Analisa Sistem Pengaman Data Jaringan Berbasis VPN

Albert Suwandhi[1)], Juni Erpin[2)]
STMIK IBBI
Jl. Sei Deli No. 18 Medan, Telp. 061-4567111 Fax. 061-4527548
e-mail : albersuwandhi@gmail.com[1)]

ABSTRAK

Saat ini sudah banyak sekali perusahaan yang mempunyai banyak cabang menggunakan jasa internet dengan teknologi yang ditawarkan oleh provider internet dengan jenis dan harga yang bervariasi untuk memenuhi kebutuhan komunikasi perusahaan. Namun, masih banyak yang menggunakan dial-up privat dari cabang ke pusat. Sistem ini lebih mengeluarkan biaya yang besar setiap koneksinya. Adapun tujuan penelitian ini adalah merancang suatu jaringan yang ekonomis dalam hal biaya koneksi dan menjamin keamanan pertukaran data antara pusat dan cabang. Metode yang dipilih dan dilakukan adalah menganalisis kebutuhan dan sistem berjalan (bandwidth, biaya, koneksi pusat dan cabang), merancang IPSec, konfigurasi site-to-site VPN. Tentunya bukan saja biaya koneksi yang mengalami penghematan, keamanan transaksi data pun menjadi fasilitas yang akan didapat dengan VPN (Virtual Private Network) yang dirancang dan di usulkan.

Kata kunci : VPN koneksi, IPSec.

ABSTRACT

There is now a lot of companies that have many branches to use internet services to the technology offered by the Internet provider with a variety of types and prices to meet the communication needs of the company. However, there are still many who use dial-up private from the center to the branch. This system is more cost very much per connection. The purpose of this research is to design a network that is economical in terms of cost of connections and ensure the security of data exchange between central and branch. The method chosen and carried out to analyze the need and the system is running (bandwidth, cost center and branch connections), IPSec designing, configuring site-to-site VPN. Surely not just the cost savings experienced connection, the data transaction security facility would also be obtained with a VPN (Virtual Private Network) is designed and proposed

.

Keywords : VPN connection, IPSec.

1. Pendahuluan

Internet merupakan sebuah jaringan global dan terbuka, dimana setiap pengguna dapat saling berkomunikasi dan bertukar informasi. Seiring dengan maraknya penggunaan *Internet*, banyak perusahaan yang kemudian beralih menggunakan *internet* sebagai bagian dari jaringan mereka untuk menghemat biaya. Akan tetapi permasalahan keamanan masih menjadi faktor utama.

Untuk mengatasi masalah keamanan dalam komunikasi data pada jaringan umum (*public network / internet*) maka lahirlah *Virtual Private Network* (VPN). Secara umum VPN merupakan suatu jaringan komunikasi lokal yang terhubung melalui media jaringan publik, infrastruktur publik yang paling banyak digunakan adalah jaringan *internet*. Didalam VPN terdapat perpaduan teknologi tunneling dan enkripsi yang membuat VPN menjadi teknologi yang handal untuk mengatasi permasalahan keamanan didalam jaringan.

Dalam implementasinya, VPN menggunakan *Site-to-site* untuk menghubungkan antara 2 tempat yang letaknya berjauhan, seperti kantor pusat dengan kantor cabang atau suatu perusahaan dengan perusahaan mitra kerjanya. Implementasi VPN yang digunakan untuk menghubungkan suatu perusahaan dengan perusahaan lain (misalnya mitra kerja, *supplier* atau pelanggan) disebut *ekstranet*. Sedangkan bila VPN digunakan untuk menghubungkan kantor pusat dengan kantor cabang, implementasi ini termasuk jenis *intranet site-to-site* VPN.

Pada VPN terdapat beberapa protokol yang paling umum digunakan, yaitu *Point to Point Tunneling Protocol* (PPTP), SOCKS, *Layer 2 Tunneling Protocol* (L2TP), *Cryptographic IP*

Encapsulation (CIPE), *Generic Routing Encapsulation* (GRE), dan *Internet Protocol Securuty* (IPSec). Protokol-protokol tersebut memiliki karakteristik yang berbeda-beda.

