BAB 1
PENDAHULUAN

1.1 Latar Belakang

Pada akhir bulan Desember 2019, *World Health Organization* (WHO) mendapat informasi tentang sekelompok kasus Pneumonia yang diketahui berasal dari kota Wuhan dan diidentifikasi sebagai virus yang dinamakan *the coronavirus disease* (COVID-2019) pada tanggal 7 Januari 2020 (who.int, 2020). Menurut WHO, COVID-19 merupakan penyakit menular yang disebabkan oleh temuan baru yaitu Coronavirus.

Untuk memutuskan penyebaran virus ini, pemerintah Indonesia melakukan berbagai strategi. Strategi tersebut dari mewajibkan individu untuk menjaga jarak atau yang disebut *physical distancing* sampai menetapkan Kejadian Luar Biasa (KLB) dengan 2 implementasi yang dilakukan yaitu bekerja dari rumah atau W*ork From Home* (WFH) (nasional.kompas, 2020).

Presiden Jokowi dalam konferensi pers di Istana Bogor tanggal 15 Maret 2020 mengatakan "Saatnya kita kerja dari rumah, belajar dari rumah, ibadah dari rumah". Imbauan ini sesuai dengan Surat Edaran oleh Dinas Tenaga Kerja dan Transmigrasi Nomor 14/SE/2020 tentang imbauan bekerja di rumah. Kebijakan pemerintah tersebut telah dipatuhi oleh beberapa perusahaan dan institusi seperti Kementerian PAN-RB, Kementerian Pertahanan, Bank Indonesia, sekolah, universitas dan lain lain (cnnindonesia.com, 2020).

Arahan pemerintah untuk WFH akan berkaitan dengan penyesuaian sistem kerja yang baru baik pada karyawan WFH maupun WFO. Hal tersebut menjadi tantangan karyawan di mana akan ada perubahan pola kerja yang mengakibatkan ketidakbiasaan. Dalam *money.kompas.com* (2020) dinyatakan karyawan WFH adalah mereka yang diperbolehkan untuk bekerja dari rumah ketimbang harus berpergian atau datang ke kantor, sedangkan karyawan yang tetap bekerja di tempat kerja atau *Work From Office (*WFO)

adalah mereka yang fungsi pekerjaannya tidak memungkinkan dilakukan dari rumah atau perusahaan tidak dapat menghentikan aktivitas kerjanya.

Ada beberapa kelebihan dalam menerapkan WFH bagi perusahaan dan pekerja, antara lain: (1) biaya operasional perusahaan menurun, (2) waktu lebih fleksibel, (3) produktivitas meningkat, (4) kepuasan kerja meningkat, dan (5) *work life balance* juga meningkat. (enigmacamp.com.2020)

Di balik banyak kelebihan WFH, ada beberapa kekurangan yang perlu diwaspadai saat menerapkanWFH. Kelemahan itu antara lain: (1) monitoring pekerja susah, (2) motivasi kerja hilang, (3) banyak gangguan kerja, (4) sering terjadi *miskomunikasi*, dan (5) masalah keamanan data (rukita.co.2020).

Keamanan menjadi salah satu isu yang perlu diperhatikan ketika WFH. Data-data pekerjaan yang penting tidak disarankan untuk dikirim menggunakan jaringan biasa. Untuk melakukan proteksi keamanan lebih maka cara yang dipilih adalah menggunakan layanan keamanan dengan *Virtual Private Network* (VPN).

PT Dunia Makmur Jaya merupakan salah satu perusahaan yang menerapkan WFH selama masa pandemi. Selama penerapan WFH pengiriman data masih dengan cara manual, seperti menggunakan fasilitas internet melalui *email*, *messenger,* fax maupun *line* telepon. Hal ini menyebabkan setiap orang masih bisa masuk ke dalam jaringan komunikasi dikarenakan masih belum tersedianya pembatasan hak akses. Di samping itu, untuk *remote acces* dan kontrol ke jaringan, PT Dunia Makmur Jaya dari luar belum memiliki akses tersebut. Untuk menjawab masalah tersebut *Virtual Private Network* (VPN) dapat memberikan solusi untuk terhubungnya jaringan PT Dunia Makmur Jaya ke jaringan luar.

Melalui teknologi VPN antara karyawan atau pimpinan yang sedang bertugas di luar kantor, terbentuk suatu jaringan komunikasi yang mudah dan tetap terjamin keamanannya.

Virtual Private Network (VPN) yaitu teknik yang dapat menghubungkan beberapa jaringan lokal melalui jaringan publik. Dengan

teknik VPN komunikasi seakan-akan kedua jaringan tersebut berada dalam satu jaringan intranet yang besar (Santoso,2018).

