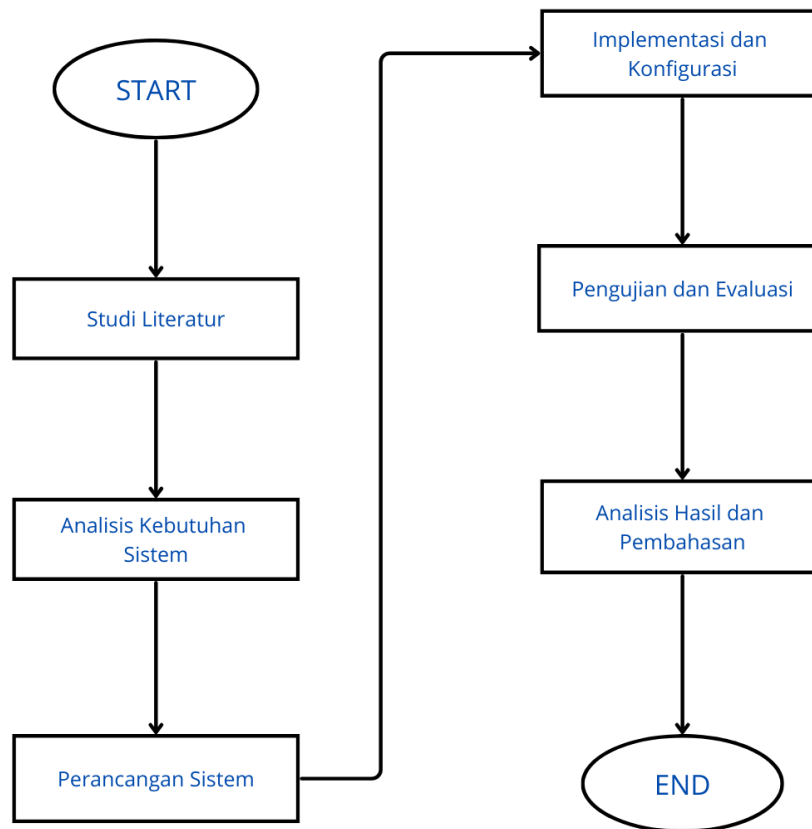


BAB III

METODOLOGI

3.1 Tahapan Penelitian

Tahapan Penelitian yang akan dilaksanakan pada penelitian ini secara keseluruhan disajikan menggunakan diagram alur penelitian. Diagram alur penelitian dapat di simak pada gambar 3.1.



Gambar 3. 1 Diagram Alur Penelitian

Berdasarkan *Gambar 3.1*, diagram alur penelitian merupakan tahapan prosedur untuk melaksanakan penelitian yang dimulai dari tahap studi literature tahap analisis kebutuhan sistem, tahap perancangan sistem, tahap implemetasi dan konfigurasi, serta terakhir di tahap analisis hasil pengujian.

3.2 Studi Literatur

Studi literatur dilakukan untuk memenuhi kebutuhan data, melakukan eksplorasi teoritis dan konseptual di bidang *Continuous Integration dan Continuous Deployment (CI/CD)*, *Virtual Private Network (VPN)* dan *Access Control List (ACL)*. Berdasarkan studi literatur yang telah dilakukan diperoleh berbagai sumber yang dijadikan acuan penelitian diantaranya jurnal, *e-book*, artikel, dokumentasi atau buku manual penggunaan, dan lain sebagainya. Kajian studi literatur yang dilakukan sendiri berdasarkan eksplorasi mandiri dan melakukan pengelolaan referensi yang dibantu oleh *Mendeley Reference Manager*. Indikator keberhasilan yang menjadi acuan dari studi literatur adalah bentuk pemahaman *research scoop*, *research contribution*, *research sector*, melakukan identifikasi peluang penelitian dan menentukan rumusan *research problem*, *question*, dan *objective*. Maka berdasarkan indikator keberhasilan tersebut dapat dihasilkannya keseluruhan Bab I Pendahuluan dan Bab II Tinjauan Pustaka.

3.3 Analisis Kebutuhan Sistem

Analisis kebutuhan sistem ini memiliki tujuan untuk melakukan pemetaan elemen yang diperlukan sebagai persiapan yang dilakukan sebelum melakukan implementasi sistem. Ini diperlukan untuk keberlangsungan penelitian dan mendapatkan gambaran umum sistem yang akan dibangun. Kebutuhan sistem yang dipetakan dalam penelitian ini terbagi menjadi dua jenis, diantaranya kebutuhan *Hardware* dan *Software*.

