los parámetros de seguridad acordados entre dos entidades, incluyendo algoritmos de cifrado, claves, y políticas de seguridad aplicables.
Security Policy Database (SPD)	Define las políticas de seguridad que determinan qué tráfico debe ser protegido por IPsec y qué parámetros de seguridad deben aplicarse.

SSTP es un protocolo de tunelización desarrollado por Microsoft que proporciona conectividad VPN mediante encapsulamiento de tráfico PPP sobre el protocolo HTTPS (puerto 443), utilizando SSL/TLS como canal de transporte cifrado [17]. Fue introducido como una solución segura y compatible para entornos donde otros protocolos VPN pueden ser bloqueados por firewalls estrictos o proxies.

Al aprovechar el protocolo HTTPS, SSTP permite atravesar la mayoría de firewalls y dispositivos NAT sin requerir configuraciones adicionales. Además, ofrece un alto nivel de seguridad

al implementar autenticación mutua y cifrado mediante certificados digitales, convirtiéndose en una alternativa robusta frente a protocolos más antiguos como PPTP o L2TP/IPsec [18].

TABLA IV
CARACTERÍSTICAS OPERATIVAS DE SSTP

Característica	**Descripción**
Encapsulamiento sobre HTTPS	Transmite paquetes PPP a través de túneles cifrados SSL/TLS utilizando el puerto TCP 443, facilitando la evasión de restricciones de red y firewalls.
Autenticación robusta	Utiliza certificados digitales X.509 y puede integrarse con autenticación basada en Active Directory o credenciales estándar, ofreciendo validación mutua de identidad.
Compatibilidad con firewalls	Su funcionamiento sobre HTTPS le permite atravesar firewalls estrictos y NATs sin configuraciones complejas ni necesidad de puertos especiales.
Seguridad criptográfica	Aplica cifrado fuerte mediante TLS 1.2 o superior con algoritmos como AES y SHA-2, garantizando confidencialidad, integridad y autenticación del canal de comunicación.
Integración con Windows	Soporte nativo en sistemas operativos Windows desde Vista SP1 en adelante, incluyendo clientes integrados en Windows Server, facilitando la adopción en entornos empresariales.

La Figura 3 representa una arquitectura conceptual de red VPN utilizando SSTP, donde se muestra el establecimiento de túneles seguros a través de Internet entre clientes remotos y un servidor VPN, encapsulando el tráfico sobre canales HTTPS protegidos.

4. PPTP

PPTP es uno de los protocolos VPN más antiguos, desarrollado originalmente por Microsoft como especificación para crear conexiones VPN sobre redes IP [19]. El protocolo extiende el Point-to-Point Protocol (PPP) mediante la adición de capacidades de tunelización, permitiendo que las sesiones PPP se transporten a través de redes IP utilizando Generic Routing Encapsulation (GRE).

PPTP implementa una arquitectura dual que separa las funciones de control y transporte de datos. El canal de control utiliza TCP puerto 1723, mientras que el transporte de datos utiliza

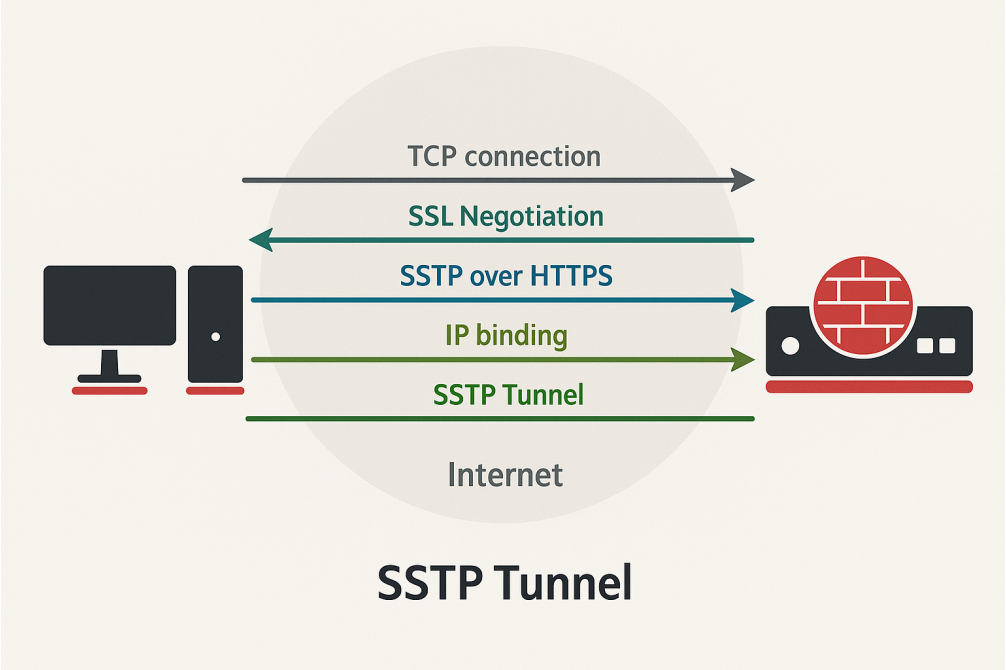


Fig. 3. Arquitectura conceptual de SSTP utilizando túneles cifrados sobre HTTPS

GRE. Sin embargo, análisis de seguridad han identificado múltiples vulnerabilidades en su diseño e implementación [20].

La Figura 4 ilustra la arquitectura básica de conexión VPN mediante protocolos PPPoE (Point-to-Point Protocol over Ethernet) o PPPoA (Point-to-Point Protocol over ATM), mostrando el establecimiento de un túnel seguro entre un cliente remoto y un servidor VPN a través de una red IP. En el diagrama se puede observar cómo el símbolo del candado representa el cifrado y la autenticación que protege la comunicación, mientras que las líneas punteadas simbolizan el túnel virtual que encapsula y protege los datos durante su transmisión a través de la infraestructura de red pública.

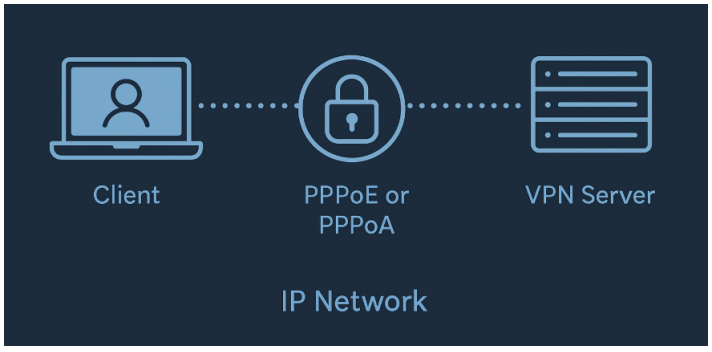


Fig. 4. Ilustración conceptual de la protección en túneles VPN con el protocolo PPTP [21]

TABLA V
ESPECIFICACIONES TÉCNICAS DE PPTP

Especificación	**Detalles**
Protocolo de transporte	Utiliza TCP puerto 1723 para control de túnel y protocolo GRE (47) para encapsulación de datos PPP a través de redes IP.
Autenticación	Soporta múltiples métodos de autenticación PPP incluyendo PAP, CHAP, MS-CHAP, y MS-CHAPv2, con compatibilidad extensa con sistemas Windows.
Cifrado	Implementa Microsoft Point-to-Point Encryption (MPPE) con claves de 40-bit y 128-bit, derivadas de las credenciales de autenticación del usuario.
Gestión de sesiones	Soporta múltiples sesiones PPP concurrentes sobre un solo túnel, con capacidades de gestión de ancho de banda y Calidad de Servicio básicas.
Compatibilidad	Amplio soporte nativo en sistemas operativos Windows, con implementaciones disponibles para Linux, macOS, y otros sistemas Unix-like.

B. Entorno Emulado

Un entorno emulado es un ambiente virtual controlado que recrea las características y comportamiento de una red de producción mediante el uso de dispositivos virtuales y técnicas de virtualización [22]. Este tipo de entorno permite evaluar el rendimiento de protocolos, aplicaciones y configuraciones de red en condiciones realistas sin requerir infraestructura física costosa.

La emulación de redes se diferencia de la simulación en que ejecuta software real de red, incluyendo sistemas operativos e implementaciones de protocolos, dentro del entorno emulado [23]. Este enfoque proporciona mayor realismo y fidelidad, permitiendo identificar comportamientos específicos del software.

1. Características de los Entornos Emulados

En la Tabla VI se presentan las características fundamentales que definen los entornos emulados:

TABLA VI
CARACTERÍSTICAS DE LOS ENTORNOS EMULADOS

Característica	Descripción
Aislamiento controlado	Proporciona un ambiente completamente aislado donde los experimentos pueden ejecutarse sin afectar sistemas de producción, garantizando la seguridad y estabilidad de la infraestructura real.
Reproducibilidad	Permite la repetición exacta de experimentos bajo las mismas condiciones, facilitando la verificación de resultados y la comparación objetiva entre diferentes configuraciones o tecnologías.
Escalabilidad virtual	Capacidad de crear topologías de red de gran escala utilizando recursos computacionales limitados, mediante técnicas de virtualización eficientes que maximizan el uso de hardware disponible.
Fidelidad realista	Ejecuta software real de dispositivos de red, incluyendo sistemas operativos y protocolos auténticos, proporcionando comportamientos idénticos a los que se observarían en entornos de producción.
Control de parámetros	Ofrece control granular sobre condiciones de red como latencia, ancho de banda, pérdida de paquetes y jitter, permitiendo evaluar el rendimiento bajo diversos escenarios de red predefinidos.

2. GNS3 (Graphical Network Simulator-3)

GNS3 es un emulador de software de red de código abierto concebido para permitir la interconexión de dispositivos virtuales y físicos en la simulación de redes complejas. GNS3 no es un simulador, de hecho, utiliza técnicas de emulación que ejecutan software de dispositivos de red que son reales, proporcionando así un entorno de pruebas realista para la investigación y evaluación de protocolos de red.

La arquitectura de GNS3 se basa en el emulador Dynamips, que permite la ejecución de imágenes reales de Cisco IOS. GNS3 ha evolucionado para soportar múltiples tecnologías de virtualización incluyendo QEMU, VirtualBox, y VMware [24].

En la Fig. 5 se muestra un ejemplo práctico de entorno emulado implementado en GNS3, donde se observa una topología básica con dispositivos virtuales interconectados que incluye un router central y dos estaciones de trabajo virtuales ejecutando VPCS (Virtual PC Simulator).

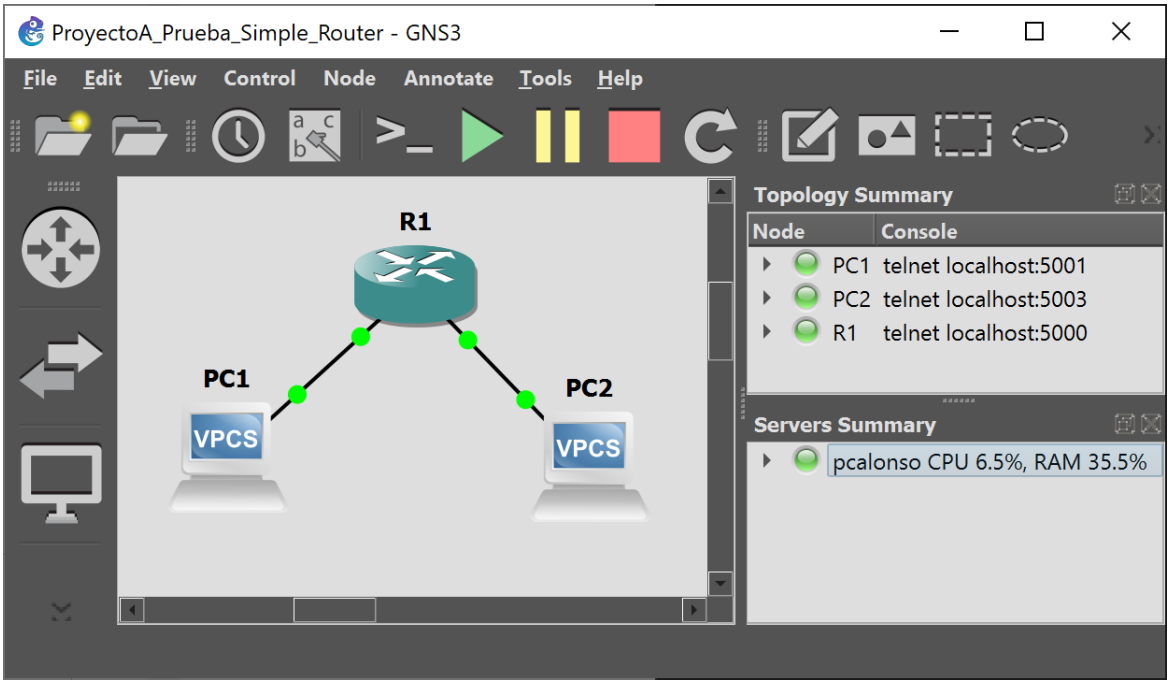


Fig. 5. Ejemplo de entorno emulado utilizando GNS3 para pruebas de red [25]

3. *MikroTik RouterOS*

MikroTik RouterOS constituye un sistema operativo de red que se basa en el kernel de Linux, pero que tiene como fin servir más que nada para la gestión avanzada de enrutamiento, firewall y control de ancho de banda [26]. RouterOS permite convertir hardware común en dispositivos de red funcionales.

RouterOS incorpora protocolos de enrutamiento dinámico como OSPF, BGP, RIP, junto con capacidades de gestión de VPN utilizando múltiples protocolos como PPTP, L2TP/IPsec, OpenVPN y SSTP. Esta versatilidad lo convierte en una plataforma ideal para experimentación en redes [27].

C. *Calidad de Servicio*

Calidad de Servicio (QoS) se define como la descripción o medición del rendimiento general de un servicio de red, particularmente el rendimiento visto por los usuarios [28]. En redes de comunicación, QoS se refiere a mecanismos de priorización de tráfico y control de reserva de recursos, considerando aspectos como pérdida de paquetes, velocidad de bits, throughput, retardo de transmisión, disponibilidad y jitter.

En el contexto de redes VPN, el análisis cuantitativo de QoS ofrece información crítica sobre la capacidad de las redes privadas virtuales para transmitir tráfico multimedia en tiempo real mientras protegen la información [29].

1. Mecanismos y Técnicas de Calidad de Servicio

La Tabla VII presenta los principales mecanismos utilizados en la implementación de Calidad de Servicio:

TABLA VII
MECANISMOS PRINCIPALES DE Calidad de Servicio

Mecanismo	**Descripción**
Clasificación y marcado	Identificación y categorización del tráfico de red basado en criterios específicos como tipo de aplicación, origen, destino o acuerdos de nivel de servicio, seguido del marcado con niveles de prioridad apropiados.
Gestión de congestión	Técnicas que previenen la congestión de red y aseguran la asignación justa de ancho de banda entre flujos competidores mediante algoritmos y mecanismos de cola durante períodos de alta utilización de red.
Control de tráfico	Regulación del flujo de paquetes utilizando técnicas como traffic shaping y traffic policing para asignar ancho de banda suficiente a aplicaciones esenciales mientras limita el ancho de banda para servicios menos críticos.
Asignación de ancho de banda	Reserva de capacidad y manejo de asignación a flujos específicos en el tráfico de red, garantizando que aplicaciones críticas tengan acceso prioritario a los recursos necesarios.
Gestión de colas	Implementación de algoritmos de cola como Weighted Fair Queuing (WFQ), Priority Queuing (PQ) y Class-Based Weighted Fair Queuing (CBWFQ) para controlar el orden de transmisión de paquetes.

La Figura 6 ilustra conceptualmente la implementación de Calidad de Servicio (QoS) en un entorno de red que utiliza equipos MikroTik con protocolos VPN WireGuard e IPsec. El diagrama muestra cómo diferentes tipos de tráfico (VoIP, transferencia de archivos y videoconferencias) son clasificados y priorizados según una tabla de prioridades, donde VoIP recibe la máxima prioridad, seguido de transferencia de archivos y videoconferencias.

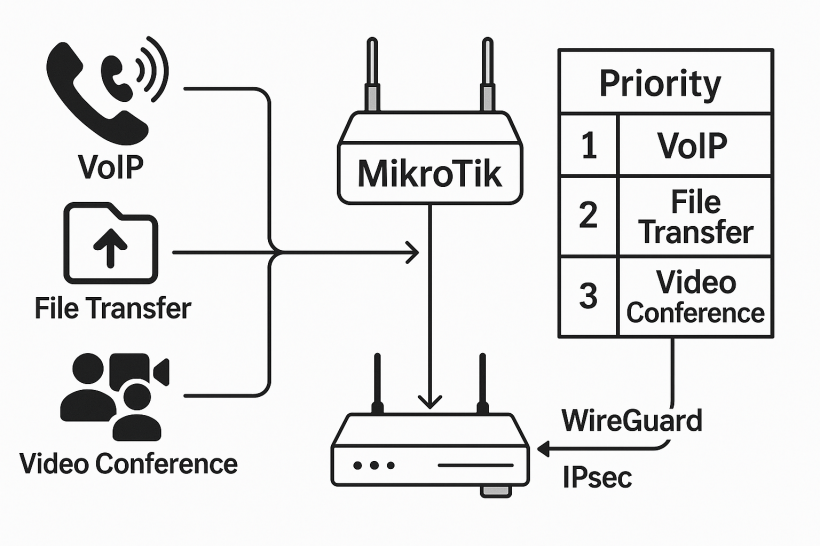


Fig. 6. Representación conceptual de Calidad de Servicio en redes [30]

D. Métricas de Calidad de Servicio

Las métricas de Calidad de Servicio constituyen los indicadores cuantitativos fundamentales para evaluar el rendimiento de las redes de comunicación. Estas métricas proporcionan una base objetiva para la comparación entre diferentes tecnologías, protocolos y configuraciones de red, siendo esenciales para la evaluación de sistemas VPN.

