BAB 5

PENUTUP

5.1 Kesimpulan

Setelah melakukan analisis terhadap topologi jaringan serta kemampuan *Router Gateway* YouVee Computer dan *Router Gateway* DragoNet, maka dapat dilakukan pembentukan *Site-to-Site VPN Tunnel* dan *VPN Network* antara *network* YouVee Computer dengan *network* Dragonet.

Implementasi *Site-to-Site VPN Tunnel* pertama – tama dilakukan dengan mengkonfigurasi *PPTP Server* pada *Router Gateway* YouVee Computer dan mengkonfigurasi *PPTP Client* pada *Router Gateway* DragoNet. Setelah konfigurasi berhasil dilakukan, maka *PPTP Tunnel* diantara kedua *Router Gateway* telah terbentuk sehingga *Site-to-Site VPN Tunnel* berhasil diimplementasikan. Selanjutnya untuk membuat *VPN Network* agar *network VPN* pada *VPN Gateway* YouVee Computer dapat berada dalam satu jaringan lokal dengan *network VPN* di *VPN Gateway* DragoNet, dilakukan konfigurasi *interface EOIP* pada kedua sisi *VPN Gateway*. Setelah konfigurasi dilakukan, maka *EOIP Tunnel* diantara kedua *VPN Gateway* telah terbentuk. *EOIP Tunnel* ini akan berjalan diatas *PPTP Tunnel* yang telah terbentuk sebelumnya. Langkah terakhir adalah mengkonfigurasi *bridging* antara salah satu *interface ethernet* dengan *interface EOIP* pada *VPN Gateway* YouVee Computer serta *VPN Gateway*

DragoNet. *VPN Host* pada kedua kedua sisi *VPN Gateway* harus dihubungkan dengan *interface ethernet* yang telah di-*bridge* tersebut agar dapat berada dalam satu jaringan lokal. *VPN Network* antara *network* YouVee Computer dengan *network* DragoNet telah berhasil diimplementasikan.

Packet Sniffing dengan menggunakan aplikasi **Wireshark** kemudian dilakukan untuk meng-*capture* transmisi data yang terjadi selama proses pembentukan *VPN Tunnel* diantara kedua *Router Gateway* kemudian dilakukan *sniffing* juga terhadap pembentukan *VPN Network* serta transmisi data yang dilakukan oleh *VPN Host* YouVee Computer dengan *VPN Host* DragoNet.

Hasil *sniffing* tersebut kemudian dianalisis dan dapat disimpulkan bahwa *PPTP Tunnel* menggunakan *PPTP Control Connection* yang berjalan diatas protokol *TCP* untuk memulai, menjaga serta mengakhiri koneksinya. Selain itu juga terdapat *PPTP* Data *Tunnel*ing yang memanfaatkan protokol *GRE* sebagai protokol enkapsulasi. *PPTP* Data *Tunnel*ing digunakan untuk transmisi data. Pada proses pembentukan *PPTP Tunnel*, metode autentikasi antara *PPTP* Server dengan *PPTP* Client menggunakan protokol *PPP CHAP*. Hal ini akan membuat autentikasi berjalan aman karena User name serta Password *PPTP* pada kedua sisi *Router Gateway* tidak akan dikirimkan ke jaringan. Kemudian dari trafik data *EOIP Tunnel*, dapat disimpulkan bahwa *EOIP Tunnel* berjalan diatas *PPTP Tunnel* dan juga menggunakan protokol GRE untuk mengenkapsulasi. Hanya saja karena protokol *EOIP* masih berupa draft *RFC*, maka dokumentasi dan referensi untuk field –field dari protokol ini masih sangat terbatas. Analisis pada transmisi data antara *VPN Host* YouVee Computer dengan *VPN Host* DragoNet dapat

ditarik kesimpulan bahwa transmisi data berlangsung dengan aman karena data yang disembunyikan selain di-*enkapsulasi* dengan protokol *PPTP* juga masih akan di-*enkapsulasi* lagi dengan *GRE* oleh protokol *EOIP*. Hanya saja akan terdapat banyak fragmentasi karena tingginya protokol *overhead*.

5.2 Saran

Dari hasil analisis di lapangan, maka di sisi *network* YouVee Computer perlu disediakan *bandwidth* yang lebih lebar untuk mengatasi protokol *overhead* jika akan dilakukan implementasi serta penelitian lebih lanjut tentang *VPN*. Masih banyak lagi metode *VPN* yang dapat diimplementasikan seperti *L2TP*, *L2F* dan *IPSec*. Penelitian yang lebih mendalam dapat dilakukan untuk membandingkan segi keamanan protokol *PPTP* dan *EOIP* dengan protokol *VPN* yang lain. Kemudian dapat juga dilakukan penelitian untuk mengetahui protokol *VPN* yang protokol *overhead*-nya paling rendah di dalam melakukan transmisi data.