Tabel 3. 1 Spesifikasi Hardware

Minimal Requirement	Hardware Specification
4 Core Processor	Intel® Core™ i5-12500H 12th Generation Total Cores 12, Total Threads 16.
4 GB+ of RAM	16 GB RAM
50 GB+ of Drive Space	512 GB SSD

Tabel 3.1 merupakan spesifikasi perangkat keras yang dibutuhkan oleh sistem *Continuous Integration and Continuous Deployment* berbasis Jenkins sesuai dengan dokumentasi dari website resmi (Jenkins, 2025), dan juga hardware yang dimiliki untuk digunakan pada penelitian.

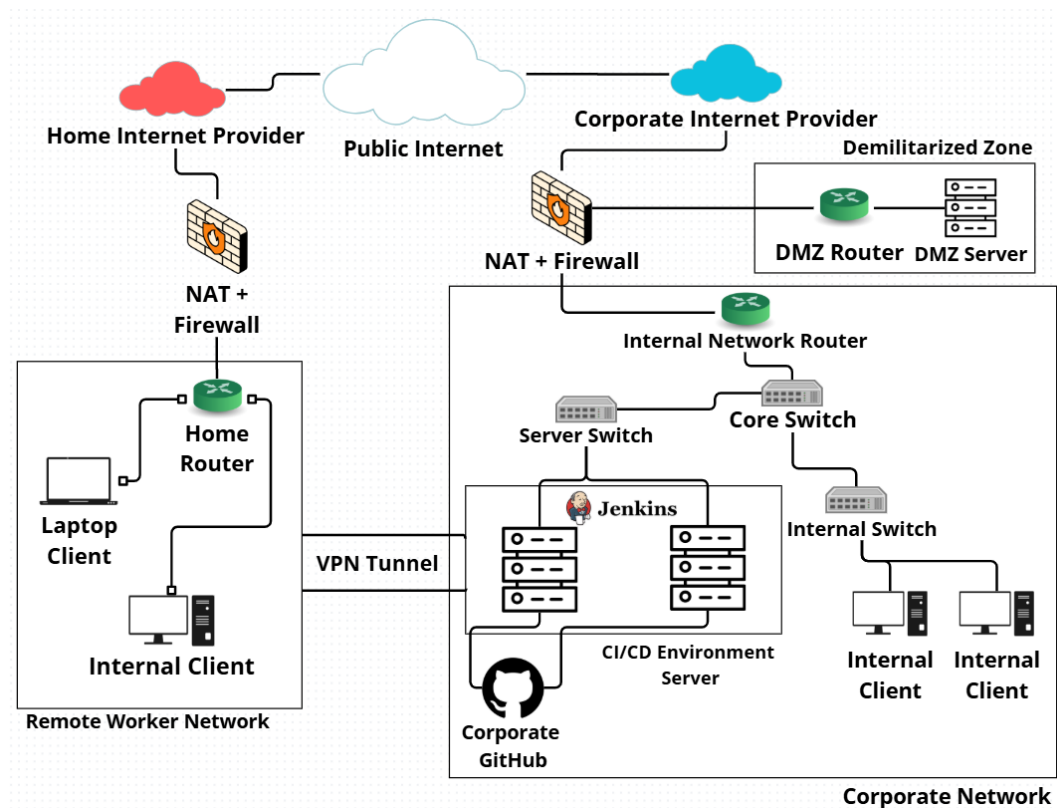
Tabel 3. 2 Spesifikasi Software

Operating System	CI/CD Tools	Router-Based VPN	Modern Kernel-Level VPN	Zero-Configuration VPN
Microsoft Windows 11 Pro & Ubuntu Server 24.04.1 LTS	Jenkins	Mikrotik via L2TP/IPSec	WireGuard	Tailscale

Tabel 3.2 merupakan spesifikasi perangkat lunak yang dibutuhkan oleh sistem rancang bangun lingkungan pengembangan perangkat lunak berbasis *Continuous Integration and Continuous Deployment* dengan berbagai *Virtual Private Network system*, list perangkat lunak yang digunakan didapat berdasarkan studi literatur dan akan di gunakan sebagai acuan realisasi penelitian ini.