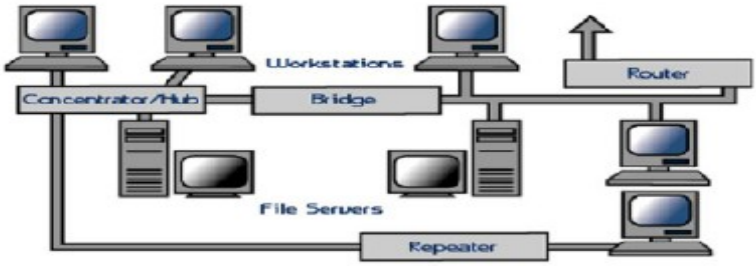
Berdasarkan ruang lingkup geografisnya terdapat empat jenis jaringan komputer, antara lain:

1. *Local Area Network* (LAN)
   Jarak jangkauan *Local Area Network* (LAN) tidak terlalu jauh. Biasanya diterapkan pada suatu gedung atau antar gedung dalam suatu kompleks perkantoran atau sekolah.
2. *Metropolitan Area Network* (MAN)
   MAN jarak jangkaunya lebih luas dari LAN. Jangkauan MAN dapat mencapai antar kota. Contoh penerapan dari MAN ialah peyediaan layanan internet oleh Internet Service Provider (ISP). Pengguna jasa ISP ini akan tercakup dalam jaringan MAN yang disediakan oleh ISP tersebut.
3. *Wide Area Network* (WAN)
   Jaringan *Wide Area Network* (WAN) mempunyai cakupan terluas, bahkan dapat dikatakan mencakup seluruh dunia. Jaringan ini sendiri dapat dihubungkan dengan menggunakan satelit dan media kabel fiber optic.
4. *Global Area Network* (GAN)
   Jaringan *Global Area Network* (GAN) merupakan suatu jaringan yang menghubungkan negara-negara di seluruh dunia. Kecepatan GAN bervariasi mulai dari 1,5 Mbps sampai dengan 100 Gbps dan cakupannya mancapai ribuan kilometer. Contoh yang sangat baik dari GAN ini adalah *internet*.

Media transmisi merupakan jalur yang digunakan untuk dapat melakukan perpindahan data, baik berupa kabel maupun nirkabel (*wireless*). Dalam pemilihan media transmisi perlu mempertimbangkan aspek-aspek sebagai berikut.

1. *Bandwith*
   Bandwith adalah jumlah frekuensi yang dapat diakomodasi oleh media transmisi. Dengan media yang dapat mengakomodasi jumlah frekuensi lebih banyak, jumlah data yang dikirim atau diterima akan lebih banyak dan dengan waktu pengiriman yang lebih cepat.
2. *Attenuation*
   Attenuation adalah luas jangkauan yang dapat diberikan oleh media transimsi. Luas jangkau ini sendiri dikarenakan adanya hambatan yang dimiliki media transmisi itu sendiri.
3. *Cost*
   Cost adalah dana yang dipunyai dan biaya yang harus dikeluarkan untuk instalasi jaringan tetap harus dibandingkan dengan kebutuhan yang ada.

Perangkat keras yang dibutuhkan untuk membangun sebuah jaringan komputer yaitu: Komputer, Card Network, Hub, dan segala sesuatu yang berhubungan dengan koneksi jaringan seperti: Printer, CDROM, Scanner, Bridges, Router dan lainnya yang dibutuhkan untuk process transformasi data didalam jaringan.



Gambar 1. Perangkat keras pada LAN

1. File Server.
2. Workstations.
3. Network Interface Cards.
4. Concentrators/Hubs.
5. Repeaters.
6. Bridges.
7. Routers.

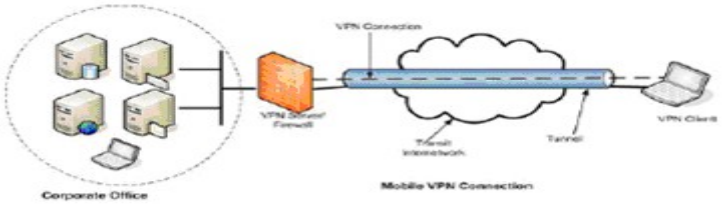
Didalam implementasinya VPN dibagi menjadi dua jenis yaitu *remote access* VPN dan s*ite-to-site* VPN:

1. *Remote Access* VPN

Jenis implementasi yang pertama adalah *Remote access* yang biasa juga disebut *virtual private dial-up network* (VPDN), menghubungkan antara pengguna yang *mobile* dengan *local area network*

(LAN). Jenis VPN ini digunakan oleh pegawai perusahaan yang ingin terhubung ke jaringan khusus perusahaannya dari berbagai lokasi yang jauh (*remote*) dari perusahaannya. Biasanya perusahaan yang ingin membuat jaringan VPN tipe ini akan bekerjasama dengan *enterprise service provider* (ESP). ESP akan memberikan suatu *network access server* (NAS) bagi perusahaan tersebut. ESP juga akan menyediakan *software* klien untuk komputer-komputer yang digunakan pegawai perusahaan tersebut. Untuk mengakses jaringan lokal perusahaan, pegawai tersebut harus terhubung ke NAS dengan men-*dial* nomor telepon yang sudah ditentukan. Kemudian dengan menggunakan *sotware* klien, pegawai tersebut dapat terhubung ke jaringan lokal perusahaan.

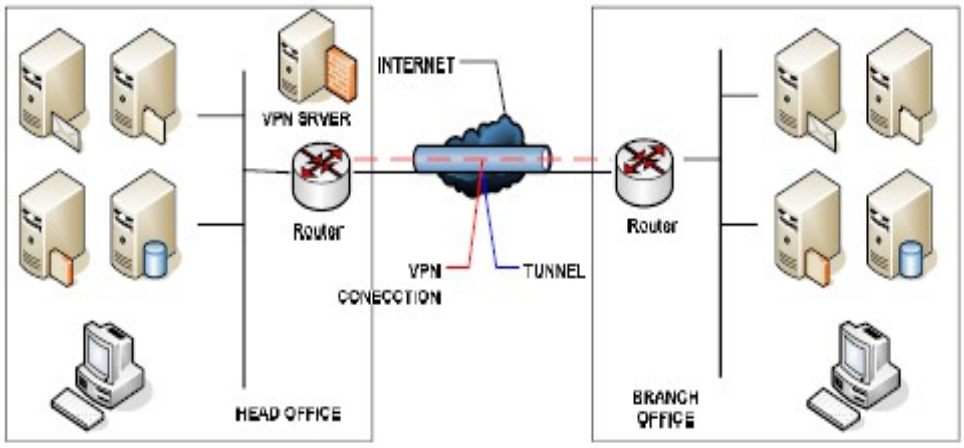
Perusahaan yang memiliki pegawai yang ada di lapangan dalam jumlah besar dapat menggunakan *remote access* VPN untuk membangun WAN. VPN tipe ini akan memberikan keamanan, dengan mengenkripsi koneksi antara jaringan local perusahaan dengan pegawainya yang ada di lapangan. Pihak ketiga yang melakukan enkripsi ini adalah ISP.



Gambar 2. *Remote Access* VPN

2. *Site-to*-site VPN

Jenis implementasi VPN yang kedua adalah *site-to-site* VPN. Implementasi jenis ini menghubungkan antara dua tempat yang letaknya berjauhan, seperti halnya kantor pusat dengan kantor cabang atau suatu perusahaan dengan perusahaan mitra kerjanya. VPN yang digunakan untuk menghubungkan suatu perusahaan dengan perusahaan lain (misalnya mitra kerja, *supplier* atau pelanggan) disebut ***ekstranet***. Sedangkan bila VPN digunakan untuk menghubungkan kantor pusat dengan kantor cabang, implementasi ini termasuk jenis ***intranet*** *site-to-site* VPN.



Gambar 3. *Site-to-site* VPN

Berdasarkan permasalahan yang diteliti, maka maksud dari penulisan ini adalah untuk menganalisis dan merancang *site-to-site* VPN berbasis IPsec dengan MikroTik Router Operating System. Sedangkan yang menjadi tujuan penulisan ini adalah:

1. Menerapkan *site-to-site* VPN dengan protokol IP security
2. Membuktikan bahwa VPN memberikan solusi keamanan dalam trasmisi data atau informasi pada jaringan komputer.
3. Menganalisis perbandingan data yang diperoleh dari layanan yang menggunakan VPN dengan layanan yang tidak menggunakan VPN.

