

BAB I

PENDAHULUAN

1.1 Latar Belakang

Pengembangan perangkat lunak berbasis *Continuous Integration and Continuous Deployment (CI/CD)* telah menjadi pendekatan utama dalam meningkatkan kecepatan rilis, kualitas perangkat lunak, serta konsistensi proses integrasi dan deployment aplikasi. Penerapan CI/CD secara fundamental mengubah pola kolaborasi antara pengembang perangkat lunak dengan infrastruktur sistem, sehingga menuntut keterhubungan jaringan yang stabil, aman, dan terkelola secara efisien (Jani, 2023). Dalam konteks tersebut, infrastruktur jaringan komputer berperan sebagai komponen krusial yang menentukan keberhasilan skalabilitas dan kontinuitas operasional lingkungan CI/CD (Istifarulah & Tiaharyadini, 2023).

Keterhubungan antara developer dan infrastruktur CI/CD umumnya dibangun melalui jalur jaringan privat yang bersifat terbatas (*private dan limited access*). Kondisi ini menimbulkan tantangan tersendiri, karena pemilihan dan implementasi teknologi infrastruktur jaringan komputer dapat memengaruhi efektivitas kolaborasi, fleksibilitas pengembangan, serta beban operasional jaringan (Zdun dkk., 2020). Penelitian sebelumnya juga menunjukkan bahwa performa dan desain infrastruktur jaringan memiliki pengaruh signifikan terhadap aspek kolaboratif CI/CD, terutama ketika sistem harus menangani skalabilitas dinamis dan peningkatan beban jaringan secara simultan (Akinsanya dkk., 2024). Oleh karena itu, diperlukan pendekatan jaringan yang tidak hanya aman, tetapi juga efisien dan adaptif terhadap kebutuhan DevOps.

Salah satu pendekatan yang umum digunakan untuk menjembatani komunikasi antara pengembang dan infrastruktur CI/CD adalah pemanfaatan teknologi *Virtual Private Network (VPN)* (Zdun dkk., 2020). Implementasi VPN yang umumnya dilakukan pada lingkungan organisasi menggunakan pendekatan berbasis router dengan protokol L2TP/IPSec, yang memungkinkan terbentuknya jalur komunikasi privat melalui jaringan publik (Aung & Thein, 2020; Hauser dkk., 2020; Putra dkk., 2022). Meskipun pendekatan ini terbukti stabil dan aman, *router-based VPN* memiliki tingkat kompleksitas konfigurasinya yang tinggi, melibatkan penguasaan konfigurasi jaringan Layer 3, routing, manajemen sertifikat, firewall, sistem otentikasi, serta penerapan Access Control List (ACL) untuk pengelolaan hak akses pengguna (Firmansyah & Wahyudi, 2021; Hardikar dkk., 2023). Kompleksitas tersebut menjadikan proses implementasi dan pemeliharaan *router-based VPN* membutuhkan sumber daya teknis yang signifikan serta evaluasi ulang terhadap topologi jaringan internal organisasi (Cho, 2024).

Seiring perkembangan teknologi jaringan, bidang Computer Network telah memperkenalkan pendekatan VPN yang lebih modern, salah satunya melalui teknologi *Modern Kernel-Level VPN* seperti WireGuard. WireGuard dirancang untuk menyederhanakan konfigurasi dan pemeliharaan VPN tanpa mengorbankan aspek keamanan, sehingga berpotensi meningkatkan efisiensi implementasi jaringan pada lingkungan organisasi (MikroTik, 2025; Ostroukh dkk., 2024). Beberapa penelitian menegaskan bahwa WireGuard mampu mereduksi kompleksitas konfigurasi VPN tradisional dan lebih mudah diintegrasikan dalam infrastruktur modern (Novianto dkk., 2022). Meskipun demikian, efektivitas dan

karakteristik implementasi WireGuard pada lingkungan CI/CD masih memerlukan kajian lebih lanjut melalui pendekatan implementatif dan simulatif (Novianto dkk., 2022; Ostroukh dkk., 2024).

Perkembangan teknologi VPN juga melahirkan pendekatan yang lebih mutakhir, yaitu *Zero-Configuration Virtual Private Network*, seperti Tailscale, yang menawarkan kemudahan implementasi dengan minim konfigurasi manual (Fenton, 2024). Pendekatan ini memperkenalkan paradigma baru dalam pengelolaan konektivitas jaringan privat dengan memanfaatkan otomasi, identitas pengguna, dan manajemen akses terpusat, sehingga menjadi alternatif menarik untuk diintegrasikan dalam lingkungan CI/CD modern (Voisey, 2025). Hingga saat ini masih terbatas penelitian yang secara komparatif mengkaji dan mengevaluasi perbedaan implementasi *VPN router-based*, *Modern Kernel-Level VPN*, dan *Zero-Configuration VPN* secara spesifik dalam konteks lingkungan CI/CD, baik dari sisi kompleksitas konfigurasi, efisiensi implementasi, maupun dukungan terhadap integrasi *DevOps* (Kjorveziroski dkk., 2024; Zdun dkk., 2020).

