BAB I
PENDAHULUAN

1.1 Latar Belakang

Jaringan publik (*public network/ internet*) merupakan jaringan yang dapat dilalui oleh siapapun pengguna jasa layanan tersebut. Oleh karena itu, setiap pengguna dapat memanfaatkan kesempatan tersebut untuk melakukan gangguan terhadap privasi komunikasi yang dilakukan oleh pengguna lain, seperti pencurian *username* dan *password* saat autentikasi *client* ke *server*. Sehingga pada dasarnya jaringan publik yang digunakan rentan terhadap serangan keamanan. VPN dapat menjadi solusi dalam permasalahan tersebut.

Virtual Private Network (VPN) merupakan salah satu teknologi pengamanan data yang mampu membentuk jaringan komunikasi secara *private* didalam jaringan publik sehingga mampu menjaga kerahasian paket data/ informasi penting dalam koneksi *client* dan *server*. Teknologi ini memadukan konsep *tunneling* dan enkripsi sehingga VPN menjadi teknologi yang handal untuk mengatasi permasalahan keamanan didalam jaringan.

Dalam implementasinya, telah banyak beredar *tool* VPN yang dapat dengan mudah diperoleh yang berbayar maupun gratis. OpenVPN merupakan salah satu *opensource* gratis untuk teknologi VPN yang dapat bekerja dibanyak *platform*, seperti Windows, Linux freeBSD, Mac OS, dan Solaris. OpenVPN menggunakan protokol enkripsi SSL dengan menerapkan sertifikat digital dalam koneksi *client* dan *server.*

Secure Socket Layer (SSL) adalah protokol keamanan yang diterapkan pada openVPN dengan menerapkan 3 jenis keamanan, yaitu CA (*Certificate Authority*), *private key*, dan kunci DH (Diffie-Hellman). Pada proses pembuatan CA akan diminta konfirmasi terhadap informasi yang akan menjadi autentikasi antar *client* dan *server* yang nantinya secara default informasi tersebut akan masuk dalam *key* yang digunakan.

Pada tugas akhir ini penulis ingin menganalisis kemanan data yang dibentuk oleh jaringan VPN menggunakan *opensource* openVPN pada sistem operasi

Linux Ubuntu terhadap ancaman keamanan berupa *sniffing* dan *disclosure attack*. Untuk mendapatkan kejelasan yang lebih rinci mengenai performansi yang dihasilkan VPN-SSL, maka penulis juga akan melakukan perbandingan kualitas yang dihasilkan dengan melakukan perancangan IPv4 murni dan VPN-GRE serta akan menganalisis performansi unjuk kerja, yaitu *throughput*, *delay*, *jitter*, dan *packet loss*.

1.2 Perumusan Masalah

Permasalahan yang dijadikan objek penelitian dalam tugas akhir ini adalah sebagai berikut :

1. Melakukan perancangan dan realisasi sistem pada jaringan IPv4 murni, VPN-SSL dan VPN-GRE.
2. Menganalisis hasil monitoring data yang dilakukan menggunakan wireshark pada setiap perancangan yang dibangun.
3. Membangun koneksi PC *server* dan PC *client* dengan aplikasi FTP.
4. Membandingkan performansi jaringan yang telah direalisasikan pada layanan *video streaming* menggunakan VLC *media player* dengan parameter unjuk kerja : *throughput*, *delay*, *jitter* dan *packet loss*.

1.3 Batasan Masalah

Untuk menghindari meluasnya pembahasan materi tugas akhir ini, maka penulis membatasi permasalahan hanya mencakup hal-hal berikut :

1. Jenis implementasi yang digunakan adalah VPN-SSL dan VPN-GRE sehingga tidak membahas metode enkripsi lainnya.
2. Tidak menganalisis algoritma yang digunakan dalam autentikasi dan enkripsi pada VPN yang digunakan.
3. Ancaman keamanan yang digunakan adalah *sniffing* dan *disclosure attack*.
4. Perangkat lunak yang digunakan untuk membangun VPN-SSL adalah openVPN Linux Ubuntu.
5. Perangkat lunak yang digunakan untuk membangun VPN-GRE adalah pptpd Linux Ubuntu.

6. Menggunakan software wireshark, , Filezilla FTP Client, dan Xlight FTP Server.
7. Menggunakan HTB-*tools* sebagai manajemen bandwidth dalam jaringan.
8. Perancangan dan realisasi sistem menggunakan 1 buah hub, 2 buah laptop dan 1 buah PC *desktop* yang diinstal aplikasi *opensource* Oracle VM VirtualBox sebagai mesin *virtual* dengan 4 buah sistem operasi.

1.4 Tujuan Penelitian

Tujuan penelitian dalam tugas akhir ini adalah, sebagai berikut :

1. Melakukan perancangan dan realisasi pada sistem jaringan IPv4 murni, VPN-SSL dan VPN-GRE.
2. Menganalisis monitoring data/ *sniffing* dan *disclosure attack* dalam jaringan pada setiap topologi jaringan yang dibuat.
3. Membandingkan performasi jaringan pada layanan *video streaming* dengan parameter QoS, yaitu *throughput*, *delay*, *jitter*, dan *packet loss*.

1.5 Metode Penelitian

Metode yang akan digunakan dalam tugas akhir ini adalah :

1. Studi Literatur

   Merupakan suatu metode yang mempelajari dasar teori tentang segala literatur mengenai konsep keamanan jaringan dan implementasinya.
2. Tahapan perancangan dan realisasi sistem

   Melakukan perancangan dan pemodelan pada sistem yang akan diuji.
3. Tahap pengujian dan analisis data

   Mengumpulkan dan menganalisis data-data dari parameter yang telah ditentukan dari hasil pengujian pada implementasi jaringan.
4. Tahap penarikan kesimpulan

   Menarik suatu kesimpulan berdasarkan hasil analisis data yang diperoleh dalam pengujian sistem.

1.6 Sistematika Penulisan

BAB I Pendahuluan

Pada bab ini akan dibahas tentang latar belakang, perumusan masalah, batasan masalah, tujuan penelitian, metode penelitian dan sistematika penulisan.

BAB II Dasar Teori

Pada bab ini dijelaskan dasar teori sebagai penunjang realisasi sitem yang dibuat, meliputi *Internet Protocol* (IP), konsep keamanan jaringan, *Virtual Private Network* (VPN), *File Transfer Protocol* (FTP) dan parameter-parameter QoS.

BAB III Perancangan dan Realisasi Sistem

Bab ini berisi konsep perancangan dan implementasi sistem jaringan IPv4 murni, VPN-SSL dan VPN-GRE pada komunikasi FTP dan layanan *video streaming* menggunakan VLC *media player*.

BAB IV Analisis Kinerja Sistem

Menjelaskan serta menganalisis sistem keamanan pada komunikasi FTP yang terbentuk oleh VPN-SSL dan performansi jaringan dengan parameter QoS serta membandingkannya dengan topologi IPv4 murni dan VPN-GRE.

BAB V Kesimpulan dan Saran

Pada bab ini berisi kesimpulan dari hasil analisis dan saran yang berkaitan dengan tugas akhir yang dapat digunakan untuk pengembangan penelitian selanjutnya.