3.4 Perancangan Sistem

Perancangan sistem dilakukan untuk membuat desain perencanaan arsitektur jaringan yang akan tergambar secara umum bagaimana sistem akan berjalan normal menggunakan VPN.



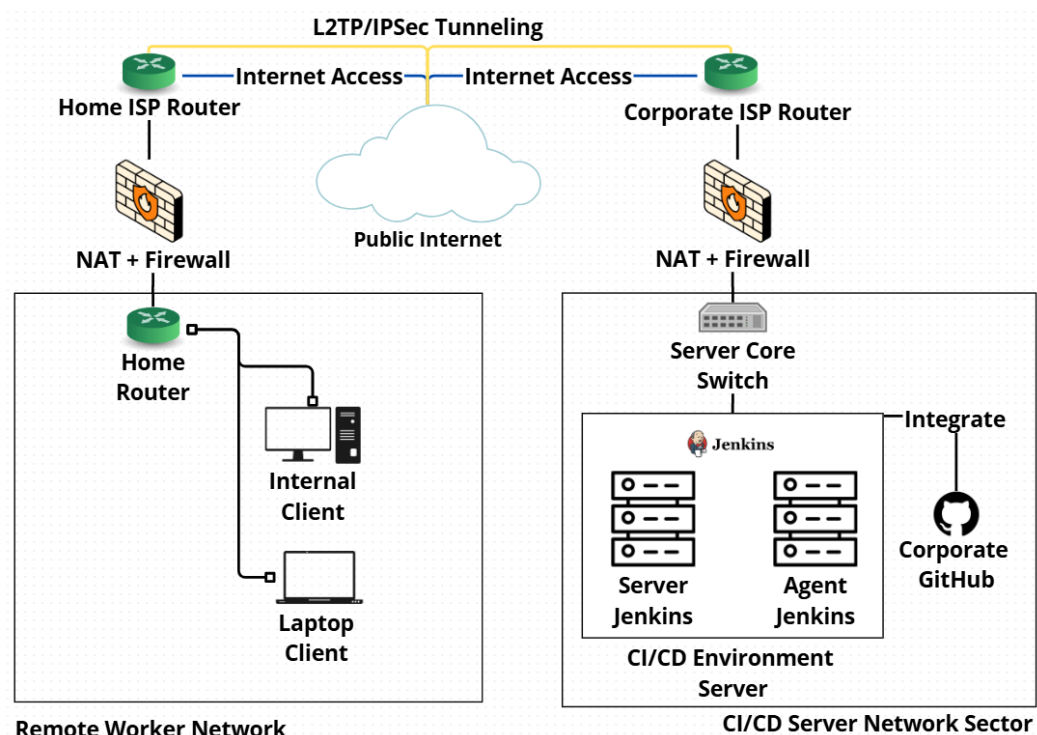
Gambar 3. 2 Topologi Perancangan Sistem

Gambar 3.2 merupakan rencana topologi sistem standar yang ada pada suatu organisasi. Topologi model ini memiliki orientasi lebih ke *router-oriented*, dimana router menjadi tumpuan utama dalam melakukan konfigurasi *Virtual Private Network* maupun *Access Control List* yang ada pada infrastruktur jaringan organisasi. *Tunnel Virtual Private Network* yang dibangun menggunakan teknologi yang disediakan oleh vendor router sendiri yang akan menciptakan jalur tersendiri yang menghubungkan antara dua *area network* berbeda. Banyak Metode yang

