ISSN : 2337-6341

PEMANFAATAN PROTOKOL PPPT DAN L2TP DALAM MEMBANGUN VIRTUAL PRIVATE NETWORK (VPN) PADA MIKROTIK OS

Sartana Sinurat
(Dosen AMIK MBP Medan)
Janner Simarmata
(Dosen Universitas Negeri Medan)

ABSTRAK

Setiap orang membutuhkan informasi dalam waktu yang cepat, singkat dan akurat oleh karena itu dibutuhkan suatu sarana yang dapat mendukung hal tersebut. Salah satunya adalah koneksi internet yang cepat dan stabil.

Semakin lama teknologi semakin berkembang, kebutuhan akan suatu informasi meningkat pula. maka dibutuhkan suatu cara agar dapat memperoleh suatu informasi data, tukar menukar data, dilakukan dengan aman dan stabil. Oleh karena itu lah VPN diciptakan untuk menyelesaikan permasalahan dalam jaringan yang tidak aman.

Dengan adanya teknologi VPN ini kekhawatiran akan jaringan yang tidak aman dapat teratasi tanpa harus mengurangi atau melanggar aturan – aturan yang sudah ada.

Kata kunci : *Internet*, VPN, jaringan, Mikrotik os, PPT dan L2PT

1. PENDAHULUAN

1.1 Latar Belakang

Semakin berkembangnya teknologi informasi sekarang ini, maka kebutuhan akan informasi semakin meningkat pula. Dimana setiap orang membutuhkan informasi dalam waktu yang cepat, singkat dan akurat oleh karena itu dibutuhkan suatu sarana yang dapat mendukung hal tersebut. Salah satunya adalah koneksi *internet* yang cepat dan stabil.

Dari sudut pandang jaringan, salah satu masalah jaringan *internet* (*ip public*) adalah tidak mempunyai dukungan yang baik terhadap keamanan. Internet dahulu didesain oleh perguruan – perguruan tinggi sebagai sebuah jaringan terbuka dimana pengguna dapat mengakses, berbagi, dan menambah informasi semudah mungkin. Sebuah cara harus di temukan untuk mengamankan sebuah jaringan *public* tanpa harus melanggar sifat-sifat yang telah ada. Sesungguhnya sebuah jawaban yang ideal harus menyediakan tidak saja tingkat keamanan yang tinggi tetapi juga keamanan yang sedemikian rupa sehingga pengguna dapat dengan mudah mengakses, mengubah dan berbagi lebih banyak informasi, tidak lupa, dibawah kondisi – kondisi yang secara hati-hati dikendalikan dan di pelihara.

VPN muncul untuk mengatasi permasalahan tersebut. Secara umum, VPN (*virtual private network*) adalah sebuah proses dimana jaringan umum (*public network* atau *internet)* diamankan untuk memfungsikannya sebagaimana jarigan privat (*private network*). Sebuah VPN tidak didefinisikan oleh rangkaian khusus atau router, tetapi didefinisikan oleh mekanisme keamanan dan prosedur-prosedur yang hanya mengijinkan penggunanya yang ditunjuk akses ke VPN dan informasi yang mengalir melaluiya.

1.2 Rumusan Masalah

Terdapat beberapa perumusan masalah yang akan dibahas dalam Proyek Penelitian ini diantaranya adalah :

1. Bagaimana melakukan konfigurasi VPN pada mikrotik.
2. Bagaimana meningkatkan keamanan suatu jaringan menggunakan VPN.
3. Bagaimana membuat konfigurasi VPN menggunakan konsep tunneling.
4. Bagaimana cara mengimplementasikan VPN.

1.3 Batasan Masalah

Adapun batasan-batasan masalah dalam Proyek Penelitian ini adalah sebagai berikut.

1. Proyek Penelitian ini hanya terfokus pada implementasi VPN di mikrotik.
2. Implementasi yang dilakukan hanya pada jaringan public.
3. Implementasi di bangun dengan protokol PPTP dan L2TP, tidak membahas IPsec pada protocol L2TP.
4. Tidak membahas masalah performansi jaringan.
5. Tidak membahas tentang web yang berada di localhost.
6. Implementasi yang dilakukan tidak membahas mengenai interface website yang dibuat.
7. Implementasi yang dilakukan hanya menggunakan Sistem Operasi Windows Vista Home Premium dengan client Windows Xp Sp2 karena dalam proyek Penelitian ini tidak membahas mengenai keamanan server.
8. Adapun penggunaan tools yang digunakan dalam implementasi Proyek Penelitian ini yaitu, wireshark, winbox.
9. Implementasi dilakukan dengan 1(satu) server mikrotik.