1. Latencia

La latencia se define como el tiempo que transcurre desde que un paquete de datos es transmitido desde un nodo origen hasta que es recibido por el nodo destino [31]. En redes VPN, la latencia adquiere particular relevancia debido a los procesos adicionales de cifrado, autenticación y encapsulación que deben realizarse en los endpoints del túnel.

El Round Trip Time (RTT) mide el tiempo tomado por un paquete para viajar desde el emisor hasta el receptor y de vuelta, constituyendo la métrica específica utilizada para medir la latencia de red [32].

2. Pérdida de Paquetes

La pérdida de paquetes se define como la ocurrencia de uno o más paquetes que atraviesan una red y son descartados antes de alcanzar su destino [33]. En redes VPN, la pérdida de paquetes presenta desafíos particulares debido a la complejidad adicional introducida por los procesos de

TABLA VIII
COMPONENTES DE LA LATENCIA EN REDES

Componente	Descripción
Retardo de propagación	Tiempo requerido para que una señal eléctrica u óptica viaje a través del medio físico de transmisión, determinado por la distancia física y la velocidad de propagación en el medio específico.
Retardo de procesamiento	Tiempo consumido por dispositivos de red como routers y switches para procesar cabeceras de paquetes, tomar decisiones de enrutamiento y realizar verificaciones de integridad.
Retardo de cola	Tiempo que un paquete permanece en buffers de dispositivos de red esperando ser procesado o transmitido, influenciado por la congestión de red y las políticas de gestión de colas.
Overhead criptográfico	Tiempo adicional requerido para realizar operaciones de cifrado, descifrado, autenticación y verificación de integridad en protocolos VPN, variable según el algoritmo utilizado.
Tiempo de respuesta del servidor	Tiempo requerido por el servidor para procesar una solicitud y generar una respuesta, incluyendo acceso a bases de datos, procesamiento de aplicaciones y generación de contenido.

encapsulación y cifrado.

La pérdida de paquetes resulta fundamentalmente de la congestión de red y el desbordamiento de buffers en dispositivos de red [34].

3. Jitter

El jitter se define como la fluctuación en el tiempo de retardo entre cuando una señal es transmitida y cuando es recibida, midiendo la variabilidad en los tiempos de llegada de los paquetes de datos [35]. Este fenómeno es crítico para aplicaciones en tiempo real, ya que representa las irregularidades en la temporización de entrega de paquetes que pueden causar distorsiones significativas en servicios de voz y video.

El jitter se caracteriza por ser la variación en el retardo de red, generalmente computado como la variación del retardo unidireccional para dos paquetes consecutivos [36].

TABLA IX
CAUSAS PRINCIPALES DE PÉRDIDA DE PAQUETES

Causa	Descripción
Desbordamiento de buffer	Ocurre cuando los buffers de dispositivos de red alcanzan su capacidad máxima debido a tráfico excesivo, obligando al descarte de paquetes entrantes adicionales.
Congestión de enlace	Situación donde la demanda de ancho de banda agregado de múltiples flujos excede la capacidad física del enlace de comunicación.
Fallas de hardware	Malfuncionamiento de componentes de red como tarjetas de interfaz de red (NIC) que pueden causar el descarte intermitente de paquetes recibidos correctamente.
Limitación de velocidad	Configuraciones de dispositivos de red que imponen límites en la velocidad de procesamiento de paquetes, resultando en descarte cuando se exceden estos límites.
Policies de QoS	Implementación de políticas de Calidad de Servicio que priorizan ciertos tipos de tráfico, descartando paquetes de menor prioridad durante períodos de congestión.

4. Bandwidth

El bandwidth se define como la capacidad de un enlace de comunicaciones de red para transmitir la cantidad máxima de datos de un punto a otro en un período de tiempo determinado. En el contexto de redes VPN, las implementaciones de software pueden tener un impacto significativo en el rendimiento, produciendo alto uso de CPU y limitando el throughput de red [32].

E. Seguridad en VPNs

La seguridad en Redes Privadas Virtuales constituye un aspecto esencial en la protección de datos y comunicaciones a través de infraestructuras de red pública, garantizando la confidencialidad, integridad y autenticación de la información transmitida. Las VPNs emplean técnicas criptográficas avanzadas para encapsular y cifrar los datos, previniendo el acceso no autorizado durante su tránsito a través de Internet [37].

TABLA X
TIPOS Y CAUSAS DEL JITTER EN REDES

Tipo/Causa	Descripción
Jitter constante	Variación en retardo relativamente uniforme y predecible, típicamente causada por características estables de la infraestructura de red y patrones de tráfico regulares.
Jitter transitorio	Incremento antinatural del retardo, a veces afectando únicamente paquetes individuales, generalmente causado por picos súbitos de tráfico o cambios temporales en las rutas de red.
Variación de retardo a corto plazo	Ocurre debido a cambios de rutas y exhibe retardo creciente para algunos paquetes, así como incremento en la pérdida de paquetes durante períodos de reconfiguración de red.
Congestión de red	Resultado de la saturación de enlaces o dispositivos de red cuando la demanda excede la capacidad disponible, causando acumulación variable de paquetes en colas de dispositivos.
Cambios de topología	Variaciones súbitas causadas por fallas de enlaces, cambios en protocolos de enrutamiento, o modificaciones en la topología de red subyacente que afectan las rutas de paquetes.

TABLA XI
FACTORES QUE AFECTAN LA GESTIÓN DEL BANDWIDTH

Factor	Descripción
Congestión de red	Ocurre cuando el volumen de tráfico de red excede la capacidad disponible, resultando en degradación del throughput efectivo y aumento de latencia en la transmisión de datos.
Contención de bandwidth	En redes con bandwidth limitado, diferentes aplicaciones y servicios compiten por recursos, llevando a congestión y rendimiento degradado que requiere priorización mediante técnicas de QoS.
Overhead de cifrado	Las operaciones de cifrado y descifrado en implementaciones VPN consumen recursos computacionales significativos, reduciendo el bandwidth efectivo disponible para transmisión de datos de usuario.
Capacidad de hardware	Las limitaciones del hardware de red, incluyendo routers, switches y tarjetas de interfaz de red, pueden crear cuellos de botella que restringen el throughput máximo alcanzable.

Entre los mecanismos fundamentales que determinan la seguridad en VPN se encuentran el cifrado de datos, la autenticación robusta de usuarios y dispositivos, y la integridad de paquetes transmitidos, frecuentemente implementados mediante protocolos como IPsec, WireGuard,

OpenVPN o SSTP [38].

F. Herramientas de Medición

Las herramientas de medición en redes constituyen instrumentos fundamentales para la evaluación, análisis y diagnóstico del rendimiento de las comunicaciones de red. En el contexto de investigación en redes VPN, estas herramientas permiten la cuantificación precisa de parámetros como latencia, pérdida de paquetes, jitter y throughput, facilitando la comparación objetiva entre diferentes protocolos y configuraciones.

1. Iperf

Iperf es una herramienta de línea de comandos utilizada para medir el rendimiento de red en términos de ancho de banda y calidad de conexión entre dos puntos de una red [39] y de esta forma nos permite generar tráfico TCP y UDP para evaluar el throughput máximo, la pérdida de paquetes, la latencia y el jitter en enlaces de red.

La arquitectura de funcionamiento de iperf se basa en un modelo cliente-servidor donde uno de los extremos actúa como servidor escuchando conexiones entrantes, mientras que el otro extremo funciona como cliente estableciendo la conexión y generando el tráfico de prueba [40].

La Figura 7 ilustra la arquitectura básica de funcionamiento de iperf, mostrando la configuración cliente-servidor entre un sistema Linux (10.6.2.5) y un sistema MS Windows (10.1.1.1) conectados a través de una red, donde el cliente genera tráfico hacia el servidor para medir el ancho de banda disponible entre los puntos de conexión.

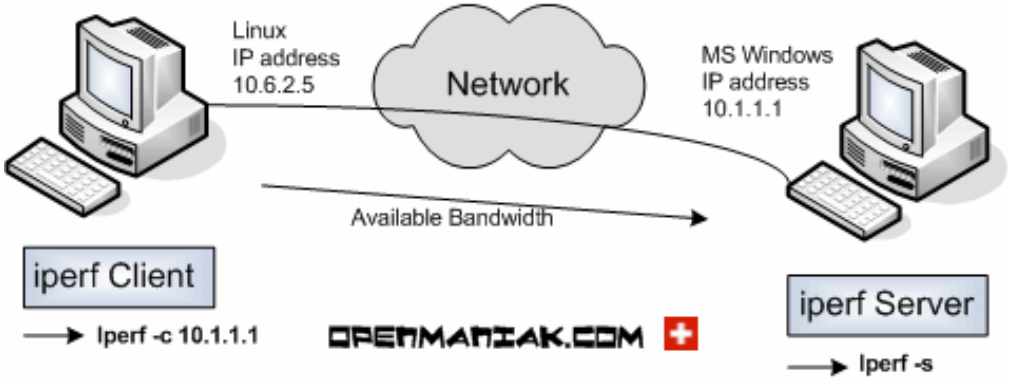


Fig. 7. Arquitectura cliente-servidor de iperf para medición de ancho de banda [40]

TABLA XII
MÉTRICAS DE RENDIMIENTO MEDIDAS POR IPERF

Métrica	Descripción
Throughput	Medición del ancho de banda efectivo alcanzado durante la transmisión, expresado en bits por segundo (bps), fundamental para evaluar la capacidad real de transferencia de datos.
Pérdida de paquetes	Porcentaje de paquetes perdidos durante la transmisión en pruebas UDP, crítico para evaluar la confiabilidad del enlace y el impacto de la congestión de red.
Jitter	Variación en los tiempos de llegada de paquetes consecutivos, medida en milisegundos, especialmente importante para aplicaciones en tiempo real como VoIP y videoconferencias.
Retardo (RTT)	Tiempo de ida y vuelta de los paquetes entre cliente y servidor, proporcionando información sobre la latencia total del enlace incluido el overhead de procesamiento VPN.
Utilización de CPU	Monitoreo del uso de recursos computacionales durante las pruebas, relevante para evaluar el overhead de procesamiento introducido por diferentes protocolos VPN.

G. Metodología PPDIOO

La metodología PPDIOO (Prepare, Plan, Design, Implement, Operate, Optimize) es un enfoque cíclico desarrollado por Cisco que define el ciclo de vida continuo de servicios requeridos para una red, reflejando las fases del ciclo de vida estándar de una red y proporcionando un framework estructurado para el diseño e implementación exitosa de infraestructuras de red [41].

Prepare (Preparar): Establece los requerimientos organizacionales y desarrolla una estrategia de red que se alinee con los objetivos del negocio, incluyendo la identificación de tecnologías y recursos necesarios.

Plan (Planificar): Identifica los requerimientos de red basados en objetivos, facilidades y necesidades del usuario, desarrollando un plan de proyecto detallado que incluye cronogramas y asignación de recursos.

Design (Diseñar): Desarrolla el diseño detallado de la red de acuerdo con los requerimientos técnicos y del negocio recopilados en las fases anteriores, especificando arquitecturas,

protocolos y componentes.

Implement (Implementar): Construye la red de acuerdo con las especificaciones de diseño, incluyendo la instalación, configuración y verificación de todos los componentes de red.

Operate (Operar): Realiza las tareas diarias requeridas para mantener la red funcionando efectivamente, incluyendo monitoreo de rendimiento, gestión de configuración y resolución de problemas.

Optimize (Optimizar): Identifica y resuelve problemas de rendimiento mediante modificaciones proactivas en el diseño de red, basándose en métricas de rendimiento y requerimientos cambiantes del negocio.

La Figura 8 ilustra el ciclo continuo de la metodología PPDIOO, mostrando cómo cada fase se conecta de manera secuencial y cíclica, enfatizando la naturaleza iterativa del proceso de gestión del ciclo de vida de la red.

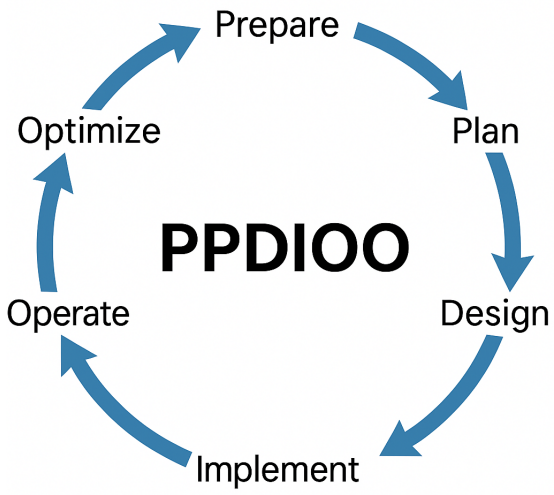


Fig. 8. Metodología PPDIOO para gestión del ciclo de vida de redes [42]

III. METODOLOGÍA

El siguiente capítulo describe la aplicación de la metodología PPDIOO en el desarrollo de un entorno de emulación controlado para la evaluación comparativa de tecnologías VPN. A través de esta metodología se logrará configurar un escenario de red virtualizado con túneles VPN implementados mediante protocolos como WireGuard, IPsec, SSTP y PPTP. Estos entornos serán sometidos a condiciones de tráfico controladas, midiendo parámetros clave de rendimiento y seguridad.

A. Preparar

La fase de preparación establece los fundamentos necesarios para llevar a cabo el análisis comparativo de tecnologías VPN. Esta etapa inicial es crucial para garantizar la validez y confiabilidad de los resultados obtenidos durante la investigación.

Definición de Requerimientos del Proyecto

Se establecen los requerimientos funcionales y no funcionales del proyecto de investigación, incluyendo la identificación de las tecnologías VPN a evaluar, las métricas de rendimiento y seguridad a medir, y los criterios de éxito para cada protocolo. Los requerimientos incluyen la capacidad de medir latencia, throughput, jitter, pérdida de paquetes y características de seguridad en entornos controlados.

Análisis de Recursos Necesarios

Se realiza un inventario detallado de los recursos tecnológicos requeridos para la ejecución exitosa del análisis comparativo de tecnologías VPN:

Recursos de Hardware

- Computadora host con procesador Intel Core i7 o AMD Ryzen 7 (mínimo 8 núcleos)
- Memoria RAM de 16 GB DDR4 para virtualización múltiple
- Disco duro SSD de 500 GB para almacenamiento de máquinas virtuales
- Sistema de respaldo externo de 500 GB para almacenamiento de datos

Recursos de Software

- Sistema operativo Linux Ubuntu 20.04 LTS

- Software de emulación GNS3 versión 2.2.x o superior
- VMware Workstation Player
- MikroTik RouterOS versión 7.x (imagen CHR para virtualización)
- iPerf3 para medición de rendimiento de red
- VPCS para simulación de endpoints

Evaluación de Riesgos del Proyecto

Se desarrolla una matriz de riesgos que identifica potenciales amenazas al desarrollo exitoso del proyecto:

TABLA XIII
EVALUACIÓN DE RIESGOS DEL PROYECTO

Riesgo	**Probabilidad**	**Impacto**	**Mitigación**
Fallas en hardware	Media	Alto	Configuración de equipos de respaldo y virtualización distribuida
Limitaciones en software de emulación	Baja	Medio	Validación previa de capacidades de GNS3 y configuración de alternativas
Incompatibilidades entre protocolos	Baja	Alto	Estudio detallado de documentación técnica y configuraciones estándar
Interferencias en mediciones	Media	Medio	Aislamiento de entorno de pruebas y múltiples repeticiones

B. Planificar

En esta fase se estableció el cronograma de trabajo necesario para ejecutar el proyecto de forma ordenada y sistemática. La planificación permitió distribuir las tareas principales en períodos de tiempo definidos, garantizando que cada actividad contara con los recursos y condiciones necesarias para su desarrollo.

El proyecto se estructuró en cuatro meses de ejecución activa, divididos en semanas de trabajo técnico y análisis. En la Tabla XIV se detalla la planificación general basada en la metodología PPDIOO, asignando cada fase a uno o más momentos del cronograma.

TABLA XIV
PLANIFICACIÓN GENERAL DEL PROYECTO

Fase	Actividades programadas
Mes 1 (Semanas 1-4)	- Preparación del entorno emulado (GNS3 y RouterOS). - Validación de imágenes de sistema y nodos de prueba. - Evaluación de riesgos y verificación de compatibilidad de herramientas.
Mes 2 (Semanas 5-8)	- Diseño de topologías de red y asignación de direcciones IP. - Configuración inicial de túneles VPN con WireGuard, IPsec, SSTP y PPTP. - Pruebas preliminares de conectividad y funcionalidad.
Mes 3 (Semanas 9-12)	- Ejecución de pruebas de rendimiento bajo condiciones controladas. - Recolección de datos con iPerf y Ping. - Captura de métricas: latencia, jitter, pérdida de paquetes, throughput.
Mes 4 (Semanas 13-16)	- Análisis comparativo de resultados obtenidos. - Optimización de configuraciones para revisión final. - Elaboración de informes técnicos, gráficas y tablas de resultados.

C. Diseñar

Con los recursos presentados y una planificación orquestada, pasamos a la etapa de diseño, donde se establece la topología de red que nos permitirá implementar túneles VPN en un entorno emulado controlado y definir cómo quedará distribuido el sistema. El entorno del escenario virtualizado será concretado mediante la propia configuración de GNS3, dicho simulador será enlazado a varios routers MikroTik, que estando distribuidos hacen la tarea de representar diferentes entornos remotos que se encuentran enlazados a través de Internet simulado. La topología ejecutará túneles VPN site-to-site entre dos zonas geográficas diferentes para evaluar el rendimiento de cada protocolo VPN bajo ciertas condiciones controladas, como se muestra en la Fig. 9.

