BAB I PENDAHULUAN

A. Latar Belakang

Perkembangan dunia internet sangat pesat seiring dengan perkembangan zaman peningkatan kebutuhan layanan yang cepat dan efisien.Jaringan internet saat ini merupakan suatu layanan yang sangat dibutuhkan. Jaringan internet mempunyai manfaat yang lebih dibandingkan dengan komputer yang berdiri sendiri. Sehingga kelompok kerja dapat berkomunikasi lebih efektif dan efisien. Kebutuhan akan perluasan jaringan pada perusahaan sekarang ini semakin tinggi. Perluasan dapat berupa pembukaan *remote access system* ataupun *remote client* yang dapat mengakses jaringan korporat, yang menuntut efisiensi dan keamanan pada jaringan yang lebih tinggi. Berbagai solusi ditawarkan untuk membentuk keamanan jaringan yang handal, diantaranya adalah membentuk sebuah jaringan privat dengan *leased line* (saluran sewa).

Pada saat jaringan privat mempunyai skala jaringan yang kecil atau menengah, investasi yang ditanam tidaklah terlalu menjadi masalah. Tetapi pada saat skala jaringan menjadi besar, hal ini akan menjadi masalah. Karena menyangkut pengembangan investasi yang semakin tinggi, dan ketersediaan akses akan menjadi masalah yang krusial.

Solusi yang lebih efisien adalah pembentukan jaringan privat melalui jaringan publik yang sering dikenal dengan VPN (Virtual Private Network). Bentuk jaringan seperti ini membutuhkan sebuah sistem keamanan yang baik sehingga jaringan privat tersebut tidak dapat diakses oleh pengguna yang tidak berwenang.

RouterOS adalah salah satu sistem operasi yang dapat digunakan sebagai router jaringan yang handal, mencakup berbagai fitur lengkap untuk jaringan. Selain itu MikroTik dapat juga berfungsi sebagai firewallbagi komputer lain dan memberikan prioritas bagi komputer lain agar bias mengakses data Internet maupun data lokal. MikroTik bertujuan untuk mengatur bandwith serta melakukan manajemen jaringan komputer.

Routerboard bertujuan untuk mengatur dan melakukan manajemen jaringan internet. Selain berfungsi sebagai *firewall* Routerboard yang dihasilkan dapat memenuhi kebutuhan sistem khususnya dalam melakukan pemfilteran aplikasi, virus sesuai dengan kebutuhan pengguna, sehingga aplikasi dan tersebut tidak dapat diakses dan virus tidak bisa masuk ke dalam jaringan kita sesuai dengan ketentuan yang di rancang.

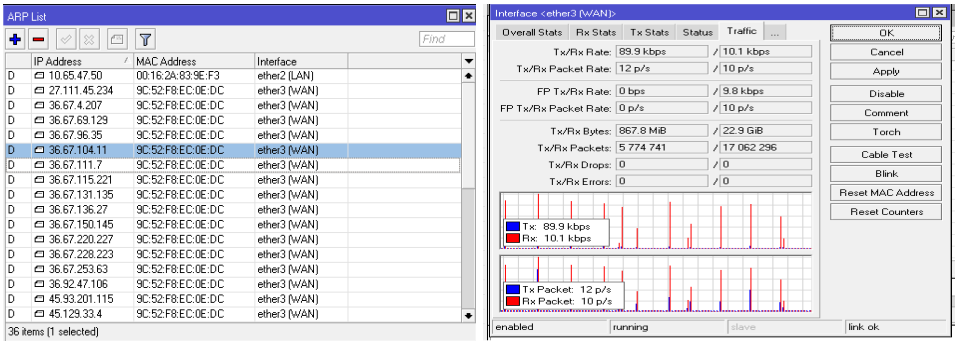
Penerapan VPN Server (*Virtual Private Network*) adalah Dengan VPN Server ini kita seolah-olah membuat jaringan didalam jaringan atau biasa disebut *tunnel* (terowongan) di dalam Routerboard. *Tunneling* adalah suatu cara membuat jalur privat dengan menggunakan infrastruktur pihak ketiga. VPN Server menggunakan salah satu dari tiga teknologi *tunneling* yang ada yaitu: *PPTP,L2TP* dan standar terbaru, *Internet Protocol Security* (biasa disingkat menjadi IPSec). VPN Server merupakan perpaduan antara teknologi *tunneling* dan enkripsi.

