

ABSTRAK

Implementasi *Virtual Private Network* (VPN) menimbulkan overhead enkapsulasi dan enkripsi yang memengaruhi ukuran paket, sehingga meningkatkan risiko fragmentasi ketika paket melampaui batas *Maximum Transmission Unit* (MTU). Kondisi ini berdampak pada penurunan kualitas jaringan berupa peningkatan *delay*, penurunan *throughput*, dan *packet loss* yang lebih tinggi. Meskipun WireGuard dan IPsec merupakan protokol VPN yang paling banyak digunakan, analisis sistematis mengenai pengaruh variasi MTU terhadap performa keduanya pada kondisi *high latency* masih terbatas. Penelitian ini menggunakan pendekatan eksperimental berbasis simulasi jaringan dengan topologi *site-to-site* yang dibangun pada GNS3 terintegrasi dengan VMware, menggunakan MikroTik CHR dan VyOS sebagai perangkat gateway virtual.

Tiga skenario diuji, yaitu NoVPN sebagai *baseline*, WireGuard, dan IPsec, dengan kondisi *high latency* berupa penambahan *delay* 100 ms dan *packet loss* 1%. Variasi nilai MTU pada rentang 1.280 hingga 1.500 byte diuji secara sistematis menggunakan iperf3 untuk pengukuran trafik TCP dan UDP, ping untuk *delay*, serta Wireshark untuk validasi fragmentasi. Data performa dianalisis menggunakan statistik deskriptif, Coefficient of Variation, klasifikasi kualitas TIPHON, dan analisis konsensus. Hasil menunjukkan bahwa variasi MTU berpengaruh signifikan terhadap performa jaringan, dengan dampak yang berbeda pada setiap protokol dan jenis trafik.

WireGuard menunjukkan penggunaan CPU yang lebih rendah dibandingkan IPsec pada seluruh skenario. Nilai MTU optimal yang diperoleh adalah 1.320 untuk IPsec TCP, 1.488 untuk IPsec UDP, 1.408 untuk WireGuard TCP, dan 1.392 untuk WireGuard UDP. Tidak ada satu nilai MTU yang optimal secara universal, sehingga penyesuaian berbasis protokol sangat diperlukan dalam implementasi VPN pada kondisi jaringan *high latency*.

Kata Kunci: Maximum Transmission Unit, WireGuard, IPsec, Virtual Private Network, Quality of Service

ABSTRACT

The implementation of a Virtual Private Network (VPN) introduces encapsulation and encryption overhead that increases packet size, thereby raising the risk of fragmentation when packets exceed the Maximum Transmission Unit (MTU). This condition degrades network performance by increasing delay, reducing throughput, and causing higher packet loss. Although WireGuard and IPsec are among the most widely used VPN protocols, systematic analyses of the impact of MTU variations on their performance under high-latency network conditions remain limited. This study employed an experimental approach based on network simulation using a site-to-site topology developed in GNS3 integrated with VMware, with MikroTik CHR and VyOS serving as virtual gateway devices.

Three scenarios were evaluated: NoVPN as the baseline, WireGuard, and IPsec, under high-latency conditions simulated by introducing 100 ms of delay and 1% packet loss. MTU values ranging from 1,280 to 1,500 bytes were systematically tested using iperf3 for TCP and UDP traffic measurements, ping for delay measurement, and Wireshark for fragmentation validation. Network performance data were analyzed using descriptive statistics, the Coefficient of Variation (CoV), TIPHON quality classification, and consensus analysis. The results indicate that MTU variation significantly affects network performance, with different impacts depending on the VPN protocol and traffic type.

WireGuard consistently demonstrated lower CPU utilization than IPsec across all test scenarios. The optimal MTU values identified were 1,320 bytes for IPsec TCP, 1,488 bytes for IPsec UDP, 1,408 bytes for WireGuard TCP, and 1,392 bytes for WireGuard UDP. No single MTU value was found to be universally optimal, indicating that protocol-specific MTU optimization is essential for achieving optimal VPN performance under high-latency network conditions.

Keywords: Maximum Transmission Unit, WireGuard, IPsec, Virtual Private Network, Quality of Service.