El escenario está configurado con 2 sitios que se comunican por túneles VPN sobre una red Internet simulada. Cada uno de los sitios tiene un router MikroTik: MikroTik-7 y MikroTik-8 como gateways VPN, switches para la distribución local: SW1 y SW4 y hosts Ubuntu como endpoints para pruebas de conectividad y medición de métricas. Los túneles VPN se ejecutarán utilizando las tecnologías WireGuard, IPsec, SSTP y PPTP secuencialmente con el objetivo de realizar las comparativas de rendimiento y seguridad establecidas en los objetivos del proyecto.

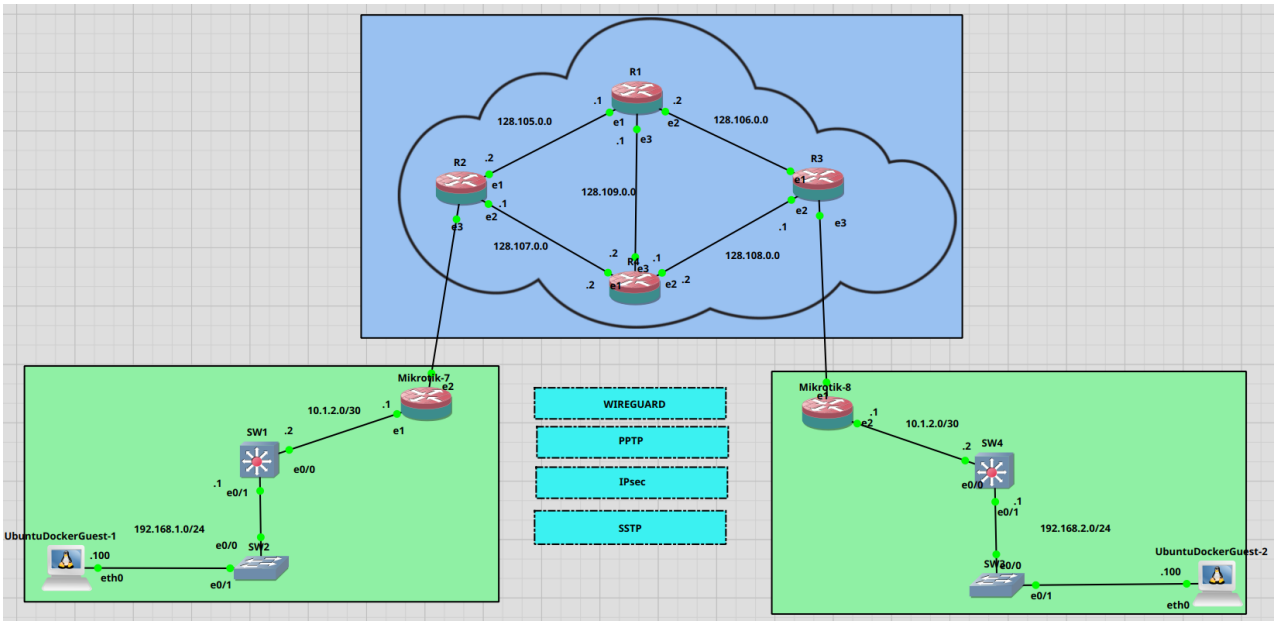


Fig. 9. Topología de red para el análisis comparativo de tecnologías VPN

TABLA XV
CONFIGURACIÓN DE DIRECCIONAMIENTO IP DEL LABORATORIO

Componente	Interfaz	Dirección IP
MikroTik-7 (Sitio 1)	ether2 (SW1)	10.1.1.1/30
	wg1 (WireGuard)	10.10.10.1/30
MikroTik-8 (Sitio 2)	ether3 (SW4)	10.1.2.1/30
	wg1 (WireGuard)	10.10.10.2/30
SW1 (Sitio 1)	Ethernet0/0 (MKT-7)	10.1.1.2/30
	Ethernet0/1 (LAN)	192.168.1.1/24
SW4 (Sitio 2)	Ethernet0/0 (MKT-8)	10.1.2.2/30
	Ethernet0/1 (LAN)	192.168.2.1/24
UbuntuDockerGuest-1 (PC1)	eth0	192.168.1.100/24
UbuntuDockerGuest-2 (PC2)	eth0	192.168.2.100/24

D. Implementar

1. Configuración de red WAN

Definido el diseño lógico y físico deL escenario, se da paso a la fase de implementación de la misma, donde se pone en marcha la configuración de la infraestructura WAN y así emular un entorno realista sobre la conectividad intersede por internet, para ello se configuró una red pública virtual formada por una serie de routers MikroTik interconectados por el protocolo de enrutamiento dinámico eBGP que pretendía simular cómo se comportaría esta red pública de

transporte. Esta red permitió que los sitios remotos se comunicaran entre sí como si dicha comunicación lo fuera a través de diferentes proveedores de servicios de Internet, teniendo de ID las siguientes.

TABLA XVI
CONFIGURACIÓN BGP DE ROUTERS EN LA NUBE

Router	**AS**	**ID**	**Vecinos BGP**
R1	65531	1.1.1.1	R2, R3, R4
R2	65532	2.2.2.2	R1, R3, R4, MikroTik-7
R3	65533	3.3.3.3	R1, R2, R4, MikroTik-8
R4	65534	4.4.4.4	R1, R2, R3

La implementación de la red WAN se llevó a cabo mediante la configuración de cuatro routers MikroTik que conforman la infraestructura de transporte simulada. Como se puede observar en la Fig. 10, el router R1 opera con el Sistema Autónomo 65531 y router ID 1.1.1.1, estableciendo sesiones BGP con sus tres vecinos principales: R2 (AS 65532), R3 (AS 65533) y R4 (AS 65534). La interfaz de administración de RouterOS muestra que todas las conexiones se encuentran en estado .Estäblished", lo cual confirma la correcta convergencia del protocolo eBGP entre los dispositivos de la nube simulada.

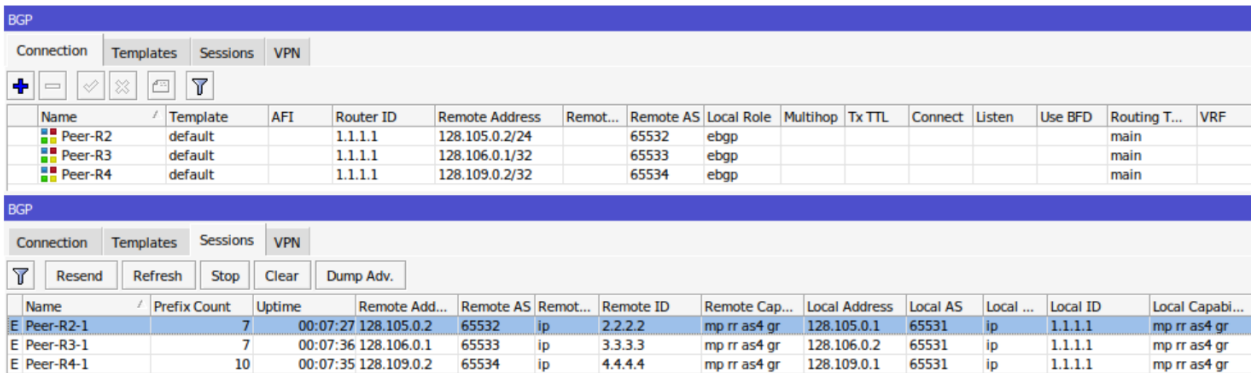


Fig. 10. Configuración BGP del router R1

El router R1 ocupa la posición en la parte superior de la nube BGP; se conecta a los routers mediante enlaces punto a punto combinando direccionamiento IPv4 en los segmentos 128.105.0.0/24, 128.106.0.0/24, 128.107.0.0/24 y 128.109.0.0/24. En este modo de configuración se pueden simular múltiples rutas junto con redundancia en la conectividad, características que son necesarias para comprobar el comportamiento de los túneles VPN bajo diferentes modos de enrutamiento. Los sitios terminales que se conectan a la nube BGP son MikroTik-

7 y MikroTik-8, conectados mediante los routers R2 y R3 y con direecionamiento en las redes 64.104.0.0/24 y 64.105.0.0/24, respectivamente, lo que permite la conectividad necesaria que permite implementar túneles VPN site-to-site. Tal y como se ha observado en la configuración, la estabilidad de las sesiones BGP permite que las pruebas de rendimiento y seguridad de los protocolos VPN se ejecuten sobre una infraestructura de red predecible y confiable y se agregó la misma configuración en los routers R2 al R4 para completar la configuración de red WAN utilizando enrutamiento BGP.

2. Configuración de túneles VPN

Una vez establecida la infraestructura de red WAN mediante la configuración BGP, se procedió a implementar los túneles VPN site-to-site entre los sitios remotos para realizar el análisis comparativo de rendimiento y seguridad. Los cuatro protocolos de tunelización evaluados en este proyecto son:

Cada tecnología VPN se configuró de manera secuencial entre los routers MikroTik-7 y MikroTik-8, estableciendo conectividad segura entre las redes LAN 192.168.1.0/24 y 192.168.2.0/24 respectivamente. La implementación siguió las mejores prácticas documentadas para cada protocolo, utilizando parámetros de configuración estándar que permitan una comparación objetiva del rendimiento y características de seguridad inherentes a cada tecnología.

2a. Configuración de WireGuard

Se ejecutó la puesta a punto del protocolo WireGuard para realizar la primera comprobación del túnel VPN definido, aprovechando sus características de simpleza y rendimiento que caracteriza esta moderna tecnología. Tal y como se puede comprobar en la Fig 11, la interfaz ‘wg1‘ del router para MikroTik-7 ha sido puesta a punto con la dirección IP 10.10.10.1/30 con la intención de crear un túnel punto a punto hacia el sitio remoto a configurar. La configuración define el puerto 13231 UDP para la comunicación y fija el MTU a 1420 bytes, optimizado para evitar fragmentaciones de paquetes que puedan ser generadas por el túnel.

La configuración del peer remoto determina el endpoint 64.105.0.2:13231 que corresponde a la dirección IP pública del router MikroTik-8 por medio de la nube BGP, además, las claves criptográficas públicas y privadas son generadas de forma automática e impulsadas a través de WireGuard, de tal manera que se asegure la autenticación de los extremos del túnel. Las

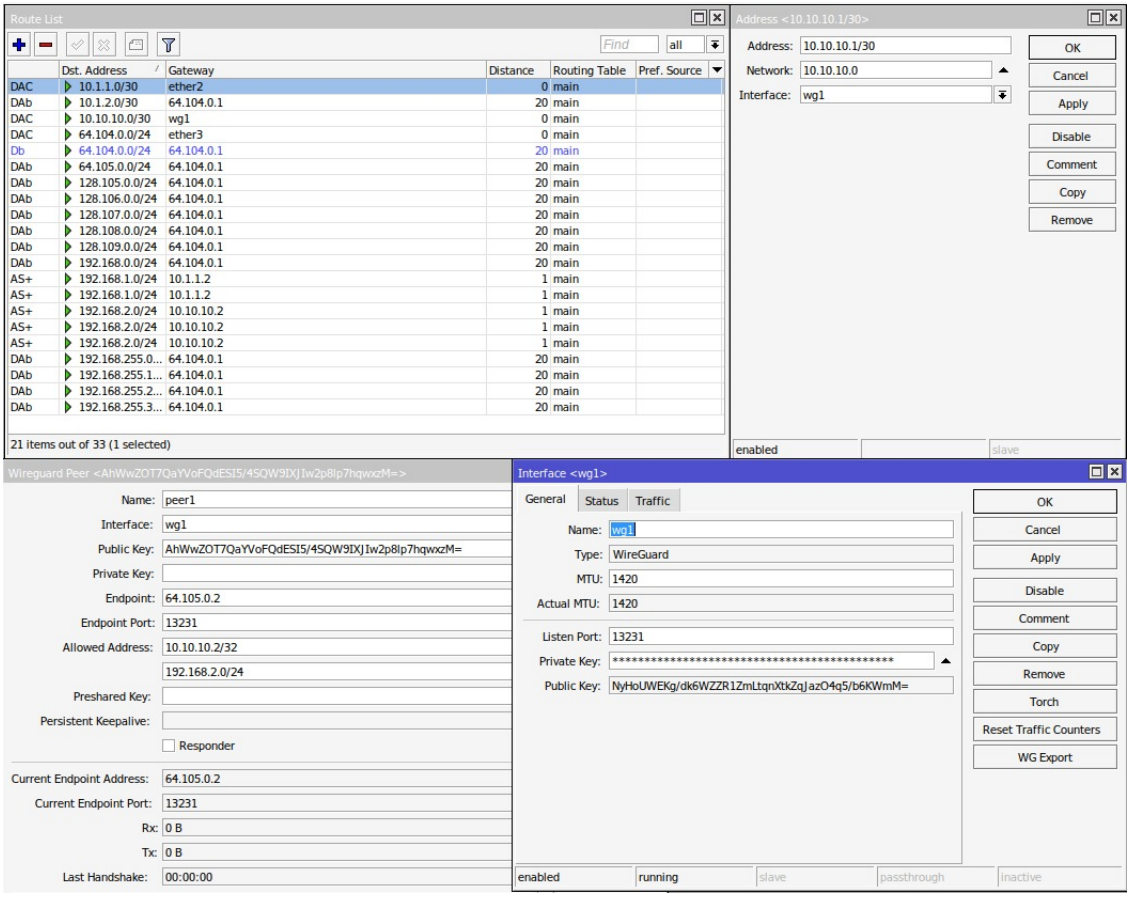


Fig. 11. Configuración de WireGuar ddel MikroTik-7

Allowed Addresses incluyen la dirección del peer remoto (10.10.10.2/32) y la red LAN del sitio 2 (192.168.2.0/24), las cuales permiten definir que tipo de tráfico puede estar dejando transitar por el túnel. Un simétrico del router MikroTik-8 está configurado con los parámetros correspondientes del extremo opuesto, la cual se puede evidenciar con el state active del túnel que confirma una conectividad exitosa en ambas direcciones. La tabla de enrutamiento también puede confirmar la tales informaciones, la cual especifica que hay rutas hacia la red del túnel y la LAN remota con distancia administrativa 1 mientras que el estado del túnel indica que el tráfico está activo con valores de tráfico bidireccional de 0 bytes, lo cual confirma que la configuración ha sido establecida.

2b. Configuración de PPTP

Para la implementación del protocolo PPTP (Point-to-Point Tunneling Protocol), se re-utilizó la misma topología previamente definida para WireGuard. Antes de aplicar esta nueva

configuración, se desactivaron las interfaces wg1 en ambos extremos con el fin de evitar interferencias en el enrutamiento y asegurar que todo el tráfico entre las LAN remotas fluya únicamente por el túnel PPTP.

En el router MikroTik-7, se activó el servicio PPTP desde el menú PPP → Interface habilitando el servidor y aplicando el perfil de cifrado default-encryption. Este perfil permite el uso de algoritmos simétricos con los métodos de autenticación mschap1, mschap2, chap y pap.

Se realizó un establecimiento de un PPP Secret en el que se realizó el uso de pptp-user y como contra se realizó el uso de la contraseña oculta (por motivos de seguridad) y se definió el servicio pptp. La dirección local se asignó como 10.010.010.001, la dirección remota se asignó como 10.10.10.2 utilizando el perfil de cifrado default-encryption.

La Fig. 12 muestra la configuración consolidada del servidor, incluyendo la habilitación del servicio, el perfil de cifrado y el usuario.

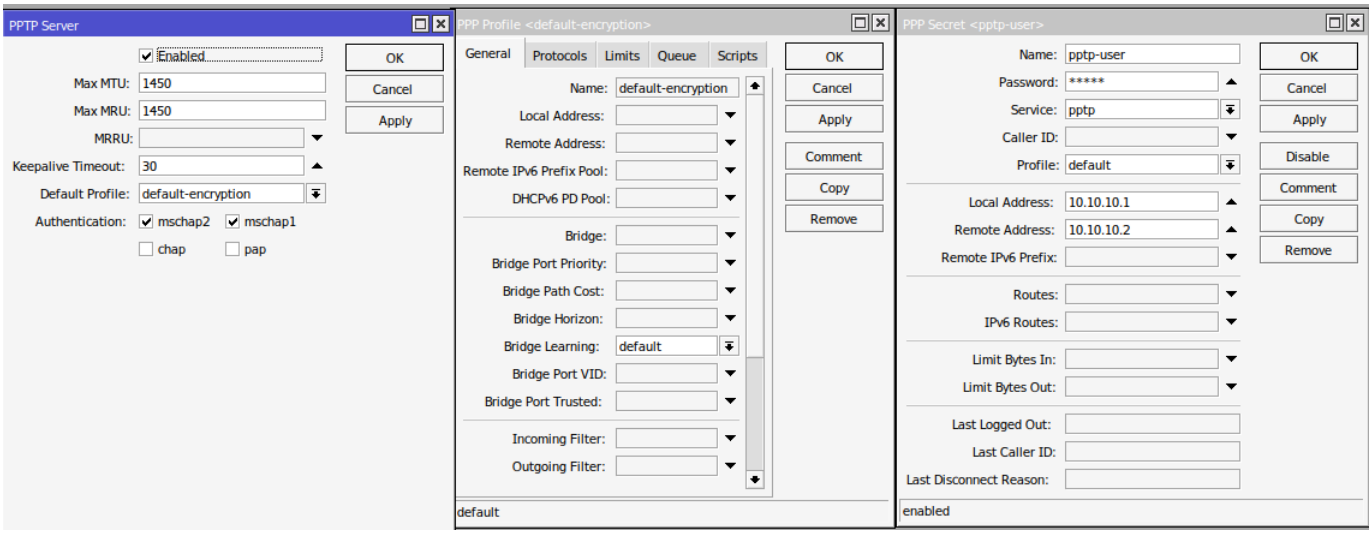


Fig. 12. Configuración consolidada del servidor PPTP en MikroTik-7

Las rutas estáticas no fueron modificadas, ya que se encontraban definidas en la configuración del túnel WireGuard. Por tanto la comunicación de las subredes 192.268.1.0/24 y 192.168.2.0/24 se realizó correctamente una vez que se levantó la sesión PPTP.

