BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi jaringan komputer sangat pesat dan menjadi kebutuhan sangat penting bagi perusahaan yang berguna untuk mempermudah dalam hal pengolahan dan pengiriman data antar beberapa komputer dan perangkat lainnya dalam satu perusahaan maupun antar perusahaan. Dengan menggunakan jaringan komputer pengguna mendapatkan berbagai macam keuntungan dalam berkomunikasi pertukaran data jadi lebih mudah, mengurangi resiko rusaknya data, menghemat waktu, dan mempermudah pekerjaan.

PT DAK (PT Dok dan Perkapalan Air Kantung) merupakan perusahaan galangan kapal yang bergerak dalam bidang *Ship Repair, Ship Building, Docking dan Repair Engineering, Construction, Ship Equipment Supplies* dengan spesialisasi dalam pembuatan dan perbaikan kapal. Untuk menjalankan operasional dan saling bertukar informasi data dan *file*, perusahaan ini menggunakan layanan jaringan internet dari ISP (*Internet Service Provider*) Indihome serta *Mikrotik outerboard*.

Selama ini para pegawai banyak menggunakan aplikasi, sistem informasi dan sumber daya lainnya yang terdapat di jaringan lokal kantor pusat, akan tetapi jaringan lokal ini hanya bisa diakses dari dalam kantor. Sedangkan PT DAK sendiri terdapat beberapa kantor cabang yang membutuhkan berbagai data dan informasi tersebut, tetapi hanya bisa diakses dari dalam kantor pusat saja. Sistem yang dibutuhkan oleh pegawai untuk membuat laporan dan lain-lain tidak bisa dilakukan diluar kantor, disamping itu banyak sumber daya lain yang hanya dapat diakses melalui jaringan lokal.

Berdasarkan permasalahan tersebut, penulis mengusulkan sistem jaringan koneksi VPN yang memanfaatkan jaringan telekomunikasi publik seperti internet tetapi tetap menjaga keamanan dan privasi melalui penggunaan protokol dan keamanan jaringan *tunneling* atau jaringan *private*. Sistem tersebut diharapkan

dapat membantu sistem jaringan pada kantor cabang dan karyawan-karyawan PT DAK agar bisa melakukan akses ke jaringan lokal kantor pusat meski dari jarak jauh. *Remote access* VPN adalah akses jarak jauh yang memungkinkan pengguna atau pegawai dapat bekerja dari jarak jauh untuk mengakses dan menggunakan aplikasi dan data secara aman yang berada di pusat data atau kantor pusat perusahaan. Untuk mengaplikasikan koneksi VPN tersebut diperlukan protokol yang bisa menunjang keamanan dan kerahasiaan saat transmisi data berlangsung. Karena aplikasi, data, sistem informasi itu bersifat rahasia dan tidak boleh diketahui oleh orang yang tidak berwenang, oleh karena itu diperlukan suatu sistem jaringan yang bisa menjamin kerahasiaan sumber daya jaringan lokal tersebut. Maka, dalam penelitian ini kami mengusulkan perancangan suatu sistem jaringan VPN untuk menyelasaikan masalah tersebut. Disini kami menggunakan koneski VPN berbasis L2TP/IPsec karena jika dibandingkan dengan protokol sejenisnya, L2TP/IPsec jauh lebih aman dan memiliki tingkat enkripsi yang lebih kompleks, dan juga lebih baik dalam komunikasi berbasis real time.

Implementasi jaringan VPN dan penelitian terkait keamanan jaringan komputer telah dilakukan pada studi sebelumnya, dan penelitian-penelitian terdahulu akan penulis jadikan sebagai referensi dan bahan penelitian. Penelitian Dian dan Helmud pada tahun 2019 mengenai "Implementasi *Failover* dengan Metode *Recursive Gateway* Berbasis *Router Mikrotik* Pada STMIK Atma Luhur Pangkalpinang"[1], Penelitian Hafiz dkk pada tahun 2021 Mengenai "Analisis Jaringan VPN Menggunakan PPTP dan L2TP Berbasis *Mikrotik* pada Diskominfo Kabupaten Muko Muko"[2], Penelitian Hedy dan Puspitasari pada tahun 2020 mengenai "Penerapan Protokol L2TP/IPSec dan *Port Forwarding* untuk *Remote Mikrotik* pada Jaringan *Dynamic* IP"[3], Penelitian Khairan dkk pada tahun 2022 mengenai "*Bandwith Optimization on Hotspot using PCQ Method and L2TP VPN Routing for Online Game Latency*"[4], Penelitian Sulistiyono dkk pada tahun 2020 mengenai "Perancangan Jaringan *Virtual Private Network* Berbabsis IP *Security* Menggunakan *Router Mikrotik*"[5].

Berdasarkan masalah yang telah diuraikan pada latar belakang tersebut, maka kelompok kami mengusulkan penelitian kuliah praktek berjudul "**Perancangan**

Jaringan *Virtual Private Network* (VPN) Berbasis L2TP/IPsec Pada *Router Mikrotik* Di PT DAK (Dok dan Perkapalan Air Kantung)".