Virtual Private Network (VPN) adalah sebuah teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan publik untuk dapat bergabung dengan jaringan lokal. Dengan cara tersebut maka akan didapat hak dan pengaturan yang sama, walaupun sebenarnya menggunakan jaringan publik dan tidak terhubung langsung pada sebuah jaringan lokal (Nugroho,dkk.2019:1).

Virtual Private Network (VPN) merupakan salah satu cara yang dapat digunakan untuk membuat jaringan bersifat *private* dan koneksi jarak jauh (*remote acces*) dengan tingkat keamanan yang tinggi di atas jaringan publik atau internet (Rosmana dan Latifah, 2015: 23).

Virtual Private Network (VPN) merupakan suatu teknologi membangun jaringan *private* dalam jaringan publik. Teknologi tersebut mampu meningkatkan keamanan komunikasi pada jaringan publik karena komunikasi tersebut seolah-olah berada pada sebuah jaringan *private.*

Dengan demikian, teknologi *Virtual Private Network* (VPN) memungkinkan untuk membuat saluran aman dalam jaringan publik sehingga tidak ada yang bisa mengaksesnya kecuali hanya pengirim dan penerima saja. Karena keunggulan tersebut, VPN telah banyak diimplementasikan pada jaringan internet.

Ada beberapa jenis *tunneling* yang biasa digunakan pada *Virtual Private Network* (VPN), seperti *Internet Protocol Security* (IPSec), *Secure Socket Layer* (SSL), *Point-to-Point Tunnelling Protocol* (PPTP), dan *Layer 2 Tunneling Protocol* (L2TP).

Penelitian ini difokuskan pada *performance remote acces.* Untuk mengetahui tingkat performansinya digunakan *tunneling Point-to-Point Tunnelling Protocol* (PPTP), dan *Layer 2 Tunneling Protocol* (L2TP). Selanjutnya akan dilihat perbandingan tingkat performansinya dengan menggunakan kedua teknologi VPN tersebut. Penggunaan *tunneling* ini perlu dilakukan pengujian karena dikhawatirkan akan mengganggu

performansi jaringan tersebut pada saat melakukan pertukaran data. Parameter QoS yang akan digunakan adalah *throughput*, *delay*, *packet loss*, dan *jitter.*

Pemilihan *tunneling* PPTP dan L2TP dikarenakan PPTP (*Point-to-Point Tunneling Protocol*) dan L2TP (*Layer 2 Tunneling Protoco*l) adalah dua *tunneling* VPN yang telah ada dalam penggunaan selama beberapa dekade. Meskipun PPTP dan L2TP sudah lama, kedua *tunneling* ini masih didukung oleh banyak perangkat dan sistem operasi. Ini membuatnya cocok untuk situasi di mana perangkat atau aplikasi tertentu memerlukan *tunneling* yang lebih tua untuk koneksi VPN. Kedua *tunneling* ini (PPTP dan L2TP) masih digunakan dan populer sampai sekarang karena beberapa alasan:

1. Dukungan bawaan: PPTP dan L2TP masih didukung oleh banyak sistem operasi dan perangkat, termasuk Windows, macOS, iOS, dan Android. Karena dukungan bawaan ini, pengguna tidak perlu menginstal perangkat lunak tambahan untuk menggunakan *tunneling* ini.
2. Kemudahan konfigurasi: Konfigurasi VPN PPTP dan L2TP relatif mudah dibandingkan dengan *tunneling* VPN yang lebih kompleks. Keduanya dapat dengan cepat dikonfigurasi di banyak perangkat dan platform, membuatnya menjadi pilihan yang menarik untuk pengguna yang mencari solusi VPN yang sederhana.
3. Kinerja: Meskipun tidak seaman *tunneling* VPN modern, PPTP dan L2TP sering kali menawarkan kinerja yang cukup baik dalam kondisi tertentu. Mereka dapat menjadi pilihan yang memadai untuk pengguna yang membutuhkan koneksi VPN dengan latensi rendah dan *throughput* yang tinggi.
4. Kompatibilitas: Beberapa aplikasi atau layanan mungkin masih menggunakan atau mensyaratkan penggunaan PPTP atau L2TP. Dalam kasus seperti itu, pengguna harus menggunakan *tunneling* ini untuk berkomunikasi dengan layanan atau aplikasi tersebut.

5. Sejarah penggunaan yang panjang: Karena PPTP dan L2TP telah ada dalam penggunaan untuk waktu yang lama, banyak organisasi dan pengguna terbiasa dengan konfigurasi dan penggunaannya. Ini bisa membuatnya sulit untuk beralih ke *tunneling* VPN yang berbeda, terutama jika tidak ada alasan kritis untuk melakukannya.

