

ABSTRAK

Perkembangan teknologi informasi mendorong kebutuhan akan konektivitas jaringan yang aman, stabil, dan mampu menghubungkan banyak lokasi secara bersamaan. Permasalahan muncul ketika komunikasi data antar kantor pusat, cabang, dan layanan eksternal harus dilakukan melalui jaringan publik yang rentan terhadap penyadapan, manipulasi, dan gangguan kestabilan koneksi. Penggunaan metode konvensional terkadang tidak memberikan performa optimal, baik dari sisi kecepatan maupun efisiensi penggunaan sumber daya, sehingga dibutuhkan solusi alternatif yang lebih ringan dan mudah diimplementasikan. Solusi yang diusulkan pada penelitian ini adalah membangun sistem jaringan VPN Multi-Site berbasis protokol WireGuard. Protokol ini dipilih karena memiliki arsitektur sederhana dan performa tinggi. Sistem dirancang untuk menghubungkan tiga lokasi berbeda, yaitu MikroTik RouterBoard sebagai pusat jaringan, server virtual berbasis VMware sebagai simulasi cabang, dan server cloud VPS sebagai node publik. Dengan pendekatan ini, jalur komunikasi antar lokasi dapat diamankan sepenuhnya tanpa mengorbankan performa jaringan. Metode penelitian yang digunakan meliputi tahap analisis kebutuhan, perancangan topologi, implementasi konfigurasi WireGuard di setiap bagian, dan pengujian performa jaringan. Pengujian dilakukan menggunakan parameter throughput, delay, jitter, dan packet loss untuk mengevaluasi kualitas koneksi. Perangkat keras yang digunakan meliputi MikroTik RouterBoard, server virtual berbasis VMware, dan server cloud VPS, sedangkan perangkat lunak yang digunakan mencakup RouterOS v7, WireGuard, VMware Workstation, serta alat uji seperti Wireshark. Hasil penelitian menunjukkan bahwa VPN Multi-Site berbasis WireGuard mampu memberikan performa koneksi yang stabil dengan throughput tinggi, delay rendah, jitter minimal, dan packet loss mendekati nol. Sistem ini juga aman melalui autentikasi berbasis kunci publik–privat dan enkripsi end-to-end. Dengan hasil tersebut, penelitian ini membuktikan bahwa WireGuard dapat menjadi alternatif unggulan dibanding protokol VPN konvensional, serta dapat diimplementasikan pada infrastruktur dengan spesifikasi perangkat keras yang relatif terbatas tanpa mengurangi kualitas koneksi.

Kata Kunci: VPN Multi-Site, WireGuard, Mikrotik, Performa Jaringan.

ABSTRACT

Advances in information technology have driven the need for secure, stable network connectivity that can connect multiple locations simultaneously. Problems arise when data communication between headquarters, branches, and external services must be conducted over public networks that are vulnerable to interception, manipulation, and connection instability. Conventional methods often fail to deliver optimal performance, both in terms of speed and resource efficiency, necessitating an alternative solution that is lighter and easier to implement. The solution proposed in this study is to build a Multi-Site VPN network system based on the WireGuard protocol. This protocol was chosen for its simple architecture and high performance. The system is designed to connect three different locations: a MikroTik RouterBoard as the network hub, a VMware-based virtual server as a branch simulation, and a VPS cloud server as a public node. With this approach, communication paths between locations can be fully secured without compromising network performance. The research methods used include the stages of needs analysis, topology design, implementation of WireGuard configuration in each section, and network performance testing. Testing was conducted using parameters such as throughput, delay, jitter, and packet loss to evaluate connection quality. The hardware used includes MikroTik RouterBoard, VMware-based virtual servers, and VPS cloud servers, while the software used includes Winbox, WireGuard, VMware Workstation, and testing tools such as Wireshark. The research results show that the WireGuard-based Multi-Site VPN is capable of providing stable connection performance with high throughput, low delay, minimal jitter, and packet loss close to zero. The system is also secure through public-private key-based authentication and end-to-end encryption. With these results, this study proves that WireGuard can be a superior alternative to conventional VPN protocols and can be implemented on infrastructure with relatively limited hardware specifications without compromising connection quality.

Keywords: Multi-Site VPN, WireGuard, Mikrotik, Network Performance.