Algoritma RSA adalah sebuah algoritma yang memiliki kunci yang cukup panjang. Kunci RSA pada umumnya sepanjang 1024—2048 bit. Beberapa pakar meyakini bahwa kunci 1024-bit ada kemungkinan dipecahkan pada waktu dekat (hal ini masih dalam perdebatan), tetapi tidak ada seorangpun yang berpendapat kunci 2048-bit akan pecah pada masa depan yang terprediksi. Jika (sepanjang 256-bit atau lebih pendek, maka kunci RSA akan dapat ditemukan dalam beberapa jam hanya dengan menggunakan PC, dengan menggunakan perangkat lunak yang tersedia. Jika (sepanjang 512-bit atau lebih pendek, (akan dapat difaktorisasi dalam hitungan ratusan jam seperti pada tahun 1999 dengan menggunakan ratusan komputer. Secara teori, perangkat keras bernama TWIRL dan penjelasan dari Shamir dan Tromer pada tahun 2003 mengundang berbagai pertanyaan akan keamanan dari kunci 1024-bit. Saat ini disarankan bahwa setidaknya sepanjang2048-bit.

Dengan demikian penerapan perluasan jaringan IPSec dengan menggunakan RSA menjadi salah satu solusi perluasan jaringan dengan mengutamakan keamanan jaringan menggunakan system enkripsi dari algoritma RSA.

B. Permasalahan

PT.Indomarco Primatama merupakan salah satu perusahaan yang bergerak dibidang retail , dengan banyaknya jumlah cabang dan toko yang menyebar maka diperlukan suatu komunikasi data yang bersifat nirkabel, pribadi dan virtual (VPN). Pada instalasi jaringan ini terdapat dua perangkat utama yaitu Modem ISP dan Router, yang tentunya sangat rentan terhadap serangan para peretas jaringan. Salah satunya yang sering terjadi yaitu serangan DDoS . Jenis serangan DDoS berupa memadatkan lalu lintas pada jaringan yang saling terhubung. Serangan ini seringkali terjadi pada jaringan privat yang menghubungkan antara cabang perusahaan dengan dengan toko dan menyebabkan gangguan jaringan keseluruhan.
Pada gambar 1.1 dijelaskan traffic lalu lintas data antar cabang dan toko yang terkena serangan DDoS



Gambar 1. 1 Serangan Attack Hacker DDoS

Dengan demikian jaringan privat harus bersih dari segala serangan jaringan seperti DDoS, karena dapat menghambat transaksi data pada suatu jaringan privat, jika diamati keamanan jaringan menjadi hal yang sangat prioritas dalam perluasan jaringan, maka dapat diidentifikasi masalah, yaitu:

1. **Identifikasi Masalah**

   Berdasarkan permasalahan diatas maka dapat diidentifikasikan sebagai berikut :

   a. Belum tepatnya management keamanan jaringan.

      Masalah IP public pada router jaringan memiliki resiko terutama masalah keamanan.

   b. Belum optimalnya perangkat sistem jaringan untuk perluasan jaringan.

      Belum optimalnya perangkat sistem jaringan, karena semakin banyak investasi yang ditanamkan.

2. **Pernyataan Penelitian (*Problem Statement*)**

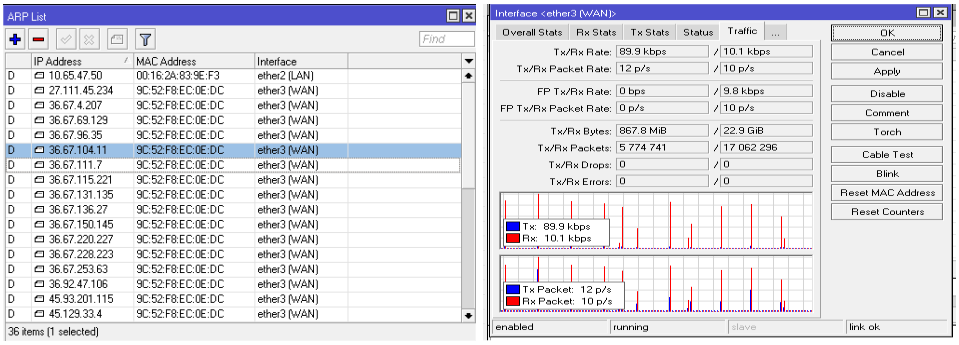
   Berdasarkan identifikasi masalah maka dapat disimpulkan pokok masalah yaitu belum dapat diperoleh tingkat ketepatan dan keoptimalan perangkat sistem untuk perluasan jaringan.

3. **Pertanyaan Penelitian (*Research Question*)**

   Pertanyaan penelitian yang dapat diajukan adalah sebagai berikut :

   a. Bagaimana Penerapan Algoritma Rivest Shamir Adleman Pada IPSec (*Internet Protocol Security*) untuk Router dalam Perluasan Jaringan?

   b. Bagaimana cara mengoptimalkan untuk Router dalam Perluasan dan Keamanan Jaringan agar lebih efisien?



Gambar 1. 2 Serangan Attack Hacker DDoS

C. Maksud dan Tujuan

Maksud dari penelitian ini adalah menerapkan Algoritma Riverst Shamir Adleman Pada IPSec (*Internet Protocol Security*) untuk Router dalam Perluasan Jaringan untuk perluasan jaringan privasi atau private network.