1.4 Tujuan

Tujuan dari proyek Penelitian ini adalah:

1. Mengimplementasikan teknologi VPN di Mikrotik OS.
2. Mengimplementasikan proses tunneling.
3. Mengimplementasikan cara kerja VPN dari proses penginstallan, konfigurasi, sampai proses uji coba.

1.5 Metodologi Pengerjaan Proyek

1.5.1 Tahap Study Literature

Metodologi penelitian ini akan berisi tentang metodologi yang akan digunakan untuk mendukung dan menyelesaikan proyek Penelitian, yaitu Implementasi VPN di mikrotil. Dalam mengerjakan proyek Penelitian ini terdapat teknik dalam pengumpulan data antara lain adalah:

a. Pencarian referensi dan sumber-sumber yang berhubungan dengan *tunneling* VPN dan Pengimplementasiannya.
b. Pencarian referensi dan sumber-sumber yang berhubungan dengan mikrotik.
c. Mempelajari dan memahami proses konfigurasi *vpn* pada mikrotik.Problem atau masalah

1.5.2 Tahap Perancangan Sistem dan Implementasi

Pada tahap ini akan dirancang design sistem dan pembuatan VPN yang menggunakan mikrotik pada protocol *PPTP* sebagai hasil Penelitian dari pembuatan Proyek Penelitian. Design dari teknologi VPN ini meliputi perancangan terhadap sistem yang ada seperti, penentuan OS pada server dan client, serta aplikasi/*software* pendukung yang tepat. Setelah dilakukannya perancangan maka langkah selanjutnya akan dilakukan pengimplementasian pada jaringan yang telah di design

1.5.3 Tahap Analisa Dan Pengujian

Analisa sistem akan dilakukan dengan melakukan pengujian terhadap teknologi VPN yang telah dibuat, dengan tujuan untuk mengetahui akan adanya gangguan maupun *error* yang ada pada pembuatan teknologi VPN

2. LANDASAN TEORI DAN KONSEPTUAL

2.1 Mengenal PPTP (*Point to Point Tunneling Protocol*) lebih dekat.

Point to point tunneling protocol adalah protokol yng memiliki kemampuan untuk melakukan pengiriman data antara *remote client* dan *server* dengan membangun vpn berbasis IP (Gupta, 2003). PPtP di kembangkan oleh consurtium PPtP (Microsoft corporation, acsen *Communication*, 3COM, US *Robotics*, dan ECI *Telematics*). *PPtP* menawarkan *VPN – on demand* melalui *internetwork* yang tidak aman. PPtP tidak hanya meyediakan transmisi yang aman memalui internetwork berbasis tcp atau ip public, tetapi juga melalui internet pribadi.

2.2 L2TP (*Layer 2 Tunneling Protocol*)

L2TP adalah sebuah tunneling protokol yang memadukan dan mengombinasikan dua buah tunneling protokol yang bersifat proprietary, yaitu L2F *(layer 2 forwarding)* memiliki cisco system dengan PPtP *(point to point tunneling protocol)* milik Microsoft. Pada awalnya, semua produk cisco menggunakan L2F untuk mengurus tunnelingnya, sedangkan operating system Microsoft yang terdahulu hanya menggunakan PPtP untuk melayani penggunanya yang ingin bermain dengan tunnel. Namun saat ini, Microsoft Windows NT/2000 telah dapat menggunakan PPtP atau L2TP dan teknologi VPNnya. L2TP biasanya digunakan dalam membuat Virtual Private Dial Network (VPDN) yang dapat bekerja membawa semua jenis protocol komunikasi didalamnya. Selain itu, L2TP juga bersifat media independen karna dapat di atas media apapun. L2TP memungkinkan penggunanya untuk dapat terkoneksi dengan jaringan lokal milik mereka dengan policy keamanan yang sama dan dari manapun mereka berada, melalui koneksi VPN dan VPDN. Koneksi ini sering kali dianggap sebagai sarana memperpanjang jaringan lokal milik penggunanya, namun melalui media public. Namun, teknologi tunneling ini tidak memiliki mekanisme untuk menyediakan fasilitas enkripsi karena memang benar-benar murni hanya membentuk jaringan tunnel. Selain itu, apa yang lalu-lanang didalam tunnel ini dapat ditangkap dan di monitor dengan menggunakan protocol analizer

2.3 Pengertian Mikrotik

Mikrotik routerOS™ adalah system operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer menjadi router network yang handal, mencangkup berbagai fitur yang di buat untuk ip network dan jaringan wireless, cocok digunakan oleh ISP dan providet hotspot.

