# BAB I

# PENDAHULUAN

## 1.1 Latar Belakang

PT. Dana Tabungan dan Asuransi Pegawai Negeri Perusahaan Perseroan atau secara singkat disebut PT. TASPEN (PERSERO) Palembang yang beralamat Jl. Jenderal Sudirman KM 4 No. 104 Palembang. PT. TASPEN (PERSERO) Palembang merupakan perusahaan Badan Usaha Milik Negara (BUMN) yang menyelenggarakan dua jenis program utama yang meliputi Program Tabungan Hari Tua (THT) dan Program pensiun Pegawai Negeri Sipil (PNS). PT. TASPEN (PERSERO) Palembang sudah menerapkan jaringan *wireless* dalam jaringan komputer dalam menunjang sistem komunikasi dan pertukaran informasi bagi karyawan. PT. TASPEN (PERSERO) Palembang memanfaatkan jaringan *wireless* dengan menempatkan *Access Point* (AP) sebagai fasilitas hotspot di setiap ruangan. Sistem keamanan jaringan *wireless* yang digunakan oleh PT. TASPEN (PERSERO) Palembang adalah menggunakan sistem keamanan WPA2-PSK untuk *autentikasi user*/karyawan agar dapat mengakses *internet*. Keamanan jaringan *wireless* WPA2-PSK yaitu menggunakan *password* yang sama untuk dapat akses *internet* dan dapat digunakan banyak *users* yang tahu *password* juga kurang efektif dan juga rawan terjadi peretasan sistem jaringan *wireless* seperti pencurian data dan kejahatan *cyber* lainnya. Melihat PT. Taspen (Persero) Palembang bergerak dibidang pengelolaan dana pensiun sangat diperlukan pengembangan sistem keamanan agar tidak terjadi peretasan data atau pencurian

data  dan serta tidak adanya sistem yang me-monitoring kegiatan dalam jaringan *wireless* dan masih bersifat terbuka, Masalah lain yaitu kebebasan karyawan dalam mengakses situs – situs yang ada di internet pada saat jam kerja dapat mengganggu dan membuat lalai kinerja seorang karyawan, penerapan sistem keamanan misalnya membatasi hak akses penggunaan browsing pada jam bekerja dan membatasi mengunjungi situs-situs seperti *youtube*, *instagram*, *facebook, dll* yang tidak diperbolehkan oleh karyawan pada jam kerja. Berdasarkan permasalahan tersebut diperlukan system keamanan *Radius server* dan *firewall* untuk dapat mengakses jaringan *wireless* khusus bagi para *user*/karyawan sehingga *administrator* dapat me-monitoring dan mengelola *user* dalam jaringan *wireless.*

*Radius Server* bisa dikatakan *Authentication user* yang dimana akan memberikan suatu *login user* yang hanya akan dimiliki oleh karyawan PT. TASPEN (PERSERO) Palembang untuk dapat mengakses jaringan *wireless* sehingga dapat terkoneksi ke jaringan internet. *Firewall* sistem keamanan untuk mengatur dan mengontrol lalu lintas jaringan dan juga dapat mencegah atau memblokir terhadap situs tertentu maupun membatasi aktifitas *user*/karyawan dalam mengkases situs yang tidak diperbolehkan saat bekerja.

Keamanan jaringan *wireless LAN (Local Area Network)* pada PT. TASPEN (PERSERO) Palembang perlu pengembangan yaitu dengan mengganti sistem keamanan WPA2-PSK dengan sistem keamanan *Radius server* dan *firewall* digunakan untuk pengamanan jaringan *wireless* LAN agar tidak semua orang bisa mengakses internet menggunakan jaringan *wireless.* Hanya yang memiliki username dan password saja yang bisa mengakses internet menggunakan

jaringan *wireless* tersebut. Serta perlu adanya pengembangan sistem keamanan firewall untuk membatasi hak akses atau memblok situs tertentu yang ada di internet. *Radius Server* dan *Firewall* merupakan salah satu fitur dari mikrotik yang nantinya akan digunakan dalam penelitian ini.

Berdasarkan permasalahan tersebut, penulis tertarik untuk melakukan penelitian dengan judul **"Pengembangan Keamanan Jaringan WLAN berbasis *Radius Server* dan *Firewall* Menggunakan Mikrotik Routerboard di PT. TASPEN (PERSERO) Palembang".**

## 1.2. Identifikasi Masalah

Berdasarkan latar belakang yang telah di uraikan, maka identifikasi masalahnya adalah:

1. Bagaimana cara pengembangan keamanan jaringan *WLAN* (*Wireless Local Area Network*) berbasis *radius server* menggunakan Mikrotik *Routerboard* di PT. Taspen (Persero) Palembang?
2. Bagaimana cara pengembangan keamanan jaringan *WLAN* (*Wireless Local Area Network*) berbasis *firewall* menggunakan Mikrotik *Routerboard* di PT. Taspen (Persero) Palembang?

