BAB 2
TINJAUAN PUSTAKA

2.1 Penelitian terdahulu

Bahan kajian utama yang akan dibahas adalah penelitian mengenai penggunaan vpn untuk menghubungkan jaringan antar lokasi sebagai jalur komunikasi dan transfer data yang aman pada jalur internet. Pada kajian-kajian ini akan dikaji teknik-teknik dan jenis vpn yang digunakan dan menjadi dasar teori untuk menghubungkan jaringan antar lokasi secara keseluruhan.

2.1.1 Implementasi EoIP over VPN di jaringan berbasis dynamic IP (studi kasus PT.Validata Teknologi)

Penelitian (Mubarok, 2018) merupakan penelitian implementasi VPN menggunakan jalur public yang memiliki dynamic IP. Dzaki mengemukakan komunikasi data yang terintegrasi saat ini di Indonesia sudah menjadi kebutuhan utama bagi sebuah institusi atau perusahaan bisnis, namun kegiatan ini membutuhkan biaya yang mahal. Untuk mengatasi hal ini maka VPN digunakan untuk komunikasi pada Internet. Lalu untuk mengatasi dynamic IP yang selalu berganti digunakan fitur IP Cloud pada Mikrotik sebagai DDNS agar Mikrotik dapat memperbaharui rute secara otomatis. Jenis VPN yang digunakan dalam penelitian ini adalah PPTP

2.1.2 Rancang Bangun Automated Virtual Private Network Menggunakan Jaringan Small Office Home Office (SOHO) Di PT. Satnetcom Balikpapan

. Penelitian (Haque and Pamungkas, 2019) merupakan penelitian yang didasarkan penelitian (Mubarok, 2018) Perbedaan antara kedua penelitian ini adalah pada penelitiannya (Haque and Pamungkas, 2019) menggunakan jenis VPN IPsec pada konfigurasi yang dipasang pada Mikrotik. Sedangkan untuk melakukan pembaharuan terhadap perangkat Mikrotik yang dipasang menggunakan *script*, yaitu sekumpulan perintah otomasi untuk mendeteksi pergantian perangkat yang digabungkan dengan fitur *netwatch* milik Mikrotik. Perbedaan lainnya adalah pada jaringan yang dipasang tidak sepenuhnya menggunakan *dynamic IP* namun menggunakan *IP Address* statik pada salah satu sisinya.

2.1.3 Penerapan VPN IP Security Site To Site Di Kementrian Perhubungan.

. Penelitian (Firdhaus, Fatmawati and Wijonarko, 2019) menggunakan jenis VPN IPsec untuk menghubungkan kantor pusat dan kantor cabang pada kementrian perhubungan. Pada implementasinya penelitian ini menggunakan router dan *firewall* ASA Cisco. Router yang digunakan berfungsi untuk membangun konektivitas VPN antar lokasi sedangkan *firewall* digunakan untuk membuat aturan untuk trafik yang dapat lewat pada tunnel VPN. Implementasi yang dilakukan pada penelitian ini memungkinkan

penggunaan VPN untuk menghubungkan jaringan lokal antar lokasi secara keseluruhan.

2.1.4 Metode VPN yang diusulkan dalam penelitian

Perbedaan pada penelitian-penelitian sebelumnya adalah implementasi dalam membuat VPN menggunakan jenis VPN berbasi IPsec. Dalam penelitian ini penulis menggunakan OPENVPN sebagai alternatif IPsec. Keunggulan OPENVPN dibandingkan dengan IPsec adalah kemudahan dalam konfigurasinya dan karena OPENVPN lebih kompatibel terhadap NAT dibandingkan dengan IPsec menurut (Crist and Keijser, 2015).

2.2 Landasan Teori

Pada landasan teori ini berisi tentang teori yang berkaitan dengan . Rancang bangun sistem site-to-site VPN menggunakan Mikrotik pada jaringan berbasis *dynamic IP*.

2.2.1 Local Area Network (LAN)

Local Area Network (LAN) adalah bagian dari jaringan yang memiliki ukuran paling kecil. Menurut (Cowley, 2007) LAN menghubungkan perangkat agar dapat berkomunikasi dengan perangkat lain untuk berbagi *resources*. Perangkat dalam sebuah jaringan *wired LAN* biasanya saling terhubung dengan kabel yang tidak mahal. Karena limitasi jarak, performa, dan pengelolaan, biasanya LAN hanya terbatas dalam sebuah kantor atau lantai dalam sebuah gedung. LAN juga tidak terbatas pada media kabel,

Akses poin juga dapat digunakan untuk menghubungkan perangkat pada jaringan *wired LAN.*

LAN merupakan sekumpulan komputer pada tiap lokasi yang memiliki alamat dalam satu segmen. LAN dapat digunakan untuk berkomunikasi dengan perangkat yang memiliki alamat IP dalam segmen yang sama, namun tidak bisa digunakan untuk berkomunikasi dengan perangkat dalam segmen yang lain.

2.2.2 Wide Area Network (WAN)

Wide Area Network (WAN) menghubungkan jaringan-jaringan LAN. Menurut (Cowley, 2007) secara tradisional, LAN menjadi WAN saat terhubung dengan jaringan telepon publik yang biasanya menggunakan jalur *leased lines* yang dimiliki oleh perusahaan telepon lokal. WAN memiliki limitasi jarak yang lebih besar dibandingkan dengan LAN biasanya dapat menghubungkan antar jaringan yang berbeda geografis. Dengan menghubungkan LAN antar lokasi menggunakan WAN maka pengguna dapat berbagi *resource*.