2.4 Konsep dasar VPN

Gammu bukanlah Aplikasi jadi, tapi Gammu merupakan sebuah modul yang bisa digabungkan dengan Bahasa pemrograman apa saja. Kelebihan Gammu diantaranya adalah :

1. Gammu bisa di jalankan di Windows maupun Linux
2. Banyak device yang compatible oleh Gammu
3. Gammu menggunakan database MySql
4. Baik kabel data USB maupun SERIAL, semuanya compatible di Gammu.

2.5 XAMPP

XAMPP adalah suatu aplikasi web server yang terdiri dari Apache, PHP, MySQL dan PHP MyAdmin.XAMPP merupakan tool yang menyediakan paket perangkat lunak ke dalam satu buah paket. Dengan menginstall XAMPP maka tidak perlu lagi melakukan instalasi dan konfigurasi web server Apache, PHP dan MySQL secara manual. XAMPP akan menginstalasi dan mengkonfigurasikannya secara otomatis atau auto konfigurasi.

3. ANALISIS KEBUTUHAN DAN PERANCANGAN

Kebutuhan Perangkat Keras

Perangkat keras yang dibutuhkan dalam proyek Penelitian ini antara lain :

1. PC/komputer untuk server
2. PC/komputer untuk client
3. 2 buah NIC untuk Server
4. 1 buah modem articonet
5. 1 buah switch

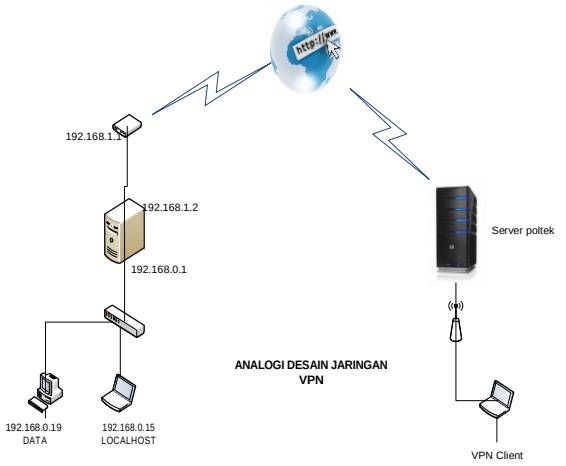
Kebutuhan Perangkat Lunak

Selain perangkat keras, dalam pengerjaan proyek Penelitian ini ada beberapa perangkat lunak yang dibutuhkan, diantaranya :

1. Winbox 2.2.13
2. Xampp
3. Ms. Visio 2007
4. Wireshark
5. OS Windows XP
6. Browser (Mozilla Firefox)
7. OS Mikrotik 2.9.27

ISSN : 2337-6341

Perancangan



Gambar 3.1. Perancangan Sistem

Perancangan Sistem

Sistem yang dibangun melibatkan beberapa tahapan, yaitu mengambil username dan password dari textbox, mengubah data text dari String menjadi ASCII, enkripsi data, mengirimkan data yang telah dienkripsi, dekripsi data yang telah diterima oleh server. Tahapan pembangunan sistem sebagai berikut :

1. **Proses Pada Client.**

   Pada tahap ini diawali dengan user pada sisi client mengetikkan username dan password pada textbox halaman login kemudian menekan tombol “Connect”. Kemudian data tersebut diubah ke bentuk ASCII lalu dilakukan proses encapsulasi dengan vpn menggunakan protocol *pptp*. Setelah itu data dikrimkan melalui jaringan.