## 1.3 Batasan Masalah

Agar pembahasan lebih terarah dan tidak menyimpang, maka penulis hanya membatasi masalah pada:

1. Pengembangan penelitian ini dilakukan di lantai 1 Ruangan Divisi Pelayanan dengan 1 buah *Access Point* (AP) dan Ruangan Keuangan dengan 1 buah *Access Point* (AP) Pada PT. Taspen (Persero) Palembang.
2. Pengembangan keamanan jaringan WLAN dengan penerapan *radius server* menggunakan *Mikrotik router board.*
3. Pengembangan keamanan jaringan WLAN dengan penerapan *firewall filter rules* menggunakan *Mikrotik router board.*
4. Penerapan penelitian ini hanya sebatas *analysis, design, simulation prototyping.*

## 1.4 Tujuan dan Manfaat Penelitian

### 1.4.1 Tujuan Penelitian

Tujuan dari penulisan tugas akhir ini adalah pengembangan sistem keamanan jaringan *wireless* LAN pada PT. Taspen (Persero) Palembang berbasis *radius server* dan *firewall* menggunakan *Mikrotik RouterBoard* agar administrator dapat me-monitoring dan mengontrol *user* yang terhubung dalam jaringan.

### 1.4.2 Manfaat Penelitian

Manfaat dari penulisan tugas akhir ini adalah sebagai berikut:

a. Manfaat bagi PT. Taspen (Persero) Palembang.

1. Dapat membantu dalam mengelola dan monitoring user dalam jaringan *wireless* LAN di PT. Taspen (Persero) Palembang.

2. Hanya *user/*pengguna memiliki *username* dan *password* terdaftar saja yang bisa mengakses internet menggunakan jaringan *wireless* di PT. Taspen (Persero) Palembang.
3. Dapat Memberikan batasan – batasan dalam mengakses internet yang tidak diperbolehkan di saat jam kerja bagi karyawan PT. Taspen (Persero) Palembang.

b. Manfaat bagi Penulis.

1. Peneliti dapat menambah wawasan tentang penggunaan Mikrotik *routerboard.*
2. Penulis dapat mengetahui cara kerja *Radius server* dan *firewall* dalam jaringan *wireless LAN*.

## 1.5 Metodologi Penelitian

### 1.5.1 Waktu dan Lokasi Penelitian

Penelitian ini dilakukan pada bulan Januari 2019 sampai dengan bulan Februari 2019 adapun lokasi penelitian yaitu pada area perkantoran PT. Taspen (Persero) Palembang.

### 1.5.2 Metode Pengumpulan Data

Pada metode ini dilakukan beberapa cara agar penulis memperoleh data yang dibutuhkan penulis：

1. Metode Pengamatan (observasi).

Pada metode ini penulis melakukan pengumpulan data secara langsung untuk mendapatkan informasi di PT. Taspen (Persero) Palembang dengan cara melihat atau mengamati seperti Topologi jaringan, keamanan jaringan, perangkat jaringan komputer secara langsung di PT. Taspen (Persero) Palembang untuk pembahasan tugas akhir.

2. Wawancara (*Interview*)

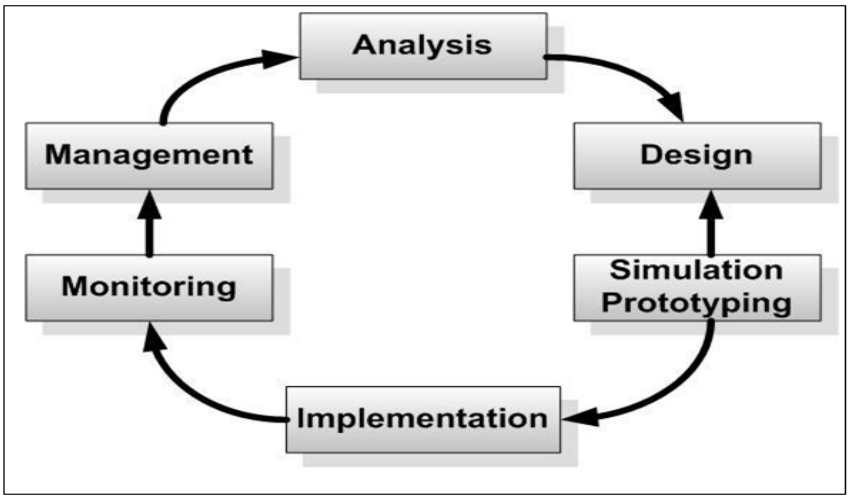
Data yang di dapat yaitu berupa laporan Topologi jaringan, keamanan jaringan, permasalahan jaringan dan perangkat jaringan komputer yang dikumpulkan dengan cara melakukan wawancara (*Interview*) langsung dengan bapak Toto karyono yakni sebagai Kepala Bidang IT yang ada di PT. Taspen (Persero) Palembang.

