BAB I PENDAHULUAN

1.1 Latar Belakang

Dengan perkembangan komunikasi jaringan yang cepat, tugas yang berkaitan dengan manajemen dan monitoring jaringan akan menjadi lebih kompleks. Perusahaan yang memiliki kantor cabang di lokasi yang terpisah secara geografis harus menggunakan *Wide Area Network* (WAN) untuk dapat terhubung. Ada banyak masalah dengan komunikasi, termasuk kecepatan, *bandwidth*, *delay*, dan redundansi jalur komunikasi [2].

Salah satu solusi yang banyak digunakan adalah *Virtual Private Network* (VPN), yang memungkinkan koneksi aman antara kantor pusat dan cabang melalui internet. Namun, VPN tradisional memiliki keterbatasan, seperti kompleksitas konfigurasi [15], biaya tinggi [16], dan kurangnya fleksibilitas dalam menghadapi kegagalan koneksi (*failover*). Untuk mengatasi masalah ini, teknologi *Software-Defined Wide Area Network* (SD-WAN) muncul sebagai solusi yang lebih canggih dan fleksibel. Teknologi SD-WAN memecahkan masalah tersebut dengan mengatur trafik jaringan melalui berbagai koneksi internet yang tersedia, sehingga jika salah satu koneksi gagal, trafik secara otomatis dialihkan ke koneksi lain [1]. Namun, implementasi SD-WAN masih memerlukan pendekatan yang tepat untuk memastikan keandalan dan keamanan jaringan, terutama dalam skenario *failover* ketika koneksi utama mengalami gangguan.

ZeroTier, sebagai salah satu solusi jaringan *overlay* berbasis *software*, menawarkan pendekatan yang sederhana namun efektif untuk membangun VPN yang aman dan terenkripsi [17]. Dengan menggunakan ZeroTier, organisasi dapat dengan mudah menghubungkan kantor pusat dan cabang tanpa memerlukan infrastruktur jaringan yang kompleks. ZeroTier juga menyediakan kemampuan *failover* yang dapat diintegrasikan dengan SD-WAN untuk memastikan ketersediaan jaringan yang tinggi dan minim *downtime* [17].

Implementasi SD-WAN menggunakan ZeroTier untuk *failover* VPN antar pengguna (kantor pusat dan cabang) menjadi solusi yang menarik untuk dieksplorasi. Pendekatan ini tidak hanya meningkatkan keandalan jaringan tetapi juga menyederhanakan manajemen konektivitas antar lokasi. Dengan memanfaatkan teknologi ini, organisasi dapat mencapai efisiensi operasional yang lebih baik, mengurangi biaya, dan memastikan kelancaran bisnis meskipun terjadi gangguan pada koneksi utama.

1.2 Rumusan Masalah

Adapun rumusan masalah dari Tugas akhir ini, sebagai berikut:

1. Bagaimana cara mengimplementasikan SD-WAN menggunakan Zerotier untuk menghubungkan kantor pusat dan cabang?
2. Bagaimana mekanisme *failover* dapat diaktifkan untuk memastikan konektivitas tetap terjaga saat terjadi kegagalan pada jalur utama?
3. Apa keuntungan dan tantangan dalam menggunakan Zerotier sebagai solusi SD-WAN untuk jaringan perusahaan?

1.3 Tujuan

Adapun tujuan dari Tugas akhir ini, sebagai berikut:

1. Merancang dan mengimplementasikan solusi SD-WAN menggunakan Zerotier untuk menghubungkan kantor pusat dan cabang.
2. Membangun mekanisme *failover* yang dapat secara otomatis beralih ke jalur cadangan saat jalur utama mengalami gangguan.
3. Mengevaluasi performa dan keandalan solusi yang diimplementasikan.

1.4 Cakupan Pengerjaan

Pada tugas akhir ini, cakupan pengerjaan yang akan dilakukan adalah:

1. Pengembangan dan implementasi solusi SD-WAN menggunakan ZeroTier untuk membangun konektivitas VPN antara kantor pusat dan minimal satu kantor cabang.
2. Perancangan dan implementasi mekanisme *failover* dasar yang memungkinkan peralihan otomatis koneksi ke jalur internet cadangan apabila jalur internet utama mengalami gangguan.
3. Produk yang dibangun akan fokus pada fungsionalitas inti SD-WAN dan *failover* VPN. Pembatasan pada implementasi ini adalah *failover* bersifat dasar dan tidak mencakup mekanisme *load balancing* yang lebih kompleks atau optimasi jalur lanjut di luar *failover* dasar.

1.5 Tahapan Pengerjaan

Tahapan pengerjaan pada tugas akhir ini, sebagai berikut:

1. Studi literatur: Mengumpulkan referensi dari buku, jurnal, artikel, dan sumber *online* terkait SD-WAN, Zerotier, dan *failover*.
2. Perancangan sistem: Membuat diagram arsitektur yang mencakup kantor pusat, kantor cabang, dan koneksi menggunakan Zerotier; Merancang mekanisme *failover*.
3. Implementasi: Mengkonfigurasi zerotier pada router di kantor pusat dan cabang; Memastikan semua komponen berfungsi.

4. Pengujian: Melakukan pengujian konektivitas antara kantor pusat dan cabang; Menguji mekanisme *failover* dengan mematikan jalur utama dan memastikan sistem beralih ke jalur cadangan; Mengevaluasi performa jaringan.
5. Analisis dan Evaluasi: Menganalisis data hasil pengujian; Mengidentifikasi hasil masalah dan memberikan perbaikan kepada sistem yang mengalami kesalahan.