Berdasarkan kesenjangan penelitian tersebut, penelitian ini difokuskan untuk menganalisis dan membandingkan implementasi tiga pendekatan teknologi VPN, yaitu VPN berbasis router (L2TP/IPSec), WireGuard, dan Tailscale, dalam lingkungan *Continuous Integration and Continuous Deployment*. Penelitian ini dirancang untuk menjawab rumusan masalah mengenai perbedaan tingkat kompleksitas konfigurasi serta efektivitas masing-masing teknologi VPN dalam mendukung efisiensi implementasi, manajemen akses, dan integrasi jaringan pada lingkungan *DevOps*. Dengan demikian, tujuan penelitian ini adalah untuk

menganalisis kompleksitas konfigurasi ketiga teknologi VPN berdasarkan skenario simulatif, serta membandingkan efektivitasnya dalam aspek efisiensi implementasi, kemudahan pengelolaan, dan dukungan integrasi *DevOps*, sehingga dapat menjadi dasar pertimbangan pemilihan teknologi VPN yang tepat untuk lingkungan CI/CD.

1.2 Rumusan Masalah

Berdasarkan penyusunan latar belakang di atas, dihasilkan rumusan masalah yang diangkat pada penelitian ini sebagai berikut.

1. Bagaimana perbedaan tingkat kompleksitas konfigurasi antara teknologi VPN berbasis router (L2TP/IPSec), WireGuard, dan Tailscale dalam mendukung integrasi lingkungan CI/CD?
2. Bagaimana efektivitas masing-masing pendekatan VPN dalam menunjang efisiensi implementasi, pengelolaan akses, serta integrasi jaringan pada lingkungan DevOps yang bersifat kolaboratif dan dinamis?

1.3 Tujuan Penelitian

Tujuan penelitian ini dispesifikasikan berdasarkan rumusan masalah yang telah dibuat sebagai berikut.

1. Menganalisis tingkat kompleksitas konfigurasi teknologi L2TP/IPSec, WireGuard, dan Tailscale dalam lingkungan CI/CD berbasis skenario simulatif terkontrol.
2. Mengevaluasi dan membandingkan efektivitas ketiga teknologi VPN dalam aspek efisiensi implementasi, kemudahan pengelolaan akses, serta dukungan terhadap integrasi DevOps.

1.4 Manfaat Penelitian

Adapun manfaat penelitian yang dilakukan sebagai berikut:

1. Manfaat Akademis

Penelitian ini memberikan kontribusi terhadap kajian teknologi jaringan komputer dalam konteks *DevOps*, khususnya dalam memahami bagaimana tingkat adaptabilitas konfigurasi *Virtual Private Network* dapat memengaruhi kontinuitas *workflow Continuous Integration and Continuous Deployment*. Hasil observasi ini diharapkan menjadi referensi awal untuk penelitian lanjutan yang bersifat kuantitatif terkait performa dan efisiensi konektivitas VPN modern.

2. Manfaat Praktis

Hasil penelitian ini dapat menjadi panduan bagi praktisi pengembang perangkat lunak dan *administrator* jaringan dalam memilih teknologi *Virtual Private Network* yang sesuai dengan kebutuhan infrastruktur *Continuous Integration and Continuous Deployment* yang dinamis, terutama dalam aspek otomasi pembaruan konfigurasi dan pengelolaan kredensial antar node.

3. Manfaat Metodologis

Penelitian ini menunjukkan model pendekatan simulatif berbasis observasi teknis sebagai alternatif penelitian empiris pada kondisi infrastruktur yang terbatas, sekaligus memberikan kerangka kerja metodologis bagi penelitian sejenis di bidang otomasi jaringan.

1.5 Batasan Masalah

1. Penelitian ini bersifat simulatif dan tidak melakukan pengukuran performa kuantitatif seperti latency, throughput, maupun waktu konfigurasi aktual karena parameter tersebut sangat bergantung pada kondisi jaringan dan kemampuan teknis operator.
2. Fokus penelitian diarahkan pada analisis adaptabilitas sistem dan kompleksitas pembaruan konfigurasi yang diamati secara deskriptif.
3. Penelitian ini bersifat simulatif yang ditujukan pada organisasi yang akan melakukan penerapan infrastruktur dan sedang melakukan riset tentang teknologi apa yang cocok untuk digunakan bukan untuk ditujukan kepada organisasi yang memiliki skala enterprise.
4. Penelitian ini juga tidak membahas aspek diluar teknis konfigurasi dan skenario yang diuji coba, seperti budgeting dan regulasi IT.