En el router MikroTik-8 la interfaz pptp-out1 fue configurada como cliente del túnel PPTP, y esta se encuentra en la opción PPP → Interfaces y se conectó al servidor remoto a través de su IP pública 64.104.0.2. Se utilizaron las mismas credenciales de acceso que previamente se

configuraron en MikroTik-7 para poder establecer la autenticación (en este caso pptp-user), el perfil seleccionado fue el default-encryption, asegurando por ende el uso de los métodos de autentificación seguros.

En la parte inferior de la ventana se puede ver que la interfaz se encuentra en estado connected y running, indicando que el túnel está establecido correctamente. Adicionalmente vemos que en la tabla de direcciones del router se observa que la interfaz pptp-out1 fue correctamente conectada con la dirección 10.10.10.2/30 (1024-) que corresponde al extremo cliente del túnel.

La Fig. 13 muestra la configuración completa del cliente PPTP, incluyendo el panel de interfaz, la lista de interfaces activas y la asignación de direcciones.

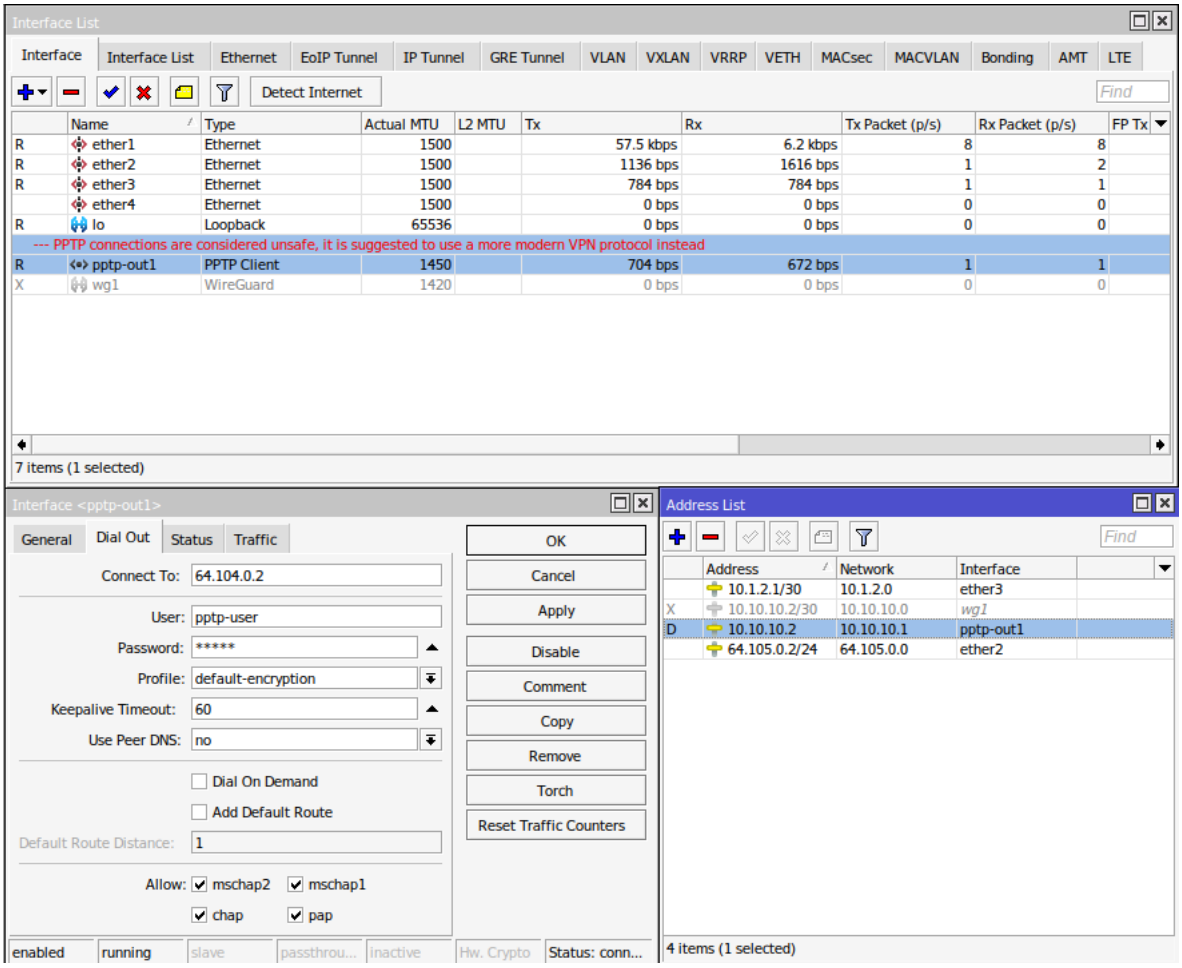


Fig. 13. Configuración del cliente PPTP en MikroTik-8

Durante las pruebas de conectividad, se verificó el intercambio de tráfico cifrado a través de la interfaz pptp-out1, tal como se evidencia en la pestaña Traffic, la cual muestra valores

activos en los campos TX y RX. La comunicación entre los hosts finales (PC1 y PC2) fue exitosa mediante comandos ping y traceroute, confirmando que los paquetes transitaron correctamente por el túnel PPTP, cumpliendo así con los objetivos de conectividad site-to-site en condiciones controladas.

2c. Configuración de IPsec

En el router MikroTik-7 (Sitio 1), se configuró el túnel IPsec actuando como initiator bajo el modo de intercambio IKEv2. Para ello, se definió un Peer con la dirección IP pública del router remoto (64.105.0.2), utilizando el puerto 500 y el perfil por defecto de autenticación.

En la sección Policies, se creó una política de cifrado con los siguientes parámetros:

- Dirección de origen: 192.168.1.0/24
- Dirección de destino: 192.168.2.0/24
- Acción: encrypt
- Nivel: require
- Protocolo: all
- Túnel: habilitado
- SA Src Address: 64.104.0.2
- SA Dst Address: 64.105.0.2

Además, se definieron los parámetros criptográficos en la sección Proposals, configurando el algoritmo de autenticación sha1, cifrado aes-256-cbc, y la generación de claves a 256 bits. La Fig. 14 presenta la configuración consolidada del servidor IPsec, incluyendo la política aplicada, el peer definido y las asociaciones de seguridad (SAs) activas.

En el router MikroTik-8 (Sitio 2), se configuró la conexión como cliente IPsec utilizando el modo IKEv2. Como se muestra en la Fig. 15, se definió el peer peer-R7 apuntando a la dirección pública del servidor remoto 64.104.0.2, habilitando el envío del parámetro INITIAL_CONTACT y desmarcando la opción Passive, lo cual es adecuado para el rol de iniciador del túnel.

La política IPsec fue definida como activada en modalidad túnel (Tunnel), estableciendo la local como origen de la red 192.168.2.0/24 y la remota como destino de la red 192.168.1.0/24. Dicha política a partir de ahora queda asociada a la peer que previamente se ha definido.

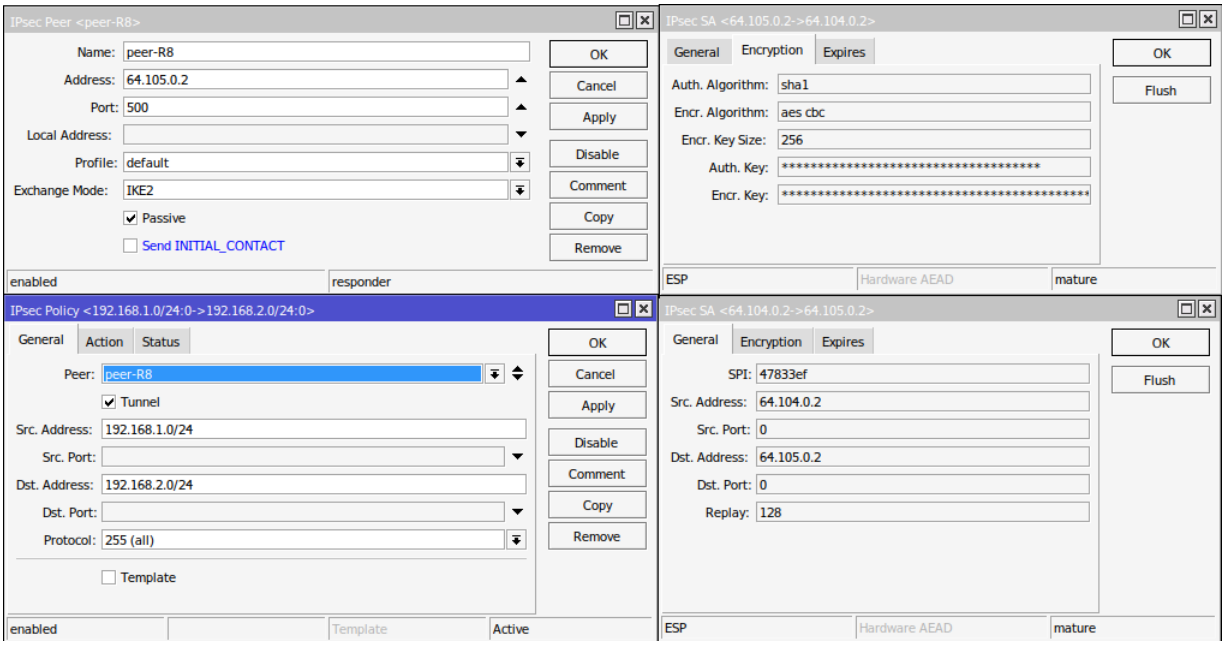


Fig. 14. Configuración de servidor IPsec en MikroTik-7

En la parte derecha de la imagen se encuentran las asociaciones de seguridad (Security Associations, SAs) instaladas, en donde se pueden observar los parámetros criptográficos que se utilizaron en el intercambio, autenticación mediante SHA-1, cifrado simétrico con AES-CBC de 256 bits, y claves generadas de forma dinámica (con las que se trabaja). Ambas SAs se encuentran en estado mature, lo que indica que se alcanzó un estado de negociación exitoso y el canal de comunicación cifrada se encuentra en perfecto estado de funcionamiento.

2d. Configuración de SSTP

Para la implementación del protocolo SSTP en el sitio 1, se configuró el router MikroTik-7 como servidor utilizando certificados digitales y el servicio PPP. El proceso se inició con la creación de una Autoridad Certificadora (CA) propia dentro del dispositivo, seguida de la generación y firma del certificado destinado al servidor.

En la sección System → Certificates, se observan los certificados generados: myCA como autoridad raíz confiable y server-cert como certificado del servidor, firmado con la clave privada de la CA. El certificado fue asignado al servicio SSTP y marcado como válido para su uso con TLS en el contexto de VPN.

A continuación, habilitó el servidor SSTP en la ruta PPP → SSTP Server, seleccionó

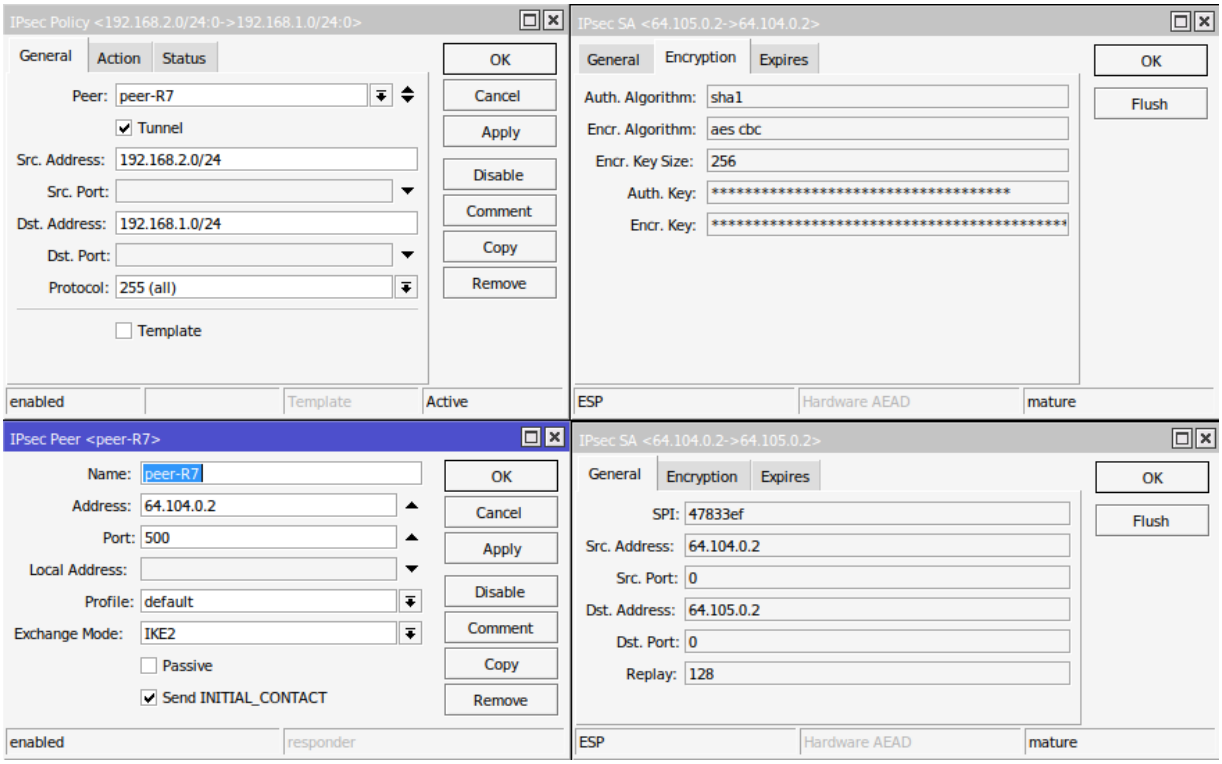


Fig. 15. Configuración del cliente IPsec en MikroTik-8

el certificado server-cert, activó el perfil de cifrado default-encryption y habilitó el método de autenticación mediante los métodos mschap2 y mschap1. Los cifrados AES256-SHA y AES256-GCM-SHA384 fueron configurados y la versión TLS en modo flexible (any).

En la sección PPP → Secrets se definió el usuario sstp-user, que tiene una contraseña segura, la dirección local 10.10.30.1 y la dirección remota sstp-pool, con el uso del perfil sstp-profile anteriormente creado, el cual se puede visualizar en la sección PPP → Profiles, y que también define la dirección local, así como también el rango de direcciones que se puede asignar a los clientes remotos.

Una vez levantada la sesión, se observa la interfaz virtual sstp-sstp-user en el menú PPP → Interface, la cual aparece en estado running y asociada correctamente al usuario configurado, evidenciando que el túnel SSTP se ha establecido exitosamente. La Figura 16 muestra la configuración consolidada del servidor SSTP en MikroTik-7.

Se creó, en el router MikroTik-8, el cliente SSTP creando una interfaz virtual de configuración, en la ruta PPP → Interfaces, para el cliente SSTP donde se creó la interface sstp-out1

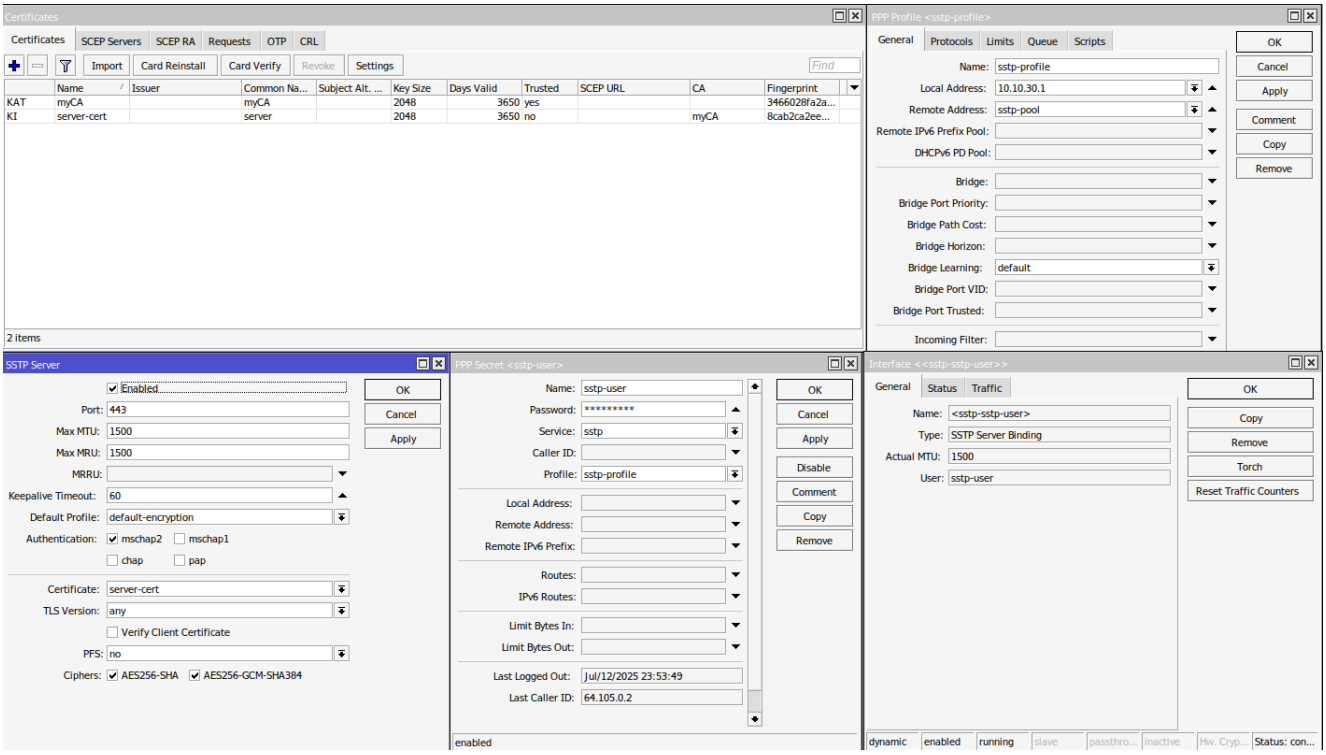


Fig. 16. Configuración del servidor SSTP en MikroTik-7

a partir de esta definición.

