INTISARI

ANALISIS PERBANDINGAN PENGGUNAAN METODE *TUNNELING CLOUD VIRTUAL PRIVATE NETWORK* DAN *WIREGUARD VIRTUAL PRIVATE NETWORK* PADA INFRASTRUKTUR *HYBRID CLOUD*

Rusdi Hermawan

20/464281/SV/18600

Perkembangan teknologi khususnya dalam infrastruktur *server*, terus mengalami kemajuan signifikan setiap tahunnya. Organisasi dan perusahaan cenderung beralih ke sistem yang lebih kompleks dan terpusat dengan mendorong penerapan migrasi infrastruktur *server* dari *on-premise* ke *public cloud*. Namun, banyak implementasi migrasi dilakukan secara bertahap karena menyangkut keamanan data yang sudah berjalan dan keterbatasan biaya. Dalam konteks ini, infrastruktur *hybrid cloud* menjadi penting untuk menciptakan solusi *bridging* yang efektif, memfasilitasi integrasi yang mulus, meminimalkan *downtime*, dan menjaga konsistensi pada kinerja operasional perusahaan seperti dalam melakukan migrasi berkala atau pengiriman file antar lingkungan *cloud*. Penerapan *hybrid-cloud* sering menggunakan metode *tunneling* untuk menghubungkan infrastruktur *server on-premise* dengan *public cloud*. *Tunneling* mengirim data melalui jalur terenkripsi antara *server on-premise* dan layanan *public cloud*, memanfaatkan teknologi *Virtual Private Network* (VPN) untuk membentuk "*tunnel*" yang aman. Dalam penelitian ini, diterapkan perbandingan dua *tools* VPN: WireGuard sebagai *open-source* dan *Cloud VPN Google Cloud Platform* (GCP) sebagai *enterprise*, dalam konteks implementasi *hybrid-cloud*. Penelitian ini difokuskan pada pengukuran kinerja parameter uji seperti *latency*, *throughput*, kestabilan koneksi, kemudahan konfigurasi, dan biaya layanan, untuk memberikan pemahaman yang mendalam tentang kecocokan masing-masing *tools* untuk skenario implementasi tertentu. Hasil penelitian menunjukkan bahwa *throughput* WireGuard VPN unggul 676,67%, dan rata-rata *latency* WireGuard VPN berkurang hingga 97,66% pada uji pertama, menunjukkan kinerja yang lebih baik dibandingkan dengan Classic Cloud VPN.

Kata kunci : *Hybrid Cloud*, *Tunneling*, VPN, WireGuard, Classic Cloud VPN

ABSTRACT

COMPARATIVE ANALYSIS OF TUNNELING CLOUD VIRTUAL PRIVATE NETWORK AND WIREGUARD VIRTUAL PRIVATE NETWORK METHODS IN HYBRID CLOUD INFRASTRUCTURE IMPLEMENTATION

Rusdi Hermawan

20/464281/SV/18600

The continuous advancement of technology, particularly in server infrastructure, undergoes significant progress each year. Organizations and companies tend to shift towards more complex and centralized systems, driving the adoption of server infrastructure migration from on-premise to public cloud. However, many migration implementations are carried out gradually, as they involve existing data security and cost limitations. In this context, hybrid cloud infrastructure becomes crucial to create effective bridging solutions, facilitating seamless integration, minimizing downtime, and maintaining operational consistency. The implementation of hybrid-cloud often utilizes tunneling methods to connect on-premise server infrastructure with the public cloud. Tunneling sends data through encrypted pathways between on-premise servers and public cloud services, leveraging Virtual Private Network (VPN) technology to form a secure "tunnel." This research applies a comparison of two VPN tools: WireGuard as an open-source solution and Google Cloud Platform's (GCP) Cloud VPN as an enterprise solution, in the context of hybrid-cloud implementation. The study focuses on measuring performance parameters such as latency, throughput, connection stability, ease of configuration, and service costs to provide a deep understanding of the suitability of each tool for specific implementation scenarios. The research findings indicate that WireGuard VPN throughput is superior by 676.67%, and its average total latency is reduced by 97.66% in the first test, indicating that WireGuard VPN performs better than Classic Cloud VPN.

Keywords: Hybrid Cloud, Tunneling, VPN, WireGuard, Classic Cloud VPN