3. Studi Pustaka (Literature)

Data diperoleh dengan mencari bahan dari jurnal dan buku tentang Pengembangan, Keamanan jaringan, Jaringan komputer, Jaringan WLAN, Sejarah WLAN, Mode *wireless* WLAN, Peralatan WLAN, *Radius Server,* Format paket data *radius server*, Prinsip kerja *radius server,* Proses AAA pada *radius server, firewall,* Fungsi *firewall, Mikrotik, Winbox.*

### 1.5.3 Metode Penelitian

Penelitian yang digunakan pada metode Network Development Life Cycle (NDLC),yaitu suatu pendekatan proses dalam komunikasi data yang menggunakan siklus yang tiada awal dan akhirnya dalam membangun sebuah jaringan provider, mencakup sejumlah tahap yaitu analisis, desain, simulasi *prototype*, implementasi, monitoring dan manajemen. Dalam jurnal (Rahmat Novrianda, 2017) dengan judul Rancang Bangun Keamanan Jaringan Wireless Pada Stiper Sriwigama Palembang Dengan Radius Server.




Gambar 1.1 Tahapan NDLC

Tahapan-tahapan pada NDLC:

1. *Analysis*, Tahap awal ini dilakukan analisa kebutuhan, analisa permasalahan yang muncul, analisa keinginan pengguna, dan analisa topologi / jaringan yang sudah ada saat ini. Metode yang biasa digunakan pada tahap ini diantaranya adalah wawancara, survey, langsung ke lapangan.

2. *Design*, Dari data-data yang didapatkan sebelumnya, tahap *Design* ini akan membuat gambar *design topology* jaringan interkoneksi yang akan dibangun, diharapkan dengan gambar ini akan memberikan gambaran seutuhnya dari kebutuhan yang ada. *Design* bisa berupa *design* struktur *topology* yang akan memberikan gambaran jelas tentang *project* yang akan dibangun.

3. *Simulation Prototype,* beberapa *networker's* akan membuat dalam bentuk simulasi dengan bantuan *Tools* khusus di bidang *network* seperti *BOSON, PACKET TRACERT, NETSIM,* dan sebagainya, hal ini dimaksudkan untuk melihat kinerja awal dari *network* yang akan dibangun dan sebagai bahan presentasi dan sharing dengan *team work* lainnya. Namun karena keterbatasan perangkat lunak simulasi ini, banyak para *networker's* yang hanya menggunakan alat Bantu tools VISIO untuk membangun topology yang akan didesain.

4. *Implementation*, di tahapan ini akan memakan waktu lebih lama dari tahapan sebelumnya. Dalam implementasi *networker's* akan menerapkan semua yang telah direncanakan dan di design sebelumnya. Implementasi merupakan tahapan yang sangat menentukan dari berhasil / gagalnya *project* yang akan dibangun dan di tahap inilah *Team Work* akan diuji di lapangan untuk menyelesaikan masalah teknis dan non teknis.

5. *Monitoring*, setelah implementasi tahapan monitoring merupakan tahapan yang penting, agar jaringan komputer dan komunikasi dapat berjalan

sesuai dengan keinginan dan tujuan awal dari user pada tahap awal analisis, maka perlu dilakukan kegiatan monitoring.

6. *Management*, di manajemen atau pengaturan, salah satu yang menjadi perhatian khusus adalah masalah *Policy*, kebijakan perlu dibuat untuk membuat / mengatur agar sistem yang telah dibangun dan berjalan dengan baik dapat berlangsung lama dan unsur *Reliability* terjaga. *Policy* akan sangat tergantung dengan kebijakan level management dan strategi bisnis perusahaan tersebut. IT sebisa mungkin harus dapat mendukung atau alignment dengan strategi bisnis perusahaan.

## 1.6 Sistematika Penulisan

Dalam penulisan tugas akhir ini, penulis menguraikan sistematika penulisan yang terdiri dari:

**BAB I PENDAHULUAN**

Bab ini terdiri dari latar belakang, identifikasi masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian dan sistematika penulisan tugas akhir.

**BAB II LANDASAN TEORI**

Dalam bab ini akan menguraikan tentang landasan teori yang didapat dari studi pustaka pengembangan, keamanan jaringan, WLAN, *radius server, firewall*, Mikrotik, *winbox*.

**BAB III ANALISIS KEBUTUHAN**

Dalam bab ini berisi objek penelitian mengenai profil perusahaan serta permasalahan-permasalahan yang ditemukan dan solusinya.

**BAB IV HASIL DAN PEMBAHASAN**

Bab ini berisikan hasil dari penelitian yang penulis lakukan dan pembahasan tentang penelitian yang telah diperoleh mengenai konfigurasi *Radius Server* dan *Firewall* pada *Mikrotik Routerboard.*

**BAB V KESIMPULAN DAN SARAN**

Bab ini berisikan tentang kesimpulan dan saran dari penelitian yang dilakukan.