1.2 Rumusan Masalah

Berdasarkkan latar belakang yang telah diuraikan pada bagian sebeumnya maka dapat dirumuskan rumusan masalah dalam bentuk pertanyaan sebagai berikut:

1. Bagaimana cara merancang jaringan *Virtual Private Network* (VPN) berbasis L2TP/IPSec pada *router Mikrotik* di PT DAK?
2. Bagaimana cara konfigurasi jaringan *Virtual Private Network* (VPN) berbasis L2TP/IPSec pada *router Mikrotik* di PT DAK?

1.3 Tujuan dan Manfaat Penulisan

Adapun tujuan dan manfaat yang ingin dicapai untuk memecahkan masalah pada kerja praktek ini antara lain:

1.3.1 Tujuan Penulisan

Tujuan yang ingin dicapai dalam penelitian ini adalah:

1. Untuk menghasilkan sebuah rancangan jaringan *Virtual Private Network* (VPN) berbasis L2TP/IPSec pada *router Mikrotik* di PT DAK.
2. Untuk mempelajari cara mengkonfigurasi jaringan *Virtual Private Network* (VPN) berbasis L2TP/IPSec pada *router Mikrotik* di PT DAK.

1.3.2 Manfaat Penulisan

Berdasarkan tujuan yang ingin dicapai diatas, adapun manfaat yang akan dicapai dalam penelitian ini adalah:

1. Diharapkan agar rancangan jaringan *Virtual Private Network* (VPN) berbasis L2TP/IPSec pada *router Mikrotik* ini dapat digunakan sebagai referensi dalam membangun dan mengembangkan jaringan koneksi VPN di PT DAK.
2. Diharapkan bagi pembaca dan penulis dapat mengetahui cara mengkonfigurasi jaringan *Virtual Private Network* (VPN) berbasis L2TP/IPSec pada *router Mikrotik*.

1.4 Batasan Masalah

Batasan masalah pada penelitian kerja praktek ini bertujuan untuk menyederhanakan masalah. Batasan-batasan ini antara lain:

1. Perancangan dan konfigurasi jaringan VPN dilakukan di lingkungan simulasi menggunakan mesin virtual pada tools GNS3 berdasarkan kebutuhan dan topologi jaringan yang ada di PT DAK.
2. *Mikrotik* yang digunakan ialah *Mikrotik* CHR (*Cloud Hosted Routed*) versi 6.46.6 yang terpasang di mesin virtual pada GNS3.
3. Konfigurasi *Mikrotik* menggunakan aplikasi WinBox versi 3.37.
4. Tidak membahas algoritma enkripsi dan autentikasi.
5. Pengujian tidak dilakukan ke dalam sistem informasi perusahaan.

1.5 Metodologi Penelitian

Dalam penelitian ini penulis menggunakan teknik pengumpulan data dan model pengembangan sistem NDLC (*Network Development Life Cycle*) dalam perancangan sistem jaringan VPN berbasis L2TP/IPSec pada *router Mikrotik* di PT DAK. Beberapa teknik pengumpulan data yang dilakukan adalah observasi, wawancara, dan studi literatur. Model pengembangan NDLC terdiri dari 6 proses atau tahapan yaitu *analysis, design, prototyping, implementation, monitoring,* dan *management*.

1.6 Sistematika Penulisan

Sistematika penulisan laporan kerja praktek ini dibuat untuk mempermudah dalam pembahasan, Adapaun susunannya sebagai berikut:

BAB I: PENDAHULUAN

Berisi pembahasan masalah umum yang berhubungan dengan penyusunan laporan kerja praktek, yang meliputi latar belakang, maksud dan tujuan kerja praktek, sistem pelaksanaan kerja praktek dan sistematika pelaporan kerja praktek.

BAB II: LANDASAN TEORI

Bab ini membahas mengenai berbagai macam teori yang digunakan untuk studi literatur guna mendukung dalam perancangan jaringan VPN berbasis L2TP/IPSec pada *router Mikrotik* di PT DAK.

BAB III: ORGANISASI

Berisi pembahasan tentang profil PT DAK, yang meliputi sejarah, struktur organisasi, visi dan misi, tugas dan wewenang, tabel spesifikasi, dan hal-hal lain yang menjelaskan tentang perusahaan.

BAB IV: PEMBAHASAN

Bab ini berisi tentang kegiatan yang dilakukan selama masa kerja praktek, yang meliputi cara/teknik kerja praktek, analisis sistem jaringan, analisis masalah, dan konfigurasi jaringan VPN berbasis L2TP/IPSec pada *router Mikrotik* di PT DAK.

BAB V: PENUTUP

Pada bab ini membahas tentang kesimpulan dari hasil perancangan dan saran untuk pengembang sistem selanjutnya.