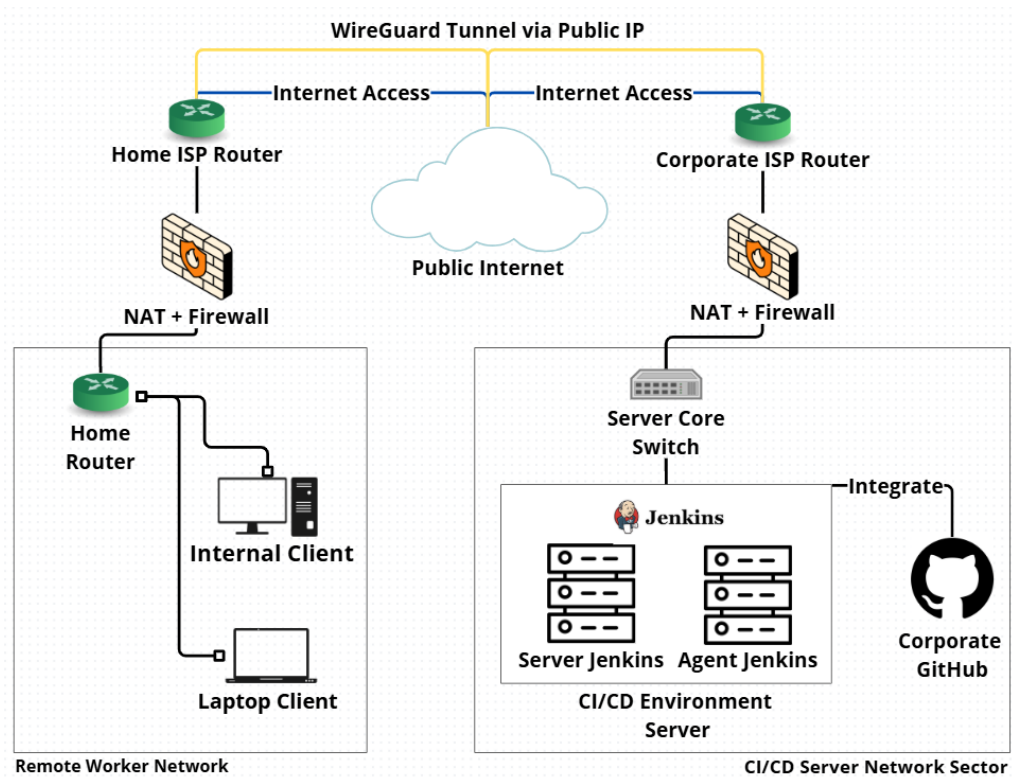
digunakan oleh vendor router itu sendiri akan tetapi secara konsep *computer network* memiliki mekanisme sejenis yang berbasis *service VPN* dibantu dengan *rules filtering*.

3.5 Implementasi dan Konfigurasi

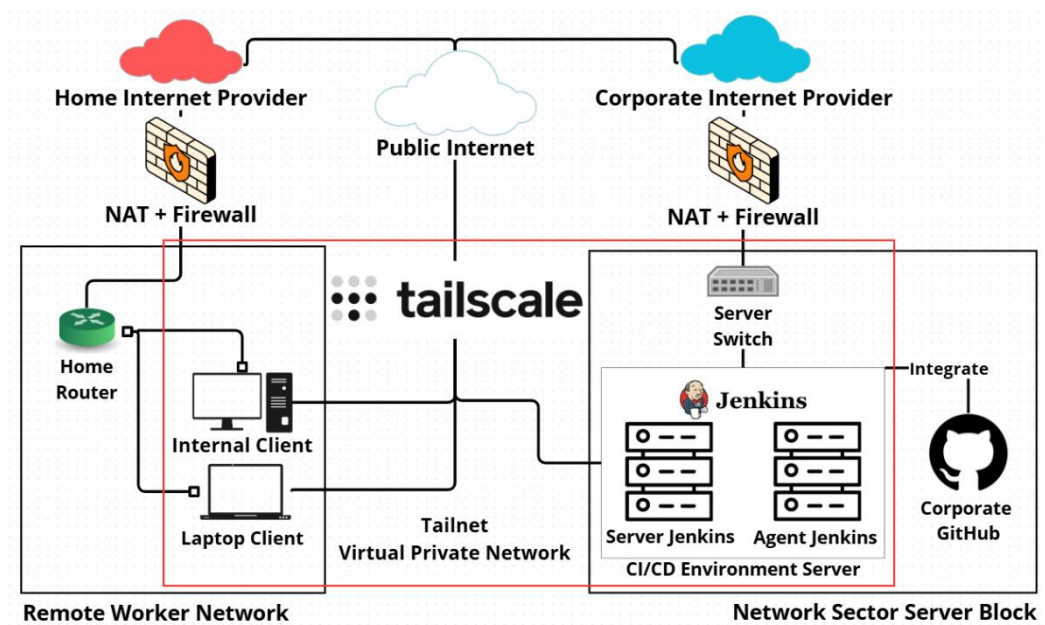
Tahap implementasi sistem merupakan bagian krusial dalam penelitian, karena bertujuan merealisasikan solusi terhadap permasalahan yang telah dirumuskan. Pada tahap ini, hasil dari perancangan sistem diimplementasikan berdasarkan topologi umum yang telah disusun sebelumnya. Proses instalasi dan konfigurasi dilakukan dengan merujuk pada dokumentasi resmi dari masing-masing perangkat lunak yang digunakan. Implementasi dibagi menjadi tiga tahapan utama, yang masing-masing merepresentasikan pengujian terhadap tiga teknologi *Virtual Private Network* berbeda yang akan dievaluasi dari sisi efektivitas dan efisiensi dalam lingkungan *Continuous Integration and Continuous Deployment*.