2. **Proses pada sisi server**

   Pada tahap ini diawali dengan proses pembuatan user yang ingin berkomunikasi dengan jaringan yang satu jaringan dengan vpn-server. Vpn server berfungsi sebagai penyedia jalur khusus yang dibuat untuk melakukan koneksi secara privat dan untuk melakukan proses enkapsulasi data terhada suatu jaringan yang dilewati oleh *client.*

4. IMPLEMENTASI DAN PENGUJIAN

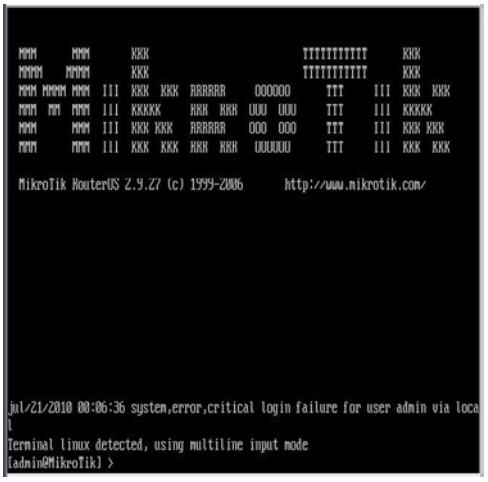
4.1 Konfigurasi

Dalam konfigurasi proyek Penelitian ini, ada beberapa hal yang harus dilakukan konfigurasi yaitu :

1. Installasi Mikrotik

Langkah-langkah yang dilakukan dalam proses instalasi *Mikrotik* adalah sebagai berikut:

a. Burning terlebih dahulu kedalam CD-R mikrotik.iso.
b. Setting bios anda,agar dapat booting CD-ROM terlebih dahulu.
c. Masukan CD-R yang sudah berisikan mikrotik.iso hasil *burning* dari step yang pertama.
d. Setelah menunggu sejenak dari proses booting maka akan keluar proses pilihan paket-paket yang ingin kita install, tekan “a” tanpa petik untuk menginstall semua paket yang ada, di lanjutkan menekan “i” tanpa petik.
e. Pada tahap ini paket-paket yang kita pilih telah terinstall, tekan “enter” untuk reboot.
f. Setelah komputer booting kembali ke mikrotik. Akan tampil pilihan login.
   - User : admin
   - Password : {kosong, (langsung tekan enter)}



Gambar 4.1. Instalasi mikrotik

2. Konfigurasi Mikrotik Sebagai Gateway Internet

Setelah mikrotik 2.9.27 sudah terinstall. Kemudian pastikan juga Ethernet sudah terdeteksi di komputer dan terhubung dengan switch. Langkah-langkah yang harus dilakukan diantaranya:

a. Menamai dua buah Ethernet di PC Server
   #set ether1 name=ISP
   #set ether2 name=LAN
b. Memberikan IP ke tiap Ethernet yang ada

ip address add address=192.168.1.2/24 interface=ISP
ip address add address=192.168.0.1/16 interface=LAN

c. Pemberian IP untuk gateway
#ip route add gateway=192.168.1.1

d. Uji koneksi
ping 192.168.1.1

```
C:\Documents and Settings\Ridha>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=1ms TTL=29
Reply from 192.168.1.1: bytes=32 time<1ms TTL=29
Reply from 192.168.1.1: bytes=32 time<1ms TTL=29
Reply from 192.168.1.1: bytes=32 time=1ms TTL=29

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

ping 192.168.1.2

```
C:\Documents and Settings\Ridha>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=64
Reply from 192.168.1.2: bytes=32 time<1ms TTL=64
Reply from 192.168.1.2: bytes=32 time<1ms TTL=64
Reply from 192.168.1.2: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

