

BAB I PENDAHULUAN

1.1 Latar Belakang

Pada era *digital* seperti saat ini, *konektivitas* jaringan yang cepat dan dapat diandalkan sangat penting untuk menjamin operasi lancar bisnis. Perusahaan menggunakan VPN (*Virtual Private Network*), yang menghubungkan kantor pusat dan cabang dalam jaringan. Namun, masalah pada koneksi jaringan seringkali menyebabkan jaringan terputus dan tidak stabil, [1]. Meskipun berbagai upaya telah dilakukan untuk mengurangi *downtime* proses *Failover* yang diteliti sebelumnya masih menggunakan metode konvensional di jaringan [2]. Penggunaan SDN sebelumnya belum banyak membahas tentang *Failover* VPN pada SD WAN (*Software Defined Wide Area Network*) *open source* seperti pada penelitian [4]. proses *Failover* dan *load balance* menggunakan metode NTH agar *distribusi traffic* terbagi secara merata, sedangkan Pada penelitian [4]. *Failover* menggunakan Netwatch, kondisi *downtime* menyebabkan client terganggu untuk mengakses internet ataupun server, sehingga implementasi *Failover* sangat penting, *Failover* adalah salah satu metode pada jaringan untuk menghindari *downtime* koneksi, [3]. Fortigate digunakan sebagai perangkat *firewall* yang berfungsi sebagai *edge* SDWAN. Fortigate dikenal karena kemampuannya dalam menyediakan keamanan jaringan yang kuat dan fitur-fitur canggih untuk manajemen trafik, [4]. SD-WAN adalah bentuk aplikasi spesifik dari teknologi *software-defined networking* SDN yang diaplikasikan pada koneksi WAN *wide area network*. Teknologi SDWAN adalah solusi yang dapat digunakan untuk memecahkan masalah tersebut, dengan mengatur trafik jaringan menggunakan beberapa koneksi internet yang tersedia sehingga jika salah satu koneksi gagal, trafik akan dialihkan secara otomatis ke koneksi lainnya. Salah satu tantangan utama dalam implementasi jaringan perusahaan adalah bagaimana memastikan konektivitas VPN antara kantor pusat dan cabang tetap berjalan tanpa gangguan meskipun terjadi kegagalan pada salah satu jalur koneksi. Dengan menerapkan SD-WAN berbasis *open source*, perusahaan dapat meningkatkan ketahanan jaringan dengan mekanisme *Failover* otomatis yang memastikan koneksi tetap berjalan tanpa interupsi signifikan. Implementasi SD-WAN *open source* ini bertujuan untuk mengevaluasi efektivitas solusi dalam mendukung *Failover* VPN antara kantor pusat dan cabang. Dengan pendekatan ini, diharapkan organisasi dapat meningkatkan efisiensi jaringan, mengurangi biaya operasional, serta mendapatkan fleksibilitas lebih dalam manajemen infrastruktur jaringan mereka.

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, masalah yang akan dikaji adalah :

1. Bagaimana mekanisme *Failover* yang optimal dalam implementasi SD-WAN berbasis *open-source* untuk memastikan konektivitas VPN antara kantor pusat dan cabang tetap stabil?
2. Bagaimana efektivitas konfigurasi dan manajemen jaringan dalam implementasi SD-WAN *open-source* untuk mendukung kebutuhan perusahaan?

3. Bagaimana dampak implementasi SD-WAN *open-source* terhadap biaya operasional dan pemeliharaan jaringan perusahaan?

1.3 Tujuan

Berdasarkan rumusan masalah tersebut, tujuan dilakukannya penelitian ini adalah sebagai berikut:

1. Menganalisis mekanisme *Failover* yang optimal dalam implementasi SD-WAN berbasis *open-source* untuk memastikan konektivitas VPN antara kantor pusat dan cabang tetap stabil.
2. Menganalisis efektivitas konfigurasi dan manajemen jaringan dalam implementasi SD-WAN *open-source* untuk mendukung kebutuhan perusahaan.
3. Menganalisis dampak implementasi SD-WAN *open-source* terhadap biaya operasional dan pemeliharaan jaringan perusahaan

1.4 Cakupan Pengerjaan

Adapun cakupan pengerjaan pada penelitian ini sebagai berikut:

1. FlexiWAN sebagai platform SD-WAN *open source*.
2. Fokus pada mekanisme *Failover* VPN untuk memastikan ketersediaan koneksi antara kantor pusat dan cabang saat terjadi gangguan pada jalur utama.

1.5 Tahapan Pengerjaan

Dalam pelaksanaan Tugas Akhir ini, peneliti menggunakan metode NDLC (*Network Development Life Cycle*) sebagai pendekatan utama. NDLC merupakan metode pengembangan jaringan yang sistematis dan terstruktur, yang terdiri dari beberapa tahapan penting mulai dari analisis kebutuhan hingga dokumentasi sistem. Tahapan-tahapan dalam NDLC yang diterapkan dalam penelitian ini adalah sebagai berikut:

1) Analisis

Pada tahap ini, dilakukan analisis terhadap konsep dasar SD-WAN, teknologi VPN, mekanisme *Failover*, dan solusi *open-source* yang dapat diterapkan. Referensi yang digunakan mencakup jurnal, buku, dokumentasi resmi FlexiWAN atau solusi *open-source* lainnya, serta studi kasus mengenai implementasi SD-WAN.

2) Desain

Pada tahap ini, peneliti akan menyusun rancangan topologi jaringan berdasarkan informasi yang telah terkumpul. Desain tersebut akan mencerminkan kebutuhan yang ada dan memberikan gambaran menyeluruh mengenai jaringan yang akan dibangun.

3) Implementasi

Pada tahap ini, peneliti akan melaksanakan implementasi sesuai dengan analisis kebutuhan dan desain yang telah disusun. Implementasi ini mencakup konfigurasi *Failover* VPN antara Kantor Pusat dan Cabang dengan memanfaatkan teknologi SD-WAN berbasis *open-source*

4) **Pengujian dan Monitoring**

Setelah implementasi selesai, tahap ini mencakup pengujian sistem untuk memverifikasi hasil implementasi. Selain itu, dilakukan pemantauan untuk mengidentifikasi potensi masalah yang mungkin timbul pada sistem dan sebagai dasar untuk pemecahan masalah di masa yang akan datang.

5) **Dokumentasi dan kesimpulan**

Tahap akhir adalah mendokumentasikan seluruh proses implementasi, hasil pengujian, serta kesimpulan mengenai keberhasilan implementasi SD-WAN berbasis *open-source* untuk *Failover* VPN di lingkungan kantor pusat dan cabang. Dokumentasi ini akan menjadi referensi untuk pengembangan lebih lanjut dan penerapan di lingkungan yang lebih luas.