2.2.3 Topologi

Topologi adalah cara untuk memetakan sebuah jaringan. Menurut (Docter, 2007) Topologi digunakan untuk membabarkan jaringan yang dapat berupa *physical topology* atau *logical topology*. *Physical topology* menjabarkan hubungan antar perangkat secara fisik satu dengan menggunakan media kabel atau *wireless*. sedangkan *logical topology* menjabarkan bagaiman paket

dalam jaringan terkirim, biasanya digambarkan dengan pengalamatan IP antar perangkat satu dengan yang lain.

2.2.4 Virtual Private Network (VPN)

Dengan menggunakan WAN maka pengguna dapat berbagi *resource* menggunakan media internet. Namun dengan menggunakan internet maka pengguna lain yang menggunakan media yang sama mampu melihat data yang dikirimkan oleh pengguna lain. Hal ini bisa diatasi dengan menggunakan jalur *dedicated* yang menghubungkan kedua lokasi *point-to-point*.

Namun permasalahan utama dalam penggunaan jalur *dedicated* adalah biaya. Menurut (Barker and Morris, 2013) lebih murah menggunakan internet untuk menghubungkan pengguna dibandingkan dengan menggunakan jalur dedicated yang menghubungkan satu lokasi ke lokasi lain.

Menurut Barker dan Morris tujuan utama dari VPN adalah kerahasiaan dan hal ini dapat dicapai dengan mengenkripsi data yang perlu didlindungi dan dikirimkan melewati VPN (Barker and Morris, 2013). Dengan menggunakan VPN pengguna di dua lokasi dapat saling terhubung dengan internet sebagai media transportasinya, dan konektivitas antar kedua pengguna akan menjadi privat hanya untuk kedua pengguna tersebut. Dengan enkripsi maka pengguna lain yang menggunakan internet tidak dapat melihat data yang dikirimkan tanpa menggunakan kunci dekripsi untuk membuka enkripsi data tersebut.

2.2.5 Tipe VPN

Menurut Barker dan Morris, VPN dapat dibagi menjadi dua kategori dilihat dari penempatan VPN (Barker and Morris, 2013) , yaitu : *remote-access* dan *site-to-site*.

- **Remote Access** : Pengguna yang menggunakan VPN sebagai media untuk mengakses data dari perusahaan atau dari suatu lokasi. Proses ini dapat disebut akses jarak jauh (*remote access VPN Connection*). Biasanya pengguna memasang VPN pada perangkat yang dipakai sebagai client yang telah dibuat pada server VPN yang berada pada perusahaan.
- **Site-to-site** : VPN diimplementasikan oleh perusahaan untuk menghubungkan dua lokasi atau lebih agar dapat saling berkomunikasi dengan aman. Proses ini disebut sebagai *site-to-site* VPN. *Site-to-site* VPN biasanya menghubungkan jaringan LAN dari satu lokasi dengan yang lain sehingga kedua lokasi dapat berkomunikasi seperti sebuah jaringan LAN.

2.2.6 IPsec

IPsec merupakan standar resmi IEEE/IETF untuk IP Security yang terdaftar dalam RFC2411. Menurut (Crist and Keijser, 2015) IPsec bekerja pada lapisan 2 atau 3 dalam OSI, dan walaupun fleksibel dan kuat tetapi sangat susah untuk dikonfigurasi dan dilakukan *troubleshoot.* Terdapat dua mode IPsec yang dapat diimplementasikan pada mikrotik yaitu digunakan bersamaan dengan *Layer 2 Tunneling Protocol (L2TP)*

atau hanya menggunakan IPsec. Kelebihan dari IPsec adalah keamanan yang kuat, terdapat pada berbagai vendor dan perangkat, dan kemampuan untuk menggunakan aturan (*policy)* untuk mengatur laju pengiriman data.

2.2.7 OpenVPN

OpenVPN adalah salah satu jenis VPN yang berbasis SSL. Menurut (Crist and Keijser, 2015) OpenVPN tidak hanya menggunakan SSL/TLS protokol untuk mengamankan koneksi, namun juga menggunakan HMAC yang dikombinasikan dengan algoritma *digest / hashing* untuk memastikan integritas data. OpenVPN bekerja pada layer 2 atau 3, namun menggunakan protokol SSL/TLS sebagia media enkripsinya. Salah satu kelebihan OpenVPN adalah kemampuannya dalam bekerja dibalik jaringan yang menggunakan NAT.

2.2.8 Dynamic DNS

Domain Name System (DNS) merupakan sebuah servis yang membuat penggunanya dapat mengartikan sebuah *hostname* menjadi alamat IP (*IP Address).* Salah satu fungsi penggunaan DNS adalah pengguna dapat mengakses website menggunakan alamat website daripada menggunakan alamat IP dari website tersebut. Menurut (Panek, 2017) pada peluncuran Windows Server 2000, Microsoft menyatakan akan menggunakan DNS sebagai metode *name resolution*. Berbeda dengan WINS, administrator harus memasukkan *record* ke dalam DNS secara manual, namun

saat peluncuran Windows Server 2000 DNS dapat beroperasi secara dinamis yang dapat disebut sebagai DDNS.

Dynamic Domain Name System (DDNS) memperbolehkan pengguna DNS untuk memperbarui informasi yang terdapat pada basis data DNS. DHCP Server dapat memberikan informasi kepada DDNS Server secara otomatis alamat IP yang diberikan kepada sebuah perangkat.