Dilatarbelakangi efektifitas VPN dan keunggulan *tunneling* PPTP dan L2TP seperti yang dikemukakan di atas, maka penulis menganalisis Performansi *Remote Acces* VPN Menggunakan PPTP dan L2TP untuk Kebutuhan *Work From Home* (WFH) bagi Karyawan PT Dunia Makmur Jaya.

1.2 Identifikasi Masalah

a. Bagaimana mengimplementasikan *remote acces* VPN dengan menggunakan *tunneling* PPTP dan L2TP?
b. Bagaimana performansi *remote acces* VPN dilihat dari parameter QoS seperti *throughput*, *delay, packet loss*, dan *jitter?*
c. Bagaimana perbandingan performansi VPN dengan menggunakan *tunneling* PPTP dan L2TP?

1.3 Tujuan Tugas Akhir

Tujuan yang ingin dicapai dalam pengerjaan tugas akhir ini adalah:

a. Mengimplementasikan *remote access* VPN dengan menggunakan PPTP dan L2TP.
b. Menganalisis performansi *remote access* VPN menggunakan PPTP dan L2TP dilihat dari parameter QoS seperti *throughput*, *delay, packet loss*, dan *jitter.*
c. Menganalisis perbandingan performansi *remote access* VPN dengan menggunakan PPTP dan L2TP .

1.4 Manfaat Tugas Akhir

Secara praktis penelitian ini bermanfaat memberikan informasi bagaimana mengimplementasikan *remote acces* VPN dengan menggunakan PPTP dan L2TP dan membandingkan efisiensi kedua *tunneling* tersebut.

Secara akademis penelitian ini digunakan sebagai sumbangan pikiran bagaimana menggunakan teknologi VPN yang lebih efektif dan efisien dengan menggunakan PPTP atau L2TP setelah dilakukan pengujian.

1.5 Lingkup Tugas Akhir

Ruang lingkup permasalahan dalam pengerjaan tugas akhir ini dibatasi dengan beberapa hal sebagai berikut:

1. *Virtual Private Network* (VPN) yang digunakan hanya dalam pelaksanaan *work from home* (WFH)
2. Parameter performansi jaringan yang digunakan adalah *throughput, delay, packet loss,* dan *jitter.*
3. Tidak membahas mengenai kemampuan VPN dari segi keamanan jaringan.
4. VPN yang dibangun dengan jenis pengimplementasian VPN *remote access.*
5. Tidak membahas enkripsi secara mendalam.
6. Layanan yang digunakan adalah *File Transfer Protocol* (FTP).