Gambar 3. 3 Topologi Jaringan berbasis VPN Tradisional



Gambar 3. 4 Topologi Jaringan berbasis Modern Kernel-Level VPN



Gambar 3. 5 Topologi Jaringan berbasis Zero-Configuration VPN

Gambar 3.3 merupakan gambaran topologi sistem yang akan di implementasikan kedalam penelitian ini. Dimana rancangan sistem *Virtual Private Network* ini akan menggunakan basis *router-oriented*. Dimana teknologi yang digunakan akan terbagi menjadi dua jenis yaitu menggunakan *VPN tunneling* berbasis SSTP dan L2TP/IPSec. Kedua protokol ini memungkinkan untuk dapat menciptakan *VPN tunneling* yang berbasis IP Publik yang memungkinkan dua *area network* terhubung via *routing table* dan Internet, sehingga dapat berkomunikasi layaknya dalam satu *area network*.

Gambar 3.4 merupakan gambaran sistem topologi yang akan di implementasikan dalam bentuk teknologi *VPN tunneling* berbasis *WireGuard*. Ini akan memungkinkan kedua *area network* dapat terhubung satu sama dengan yang lain layaknya dalam satu jaringan. Perbedaan mencolok diantara *WireGuard* dan *router-oriented* adalah dari segi enkripsi dan teknologi service yang lebih baik dimana fleksibilitas client akan sedikit lebih luas serta segi penyederhanaan kerumitan NAT Transfersal yang perlu dilakukan bila menggunakan *router-oriented*. Sesuai pada panduan *WireGuard report (Donenfeld, 2017)* teknologi *Virtual Private Network* yang digunakan berbasis *kernel level VPN tunneling*.

Gambar 3.5 merupakan gambaran topologi sistem yang akan di implentasikan dalam penelitian ini dengan menggunakan teknologi *VPN tunneling* berbasis *Zero-Configuration service*. Dimana sistem *tunneling VPN* yang digunakan dalam penelitian ini akan menggunakan basis dari *Tailnet network*. Kemudian setiap client akan terhubung dalam *Tailnet Network* milik Tailscale yang akan menjadi jembatan

penghubung antara infrastruktur diluar organisasi menjadi seolah-olah berada dalam satu jaringan. Ini selaras dengan website resmi Tailscale

3.6 Pengujian dan Evaluasi

Pada tahap ini, pengujian dilakukan untuk memastikan bahwa implementasi *Zero-Configuration Virtual Private Network* dan *Access Control List* dapat berfungsi secara efektif dalam mendukung kebutuhan lingkungan *Continuous Integration and Continuous Deployment* yang dinamis. Pengujian dimulai dengan mengukur waktu konfigurasi awal, yakni durasi dari inisialisasi hingga koneksi *Virtual Private Network* berhasil dan siap digunakan. Selanjutnya, diamati jumlah langkah konfigurasi yang diperlukan dalam proses setup, termasuk konfigurasi *Access Control List* dan otorisasi koneksi antar klien. Aspek kebutuhan keahlian teknis juga diuji dengan mencatat tingkat kesulitan teknis yang dihadapi selama setup serta keterlibatan manual dari administrator. Untuk menilai kemampuan automasi dalam pipeline *Continuous Integration and Continuous Deployment*, dilakukan integrasi *Virtual Private Network* ke dalam alur pengembangan dan deployment secara otomatis tanpa perlu konfigurasi ulang untuk tiap project atau pengguna baru. Uji konfigurasi multi-client dilakukan dengan mensimulasikan beberapa agen dan developer yang terhubung ke *Virtual Private Network* secara bersamaan, mengamati kestabilan dan efektivitas *Access Control List* dalam mengelola hak akses masing-masing. Terakhir, skenario perubahan topologi jaringan diuji dengan memindahkan node *Continuous Integration and Continuous Deployment* dan mensimulasikan gangguan koneksi, guna mengevaluasi kemampuan *Virtual Private Network* dalam melakukan *automatic recovery* dan

mempertahankan jalur komunikasi. Hasil pengujian ini menjadi dasar dalam menilai keunggulan arsitektur *Zero-Configuration VPN* dibandingkan *VPN tradisional* maupun *modern kernel-level VPN*, terutama dalam konteks *Continuous Integration and Continuous Deployment* yang mengutamakan skalabilitas, fleksibilitas, dan efisiensi proses.