Tujuan dari penelitian ini adalah :

a. Memperoleh pengaturan manajemen jaringan untuk pengamanan jaringan secara lebih tepat
b. Mengamankan jaringan dari gangguan tanpa menghalangi penggunaannya.
c. Mengembangkan perluasan jaringan yang terhindar dari *attack hacker.*
d. Memaksimalkan keamanan jaringan dengan menggunakan algoritma RSA.
e. Melindungi keamanan informasi-informasi dan sistem informasi terhadap akses, penggunaan, pengungkapan, gangguan, modifikasi atau penghancuran.

D. Spesifikasi Produk yang Diharapkan

Melalui penelitian ini dilakukan untuk merancang perluasan jaringan privasi menggunakan IPSec (*Internet Protocol Security).*

Dengan adanya sistem jaringan ini ada beberapa manfaat diantaranya :

1. Kemampuan membentuk jaringan LAN yang tidak di batasi tempat dan waktu, karena koneksitasnya dilakukan via internet.
2. Remote Access, dengan VPN kita dapat mengakses komputer atau jaringan kantor, dari mana saja selama terhubung ke internet.
3. Menghemat biaya setup jaringan, karena transmisi data teknologi VPN menggunakan media jaringan public yang sudah ada tanpa perlu membangun jaringan pribadi.
4. Jangkauan jaringan lokal yang dimiliki suatu perusahaan akan menjadi luas, sehingga perusahaan dapat mengembangkan bisnisnya di daerah lain.
5. Penggunaan VPN akan meningkatkan skalabilitas.

E. Pentingnya Pengembangan

Pentingnya pengembangan ini dilakukan dalam rangka mengembangkan peluasan jaringan privat atau *Network Private, s*ehingga kebutuhan akan perluasan jaringan data/multimedia pada perusahaan sekarang ini semakin tinggi. Perluasan dapat berupa pembukaan *remote access system* ataupun *remote client* yang dapat mengakses jaringan korporat, yang menuntut efisiensi dan keamanan pada jaringan yang lebih tinggi. Manfaat dari penelitian ini yaitu;

1. Manfaat teoritis dalam penelitian ini yaitu memberikan sumbangan ilmu pengetahuan mengenai Penerapan Algoritma Riverst Shamir Adleman Pada IPSec (*Internet Protocol Security*) untuk Router dalam Perluasan Jaringan.
2. Manfaat praktis dari penelitian ini yaitu membantu perushaan dalam berinvestasi memperluas jaringan privat atau *Network private*
3. Manfaat kebijakan penelitian ini yaitu dapat menjadi acuan perusahaan dalam pengembangan dan perluasan jaringan privat atau *Network private*

F. Asumsi dan Keterbatasan Pengembangan

Asumsi dari pengembangan ini adalah sebagai berikut:

1. Dengan adanya penelitian ini akan memudahkan dalam memanajemen jaringan
2. Sistem jaringan yang dibuat akan memudahkan perusahan membangun jaringan privasi yang lebih luas

Keterbatasan dari pengembangan ini adalah sebagai berikut:

1. Jaringan hanya digunakan pada router ke router
2. Keamanan jaringan hanya mengimplementasikan algoritma RSA.

G. Definisi Istilah atau Definisi Operasional

1. Intranet = Sebuah jaringan private atau *Private Network* yang menggunakan protocol-protokol Internet (TCP/IP), untuk membagi informasi rahasia perusahan atau operasi dalam perusahaan tersebut kepada karyawan
2. VPN = *Virtual Private Network* atau jaringan privasi
3. L2TP = Layer 2 Tunneling Protokol tunneling yang memadukan dua buah *protocol tunneling*
4. Remote Access = Sistem yang bisa digunakan dalam pengendalian suatu manajemen jaringan, dimana administrator dapat dengan mudah mengontrol dan mengawasi komputer client, berinteraksi dengan user, backup data, atau aktifitas lainnya
5. Router = Sebuah alat yang mengirimkan paket data melalui sebuah

jaringan atau Internet menuju tujuannya, melalui sebuah proses yang dikenal sebagai routing.

6. LAN = Jaringan komputer lokal menghubungkan peralatan yang terbatas pada area geografi yang kecil.
7. IpSec = Singkatan dari *IP Security* adalah sebuah protokol yang digunakan untuk mengamankan tranmisi *datagram* dalam sebuah *internetwork* berbasis TCP/IP.
8. *Datagram* = Salah satu protokol lapisan transpor TCP/IP yang mendukung komunikasi yang tidak andal (unreliable), tanpa koneksi (connectionless) antara host-host dalam jaringan yang menggunakan TCP/IP.
9. DDoS = Distributed Denial of Service atau dalam bahasa Indonesia dapat diartikan sebagai Penolakan Layanan secara Terdistribusi.