ping 192.168.0.1

```
C:\Documents and Settings\Ridha>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

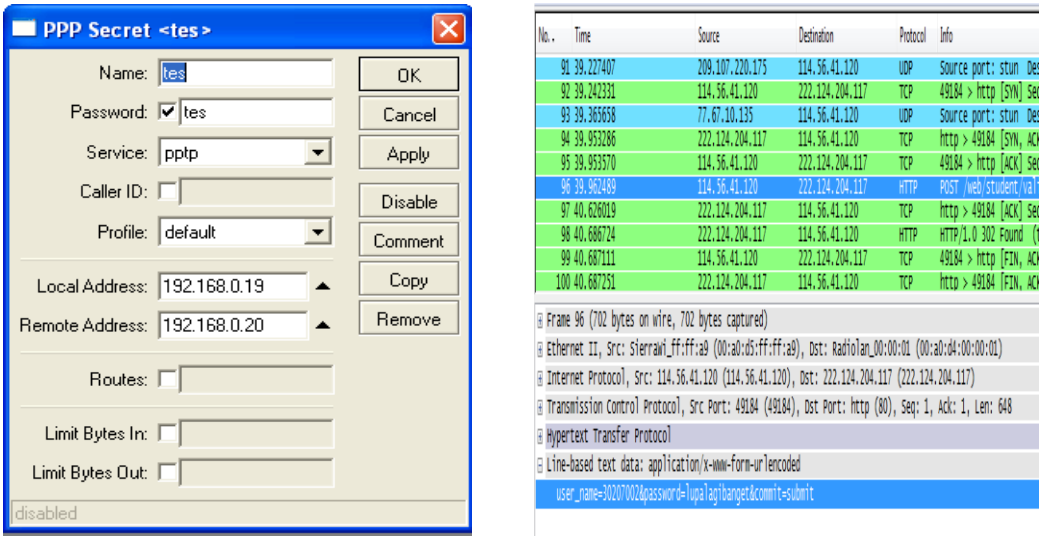
e. Menambahkan DNS
ip dns set primary-dns=125.160.14.82 allow-remote-request=yes
#ip dns set secondary-dns=222.124.204.34 allow-remote-request=yes

f. Pemberian NAT
   #ip firewall nat add chain=srcnat action=masquerade out-interface=ISP
g. Uji coba koneksi internet
   # ping www.yahoo.com

3. Konfigurasi PPTP

Langkah ini bertujuan untuk membuat VPN server dengan PPTP (*point to point tunneling protocol*). Hal-hal yang harus diperhatikan ialah bahwa paket-paket untuk tunneling pastikan sudah terinstall waktu proses installasi mikrotik. Jika sudah maka proses ini tidak memiliki masalah dalam pengkonfigurasiannya.

1. pilih menu PPP → pilih menu interface → PPTP Server. Beri nama pada tab general lalu klik ok
2. Pindah ke tab secrets → klik tombol add yang bertanda plus → isi nama kolom tersebut dengan sebagai berikut :
   User : tes
   Password : tes
   Service : pptp
   Local address : 192.168.0.19
   Remote address : 192.168.0.20



Gambar.4.3 Monitoring jaringan sebelum ada VPN

4.2 Pengujian

Pada sisi client, jaringan di hubungkan dengan mengisi ip public server VPN. Jika berhasil maka client akan di berikan *ip* oleh server berdasarkan user client yang dipakai. Jika sudah connected, maka vpn sudah dikatakan berhasil.

Pada saat client menekan tombol “connected” maka jalur telah di enkapsulasi oleh *protocol pptp*. Dan proses selanjutnya ialah dengan mengetikan alamat url localhost

yang ada dijaringan local. Missal dengan mengetikan ip 192.168.0.16/sms maka akan keluar web sms gammu.

4.2.1 Pengujian Sistem Autentikasi

Pada bagian ini akan diperlihat perbedaan antara sistem autentikasi pada jaringan yang belum menggunakan vpn dan yang sudah menggunakan vpn

Pada jaringan yang sebelum ada vpn saat ini elemen autentikasi yaitu username dan password dapat dilihat dengan mudah dengan menggunakan tools *wireshark.* Protocol yang digunakan juga masih menggunakan HTTP pada port 80. Hal ini sangat memudahkan orang lain untuk mencuri password kita. Berikut gambar hasil monitoring dengan menggunakan *wireshark* pada aktifitas yang belum di aktifkan VPN :

Pada gambar terlihat jelas semua aktifitas yang dilakukan jaringan ini tercaptur dengan wireshark. Oleh karena itu diperlukan adanya enkapsulasi data semua aktifitas dunia internet. Dengan menerapakan vpn maka elemen autentikasi dan protocol tersebut akan di enkapsulasi (di bungkus). Dalam proyek Penelitian ini digunakan vpn untuk mengenkapsulasi data. Berikut gambar hasil monitoring pada tools *wireshark* pada jaringan VPN yang terkoneksi dengan jaringan local dimana vpn server berada :

28	1.040017	192.168.0.19	110.137.121.101	PPP Comp	Compressed data
29	1.040101	192.168.0.19	110.137.121.101	PPP Comp	Compressed data
30	1.068462	192.168.0.19	110.137.121.101	PPP Comp	Compressed data
31	1.068533	192.168.0.19	110.137.121.101	PPP Comp	Compressed data
32	1.110380	110.137.121.101	192.168.0.19	PPP Comp	Compressed data
33	1.120987	192.168.0.19	110.137.121.101	PPP Comp	Compressed data
34	1.211619	192.168.0.1	192.168.0.19	TCP	8291 > hpidsadmin [PSH, ACK] S
35	1.322204	192.168.0.19	192.168.0.1	TCP	hpidsadmin > 8291 [ACK] Seq=34
