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.