

ABSTRAK

Sebagai seorang ahli keamanan dalam suatu ISP tentunya memiliki tugas untuk monitoring keamanan jaringan dan perangkat seperti switch dan router yang berjumlah tidak sedikit serta mengamankan trafik informasi yang ada di ISP. Untuk melakukan monitoring keamanan jaringan yang begitu besar tentunya tidak dapat dilakukan oleh seorang administrator saja sehingga diperlukan pengaturan *privileges* (hak akses) tertentu kepada *co-admin* di setiap router dan switch. Pemberian *privileges* tersebut kurang efisien apabila di terapkan dalam jaringan yang sangat besar. Sehingga dibutuhkan pengaturan *privileges* secara terpusat untuk memudahkan kinerja administrator dalam monitoring kondisi jaringan dan keamanan informasinya.

TACACS+ dan RADIUS menjadi solusi untuk manangani masalah akses keamanan jaringan yang sedang terjadi saat ini. Dalam tugas akhir kali ini akan menganalisa kelebihan dan kekurangan kedua protokol tersebut baik dari segi kompatibilitas layanan dan keamanan layanan data yang bersifat penting dengan cara melakukan simulasi di GNS 3 dan menambahkn layanan IPSec pada setiap router untuk melindungi trafik informasi yang ada di setiap router

Pada Tugas akhir kali ini dihasilkan bahwa delay yang dibutuhkan untuk melakukan proses otentikasi dengan AAA \pm 1 detik lebih lama jika dibandingkan otentikasi tanpa menggunakan AAA dan penambahan IPSec tidak terlalu membebani jaringan karena hanya memerlukan \pm 1% dari kapasitas yang disediakan.

Kata kunci : Teknologi berkembang, kompleksitas layanan, TACACS+, RADIUS, IPSec