Tabel 3. 3 Rencana Pengujian Konfigurasi VPN (Kjorveziroski dkk., 2024; Zhipeng dkk., 2018)

No	Parameter Uji	Router-Based VPN	Modern Kernel-Level VPN	Zero-Configuration VPN
1	Jumlah Langkah Konfigurasi			
2	Konfigurasi Multi-Client			
3	Perubahan Topologi Jaringan			

Rencana pengujian konfigurasi VPN dalam penelitian ini disusun dengan mengacu pada pendekatan sistematis yang diadaptasi dari (Kjorveziroski dkk., 2024) dan (Zhipeng dkk., 2018), dengan penyesuaian terhadap konteks dan objektivitas penelitian. Seluruh parameter pengujian ditetapkan melalui proses peninjauan ulang agar relevan terhadap kebutuhan implementasi *Virtual Private Network* dalam lingkungan *Continuous Integration and Continuous Deployment*. Enam parameter utama yang digunakan meliputi: (1) Waktu Konfigurasi Awal, untuk menilai efisiensi proses setup; (2) Jumlah Langkah Konfigurasi, sebagai indikator kompleksitas implementasi; (3) Kebutuhan Keahlian Teknis, yang mengukur tingkat kesulitan teknis; (4) Kemampuan Automasi dalam Pipeline *Continuous Integration and Continuous Deployment*, untuk mengevaluasi integrasi

terhadap alur kerja DevOps; (5) Kemampuan Konfigurasi *Multi-Client*, yang merepresentasikan skalabilitas sistem; dan (6) Respon terhadap Perubahan Topologi Jaringan, sebagai indikator fleksibilitas adaptasi. Keenam parameter ini menjadi dasar dalam membandingkan performa dan kemudahan penggunaan dari masing-masing teknologi VPN yang diuji, serta memastikan bahwa evaluasi dilakukan secara objektif, kontekstual, dan terukur.

3.7 Analisis Hasil dan Pembahasan

Pada tahap ini, hasil pengujian dianalisis untuk mengevaluasi efektivitas implementasi *Zero-Configuration VPN* dan *Access Control List* dalam mendukung lingkungan *Continuous Integration and Continuous Deployment* yang cepat dan dinamis. Analisis dilakukan dengan membandingkan data pengujian terhadap parameter uji yang telah ditetapkan. Evaluasi waktu konfigurasi awal dan jumlah langkah konfigurasi menjadi indikator efisiensi setup awal, yang menjadi acuan untuk sistem yang harus cepat beroperasi dalam pengembangan berbasis kontrak atau outsourcing. Parameter kebutuhan keahlian teknis dianalisis untuk menilai seberapa besar dependensi terhadap *System Administrator* berpengalaman, yang dapat mempengaruhi kecepatan dan skalabilitas tim devops. Kemampuan automasi dalam pipeline *Continuous Integration and Continuous Deployment* dikaji dari segi integrasi *Virtual Private Network* secara otomatis ke dalam alur kerja pengembangan tanpa hambatan konfigurasi manual. Pengujian juga mencakup konfigurasi multi-client, guna melihat sejauh mana *Virtual Private Network* dapat menangani banyak koneksi secara simultan dengan tetap mempertahankan kontrol akses berbasis *Access Control List*. Terakhir, perubahan topologi jaringan dianalisis

untuk mengevaluasi kemampuan sistem dalam merespon gangguan atau dinamika jaringan yang sering terjadi di proyek yang tersebar secara geografis. Jika ditemukan kendala, analisis juga mencakup identifikasi penyebab dan rekomendasi teknis untuk mitigasi. Hasil dari analisis ini akan memberikan gambaran menyeluruh terkait kelebihan dan keterbatasan penggunaan *Zero-Configuration VPN* dalam konteks *Continuous Integration and Continuous Deployment*, serta arahan perbaikan untuk penerapan di lingkungan produksi nyata.