BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Jaringan sangat dibutuhkan untuk keberlangsunan bisnis bagi setiap perusahaan. Agar dapat mencapai keterhubungan antar lokasi dibutuhkan perencanaan perangkat yang tepat guna memaksimalkan efektifitas tiap perangkat dan meminimalkan biaya yang dikeluarkan. Selain aspek biaya juga perlu untuk meninjau aspek keamanan untuk menjaga kerahasiaan data agar tidak terjadi kebocoran data. Menurut (Barker and Morris, 2013) salah satu dari konsep dari keamanan adalah kerahasiaan (confidentiality) yang berarti data hanya boleh diakses oleh individu yang memiliki otoritas / autentikasi terhadap data tersebut. Untuk mencapai kerahasiaan maka diperlukan jalur yang aman di dalam jaringan yang menghubungkan antar lokasi. Pentingnya jalur yang aman adalah untuk mencegah terjadinya kebocoran data saat data melewati jaringan internet.

Untuk komunikasi antar cabang dan kantor pusat, perusahaan biasanya menggunakan jaringan internet publik. Teknologi yang digunakan dalam jaringan internet publik adalah DSL *(Digital subscriber line).* Menurut (Cowley, 2007) DSL adalah teknologi yang menggunakan kabel tembaga untuk mendapatkan kecepatan data yang

tinggi dengan menggunakan kabel tembaga, teknologi ini disebut juga sebagai teknologi *broadband*. Dalam penggunaan teknologi DSL, ADSL (*Asymmetric DSL)* lebih sering digunakan daripada SDSL (*Symmetric DSL*) oleh masyarakat. ADSL memberikan kecepatan transfer data yang tinggi pada satu arah sehingga disebut dengan *Asymmetric,* sedangkan SDSL memberikan transfer data yang tinggi pada dua arah sehingga disebut *Symmetric*. ADSL mempunyai biaya yang relatif lebih murah daripada SDSL karena hanya memberikan kecepatan transfer data tinggi satu arah dan umumnya memberikan IP Address yang bersifat dinamis.

Penggunaan jaringan internet publik memiliki kelemahan yaitu data yang melewati jaringan internet publik dapat diakses pengguna lain, namun ini dapat diatasi dengan VPN. Menurut (Whitman, 2013) VPN melakukan enkapsulasi dan enkripsi data yang dikirimkan, dan menggunakan autentikasi untuk memastikan hanya pengguna yang diperbolehkan yang dapat mengakses data tersebut. Berdasarkan beberapa penelitian (Mubarok, 2018) dan (Haque and Pamungkas, 2019) menunjukkan bahwa teknologi VPN dapat diimplementasikan dalam lingkungan IP dinamis dengan menggunakan DDNS. DDNS merupakan sebuah servis yang dapat digunakan untuk mengartikan alamat IP menjadi hostname. Kedua penelitian ini menggunakan jenis VPN IPsec. Menurut Crist dan Jan Just (Crist and Keijser, 2015) IPsec

merupakan standar resmi IEEE/IETF untuk IP Security yang terdaftar dalam RFC2411. Selain IPsec, OPENVPN merupakan jenis VPN yang berbasis yang berbasis SSL yang memiliki tingkat keamanan yang serupa dengan IPsec.

Oleh karena itu, OPENVPN dapat menjadi solusi alternative dalam membangun VPN selain menggunakan IPsec. Dengan menganalisa jaringan VPN pada jenis IPsec dan OPENVPN diharapkan dapat ditemukan jenis VPN yang memiliki performa dan keamanan data yang lebih unggul.

1.2 Perumusan Masalah

Berdasarkan latar belakang masalah, maka dapat dirumuskan masalah – masalah sebagai berikut :

a. Bagaimana membangun jaringan VPN dalam jaringan berbasis IP dinamis ?
b. Bagaimana melakukan analisa keamanan data terhadap IPsec dan OPENVPN?
c. Bagaimana perbandingan performa terhadap IPsec dan OPENVPN ?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah :

a. Membandingkan performa VPN antara IPsec dan OPENVPN.
b. Menguji keamanan dan konektivitas pada jaringan internet publik menggunakan teknologi DDNS dan VPN.

1.4 Batasan Masalah

Berdasarkan beberapa pokok permasalahan yang telah diuraikan pada perumusan masalah di atas, maka penelitian ini akan dibatasi dalam ruang lingkup sebagai berikut :

a. Implementasi dilakukan menggunakan jaringan internet yang memiliki IP Dinamis.
b. Perancangan menggunakan router Mikrotik RB941 HAP-Lite.
c. DDNS menggunakan fitur IP-Cloud yang terdapat pada Mikrotik.
d. Fitur yang akan dikonfigurasi dan diuji dibatasi pada fitur yang tersedia pada router Mikrotik RB941 HAP-Lite.

1.5 Manfaat Penelitian

Penelitian ini dapat memberikan manfaat sebagai berikut ini:

1. Manfaat Teoritis
   a) Hasil dari penelitian ini dapat digunakan sebagai acuan dalam penelitian selanjutnya.

2. Manfaat Praktis

a) Sebagai wadah untuk menerapkan ilmu pengetahuan yang telah didapatkan pada pembelajaran selama masa kuliah.
b) Sebagai teknologi alternatif bagi perusahaan SOHO (*small office / home* office) yang ramah biaya namun tetap mengutamakan keamanan.

Halaman ini sengaja dikosongkan