

ABSTRAK

Dengan adanya internet sebuah perusahaan akan lebih mudah dalam menyelesaikan pekerjaan dan mengakses data penting melalui internet, oleh karena itu perlunya sebuah sistem keamanan jaringan. Maka dari itu dilakukannya sebuah percobaan menggunakan sistem keamanan jaringan berbasis *Virtual Private Network* (VPN) pada Mikrotik. Jenis VPN yang digunakan adalah *OpenVPN*, dimana aplikasi tersebut bekerja membuat koneksi *point-to-point tunnel* yang telah ter-*enkripsi*. *OpenVPN* menggunakan *private keys*, *certificate*, atau *username* dan *password* untuk melakukan autentifikasi dalam membangun sebuah koneksi. VPN yang digunakan peneliti yakni VPN dengan metode (*Source Soucket Tunneling Protocol*) SSTP. Penelitian ini dilakukan untuk mengetahui bagaimana rancangan sistem keamanan jaringan menggunakan SSTP serta mengetahui apakah sistem dengan metode SSTP mampu melakukan *enkripsi* data dengan baik. Untuk membuktikan tingkat keamanan tersebut penulis menggunakan aplikasi *Wireshark* Serta mencoba melakukan serangan menggunakan *Attacking Denial of Services* (*DoS*). Dari hasil penelitian yang diperoleh dapat disimpulkan bahwa dengan menggunakan HTTPS maka akan meminimalisir adanya pencurian data dari pihak lain karena didalam sertifikat sudah memiliki tanda pengenal tersendiri seperti organisasi, wilayah, dan lain sebagainya.

Kata Kunci: *Virtual Private Network* (VPN), *Source Soucket Tunneling Protocol* (SSTP), *Wireshark*, *Attacking Denial of Services* (*DoS*).