BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi *internet* memberikan kemudahan akses untuk mendapatkan informasi kepada para penggunanya. Akan tetapi akses informasi dengan menggunakan jaringan *internet*/publik ternyata mempunyai kelemahan dari segi keamanannya. Berbagai aktivitas *security-threat* dapat dilakukan untuk mengancam jaringan publik misalnya dengan *sniffing, spoofing, session hijacking* dll.

Ini menunjukkan bahwa jaringan publik yang digunakan sangat rentan terhadap ancaman keamanan seperti pencurian data, dan memberikan kerugian yang besar apabila data yang dicuri adalah data penting transaksi bisnis suatu perusahaan. Oleh karena itu, dibutuhkan jaringan yang tidak dapat diakses oleh publik dan aman dari pencurian data.

Untuk mengatasi permasalahan di atas, digunakanlah teknologi VPN. VPN tidak memerlukan biaya infrastruktur yang besar karena dibangun secara virtual dengan memanfaatkan jaringan publik sebagai media transmisi. VPN menyediakan jaringan *private* dan memberikan fasilitas keamanan terhadap aktifitas pencurian data yang semakin meningkat.

Dikenal tiga jenis VPN dalam implementasinya, yaitu *Trusted, Secure,* dan *Hybrid* VPN [18]. *Secure* VPN adalah perpaduan teknologi *tunneling* dan *encryption*. *Tunneling* adalah teknik mengenkapsulasi seluruh paket data dari format protokol yang lain. Untuk mendapatkan koneksi yang aman, data yang telah dibungkus dengan protokol *tunneling* harus dienkripsi terlebih dahulu untuk menjaga kerahasiaannya sehingga paket yang tertangkap ketika melewati jaringan publik tidak terbaca karena harus melewati proses dekripsi.

Dalam implementasi *secure* VPN, protokol GRE dan IPSec merupakan protokol yang sering digunakan. Oleh karena itu, penulis ingin menganalisis tingkat keamanan dari kedua implementasi VPN ini terhadap ancaman keamanan berupa *sniffing, disclosure attack* dan *SYN attack*.

1.2 Rumusan Masalah

Yang menjadi permasalahan dalam penelitian ini antara lain:

a. Bagaimana cara implementasi jaringan VPN berbasis IPSec dan GRE?
b. Bagaimana tingkat keamanan berupa *data confidentiality* ,*authentication* dan *availability* pada VPN berbasis IPSec maupun GRE?
c. Bagaimana pengaruh penggunaan teknologi kriptografi terhadap performansi jaringan VPN?

1.3 Tujuan

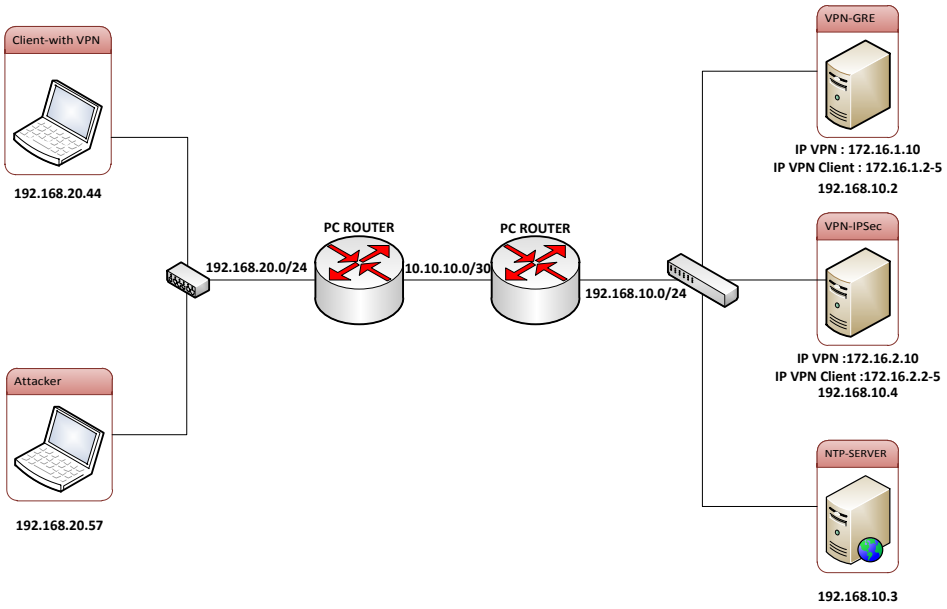
Adapun yang menjadi tujuan dalam penelitian ini antara lain:

a. Mengimplementasikan jaringan VPN berbasis IPSec dan VPN berbasis GRE.
b. Menganalisis tingkat keamanan berupa *data confidentiality* , *authentication* dan *availability* dengan melakukan *sniffing* ,*disclosure attack* dan *SYN attack* pada implementasi VPN berbasis IPSec maupun GRE.
c. Menganalisis pengaruh penggunaan teknologi kriptografi berupa enkripsi dan otentikasi terhadap performansi jaringan VPN.

1.4 Batasan Masalah

Dalam penelitian ini, terdapat beberapa batasan masalah antara lain:

a. Arsitektur jaringan fisik yang akan digunakan adalah sebagai berikut :



Gambar 1.1 Topologi Jaringan

b. VPN (*Virtual Private Network*) diimplementasikan pada *internet protocol version* 4 (IPv4).
c. *Software* yang digunakan untuk implementasi VPN berbasis IPSec adalah *IPSec Tools*.
d. *Software* yang digunakan untuk implementasi VPN berbasis GRE adalah *pptpd*.
e. Untuk implementasi IPSec menggunakan algoritma MD5 untuk otentikasi dan 3DES untuk enkripsi data. Di samping itu, IPSec yang diimplementasikan adalah IPSec *transport mode* dengan menggunakan ESP *security protocol*.
f. Untuk implementasi GRE menggunakan algoritma MSCHAPv2 untuk otentikasi dan MPPE 128 *bit* untuk enkripsi data.
g. Ancaman keamanan yang digunakan adalah *sniffing* , *disclosure attack* dan *SYN attack*.
h. *Sniffing attack* dengan wireshark, beberapa *disclosure attack tools* berupa Asleap, Ikescan, Ikeprobe dan *SYN attack* dengan *software* HPING.
i. *Security dimensions* yang dianalisis adalah *data confidentiality*, *authentication* dan *availability.*
j. Tidak menganalisis secara mendalam cara kerja teknologi kriptografi berupa algoritma enkripsi dan algoritma otentikasi yang digunakan pada masing-masing implementasi VPN.
k. Menganalisis pengaruh dari penggunaan algoritma enkripsi dan algoritma otentikasi terhadap performansi jaringan berupa *delay network* dan *throughput.*

1.5 Metodologi Penelitian

Metode yang akan digunakan dalam tugas akhir ini adalah sebagai berikut:

a. Tahap studi literatur

   Melakukan studi literatur mengenai konsep VPN, *tunneling protocol*, *data encryption*, ancaman keamanan jaringan dan implementasinya.

b. Tahap perancangan dan implementasi sistem

   Melakukan perancangan dan pemodelan pada sistem yang akan diuji.

c. Tahap pengujian dan analisis data

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

d. 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, tujuan, batasan masalah, metodologi penelitian dan sistematika penulisan

Bab II Dasar Teori

Bab ini merupakan tinjauan pustaka dari konsep VPN, *tunneling protocol IPSec & GRE*, *data encryption* dan cara mengimplementasikannya.

Bab III Perancangan dan Implementasi

Membahas tentang metode dan model yang digunakan dalam perencanaan, faktor-faktor yang mendukung dan mempengaruhi sekaligus implementasi sistem.

Bab IV Pengujian dan Analisis Hasil Pengujian

Berisi pengujian dan analisis terhadap hasil yang diperoleh dari tahap pengujian sistem.

Bab V Kesimpulan dan Saran

Bab ini berisi simpulan dari implementasi yang dilakukan serta saran untuk pengembangan di masa mendatang.