36	1.364303	110.137.121.101	192.168.0.19	GRE	Encapsulated PPP
37	1.408955	192.168.0.19	110.137.121.101	PPP Comp	Compressed data
38	1.408979	192.168.0.19	110.137.121.101	PPP Comp	Compressed data
39	1.408997	192.168.0.19	110.137.121.101	PPP Comp	Compressed data
40	1.409610	110.137.121.101	192.168.0.19	PPP Comp	Compressed data
41	1.444653	110.137.121.101	192.168.0.19	PPP Comp	Compressed data
42	1.464104	110.137.121.101	192.168.0.19	PPP Comp	Compressed data
43	1.509706	192.168.0.19	110.137.121.101	GRE	Encapsulated PPP
44	1.578760	110.137.121.101	192.168.0.19	PPP Comp	Compressed data
45	1.581432	192.168.0.19	192.168.0.1	TCP	hpidsadmin > 8291 [PSH, ACK] S
46	1.589160	192.168.0.1	192.168.0.19	TCP	8291 > hpidsadmin [PSH, ACK] S
47	1.589378	110.137.121.101	192.168.0.19	PPP Comp	Compressed data
48	1.589495	192.168.0.19	110.137.121.101	PPP Comp	Compressed data
49	1.612212	110.137.121.101	192.168.0.19	PPP Comp	Compressed data
50	1.612693	192.168.0.19	110.137.121.101	PPP Comp	Compressed data
51	1.613755	192.168.0.19	110.137.121.101	PPP Comp	Compressed data
52	1.623992	192.168.0.19	110.137.121.101	PPP Comp	Compressed data

Gambar.4.4 Monitoring Wireshark setelah ada VPN

5. SIMPULAN DAN SARAN

5.1 Simpulan

Simpulan dari pembuatan Internet VPN di proyek Penelitian ini adalah :

1. Berdasarkan hasil monitoring menggunakan tools *wireshark* bahwa jaringan yang tidak menggunakan vpn tidak lah aman karena tidak dapat di bungkus oleh suatu protokol
2. Dengan penerapan vpn menggunakan protocol *pptp* maka data tidak dapat dibaca oleh orang lain.
3. Penerapan PPTP (Point to Point Tunneling Protocol) menambah tingkat keamanan pada suatu jaringan karena jalur komunikasi yang dilewati di*enkapsulasi*.
4. Dengan adanya PPTP untuk enkapsulasi jalur komunikasi ditambah lagi dengan adanya login username dan password menggunakan login dari vpn-client dapat meningkatkan keamanan suatu jalur institusi atau office.

5.2 Saran

Beberapa saran yang dapat diberikan berdasarkan pengalaman pembuatan sistem dalam proyek Penelitian ini diantaranya :

1. Dapat dikembangkan dengan menambahkan metode *IPsec,* yang terdapat pada Protokol L2TP untuk mengenkripsi data yang lewat, dengan dua server vpn.
2. Dapat dikembangkan untuk enkripsi di sisi client dengan membuat *plug-in* enkripsi RSA sehingga kunci publik tidak dapat dilihat oleh client.
3. Dapat dikembangkan di operating system lain seperti Ubuntu, FreeBSD, MacOS, Cisco system, dll sehingga diketahui OS mana yang paling cocok untuk digunakan.

DAFTAR PUSTAKA

Ryan, Nathanagus. **Panduan Step by Step Membangung Mikrotic**. 2009. http://nathangustiryan.wordpress.com/2010/04/16/step-by-step-membangun-vpn-server-dgn-mikrotik/ (accessed April 16, 2010)

Setting Mikrotik Speedy. http://mikrotik-id.blogspot.com/search/label/Tutorial+20Mikrotik+20VPN (accessed August 6, 2010).

Mansfield, Nall (2008) **Practical TCP/IP : Mendesain, Menggunakan, dan Troubleshooting Jaringan TCP/IP di linux dan Windows (Jilid 2).** Yogyakarta : Penerbit Andi

Stiawan, Deris (2008). **Mengenal Protokol dan Sistem Keamanan.** From : http://deris.unsri.ac.id/materi/securit/bab3Protocol+20Secured.pdf 6 may 2010

Bonar, **Bagaimana dial Speedy Lewat Mikrotik 2008**.
http://arie.web.id/2008/02/26/bagaiman-dial-speedy-lewat-mikrotik/ (accessed February 28, 2010).