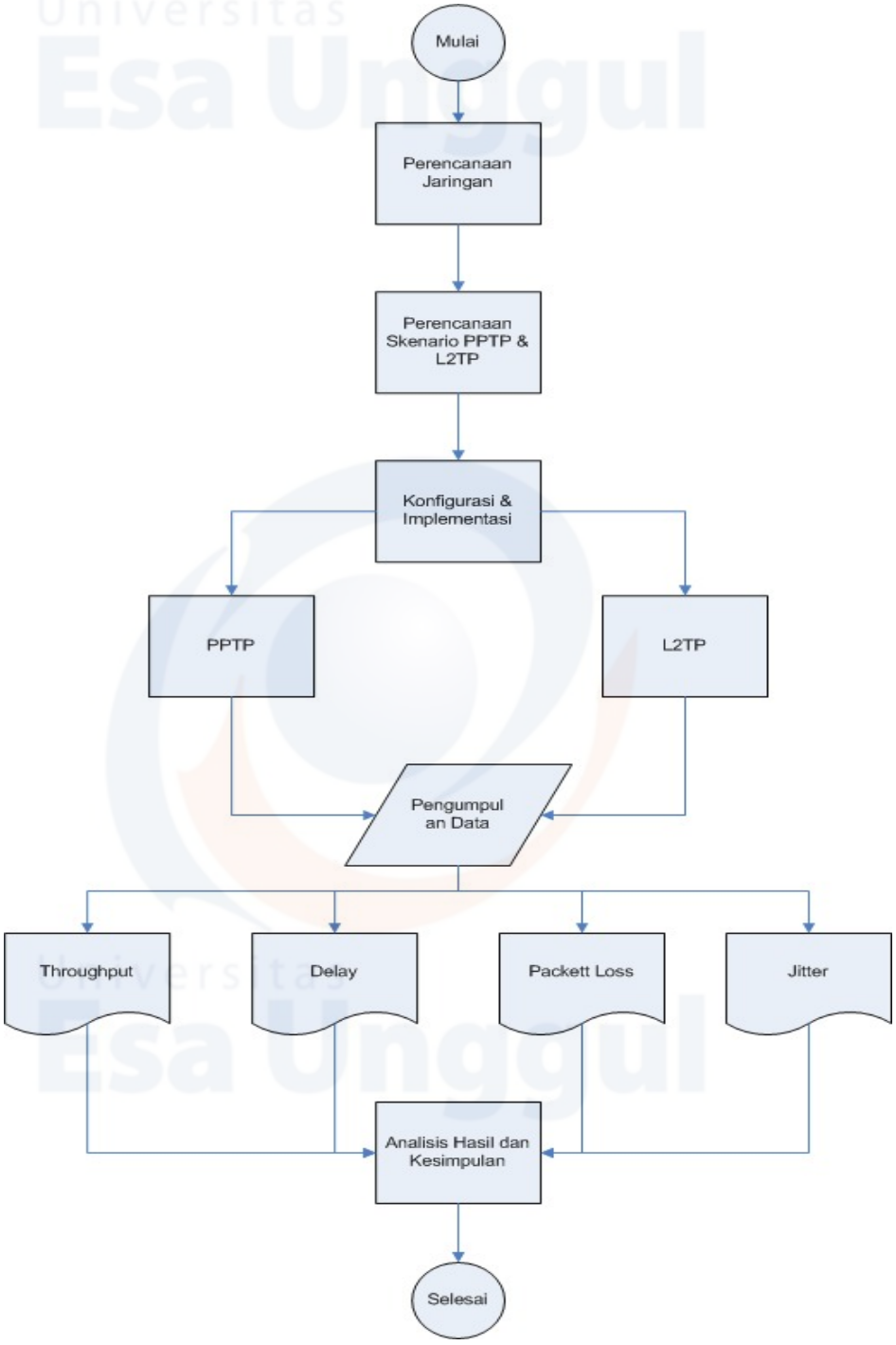
1.6 Kerangka Berpikir

Tujuan dari *Virtual Private Network* (VPN) mampu meningkatkan keamanan komunikasi pada jaringan publik karena komunikasi tersebut seolah-olah berada pada sebuah jaringan *private*. VPN memungkinkan untuk membuat saluran aman dalam jaringan publik sehingga tidak ada yang bisa mengaksesnya kecuali hanya pengirim dan penerima saja. Karena keunggulan tersebut, VPN telah banyak diimplementasikan pada jaringan internet.

Sesuai dengan pembatasan masalah yang telah dikemukakan di atas *tunneling* yang digunakan adalah PPTP dan L2TP. Proses penelitian dimulai dengan merancang jaringan untuk menentukan topologi yang akan digunakan. Tahap berikutnya adalah membuat skenario yang akan diterapkan pada *tunneling* PPTP dan L2TP. Berikutnya melakukan konfigurasi dalam menerapkan metode PPTP dan L2TP. Setelah dilakukan penerapan, maka pengujian konektifitas dilakukan. Apabila terjadi kesalahan maka konfigurasi dan penerapan diperiksa kembali. Namun jika tidak ada masalah, maka dilanjutkan dengan pengambilan data untuk dianalisis. *Tools* yang digunakan untuk menganalisis paket data adalah *Wireshark.*

Ditinjau dari efisiensi, diasumsikan metode PPTP dan L2TP dan dilakukan pengujian dengan kriteria QoS seperti *throughput*, *delay, packet loss*, dan *jitter* terdapat perbandingan efisiensi .

Berdasarkan hipotesis di atas kerangka berpikir dalam penelitian ini dapat digambarkan sebagai berikut:



Gambar 1-1 Kerangka berpikir

1.7 Sistematika Penulisan Tugas Akhir

Tugas Akhir ini disusun berdasarkan sistematika penulisan sebagai berikut :

BAB I : PENDAHULUAN

Menjelaskan tentang permasalahan yang akan dibahas secara umum dengan memperhatikan latar belakang, perumusan masalah, tujuan, manfaat, lingkup tugas akhir dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Menjelaskan teori tentang WFH, *remote acces*, VPN, PPTP, L2TP, dan performansi yang berpengaruh dalam jaringan.

BAB III : METODE PENELITIAN

Bab ini menjelaskan metode yang digunakan dalam pengumpulan data dan perancangan sistem yang akan dibangun.

BAB IV : IMPLEMENTASI, PENGUJIAN, DAN ANALISIS HASIL PENGUJIAN

Bab ini akan menampilkan konfigurasi yang dilakukan dalam implementasi, skenario pengujian, dan analisis hasil pengujian dari perancangan sistem yang telah dibuat.

BAB V : KESIMPULAN DAN SARAN

Pada bab ini akan disebutkan kesimpulan yang telah didapatkan dari proses pengujian dan analisis sebelumnya beserta saran yang dapat digunakan sebagai masukan dalam penelitian berikutnya.