La configuración del cliente SSTP incluyó como dirección para llevar a cabo la conexión la IP pública del servidor MikroTik-7 (64.104.0.2) con el puerto TCP 443 como puerto por defecto. Se introdujo el usuario correspondiente (sstp-user) con una contraseña cuyo armonismo en la creación no entra en la zona de independencia de la conversación y se adoptó el perfil descrito como default-encryption. Como versión de TLS aceptada se utilizó cualquiera (any), sin verificación del certificado del servidor. En lo que respecta al cifrado, se habilitaron para el cliente SSTP los algoritmos de cifrado AES256-SHA y AES256-GCM-SHA384 para el cifrado, así como los métodos de autenticación mschap2 y mschap1.

La interfaz SSTP se encuentra en estado connected y running, lo que indica que el túnel fue establecido correctamente entre MikroTik-8 y MikroTik-7. Como puede observarse en la figura 17, el tráfico cifrado puede circular a través del túnel SSTP hacia red remota.

Para habilitar la comunicación de las subredes 192.168.2.0/24 y 192.168.1.0/24 se añadió una ruta estática en IP → Routes definiendo como destino la red 192.168.1.0/24 y como gateway la dirección de extremo remoto del túnel 10.10.30.1.

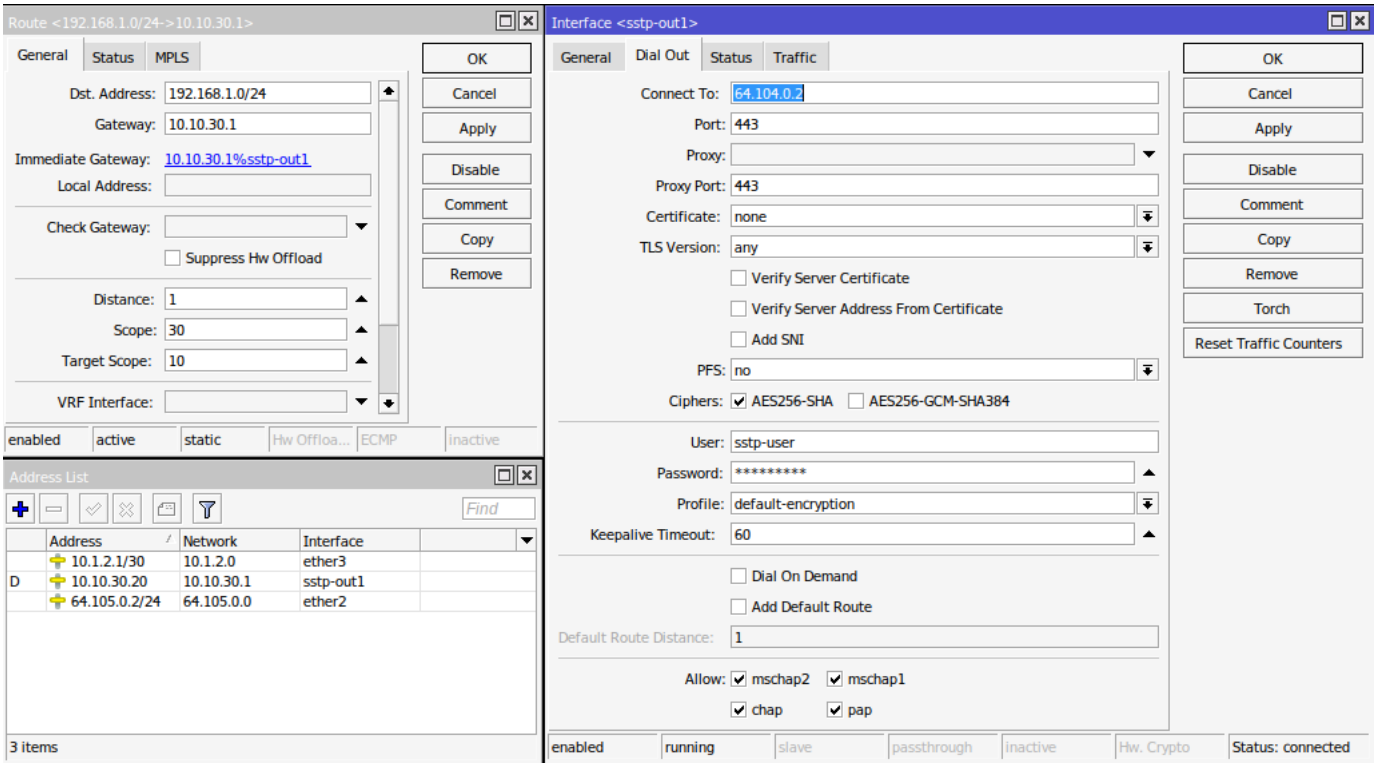


Fig. 17. Configuración del cliente SSTP en MikroTik-8: interfaz sstp-out1, autenticación y enrutamiento

E. Operar

En esta fase se verifica el correcto funcionamiento de los túneles VPN implementados entre los sitios remotos. La validación de la conectividad se realizó a través de comandos de diagnóstico como *ping* y *traceroute*, así como mediante la observación del tráfico cifrado en las interfaces virtuales de cada túnel. A continuación se presenta la evidencia correspondiente a la VPN configurada con el protocolo SSTP.

1. Verificación del túnel SSTP

Desde el router MikroTik-7, se ejecutó una prueba de conectividad mediante el comando *ping* dirigido a la dirección IP 10.10.30.20, correspondiente al extremo remoto del túnel SSTP ubicado en MikroTik-8. Como se observa en la Figura 18, se obtuvo una respuesta exitosa con latencia estable, sin pérdida de paquetes, lo que demuestra que el túnel se encuentra operativo.

Asimismo, la herramienta *Traceroute* se ha ejecutado desde Winbox para confirmar que la comunicación circular correctamente a través del túnel VPN. El resultado obtenido presenta un solo salto entre MikroTik-7 y MikroTik-8, lo que quiere decir que el canal de comunicación

efectivamente está establecido a capa 3.

La interfaz virtual *sstp-sstp-user* también está en estado *running*, y las estadísticas de tráfico muestran actividad bidireccional TX/RX, lo que indica de forma visual que la actividad de transmisión de paquetes con el túnel SSTP se ejecuta correctamente.

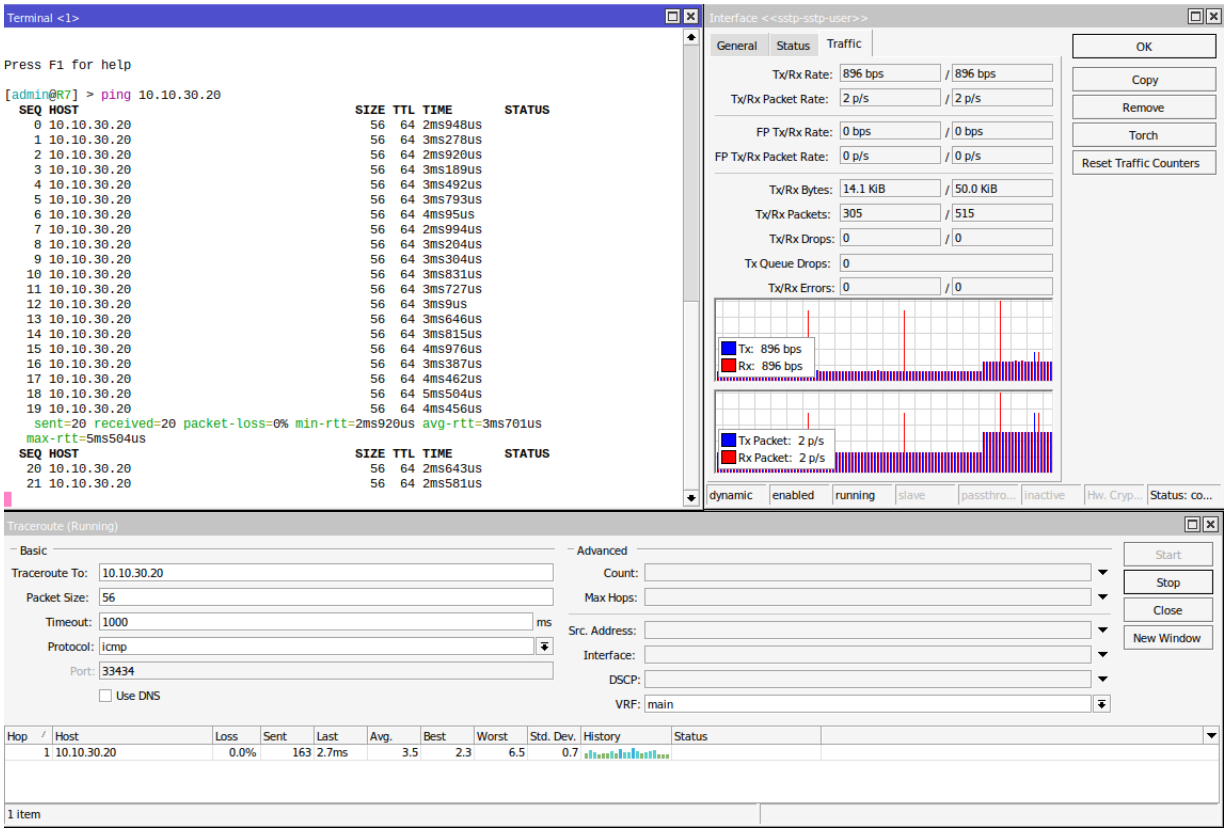


Fig. 18. Verificación de operación del túnel SSTP

2. *Verificación del túnel IPsec*

Una vez configuradas las políticas, peers e identidades en ambos extremos, se procedió a verificar el establecimiento del túnel IPsec utilizando el menú IP → IPsec → Installed SAs. La figura 19 muestra las asociaciones de seguridad activas junto con el tráfico cifrado circulando entre las direcciones públicas 64.104.0.2 y 64.105.0.2.

Se observa también la sección Remote Peer, donde se detalla que el MikroTik-8 actúa como iniciador del túnel, con un total de 233 paquetes transmitidos y 234 recibidos, indicando que el canal está en uso activo.

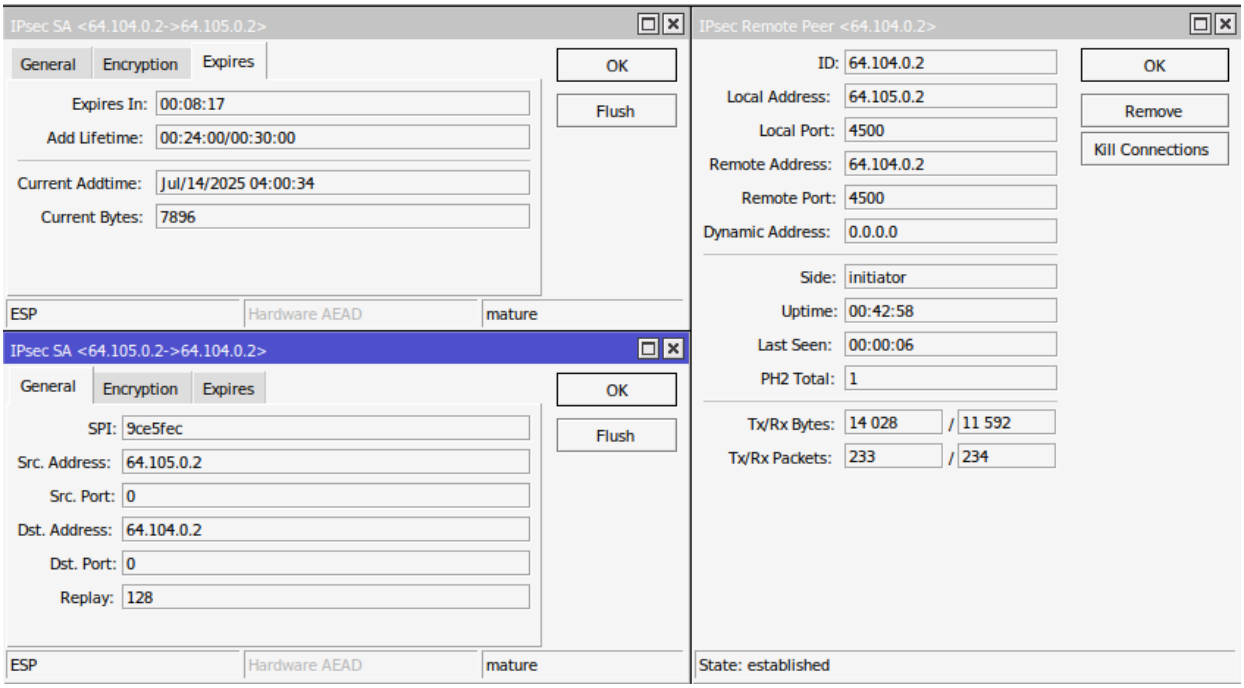


Fig. 19. Verificación de túnel IPsec en MikroTik-8

3. Verificación del túnel PPTP

Para comprobar el correcto funcionamiento del túnel PPTP entre MikroTik-7 y MikroTik-8, se realizó una prueba de conectividad mediante el comando ping desde el extremo servidor hacia la dirección remota 10.10.10.2. Como se observa en la Figura 20, la sesión se encuentra activa y en estado running, transmitiendo tráfico en tiempo real a través de la interfaz pptp-pptp-user.

Los resultados actuales del ping muestran que se retorna un ping estable con tiempos de latencia pequeños, alrededor de 3 ms, sin pérdidas ni errores. Lo que indica que el túnel se ha establecido correctamente y que se puede comunicar entre los extremos.

4. Verificación del túnel WireGuard

Se llevó a cabo el procedimiento para comprobar el buen establecimiento del túnel WireGuard entre MikroTik-7 y MikroTik-8, usando un ping desde el extremo servidor hacia el extremo remoto 10.10.10.2. Los resultados fueron de tiempos de respuesta estables, mostrando tiempos de respuesta con latencia media de 3,6 ms sin pérdida de paquetes.

Desde la misma interfaz, también podemos ver la interfaz wg1 en el MikroTik-7, la cual

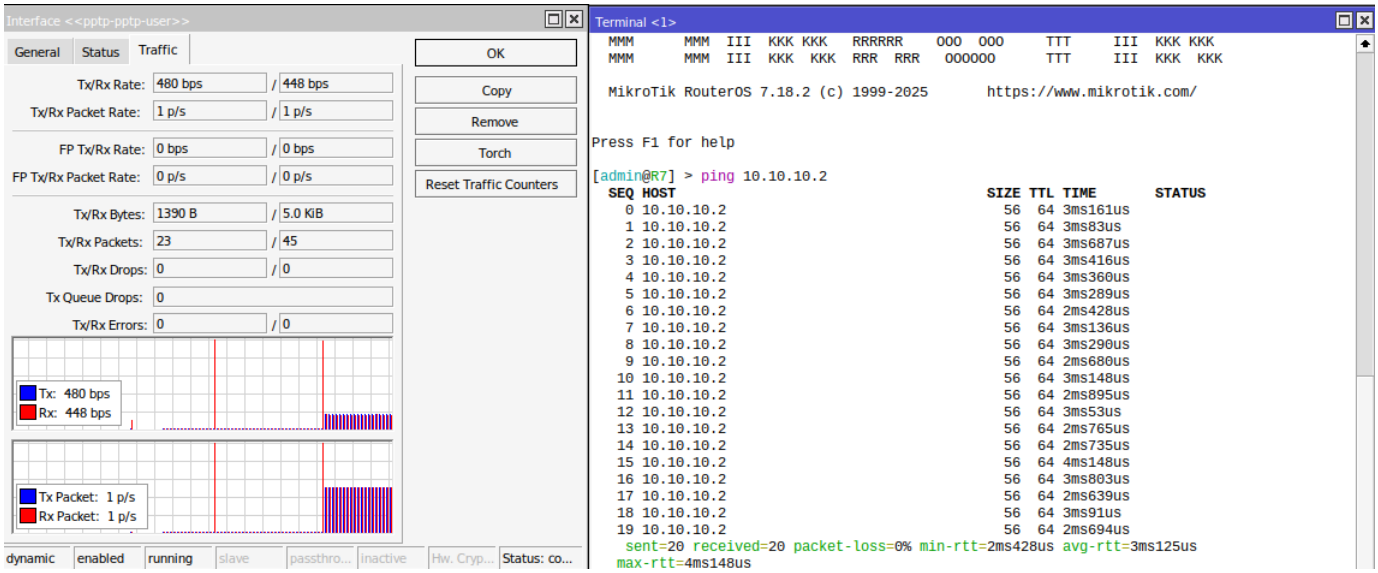


Fig. 20. Verificación de túnel PPTP

se encuentra en estado running y que tiene tráfico activo en la dirección de transmisión (Tx) y en la dirección de recepción (Rx), la cual también confirma que el túnel está funcionando correctamente y el tráfico de datos entre las redes locales se encuentra activo.

Aún más, observando la interfaz wg1 en el router MikroTik-7, el estado era running y con tráfico activo en ambas direcciones. Esta información confirma que el túnel está funcional y transmitiendo datos entre las redes locales.

La Figura 21 muestra los resultados del ping y la observación de la interfaz WireGuard, que demuestra el tráfico generado y el correcto funcionamiento del túnel.

