BAB V

PENUTUP

2.1 Kesimpulan

Berdasarkan rumusan masalah yang telah disampaikan pada bab-bab sebelumnya, telah diselesaikan permasalahan tersebut dengan beberapa kesimpulan hasil dari percobaan yang dilakukan.

Kesimpulan yang dapat diambil diantaranya:

1. Untuk menghubungkan LAN CV. Karta Widjaya Group dengan Dokter Komputer yang jaraknya berjauhan dapat dilakukan dengan membangun jaringan *Virtual Private Network*. Jaringan VPN yang tepat adalah *site-to-site* menggunakan protokol L2TP. Pembangunan jaringan ini tidak rumit dan bersifat permanen karena masing-masing kantor menggunakan *router* sebagai *gateway* VPN yang selalu terhubung selama 24 jam. *Operating Sistem router* menggunakan MikroTik Router OS yang cukup mudah dalam konfigurasinya.
2. Merancang jaringan *site-to-site* VPN membutuhkan perangkat utama yaitu dua buah *router* MikroTik yang berfungsi sebagai *gateway* VPN L2TP dan koneksi internet pada dua buah *router* tersebut. Sedangkan jaringan lokal masing-masing kantor hanya tinggal dihubungkan dengan *router* tersebut.
3. Sudah jelas komunikasi melalui internet rawan akan pencurian data sedangkan komunikasi secara *private* lebih aman, kalaupun terjadi

pencurian data sangat mudah untuk melacaknya karena untuk mengakses data harus terhubung ke jaringan lokal. Disamping membuat keamanan dengan cara membuat *private* suatu jaringan publik juga dapat diberikan keamanan ganda yaitu dengan teknologi IPsec. Dengan teknologi VPN L2TP dan IPsec menjadikan keamanan ganda yaitu otentikasi l2tp *tunnel* dan otentikasi IPsec *tunnel*, jika salah satu tidak terpenuhi maka tidak akan terbentuk *tunnel*.

4. Para *hacker* menggunakan *software* Wireshark untuk memperoleh informasi pertukaran data. Karena menggunakan VPN maka untuk memonitor pertukaran data harus dilakukan di dalam jaringan VPN tersebut, sedangkan untuk masuk ke dalam jaringan VPN harus melalui beberapa tahapan otentikasi. Pada percobaan yang dilakukan walaupun telah masuk ke dalam jaringan VPN tetapi *monitoring* menggunakan Wireshark tetap sulit dilakukan kecuali harus menguasai *gateway* atau komputer tujuan langsung. Kesimpulannya jaringan VPN tidak bisa dengan mudah dibajak orang dari luar jaringan.

Secara umun *Virtual Private Network* memberikan keamanan pertukaran data melalui jaringan internet layaknya jaringan lokal.

2.2 Saran

Untuk penelitian dengan tema yang sama berikutnya diharapkan lebih meneliti bagian keamanan data yang digunakan seperti penggunaan kemanan SSL yang

memungkikan enkripsi data yang melalui protokol HTTP+SSL (HTTPS) serta dapat mengimplementasikan IPv6 yang saat ini belum dapat digunakan.