2. Metode Analisa dan Perancangan

Adapun langkah-langkah dalam teknik analisis data dalam penelitian ini adalah:

1. Reduksi Data

Reduksi data diawali dengan menerangkan, memilih hal-hal yang pokok, memfokuskan pada hal-hal yang penting terhadap isi dari suatu data yang berasal dari lapangan, sehingga data yang telah direduksi dapat memberikan gambaran yang lebih tajam tentang hasil pengamatan. Dalam proses reduksi data ini, peneliti dapat melakukan pilihan-pilihan terhadap data yang hendak dipakai dalam sistem VPN.

2. Display Data

Display data merupakan proses menampilkan data secara sederhana dalam bentuk kata-kata, kalimat naratif, table, matrik dan grafik dengan maksud agar data yang telah dikumpulkan dikuasai oleh peneliti sebagai dasar untuk mengambil kesimpulan yang tepat dalam penggunaan sistem VPN.

3. Verifikasi dan Simpulan

Sejak awal pengumpulan data peneliti membuat simpulan-simpulan sementara. Dalam tahap akhir, simpulan-simpulan tersebut harus dicek kembali (diverifikasi) pada catatan yang telah dibuat oleh peneliti dan selanjutnya kearah simpulan yang benar. Simpulan adalah intisari dari temuan penelitian yang menggambarkan pendapat-pendapat terakhir yang berdasarkan pada uraian-uraian sebelumnya. Simpulan akhir yang dibuat harus relevan dengan fokus penelitian, tujuan penelitian dan temuan penelitian yang sudah dilakukan pembahasan. Perancangan sistem *site-to-site* VPN, yang meliputi perancangan infrastruktur VPN atau topologi jaringan, instalasi dan konfigurasi perangkat lunak.

Spesifikasi *hardware* minimal yang digunakan sebagai komputer *server* VPN dalam simulasi yang dilakukan memiliki spesifikasi sebagai berikut:

a. Prosesor: Intel Pentium IV 2,0 GHZ
b. Monitor: Flat 17" Resolusi 1024x768
c. RAM: 256 Mb
d. VGA: 128 Mb
e. NIC: 10/100
f. HDD: 20 GB P-ATA (Parallel ATA)
g. Optical Disc: CD Rom
h. Keyboard

Adapun spesifikasi *hardware* yang direkomendasikan sebagai komputer *server* VPN adalah dengan spesifikasi minimum sebagai berikut:

a. Prosesor: P2, AMD, cyrix (tidak mendukung multi-prosesor)
b. Monitor: Flat 15" Resolusi 1024x768
c. RAM: 64 MB
d. VGA: Onboard
e. NIC: 10/100
f. HDD: 128 MB *Space* P-ATA atau Compact Flash (tidak dianjurkan menggunakan UFD, SCSI dan S-ATA)
g. Optical disc: CD Rom
h. Keyboard

Spesifikasi software yang digunakan sebagai *server* VPN adalah Mikrotik Router Operation System versi 2.9.27.

Agar dalam proses selanjutnya kita dapat mengetahui apa saja yang telah ditemukan dan di interpretasi di dalam lapangan, maka kita perlu mengetahui kredibilitasnya dengan menggunakan konfigurasi sistem *site-to-site* VPN yaitu ada tahap dimana dilakukannya pengaturan-pengaturan parameter yang terdapat pada sebuah perangkat lunak. Adapun parameter-parameter yang akan kita setting pada komputer *server* dan *client* adalah:

1. Komputer yang digunakan sebagai *server* VPN

Tahapan konfigurasi yang harus dilakukan dalam tahap perancangan server adalah:

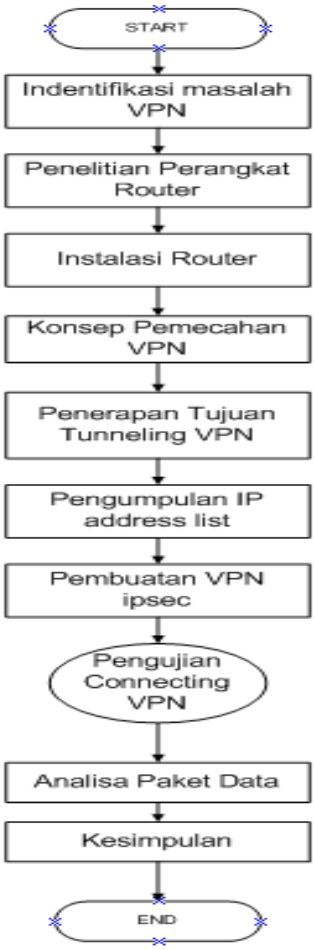
a. Tahap Instalasi mikrotik.
b. Tahap konfigurasi IP Pool.
c. Tahap konfigurasi IP Routes.
d. Tahap konfigurasi PPP sebagai server VPN.
e. Tahap konfigurasi DHCP *server.*
f. Tahap konfigurasi firewall NAT Masquerade dan NAT bypass.
g. Tahap konfigurasi IP Security.

2. Komputer *client* VPN

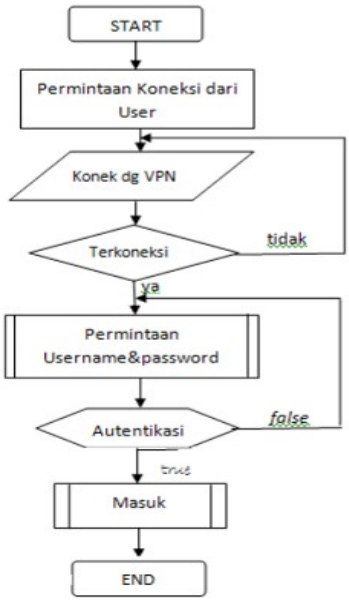
Dalam membuat setting Mikrotik VPN *Client*, tahapan-tahapan yang akan user lakukan yaitu:

a. Tahap konfigurasi akses VPN.
b. Tahap *Connecting* VPN.

Secara ringkas diagram metodologi penelitian ini ditunjukan pada gambar dibawah ini yaitu:



Gambar 4. Diagram Metodologi Penelitian



Gambar 5. Flowchart sistem berjalan

Gambar 5. diatas adalah sistem yang sedang berjalan menggunakan jalur tunneling PPTP antara kantor pusat dan cabang. Maka koneksi hanya bisa dari pusat ke cabang atau hanya satu sisi.

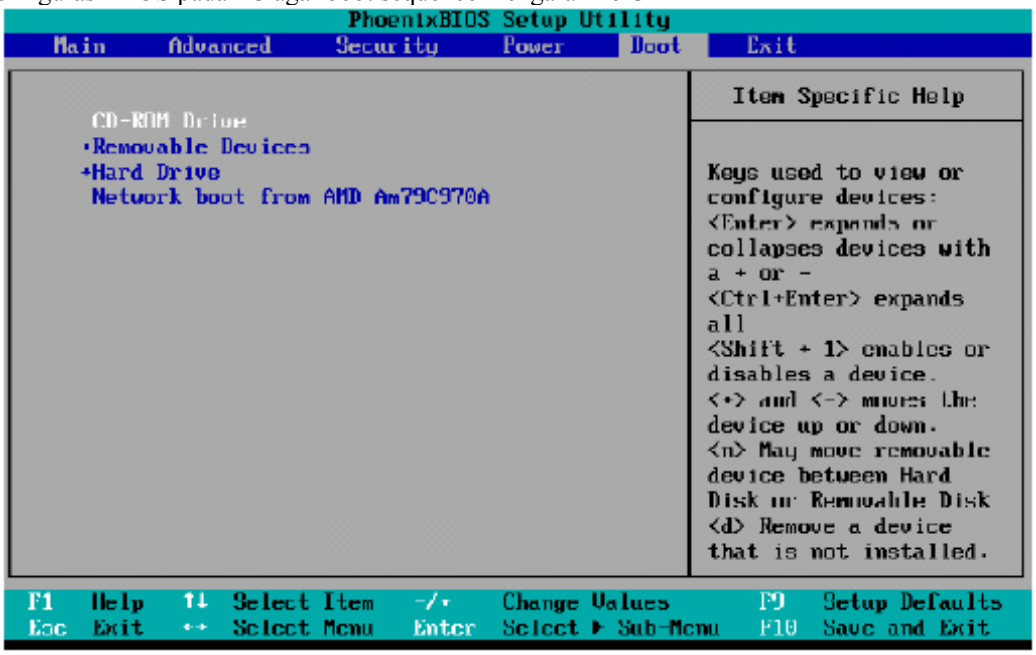
3. Hasil dan Analisis

Server VPN yang digunakan adalah mikrotik routerOS versi 2.9.27. Mikrotik routerOS adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer biasa menjadi router network yang mencakup berbagai fitur yang dibuat untuk ip network dan jaringan wireless. Untuk melakukan instalasi Mikrotik RouterOS ke dalam PC ada hal yang perlu di persiapkan antara lain:

a. Menyiapkan 1 buah PC yang telah disediakan dengan 2 NIC.

b.Menyiapkan CD instaler Mikrotik dapat bootable yang file iso download dari Internet dan membakarnya kedalam CD dengan aplikasi Nero.

c. Konfigurasi BIOS pada PC agar boot sequence mengarah ke CD

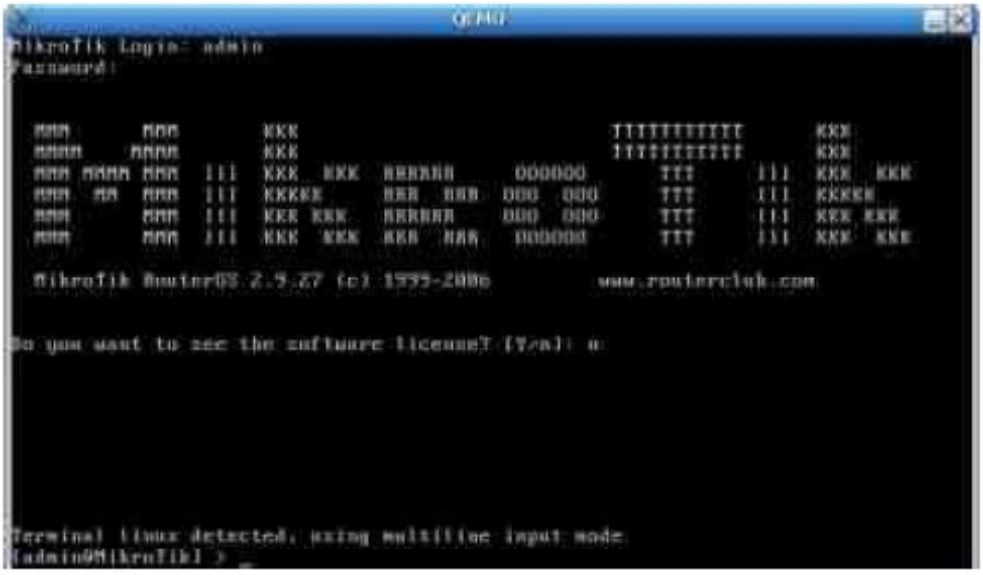


Gambar 6. Konfigurasi BIOS

Setelah itu menyimpannya dengan menekan F10 lau tekan OK. Sistem akan *restart* untuk melanjutkan proses instalasi sampai muncul seperti gambar 4.19. Sebelum proses instalasi dimulai komputer harus memiliki ethernet card (sebagai jaringaan lokal dan interlokal). Proses instalasi dimulai dari *booting* dari CD Room yang sudah berisi CD *software mikrotik routerOS*. Berikut tampilan pilihan paket-paket yang akan di install.

Gambar 7.Paket instalasi mikrotik

Select all kemudian tekan 'I' untuk melanjutkan proses instalasi. Proses instalasi dilanjutkan dengan pembuatan partisi harddisk dan format harddisk. Untuk mikrotik routerOS akan mengambil semua space yang ada di harddisk. Selanjutnya reboot PC Router mikrotik dan mikrotik telah selesai di install.



Gambar 8. Tampilan Log in Mikrotik

Setelah proses instalasi selesai, selanjutnya user akan melakukan konfigurasi. Adapun konfigurasi yang di lakukan sebagai berikut:

1. Sebelum user memulai konfigurasi, terlebih dahulu user akan mengakses mikrotik dengan login pada mikrotik RoutersOS melalui console:

```
MikroTik v2.9.27
Login    : admin
Password : (kosongkan)
```

Sampai langkah ini user telah dapat masuk pada mesin Mikrotik. User default adalah admin dan password di kosongkan, kemudian ketik admin dan tekan tombol enter.