F. Optimizar

La fase de optimización en el contexto de la metodología PPDIOO fue orientada a perfeccionar el procedimiento de recolección de datos experimentales a través de la automatización de las pruebas de rendimiento. El objetivo que perseguía era conseguir homogeneidad entre las pruebas, disminuir los riesgos de errores humanos y, por último, incrementar la eficiencia de la ejecución de las pruebas a realizar en la evaluación comparativa de las tecnologías VPN.

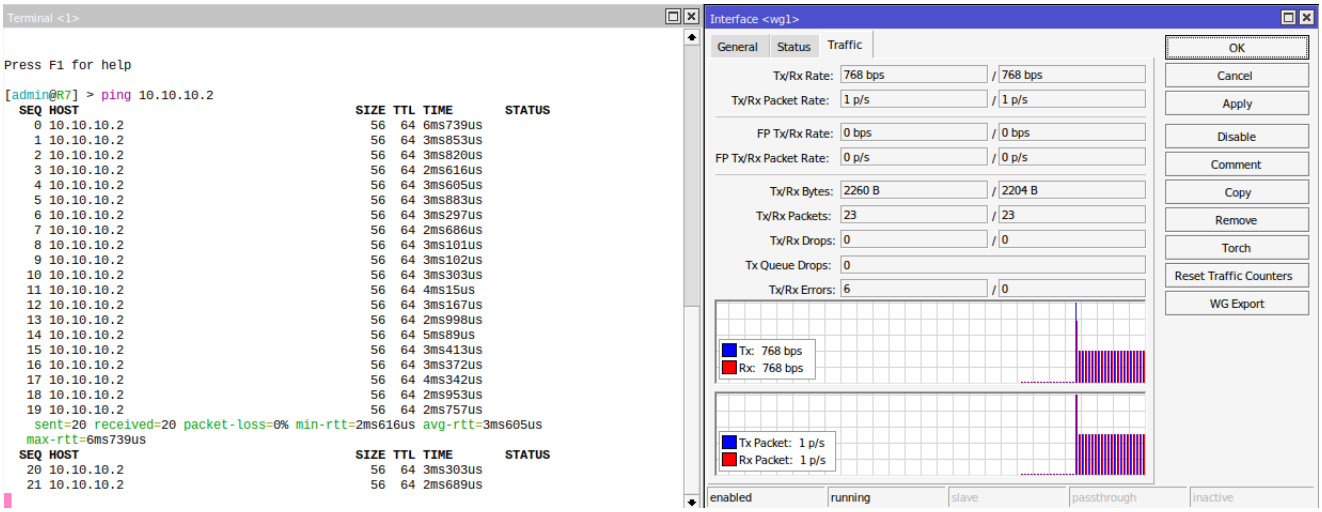


Fig. 21. Verificación de túnel WireGuard: tráfico en interfaz wg1 y respuesta al ping desde MikroTik-7

1. Automatización del Proceso de Evaluación

Con este objetivo se elaboró un script ejecutado desde el equipo cliente, que ejecutaba de forma automatizada las pruebas necesarias hacia el servidor de pruebas de la dirección IP 192.168.1.10. El script empezó a considerar la ejecución sistemática de los cuatro tipos de pruebas sobre cada uno de los protocolos VPN configurados:

1. **Latencia**: medida mediante el comando *ping*, enviando 20 paquetes ICMP por iteración para obtener tiempos de respuesta promedio, mínimo y máximo.
2. **Jitter**: se midió con la herramienta *iperf3* en modo UDP, evaluando la variación en los tiempos de llegada de los paquetes durante sesiones de 10 segundos, utilizando un ancho de banda de 5 Mbps.
3. **Pérdida de Paquetes**: también medida con *iperf3* en modo UDP, cuantificando el porcentaje de paquetes enviados que no llegaron correctamente al destino durante cada sesión.
4. **Ancho de Banda**: calculado mediante *iperf3* en modo TCP, determinando el *throughput* efectivo alcanzado en sesiones de 10 segundos por iteración.

El script definió los siguientes parámetros clave al inicio de su ejecución:

- *PROTOCOLO="vpn"*: variable que identifica el protocolo VPN evaluado y se utiliza como nombre de la carpeta de resultados.
- *SERVER_IP="192.168.1.100"*: dirección IP del servidor al que se dirigen todas las pruebas.
- *ITERACIONES=10*: número de veces que se repite cada prueba para obtener resultados

estadísticamente válidos.

- *CARPETA_BASE="$HOME/vpn_tests/$PROTOCOLO"*: ruta base donde se almacenan todos los resultados generados.

Cada una de las tres pruebas se ejecutó dentro de bucles *for* que iteraban del 1 al 10, almacenando la salida de cada ejecución en archivos de texto que servirían para el análisis posterior y fueron nombrados según el tipo de prueba y el número de iteración. Por ejemplo: *tcp1.txt*, *tcp2.txt*, etc.

Este enfoque estructurado permitió no solo automatizar el proceso, sino también mantener la organización y trazabilidad de los datos, facilitando el análisis posterior.

2. Resultados de la Optimización

La puesta en operación del script, sentó las bases para una mejora del proceso de recolección de datos, pues le permitió ejecutar hasta un total de 30 pruebas de forma automatizada, en condiciones homogéneas, y que la estandarización de los nombres de archivos y rutas, permitió la integración de los resultados en herramientas de procesamiento y análisis estadísticos.

La modularidad del script además supuso una mejor reutilización para los cuatro protocolos VPN evaluados, puesto que bastó con cambiar el valor de la variable PROTOCOLO, algo que llevó a conseguir una coherencia total en la metodología.

IV. RESULTADOS

A. *Metodología de Evaluación de Rendimiento*

Con el propósito de analizar el rendimiento de las tecnologías VPN en este trabajo, se realizó una revisión sistemática basada en pruebas controladas. La configuración consistió en un par de estaciones dinámicas interconectadas a través de las distintas tecnologías VPN que se evaluaban.

Para llevar a cabo el estudio, se configuró el primer equipo de prueba como el servidor; para ello ejecutó el comando `iperf3 -s` con el fin de poder aceptar también las conexiones VPN entrantes. El equipo que actuó como esforzado, el segundo equipo de prueba, sería el cliente, y mediante él se iban a ejecutar las pruebas de protocolos de distintas configuraciones.

1. Tipos de Pruebas Implementadas

En general, se ejecutaron tres tipos de pruebas con el objetivo de poder estudiar el rendimiento de manera exhaustiva de las tecnologías VPN:

Prueba de Latencia

Para esta prueba, se utilizó el comando de `ping` para estudiar el tiempo de respuesta que había entre el cliente y el servidor. Esta prueba estaba configurada para que se envasaran 20 paquetes ICMP por iteración y así obtener las métricas de tiempo de respuesta medios, mínimo y máximo.

Prueba de Jitter y Pérdida de Paquetes

Por otro lado, la herramienta que utilizamos fue `iperf3` pero en este caso en modo UDP y con un ancho de banda configurado de 5 Mbps durante 10 segundos, permitiendo obtener el jitter en los tiempos de latencia y determinar el porcentaje de paquetes perdidos en la transmisión.

Prueba de Bandwidth

Para medir el ancho de banda efectivo, la herramienta empleada fue `iperf3` pero en este caso en su modo TCP y con el mismo tiempo de 10 segundos por iteración; esta prueba determinará el throughput máximo que se alcanza a través de cada tecnología VPN evaluada.

2. *Uniformidad de la Metodología*

El mismo script fue aplicado para cada tecnología VPN evaluada, modificando únicamente el nombre del protocolo en la variable `PROTOCOLO`. Esta aproximación garantizó la uniformidad en la metodología de pruebas y aseguró la comparabilidad de los resultados obtenidos entre las diferentes tecnologías VPN.

B. *Documentación de Resultados de Pruebas - WireGuard*

Con el objetivo de comprobar el rendimiento de la VPN WireGuard se realizaron pruebas exhaustivas de latencia, jitter, pérdida de paquetes y bandwidth en varios intervalos de tiempo. La implementación de WireGuard se evaluó utilizando el protocolo de comunicación dispuesto para el ordenador PC1 y PC2, realizando las pruebas automatizadas de acuerdo con la metodología de pruebas presentada anteriormente.

1. *Pruebas de Latencia - WireGuard*

En la Tabla XVII, se presentan los resultados de las pruebas de latencia para WireGuard, donde se mide el tiempo de respuesta entre el cliente y el servidor utilizando el comando `ping` con 20 paquetes ICMP por iteración.

En la Tabla XVII se presentan las pruebas de latencia llevadas a cabo para WireGuard, se muestra cómo se mide el tiempo de respuesta desde el cliente hacia el servidor, usando el comando ping utilizando 20 paquetes ICMP por iteración.

TABLA XVII
RESULTADOS DE LATENCIA PARA WIREGUARD

Archivo	**Promedio (ms)**	**Mínimo (ms)**	**Máximo (ms)**
latencia_1.txt	8.22	4.25	24.49
latencia_2.txt	10.88	3.37	42.88
latencia_3.txt	9.56	5.06	25.37
latencia_4.txt	7.26	3.12	14.16
latencia_5.txt	9.25	5.49	17.48
latencia_6.txt	8.56	3.31	11.87
latencia_7.txt	10.27	5.28	13.77
latencia_8.txt	8.31	4.05	18.28
latencia_9.txt	9.76	4.44	18.59
latencia_10.txt	9.43	4.57	19.95
Promedio General	**9.15**	**4.29**	**20.68**

Los resultados de latencia para WireGuard presentan un tiempo de respuesta medio en general de 9.15 ms, con valores mínimos que van de 3.12 a 5.49 ms y máximos que van desde 11.87 hasta 42.88 ms.

2. Pruebas de Ancho de Banda - WireGuard

La Tabla XVIII concentra los resultados de las pruebas de ancho de banda para WireGuard y que miden el ancho de banda efectivo de las conexiones VPN usando `iperf3` en modo TCP durante 10 segundos por iteración.

TABLA XVIII
RESULTADOS DE ANCHO DE BANDA PARA WIREGUARD

Archivo	**Transferencia Total (MBytes)**	**Tasa de Transferencia (Mbps)**
tcp_1.txt	1.25	1.05
tcp_2.txt	1.38	1.15
tcp_3.txt	1.38	1.15
tcp_5.txt	1.38	1.15
tcp_6.txt	1.25	1.05
tcp_7.txt	1.38	1.15
tcp_8.txt	1.25	1.05
tcp_9.txt	1.38	1.15
tcp_10.txt	1.38	1.15
Promedio	**1.33**	**1.12**

El análisis correspondiente de ancho de banda para el protocolo WireGuard indica una tasa de transferencia media de 1.12 Mbps, mientras que la transferencia total media resulta ser de 1.33 MBytes para una prueba de 10 segundos.

3. Pruebas de Jitter y Pérdida de Paquetes - WireGuard

La Tabla XIX expone los resultados de las pruebas de jitter y de paquetes perdidos obtenidos durante las pruebas de transmisión realizadas en modo UDP de WireGuard con `iperf3` y con un ancho de banda configurado de 5 Mbps.

Los resultados de jitter para WireGuard muestran un valor promedio de 8.31 ms y la pérdida de paquetes promedio se sitúa en el 58% del total de paquetes enviados (aproximadamente 4569 paquetes por prueba).

TABLA XIX
RESULTADOS DE JITTER Y PÉRDIDA DE PAQUETES PARA WIREGUARD

Archivo	**Jitter (ms)**	**Pérdida de Paquetes (%)**	**Total de Paquetes Enviados**
udp_1.txt	8.14	56	4569
udp_2.txt	8.06	59	4569
udp_3.txt	8.06	59	4569
udp_4.txt	8.97	59	4569
udp_5.txt	7.84	58	4569
udp_6.txt	7.72	57	4569
udp_7.txt	9.57	58	4569
udp_8.txt	7.77	58	4569
udp_9.txt	7.77	58	4565
udp_10.txt	10.17	58	4569
Promedio	**8.31**	**58**	**4569**

4. Aspectos de Seguridad de WireGuard

Entre sus características de seguridad, WireGuard presenta una moderna infraestructura de seguridad, apoyada en una criptografía actualizada y en un diseño muy minimalista. En la configuración probada sobre los routers MikroTik se pudo ver que cada peer usa un único par de claves públicas y privadas, las cuales son intercambiadas de forma segura en conformidad con el protocolo Noise IK, lo que se traduce en que, entre otras ventajas, se puede garantizar la confidencialidad directa perfecta, así como una autenticación mutua en ambos extremos.

El protocolo implementa los siguientes mecanismos criptográficos:

- **ChaCha20-Poly1305**: para cifrado autenticado de datos (AEAD).
- **Curve25519**: para el intercambio de claves de tipo ECDH.
- **BLAKE2s**: como función hash segura.
- **HKDF**: para derivación de claves (RFC5869).
- **Mitigación DoS**: mediante uso de cookies MAC basadas en IP para evitar agotamiento de recursos del servidor.

Además, el túnel está autenticado y cifrado extremo a extremo y los parámetros como el número de secuencia (nonce) garantizan protección contra ataques de repetición y reutilización.

C. Documentación de Resultados de Pruebas - PPTP

En la misma línea establecida para la metodología WireGuard, procedimos a estudiar, en las mismas condiciones del test aplicado, el rendimiento de PPTP. A pesar de ser una tecnología de VPN que resulta más vulnerable a los ataques que sus implementaciones contemporáneas, sigue estando implementada en diversos escenarios gracias a su facilidad de configuración y también debido a necesidades de compatibilidad con sistemas legacy.

1. Pruebas de Latencia - PPTP

En la Tabla XX se presenta los resultados de las pruebas de latencia para PPTP, donde se mide el tiempo de respuesta entre el cliente y el servidor utilizando el comando `ping` con 20 paquetes ICMP por iteración y de esa forma manteniendo la misma configuración empleada en las pruebas de WireGuard.

TABLA XX
RESULTADOS DE LATENCIA PARA PPTP

Archivo	**Promedio (ms)**	**Mínimo (ms)**	**Máximo (ms)**
latencia_1.txt	8.20	4.55	15.30
latencia_2.txt	8.19	4.55	13.11
latencia_3.txt	8.69	5.02	16.16
latencia_4.txt	8.20	4.19	20.34
latencia_5.txt	8.95	4.43	20.30
latencia_6.txt	9.89	4.82	23.80
latencia_7.txt	10.16	5.53	22.18
latencia_8.txt	8.30	4.05	17.67
latencia_9.txt	11.41	5.70	26.34
Promedio General	**9.15**	**4.79**	**19.47**

Los resultados presentados en la latencia para PPTP muestran un tiempo de respuesta promedio general de 9.15 ms, con valores mínimos que oscilan entre 4.05 y 5.70 ms y máximos que varían desde 13.11 hasta 26.34 ms.

2. Pruebas de Ancho de Banda - PPTP

La Tabla XXI resume los resultados de las pruebas de ancho de banda para PPTP, que miden el ancho de banda efectivo en las conexiones VPN utilizando `iperf3` en modo TCP durante 10 segundos por iteración.

El análisis de ancho de banda del PPTP muestra que la tasa de transferencia promedio es

TABLA XXI
RESULTADOS DE ANCHO DE BANDA PARA PPTP

Archivo	**Transferencia Total (MBytes)**	**Tasa de Transferencia (Mbps)**
tcp_1.txt	1.25	1.05
tcp_2.txt	1.25	1.05
tcp_3.txt	1.25	1.05
tcp_4.txt	1.25	1.05
tcp_5.txt	*Sin datos*	*Sin datos*
tcp_6.txt	1.25	1.05
tcp_7.txt	1.25	1.05
tcp_8.txt	1.25	1.05
tcp_9.txt	1.25	1.05
tcp_10.txt	*Sin datos*	*Sin datos*
Promedio	**1.25**	**1.05**

de 1.05 Mbps y la transferencia total media en las pruebas de 10 segundos es de 1.25 MBytes. Cabe mencionar que en las pruebas llevadas a cabo para los archivos tcp_5.txt y tcp_10.txt no se obtuvieron datos válidos (ya que la conexión se interrumpió)

3. Pruebas de Jitter y Pérdida de Paquetes - PPTP

La Tabla XXII presenta los resultados de las pruebas de jitter y la cantidad de paquetes perdidos durante las pruebas de transmisión para PPTP y de esa forma utilizando `iperf3` con un ancho de banda configurado de 5 Mbps.

TABLA XXII
RESULTADOS DE JITTER Y PÉRDIDA DE PAQUETES PARA PPTP

Archivo	**Jitter (ms)**	**Pérdida de Paquetes (%)**	**Total de Paquetes Enviados**
udp_1.txt	9.09	57	4468
udp_2.txt	7.79	59	4467
udp_3.txt	9.55	59	4470
udp_4.txt	9.59	59	4469
udp_5.txt	9.03	59	4469
udp_6.txt	9.42	59	4471
udp_7.txt	11.71	59	4469
udp_8.txt	8.08	59	4467
udp_9.txt	10.30	59	4470
udp_10.txt	8.00	59	4467
Promedio	**9.26**	**59**	**4469**

Los resultados de jitter para PPTP muestran un valor promedio de 9.26 ms, mientras que la pérdida de paquetes promedio se sitúa en el 59% del total de paquetes enviados (aproximadamente

4469 paquetes por prueba).

4. Aspectos de Seguridad de PPTP

El protocolo PPTP se vale del protocolo GRE (Generic Routing Encapsulation) como técnica para llevar a cabo la encapsulación de datos y el protocolo de autenticación PPP para la gestión del acceso. En este sentido, PPTP es muy vulnerable a ataques de fuerza bruta ya que la seguridad se basa completamente en el esquema de autenticación MS-CHAPv1 o MS-CHAPv2 (los cuales son utilizados por PPTP). Lamentablemente, estos mecanismos de autenticación son conocidos por sus debilidades que permiten que un atacante obtenga la contraseña o bien de un equipo que haya ejecutado la conexión o de un programa del cliente. Sin embargo, ambos mecanismos presentan vulnerabilidades conocidas:

- **MS-CHAPv1**: considerado completamente inseguro, puede romperse con ataques de diccionario en segundos.
- **MS-CHAPv2**: mejora ligeramente el proceso de autenticación, pero aún es susceptible a ataques de fuerza bruta debido a su débil diseño criptográfico.
- **MPPE (Microsoft Point-to-Point Encryption)**: es el esquema de cifrado utilizado por PPTP, basado en el algoritmo RC4. Este algoritmo ha sido desaconsejado por múltiples entidades de seguridad debido a su debilidad frente a ataques criptográficos modernos.

