BAB I
PENDAHULUAN

1.1. Latar Belakang Masalah

Pengguna Internet di Indonesia setiap tahun nya terus bertambah, menurut survey yang dilakukan Asosiasi Penyelenggara Internet di Indonesia (APJII), tingkat Penetrasi Internet di Indonesia pada 2021-2022 mencapai 210.026.769 jiwa dari total populasi 272.682.600 jiwa penduduk Indonesia pada Tahun 2021. Penetrasi ini naik menjadi 77,02% pada tahun 2021-2022 dibandingkan tahun sebelum nya yaitu 73,70% pada tahun 2019-2020. [2]

Semakin banyak nya pengguna *Internet* yang bertukar data baik itu *voice, video, game, email,* dan lain sebagai nya di seluruh dunia. Internet merupakan jaringan komputer yang menghubungkan jutaan bahkan miliaran komputer yang ada di dunia ini. Salah satu manfaat internet dirasakan oleh perusahaan yang memiliki beberapa kantor yang berada di lokasi yang berbeda secara geografis, tapi menginginkan terjadi nya pertukaran data perusahaan secara realtime untuk keperluan bisnis seperti berkomunikasi menggunakan data *voice* melewati internet, video streaming, absensi secara global, pengiriman data apapun ke pusat atau cabang dan lain nya.

Ada beberapa metode yang bisa digunakan seperti Metro Ethernet, IP VPN, Internet VPN, MPLS, SD-WAN[14], dan lain sebagai nya. Tapi untuk solusi yang *cost effective* adalah menggunakan *Virtual Private Network (VPN)* melalui Internet. Tapi internet itu tidak aman karena jutaan jaringan komputer saling terhubung satu dengan yang lain disana. Maka dari itu perlu ada nya enkripsi data sebelum melewati internet, sehingga ketika paket data dikirimkan melalui internet sudah di proteksi dengan Kriptografi sehingga data akan dikirimkan secara aman

1.2. Rumusan Masalah

Dikarenakan internet adalah gabungan dari jutaan bahkan miliaran jaringan komputer yang saling terhubung, maka salah satu poin penting nya adalah bagaimana ketika kita melakukan pengiriman data secara aman dari host ke host lain nya. Misalnya ketika kita mengirim email dari Indonesia menuju Amerika, perlu nya mengamankan data email kita yang akan melewati negara *transit* seperti Singapore, lalu ke Jepang, lalu ke Amerika. Dalam email sudah ada keamanan data nya salah satu nya menggunakan protokol *Secure Socket Layer (SSL)* atau *Transport Layer Security (TLS)*. Begitu pula ketika konteks nya adalah pengiriman data dari kantor cabang ke kantor pusat yang berbeda secara geografis, maka perlu keamanan data yang baik dan juga pengiriman yang cepat dengan VPN, berdasarkan informasi diatas, maka didapatkan rumusan sebagai berikut :

1. Bagaimana performa dan keamanan WireGuard ketika digunakan untuk mengirimkan data dari kantor cabang ke kantor pusat ?
2. Bagaimana meningkatkan efektifitas vpn untuk menghindari *single point of failure (SPoF)* ?
3. Bagaimana hasil *throughput*, *latency*, *jitter*, *packet loss* ketika WireGuard dijalankan secara Loadbalance dan tanpa Loadbalance ?

1.3. Batasan Masalah

Berdasarkan latar belakang dan rumusan masalah di atas. Penelitian ini memiliki beberapa batasan. Berikut batasan masalah dari penelitian ini:

1. Penelitian dilakukan dengan simulator jaringan bernama *Pnetlab* untuk mendesain topologi jaringan dan melakukan pengujian secara virtual.
2. Penelitian menggunakan sistem operasi jaringan berbasis MikroTik *RouterOS* versi 7.4 yang berbasis *OpenSource*.
3. Pengujian menggunakan aplikasi *File Zilla Server over TLS (FTPS)* pengiriman 30 tipe data yang berbeda dari server ke client menggunakan protocol TCP.

4. Pengujian juga menggunakan aplikasi *Wireshark Packet Analyzer* untuk melihat dan menganalisa paket yang dikirimkan aman dan terenkripsi.

1.4. Tujuan

Tujuan penelitian ini adalah mengetahui performa dan keamanan WireGuard ketika menghubungkan kantor cabang dengan kantor pusat ketika memiliki beberapa jalur *WAN* dan dioptimalkan dengan Loadbalance sehingga pengiriman data akan terbagi di beberapa jalur tersebut., sehingga lebih efisien, cepat, dan optimal.

1.5. Manfaat

Manfaat dari pengujian ini bisa diterapkan untuk perusahaan yang memiliki beberapa kantor cabang yang terhubung ke kantor pusat dan memiliki beberapa WAN sehingga pengiriman data bisa terbagi, *throughput* yang didapatkan lebih maksimal serta ketika ada jalur yang bermasalah data tetap akan dikirimkan melalui jalur yang aktif.