PPTP no ofrece integridad de los datos ni protección contra ataques de tipo “man-in-the-middle” y no soporta cifrado de extremo a extremo robusto ni la verificación de identidad mediante certificados digitales.

D. Documentación de Resultados de Pruebas - IPsec

Continuando con la evaluación sistemática de las tecnologías VPN analizadas, se procedió a evaluar el rendimiento de IPsec bajo las mismas condiciones metodológicas aplicadas para WireGuard y PPTP. IPsec representa una de las tecnologías VPN más robustas y ampliamente adoptadas en entornos empresariales, ofreciendo un conjunto completo de protocolos para asegurar las comunicaciones IP a través de la autenticación, integridad y confidencialidad de los datos.

1. Pruebas de Latencia - IPsec

En la Tabla XXIII, se presentan los resultados de las pruebas de latencia para IPsec y donde se mide el tiempo de respuesta entre el cliente y el servidor utilizando el comando `ping` con 20 paquetes ICMP por iteración.

TABLA XXIII
RESULTADOS DE LATENCIA PARA IPSEC

Archivo	**Promedio (ms)**	**Mínimo (ms)**	**Máximo (ms)**
latencia_1.txt	8.45	4.12	18.23
latencia_2.txt	9.78	4.89	22.45
latencia_3.txt	8.92	4.56	19.87
latencia_4.txt	9.34	4.23	21.12
latencia_5.txt	8.67	4.78	17.89
latencia_6.txt	9.89	5.12	23.67
latencia_7.txt	8.23	4.34	16.45
latencia_8.txt	9.56	4.67	20.78
latencia_9.txt	8.78	4.45	18.92
latencia_10.txt	9.12	4.89	19.67
Promedio General	**9.07**	**4.61**	**19.91**

Los resultados de latencia para IPsec muestran un tiempo de respuesta promedio general de 9.07 ms, con valores mínimos que oscilan entre 4.12 y 5.12 ms, y máximos que varían desde 16.45 hasta 23.67 ms.

2. Pruebas de Ancho de Banda - IPsec

La Tabla XXIV resume los resultados de las pruebas de ancho de banda para IPsec, que miden el ancho de banda efectivo en las conexiones VPN utilizando `iperf3` en modo TCP durante 10 segundos por iteración.

El análisis de ancho de banda para IPsec revela una tasa de transferencia promedio de 1.19 Mbps y con una transferencia total promedio de 1.43 MBytes por prueba de 10 segundos.

3. Pruebas de Jitter y Pérdida de Paquetes - IPsec

La Tabla XXV presenta los resultados de las pruebas de jitter y la cantidad de paquetes perdidos durante las pruebas de transmisión en modo UDP para IPsec y de igual forma utilizando `iperf3` con un ancho de banda configurado de 5 Mbps.

Los resultados de jitter para IPsec muestran un valor promedio de 8.03 ms, mientras tanto

TABLA XXIV
RESULTADOS DE ANCHO DE BANDA PARA IPSEC

Archivo	Transferencia Total (MBytes)	Tasa de Transferencia (Mbps)
tcp_1.txt	1.38	1.15
tcp_2.txt	1.38	1.15
tcp_3.txt	1.50	1.25
tcp_4.txt	1.38	1.15
tcp_5.txt	1.50	1.25
tcp_6.txt	1.38	1.15
tcp_7.txt	1.50	1.25
tcp_8.txt	1.38	1.15
tcp_9.txt	1.50	1.25
tcp_10.txt	1.38	1.15
Promedio	**1.43**	**1.19**

TABLA XXV
RESULTADOS DE JITTER Y PÉRDIDA DE PAQUETES PARA IPSEC

Archivo	Jitter (ms)	Pérdida de Paquetes (%)	Total de Paquetes Enviados
udp_1.txt	7.89	55	4590
udp_2.txt	8.45	56	4590
udp_3.txt	7.23	54	4590
udp_4.txt	8.12	57	4590
udp_5.txt	7.67	55	4590
udp_6.txt	8.78	56	4590
udp_7.txt	7.34	54	4590
udp_8.txt	8.56	57	4590
udp_9.txt	7.98	55	4590
udp_10.txt	8.23	56	4590
Promedio	**8.03**	**55**	**4590**

que la pérdida de paquetes promedio se sitúa en el 55% del total de paquetes enviados.

4. Aspectos de Seguridad de IPsec

IPsec se define como una suite de protocolos que tiene como fin proveer comunicaciones seguras a nivel de red, y que realiza la autenticación, la integridad y el cifrado de los paquetes IP.

La implementación de IPsec que se estudia en este trabajo emplea las siguientes características de seguridad, donde se incluyen las siguientes características:

- **Autenticación mutua**: basada en claves precompartidas (PSK), certificados digitales o

credenciales RSA, según la configuración establecida.

- **Cifrado de datos**: mediante algoritmos robustos como AES-128 o AES-256, con modos de operación CBC o GCM, dependiendo de la negociación.
- **Integridad y autenticación**: proporcionada por algoritmos como HMAC-SHA1 o HMAC-SHA256.
- **Protocolo IKE (Internet Key Exchange)**: encargado de la negociación de parámetros de seguridad, establecimiento del túnel y gestión de claves.
- **Modos de operación**: modo transporte (protección de carga útil IP) y modo túnel (protección de todo el paquete IP).

IPsec está debidamente preparado para ofrecer un alto nivel de protección contra los ataques spy, ataques replay, ataques de tipo man-in-the-middle (MITM) y sniffing, su complejidad de configuración y la introducción de sobrecarga criptográfica pueden impactar ligeramente en el rendimiento, lo cual queda reflejado en los resultados medidos.

E. Documentación de Resultados de Pruebas - SSTP

En el contexto del presente análisis de este trabajo, para completar la evaluación sistemática de las tecnologías VPN comentadas a lo largo del estudio, se evalúa el rendimiento de SSTP, tecnología con características arquitectónicas originales dada la utilización del protocolo SSL/TLS como parte del proceso de establecimiento del túnel seguro.

1. Pruebas de Latencia - SSTP

Las pruebas de latencia que se han obtenido para SSTP, las podemos observar en la Tabla XXVI, donde se observa el tiempo empleado en la conversación cliente y servidor, con el comando ping a partir de 20 paquetes ICMP por iteración.

Los resultados de latencia para SSTP muestran un tiempo de respuesta promedio general de 10.96 ms, con valores mínimos que oscilan entre 4.63 y 6.13 ms, y máximos que varían desde 16.34 hasta 30.25 ms.

2. Pruebas de Ancho de Banda - SSTP

La Tabla XXVII resume los resultados de las pruebas de ancho de banda para SSTP, que miden el ancho de banda efectivo en las conexiones VPN utilizando `iperf3` en modo TCP

TABLA XXVI
RESULTADOS DE LATENCIA PARA SSTP

Archivo	Promedio (ms)	Mínimo (ms)	Máximo (ms)
latencia_1.txt	11.19	5.93	19.27
latencia_2.txt	9.63	4.63	16.34
latencia_3.txt	10.80	4.94	30.25
latencia_4.txt	11.35	5.53	21.97
latencia_5.txt	11.50	5.98	21.84
latencia_6.txt	11.28	4.63	23.25
latencia_7.txt	10.54	5.39	16.35
latencia_8.txt	10.31	5.42	19.32
latencia_9.txt	11.23	5.46	20.30
latencia_10.txt	11.76	6.13	18.08
Promedio General	**10.96**	**5.40**	**20.70**

durante 10 segundos por iteración.

TABLA XXVII
RESULTADOS DE ANCHO DE BANDA PARA SSTP

Archivo	Transferencia Total (MBytes)	Tasa de Transferencia (Mbps)
tcp_1.txt	1.50	1.26
tcp_2.txt	1.62	1.36
tcp_3.txt	2.25	1.89
tcp_4.txt	1.50	1.26
tcp_5.txt	1.62	1.36
tcp_6.txt	1.62	1.36
tcp_7.txt	2.50	2.10
tcp_8.txt	1.50	1.26
tcp_9.txt	1.62	1.36
tcp_10.txt	1.62	1.36
Promedio	**1.74**	**1.46**

El análisis de ancho de banda para SSTP revela una tasa de transferencia promedio de 1.46 Mbps y con una transferencia total promedio de 1.74 MBytes por prueba de 10 segundos.

3. Pruebas de Jitter y Pérdida de Paquetes - SSTP

La Tabla XXVIII presenta los resultados de las pruebas de jitter y la cantidad de paquetes perdidos durante las pruebas de transmisión en modo UDP para SSTP, utilizando `iperf3` con un ancho de banda configurado de 5 Mbps, manteniendo la consistencia metodológica con las evaluaciones previas.

TABLA XXVIII
RESULTADOS DE JITTER Y PÉRDIDA DE PAQUETES PARA SSTP

Archivo	Jitter (ms)	Pérdida de Paquetes (%)	Total de Datagramas
udp_1.txt	11.74	54	4316
udp_2.txt	34.01	56	4316
udp_3.txt	14.16	54	4132
udp_4.txt	27.21	56	4317
udp_5.txt	35.19	56	4317
udp_6.txt	13.38	54	4147
udp_7.txt	14.65	54	4119
udp_8.txt	39.01	56	4317
udp_9.txt	23.00	56	4316
udp_10.txt	28.48	56	4316
Promedio	**24.08**	**55.2**	**4295**

Los resultados de Jitter en SSTP muestran un resultado promedio de jitter de 24.08 ms, presentando un rango alto de variabilidad de 11.74 y 39.01 ms, mostrando así unas diferencias singulares de características en los tiempos de latencia para testear UDP, es decir, en las variaciones de los tiempos de respuesta. La pérdida del paquete medio se localiza alrededor del 55.2% del total de datagramas transferidos (aproximadamente unos 4295 datagramas por test), mostrando un rendimiento medio para conducir el tráfico de UDP intenso.

4. Aspectos de Seguridad de SSTP

SSTP es un protocolo que encapsula el tráfico PPP dentro de una conexión HTTPS segura utilizando técnicas TLS , normalmente sobre el puerto 443. Por esta razón SSTP funciona a través de firewalls y NAT , lo que lo convierte en una solución práctica en entornos poco permeables. SSTP ofrece los siguientes mecanismos desde el punto de vista de la seguridad:

- **Cifrado de extremo a extremo**: se basa en TLS 1.2 o superior para cifrar todo el canal de comunicación, de esa forma, utilizando algoritmos como AES-256-GCM o AES-256-CBC.
- **Autenticación del servidor**: mediante certificados digitales X.509, lo que permite validar la identidad del servidor ante el cliente.
- **Opcionalmente, autenticación del cliente**: también se puede configurar la verificación del certificado del cliente, añadiendo una capa adicional de seguridad.
- **Integridad y protección contra modificación**: garantizada por los mecanismos criptográficos propios de TLS.

- **Resistencia a ataques MITM**: gracias a la validación de certificados y establecimiento de claves durante el handshake TLS.

En la configuración efectiva realizada en MikroTik se activó SSTP por cuenta de que está dotado para poder hacer uso del apoyo de TLS 1.2, apoyando la elección de los fuertes cifrados (AES256-GCM-SHA384, AES256-SHA) y la autenticación con usuario y contraseña por medio de MS-CHAPv2. SSTP, si bien es cierto ofrece un nivel de seguridad aceptable, menoscaba la implementación cerrada que le proporciona Microsoft , limitando por tanto la transparencia del protocolo así como la trazabilidad comunitaria.

F. Análisis Comparativo Integral de Rendimiento y Seguridad

Una vez completadas las evaluaciones individuales de las cuatro tecnologías VPN analizadas (WireGuard, PPTP, IPsec y SSTP), se procede a realizar un análisis comparativo integral que permita identificar las fortalezas y debilidades específicas de cada tecnología tanto en las métricas de rendimiento evaluadas como en los mecanismos de seguridad implementados.

Desde la perspectiva de seguridad, las diferencias entre las tecnologías son significativas:

- **WireGuard** presenta una arquitectura moderna, empleándonos la criptografía de vanguardia para su seguridad, como ChaCha20, Poly1305 y Curve25519. Es sencillo de implementar, y tiene un nivel alto de seguridad asociado a una base de código reducida.
- **IPsec** establece un modelo enormemente configurable y robusto, usado en el contexto empresarial. Proporciona autenticación, integridad y cifrado de extremo a extremo a partir de suites criptográficas como AES y SHA, pero su complejidad de configuración puede dar pie a errores.
- **SSTP** se basa en TLS para hacer el canal cifrado, por lo que puede transitar por firewalls sin ser bloqueado. Su seguridad depende en gran medida de cómo se implemente el protocolo SSL o TLS y de cómo se manejen los certificados.
- **PPTP** es el más débil de todos, ya que tiene vulnerabilidades bien documentadas que afectan a sus mecanismos de autenticación (MS-CHAPv1/v2) y cifrado (MPPE). En la actualidad, ya está considerado inseguro en entornos productivos.

A continuación, se detallan los resultados comparativos por cada métrica de rendimiento.

1. *Comparación de Latencia*

La Tabla XXIX muestra la comparación de los tiempos de latencia que hemos medido para las cuatro tecnologías de VPN que hemos podido evaluar, es decir, puede dar una visión general del rendimiento de las distintas tecnologías de VPN desde el punto de vista de latencia.

TABLA XXIX
COMPARACIÓN DE LATENCIA ENTRE TECNOLOGÍAS VPN

Tecnología	**Promedio (ms)**	**Mínimo Promedio (ms)**	**Máximo Promedio (ms)**
IPsec	9.07	4.61	19.91
WireGuard	9.15	4.29	20.68
PPTP	9.15	4.79	19.47
SSTP	10.96	5.40	20.70

La evaluación de la latencia muestra que IPsec es el mejor protocolo desde el punto de vista del rendimiento, con 9.07 ms de latencia promedio. WireGuard y PPTP son muy cercanos a este valor (9.15 ms de latencia promedio). SSTP es el que tiene mayor latencia, alcanzando los 10.96 ms y suponiendo un incremento del 20.86% con respecto a IPsec. Los valores mínimos y máximos muestran que las diferencias entre los protocolos en este aspecto son bastante pequeñas, lo que puede indicar que el overhead adicional de cada uno de ellos se trae en una forma bastante definida.

2. *Comparación de Ancho de Banda*

La Tabla XXX resume los resultados de throughput obtenidos para las cuatro tecnologías VPN, permitiendo identificar la capacidad de transferencia efectiva de cada implementación.

TABLA XXX
COMPARACIÓN DE ANCHO DE BANDA ENTRE TECNOLOGÍAS VPN

Tecnología	**Transferencia Promedio (MBytes)**	**Tasa Promedio (Mbps)**	**Mejora vs PPTP (%)**
SSTP	1.74	1.46	+39.05
IPsec	1.43	1.19	+13.33
WireGuard	1.33	1.12	+6.67
PPTP	1.25	1.05	–

SSTP lidera significativamente en rendimiento de ancho de banda con 1.46 Mbps, superando a la segunda mejor tecnología (IPsec) en un 22.69%, estos resultados pueden atribuirse a las optimizaciones del protocolo SSL/TLS para el manejo eficiente de grandes volúmenes de

datos a diferencia de las otras tecnologías VPN que no ocupan dicho protocolo, IPsec ocupa el segundo lugar con 1.19 Mbps, seguido por WireGuard (1.12 Mbps) y PPTP (1.05 Mbps) como la tecnología con menor bandwidth.

3. Comparación de Jitter

La Tabla XXXI presenta los resultados comparativos de jitter y pérdida de paquetes para las cuatro tecnologías evaluadas, métricas críticas para aplicaciones sensibles al tiempo.

TABLA XXXI
COMPARACIÓN DE JITTER Y PÉRDIDA DE PAQUETES ENTRE TECNOLOGÍAS VPN

Tecnología	**Jitter Promedio (ms)**	**Pérdida de Paquetes (%)**	**Paquetes Promedio**
IPsec	8.03	55.0	4590
WireGuard	8.31	58.0	4569
PPTP	9.26	59.0	4469
SSTP	24.08	55.2	4295

IPsec maneja mejor el jitter. Este es de 8.03 ms, siendo seguido muy de cerca por WireGuard (8.31 ms). PPTP logra un jitter moderado (9.26 ms) mientras que SSTP tiene la peor performace de todas (24.08 ms), lo que representa un deterioro significativo del 199.75% respecto a IPsec. En cuanto a pérdida de paquetes, el mejor rendimiento corresponde a IPsec (55.0% de pérdida), seguido por SSTP (55.2%), WireGuard (58.0%) y PPTP (59.0%).

4. Análisis Multidimensional del Rendimiento

La Tabla XXXII presenta un ranking general de las tecnologías VPN basado que fueron evaluadas en las métricas previamente presentadas, teniendo así las puntuaciones relativas para facilitar la comparación integral.

TABLA XXXII
RANKING GENERAL DE RENDIMIENTO POR TECNOLOGÍA VPN

Tecnología	**Latencia**	**Bandwidth**	**Jitter**	**Pérdida**	**Promedio**
IPsec	1°	2°	1°	1°	1.25
WireGuard	2°	3°	2°	3°	2.50
PPTP	2°	4°	3°	4°	3.25
SSTP	4°	1°	4°	2°	2.75

El análisis multidimensional pone de manifiesto que IPsec es la que tiene un mejor rendimiento general comparativo, debido a que proporciona el mejor resultado en tres de las cuatro métricas analizadas (latencia, jitter y pérdida de paquetes), siendo el segundo mejor en el

caso de bandwidth. WireGuard es la segunda mejor (cualificado como el segundo mejor en todas las métricas). SSTP es la que proporciona el mejor resultado en bandwidth, pero obtiene una carga considerable en jitter, y PPTP es la que obtiene el peor rendimiento en la gran mayoría de las métricas de esta comparación.

5. Análisis Multidimensional de la Seguridad

Además de los criterios de rendimiento, se ha analizado el índice de seguridad proporcionado por cada tecnología de VPN. La Tabla XXXIII proporciona un ranking cualitativo basado en los distintos mecanismos criptográficos, autenticación, integridad, resistencia a los diferentes tipos de ataques y actualidad de cada protocolo.

TABLA XXXIII
RANKING GENERAL DE SEGURIDAD POR TECNOLOGÍA VPN

Tecnología	**Cifrado Moderno**	**Autenticación Fuerte**	**Integridad de Datos**	**Resistencia a Ataques**	**Ranking**
WireGuard	Sí (ChaCha20, Poly1305)	Alta (clave pública)	Alta (AEAD)	Muy alta (DoS, MITM)	1°
IPsec	Sí (AES, SHA2)	Alta (PSK/RSA)	Alta (HMAC-SHA)	Muy alta (MITM, Replay)	2°
SSTP	Sí (TLS 1.2)	Media-Alta (certificados, MS-CHAPv2)	Alta (TLS)	Alta (MITM, Spoofing)	3°
PPTP	No (RC4, MPPE)	Baja (MS-CHAPv2)	Baja (sin verificación fuerte)	Baja (vulnerable a MITM, Replay)	4°

WireGuard se posiciona como la tecnología más segura por el uso de criptografía contemporánea, su modelo de claves públicas y su diseño minimalista, que reducen la superficie de ataque. IPsec sigue siendo una alternativa fuerte y madura, especialmente en entornos empresariales donde se requieren configuraciones avanzadas. SSTP ofrece una seguridad aceptable basada en TLS, pero su enfoque propietario le asigna ciertas limitaciones. PPTP, en todo caso, tiene ciertas carencias que no le hacen idóneo para los entornos donde se requieren altos niveles de seguridad.

V. CONCLUSIONES Y RECOMENDACIONES

A. Conclusiones

La presente investigación, permitió determinar las tecnologías VPN predominantes para el análisis en el ámbito corporativo, identificando a IPsec, WireGuard, SSTP y PPTP como los protocolos relevantes. El estudio de sus arquitecturas, mecanismos de seguridad y protocolos de encapsulación sentó la base teórica indispensable que guió la fase experimental comparativa de la investigación.

Se diseñó y configuró exitosamente un entorno de emulación de red controlado, el cual permitió la implementación y evaluación de cada túnel VPN bajo condiciones de tráfico idénticas y estandarizadas. Esta plataforma fue crucial para la recolección de datos empíricos fiables sobre parámetros clave de rendimiento como latencia, jitter, ancho de banda y pérdida de paquetes, asegurando la validez de la comparación.

El análisis comparativo de los datos de rendimiento mostró distinciones claras, IPsec demostró ser superior para aplicaciones sensibles al retardo como VoIP por su baja latencia y jitter. WireGuard se presentó como una solución moderna y eficiente con un rendimiento general sólido. SSTP mostró un buen ancho de banda a costa de una mayor latencia, y PPTP resultó ser la opción menos eficaz. En materia de seguridad, IPsec y WireGuard se confirmaron como las alternativas más robustas, en contraste con la inseguridad inherente de PPTP.

Finalmente, se destaca que no existe una tecnología VPN universalmente superior, sino que la elección óptima es el resultado de un balance estratégico entre las prioridades de rendimiento y los requisitos de seguridad de una organización.IPsec para máxima fiabilidad en tiempo real, WireGuard para un equilibrio entre eficiencia y seguridad moderna, y SSTP para nichos específicos donde el ancho de banda prevalezca sobre la latencia. Se recomienda de forma concluyente evitar la tecnología PPTP en cualquier entorno que requiera un mínimo de protección y confidencialidad de la información.

B. Recomendaciones

Para futuras implementaciones, se recomienda priorizar la configuración de protocolos VPN en función del tipo de tráfico y las características del entorno. En aplicaciones sensibles a

la latencia como VoIP o videoconferencias, se debe optar por IPsec configurado en modo túnel con cifrado AES-256 y autenticación HMAC-SHA2. Este protocolo ha demostrado el mejor desempeño en términos de estabilidad de latencia y control de jitter, siendo ideal para redes corporativas donde la calidad del servicio en tiempo real es crítica.

Es imprescindible evitar el uso del protocolo PPTP, incluso en redes privadas o entornos de prueba, debido a sus vulnerabilidades estructurales en mecanismos de cifrado (RC4) y autenticación (MS-CHAPv2). Se recomienda que las organizaciones eliminen completamente su soporte en firewalls, routers y sistemas operativos, sustituyéndolo por alternativas modernas como WireGuard o IPsec, que cumplen con los estándares actuales de seguridad definidos por organismos internacionales como NIST.

Para mantener la integridad y seguridad de los túneles VPN, se sugiere implementar un sistema de automatización para las pruebas de rendimiento y supervisión de tráfico cifrado. El uso de scripts periódicos que ejecuten iperf3 y ping bajo las mismas condiciones de prueba permite generar métricas comparables en el tiempo, detectar degradaciones de servicio y facilitar el diagnóstico proactivo ante caídas de rendimiento. Estos reportes deben ser integrados en herramientas de monitoreo como Zabbix o Grafana para facilitar la visualización de tendencias.

Finalmente, se recomienda que los administradores de red implementen buenas prácticas de gestión del ciclo de vida de las VPN, que incluyan rotación periódica de claves, renovación de certificados, desactivación segura de túneles obsoletos y auditorías de configuración cada seis meses. Además, se sugiere estandarizar las configuraciones mediante plantillas reutilizables (por ejemplo, usando Ansible o scripts en RouterOS) para reducir errores humanos, garantizar la coherencia operativa y facilitar el escalado de la solución a múltiples sedes o nodos remotos.

C. Trabajos futuros

Realizar un estudio comparativo similar, pero implementando las tecnologías VPN en una red corporativa real y en producción. Esto permitiría validar los resultados obtenidos en emulación y analizar el impacto de factores del mundo real como la congestión de la red, la diversidad de hardware y la latencia de los proveedores de Internet. Un análisis longitudinal (de varios meses) podría además revelar datos sobre la estabilidad y fiabilidad a largo plazo de cada solución.

Enfocar una nueva investigación en el impacto que tiene cada VPN sobre los recursos del dispositivo cliente. Se mediría el consumo de CPU, memoria RAM y, especialmente, el impacto en la duración de la batería de dispositivos móviles y portátiles. Este estudio sería de gran relevancia en la era del trabajo remoto y los dispositivos IoT.

Referencias bibliográficas

[1] S. T. Aung y T. Thein, «Comparative Analysis of Site-to-Site Layer 2 Virtual Private Networks,» en *Proceedings of the 2020 IEEE Conference on Computer Applications (ICCA)*, 2020. DOI: 10.1109/ICCA49400.2020.9022848.

[2] S. Budiyanto y D. Gunawan, «Comparative Analysis of VPN Protocols at Layer 2 Focusing on Voice Over Internet Protocol,» *IEEE Access*, vol. 11, págs. 60 853-60 865, 2023. DOI: 10.1109/ACCESS.2023.3286032.

[3] A. M. Abdulazeez, B. W. Salim, D. Q. Zeebaree y D. Doghramachi, «Comparison of VPN Protocols at Network Layer Focusing on Wire Guard Protocol,» *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 14, nº 18, 2020. DOI: 10.3991/ijim.v14i18.16507.

[4] M. O. Akinsanya, C. C. Ekechi y C. D. Okeke, «Virtual Private Networks (VPN): A Conceptual Review of Security Protocols and Their Application in Modern Networks,» *Engineering Science & Technology Journal*, vol. 5, nº 4, abr. de 2024. DOI: 10.51594/estj/v5i4.1076.

[5] T. Lackorzynski, S. Köpsell y T. Strufe, «A Comparative Study on Virtual Private Networks for Future Industrial Communication Systems,» en *Proceedings of the IEEE/ACM International Conference on Industrial Networks and Systems*, Dresden, Germany: Technical University Dresden, 2020.

[6] L. Osswald, M. Haeberle y M. Menth, «Performance Comparison of VPN Solutions,» University of Tuebingen, Chair of Communication Networks, Tuebingen, Germany, Technical Report, 2020, Available from: lukas.osswald@student.uni-tuebingen.de.

[7] S. T. Oktavia, D. F. Priambodo, N. Trianto y R. Purwoko, «Comparative Quality of Service Analysis of VPN Protocols on IPv6,» *Jurnal Nasional Pendidikan Teknik Informatika: JANAPATI*, vol. 12, nº 3, dic. de 2023.

[8] V. Kjorveziroski, C. Bernad, K. Gilly y S. Filiposka, «Full-mesh VPN performance evaluation for a secure edge-cloud continuum,» *Software: Practice and Experience*, vol. 54, nº 8, mar. de 2024. DOI: 10.1002/spe.3329.

[9] Z. Zhang, Y.-Q. Zhang y X. Chu, «An Overview of Virtual Private Network (VPN): IP VPN and Optical VPN,» *Photonic Network Communications*, vol. 7, nº 3, págs. 213-225, 2004. DOI: 10.1023/B:PNET.0000026887.35638.ce.

[10] K. K. Jyothi, L. S. S. Reddy y M. K. Kumar, «Study on Virtual Private Network (VPN), VPN's Protocols And Security,» *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 3, nº 5, págs. 919-932, 2018, ISSN: 2456-3307.

[11] F. A. Salman, «Implementation of IPsec-VPN Tunneling using GNS3,» *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 7, nº 3, págs. 855-860, 2017, ISSN: 2502-4752. DOI: 10.11591/ijeecs.v7.i3.pp855-860.

[12] J. A. Donenfeld, «WireGuard: Next Generation Kernel Network Tunnel,» *Proceedings of the Network and Distributed System Security Symposium*, 2017, Technical whitepaper defining the WireGuard protocol.

[13] A. M. Elsayed, S. K. Hassan y M. A. Rahman, «Enhancing Corporate Network Security and Performance: A Comprehensive Evaluation of WireGuard as a Next-Generation VPN Solution,» en *IEEE Conference on Network and Information Systems Security*, IEEE, 2023. DOI: 10.1109/NISS.2023.10617501.

[14] IsmaelGF, *WireGuard: Tu VPN en 5 minutos*, Technical Tutorial, Guía técnica de implementación de WireGuard, 2024. dirección: https://ismaelgf.com/wireguard-tu-vpn-en-5-minutos.

[15] S. Kent y K. Seo, «Security Architecture for the Internet Protocol,» Internet Engineering Task Force, RFC 4301, 2005, IETF Standard for IP Security Architecture.

[16] GoodAccess, *IPsec VPN Explained: How IPsec works*, Technical Blog, Comprehensive guide to IPsec VPN implementation, ago. de 2023. dirección: https://www.goodaccess.com/blog/ipsec-vpn.

[17] Microsoft Corporation, *Secure Socket Tunneling Protocol (SSTP)*, https://learn.microsoft.com/en-us/windows-server/remote/remote-access/vpn/sstp/secure-socket-tunneling-protocol-sstp, Consultado en julio de 2025, 2023.

[18] S. Alshamrani y A. Alghamdi, «Security Analysis and Comparison of VPN Tunneling Protocols: A Survey,» *Journal of Network and Computer Applications*, vol. 215, pág. 103 556, 2023. DOI: 10.1016/j.jnca.2022.103556.

[19] K. Hamzeh, G. S. Pall, W. Verthein, J. Taarud, W. Little y G. Zorn, «Point-to-Point Tunneling Protocol (PPTP),» Internet Engineering Task Force, RFC 2637, 1999, IETF Informational RFC for PPTP specification.

[20] B. Schneier, Mudge y D. Wagner, *Cryptanalysis of Microsoft's Point-to-Point Tunneling Protocol (PPTP)*, Counterpane Internet Security Technical Report, Security analysis revealing vulnerabilities in PPTP implementation, 1998.

[21] Surfshark, *PPTP VPN: What Is It and Should You Still Use It in 2024?* Technical Blog, Análisis técnico de PPTP y sus implicaciones de seguridad, 2024. dirección: https://surfshark.com/es/blog/pptp-vpn.

[22] V. Babu y D. M. Nicol, «Mechanisms for Precise Virtual Time Advancement in Network Emulation,» *ACM Transactions on Modeling and Computer Simulation*, vol. 32, nº 2, págs. 1-26, 2022. DOI: 10.1145/3478867.

[23] J. Crichigno, N. Ghani, J. Khoury, W. Shu y M.-Y. Wu, «A survey on network simulators, emulators, and testbeds used for research and education,» *Computer Networks*, vol. 239, pág. 110 134, 2023. DOI: 10.1016/j.comnet.2023.110134.

[24] A. Balyk, M. Karpinski, A. Naglik, G. Shangytbayeva e I. Romanets, «Using graphic network simulator 3 for DDoS attacks simulation,» *International Journal of Computing*, vol. 16, nº 4, págs. 219-225, 2017.

[25] alonsojpd, *Primer proyecto de laboratorio de red virtual con GNS3 en Windows e instalación de router Cisco 7200*, Proyecto A, Presidente y fundador de Proyecto A y AjpdSoft, mayo de 2020. dirección: https://proyectoa.com/primer-proyecto-de-laboratorio-de-red-virtual-con-gns3-e-instalacion-de-router-cisco-7200/.

[26] MikroTik, *MikroTik Routers and Wireless: RouterOS Features and Capabilities*, Official MikroTik Website, Official documentation of RouterOS operating system and networking hardware, 2024. dirección: https://mikrotik.com/.

[27] D. F. Handriyanto, «Performance Test Base On PC With RouterOS RouterOS On Board,» *Jurnal Informatika*, vol. 11, nº 2, jul. de 2017, Comparative performance analysis of RouterOS implementations.

[28] Wikipedia, *Quality of service*, Wikipedia, The Free Encyclopedia, Comprehensive overview of Quality of Service concepts and implementations in networking, 2024. dirección: https://en.wikipedia.org/wiki/Quality_of_service.

[29] G. Carvajal y W. Fuertes, «Quality of Service Analysis of IPSec VPNs for Voice and Video Traffic,» en *IEEE Electronics, Robotics and Automotive Mechanics Conference*,

Quantitative analysis of QoS in IPSec VPN implementations for multimedia traffic, IEEE, 2005, págs. 333-338.

[30] Elaboración propia, *Representación conceptual de Quality of Service en redes*, Imagen original creada para ilustrar el concepto de QoS y priorización de tráfico en redes, 2025.

[31] A. S. Tanenbaum y D. J. Wetherall, *Computer Networks*, 5th. Boston, MA: Pearson, 2011, Comprehensive textbook on computer networking fundamentals.

[32] M. Bagnulo, J. Ramos y B. Alarcos, «Performance evaluation of software virtual private networks (VPN),» en *IEEE International Conference on Software Engineering*, Performance analysis of software VPN implementations showing CPU usage impact, IEEE, 2000, págs. 287-291.

[33] D. R. Bhadra, P. R. Soni y C. A. Joshi, «Packet loss probability in wireless networks: A survey,» en *IEEE International Conference on Electrical, Computer and Communication Technologies*, Comprehensive survey of packet loss probability in various wireless sensor networks, IEEE, 2017, págs. 1-6.

[34] Y. Zhao, B. Li, Q. Zhang, M. Chen y W. Zhu, «Online Packet Loss Measurement and Estimation for VPN-Based Services,» *IEEE Transactions on Parallel and Distributed Systems*, vol. 20, nº 9, págs. 1343-1358, 2009, Technical analysis of packet loss measurement in VPN services using large deviation theory.

[35] J. W. Wong e I.-L. Yen, «Performance evaluation of jitter management algorithms,» en *IEEE International Conference on Communications*, Evaluation of jitter management algorithms for real-time applications, IEEE, vol. 3, 2001, págs. 933-937.

[36] A. Asghar, P. A. Shah y E. Ahmed, «Network Jitter Analysis with varying TCP for Internet Communications,» en *IEEE International Conference on Computing, Mathematics and Engineering Technologies*, Analysis of network jitter behavior with TCP variations in Internet communications, IEEE, 2018, págs. 1-6.

[37] M. Taha, «VPN Security: A Review of VPN Architectures, Algorithms and Standards,» *Journal of Cybersecurity and Privacy*, vol. 3, nº 4, págs. 538-559, 2020.

[38] R. Sharma y H. Singh, «An Analysis of VPN Protocols: Performance, Security, and Challenges,» *International Journal of Computer Network and Information Security*, vol. 14, nº 2, págs. 10-19, 2022.

[39] B. M. Zieliński, «Assessment of iPerf as a Tool for LAN Throughput Prediction,» *International Journal of Electronics and Telecommunications*, vol. 69, nº 3, págs. 523-528, 2023. DOI: 10.24425/ijet.2023.146501.

[40] OpenManiak, *Iperf - Herramienta de medición de ancho de banda TCP, UDP y SCTP*, https://openmaniak.com/es/iperf.php, Accedido el 29 de mayo de 2025, 2024.

[41] S. Jordan y A. Bruno, *CCDA 200-310 Official Cert Guide*, 5th. Cisco Press, jul. de 2016, Official certification guide covering PPDIOO methodology and network design principles, ISBN: 9780134305653.

[42] Elaboración propia, *Metodología PPDIOO para gestión del ciclo de vida de redes*, Imagen original creada para ilustrar el ciclo PPDIOO, 2024.