2. Kemudian Untuk keamanan akses mikrotik, ganti username dan password default sesuai dengan yang user inginkan. Dalam simulasi ini, login default user ganti dengan "server" dan password user ganti dengan "vpn".

```
[admin@Mikrotik] > password
old password:
new password: ****
retype new password: ****
[admin@ Mikrotik] >
```

3. Setelah user mengganti password default, user juga dapat mengganti nama Mikrotik Router, pada langkah ini nama server akan user ganti menjadi "vpn"

```
[admin@Mikrotik] > system identity set name=vpn
[admin@vpn] >
```

4. Selanjutnya user dapat melihat interface pada mikrotik router dengan mengetikkan *statement* pada *console*:

```
[admin@vpn] > interface print
Flags: X - disabled, D - dynamic, R - running
# NAME TYPE RX-RATE TX-RATE MTU
0 R ether1 ether 0 0 1500
1 R ether2 ether 0 0 1500
[admin@vpn] >
```

5. Kemudian user masuk ke tahap pemberian IP address pada *interface m*ikrotik. Adapun parameter-paremeter yang akan user setting untuk interface:

a. ether1 IP address: 192.168.1.1

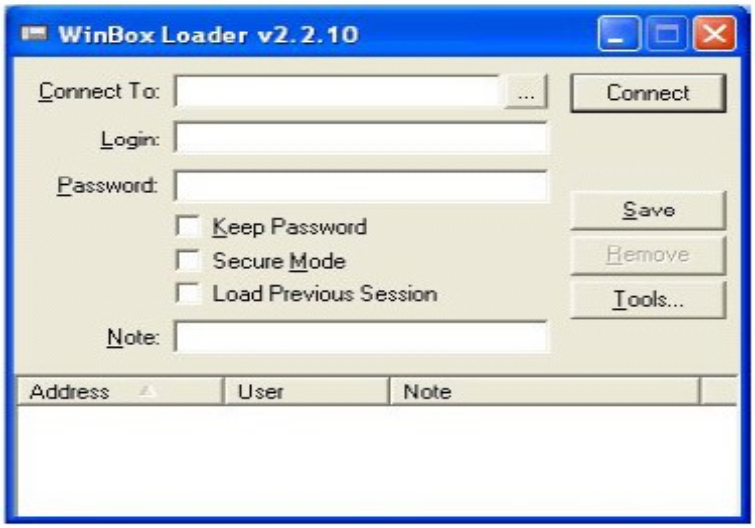
b. ether2 IP address: 172.16.1.2

```
[admin@vpn] > ip address add address=192.168.1.1 /
netmask=255.255.255.0 interface=ether1
[admin@vpn] > ip address add address=172.16.1.2 /
netmask=255.255.255.0 interface=ether2
```

6. Melihat konfigurasi IP address yang sudah user berikan dengan mengetikkan *statement* pada *console*:

```
[admin@vpn] >ip address print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS  NETWORK  BROADCAST  INTERFACE
0  192.168.1.1/24  192.168.1.0   192.168.1.255
ether1
1  172.16.1.2/24   172.16.1.0   172.16.1.255
ether2
[admin@vpn] >
```

Selanjutnya mikrotik telah dapat diremote dengan winbox. Winbox adalah sebuah *utility* untuk melakukan *remote* ke *server* mikrotik dalam mode GUI (*Grapihcal User Interface*).



Gambar 9. WinBox Loader

Setelah selesai melakukan konfigurasi di sisi *server,* di sisi *client* dan *router* mikrotik, langkah terakhir adalah melakukan ke tahap pengujian sistem. Dalam tahap ini, akan dilakukan beberapa tahap pengujian untuk mengetahui kinerja dari sistem VPN. Adapun di dalam pengujian sistem akan dilakukan beberapa skenario diantaranya:

1) Menguji konektivitas VPN:

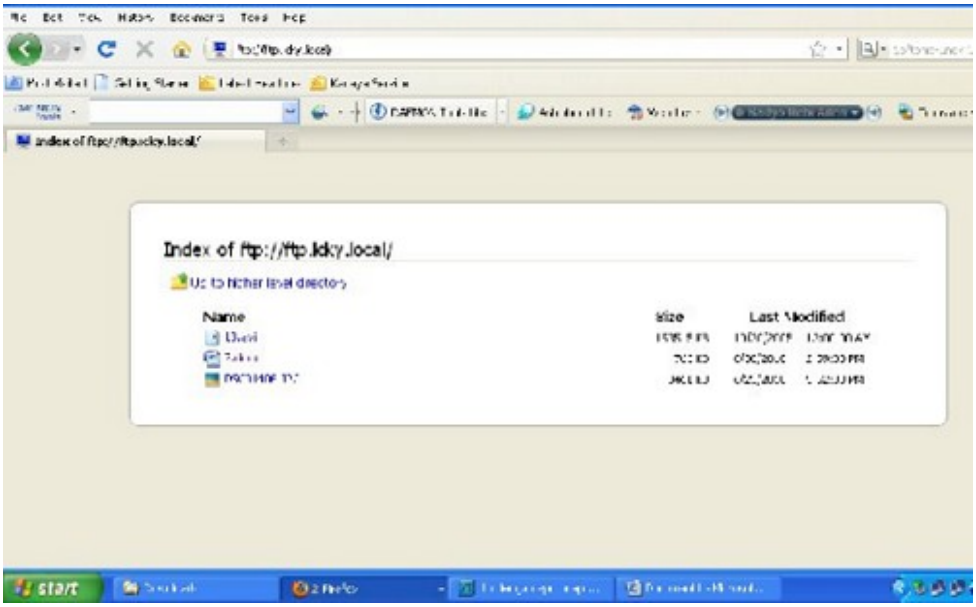
a. Mengakses web *server*

Dibawah ini merupakan gambar pada saat user mengakses web *server*

Gambar 10. Tampilan interface web *server*

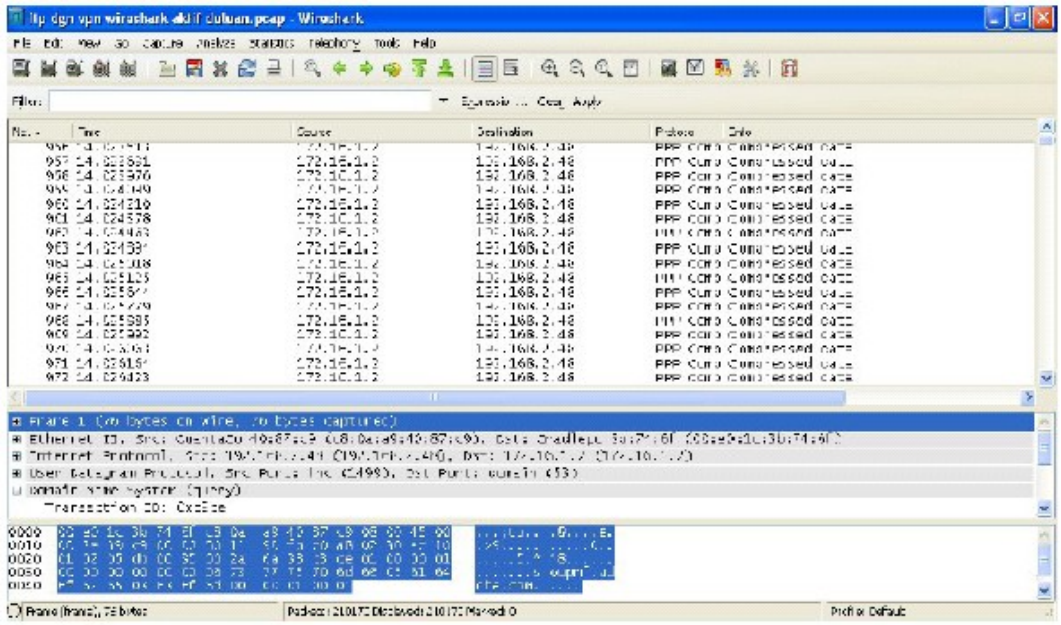
b. Melakukan *download* file dari file *server* menggunakan FTP *service*

Dibawah ini merupakan gambar pada saat user mengakses file *server*



Gambar 11. Tampilan file *server*

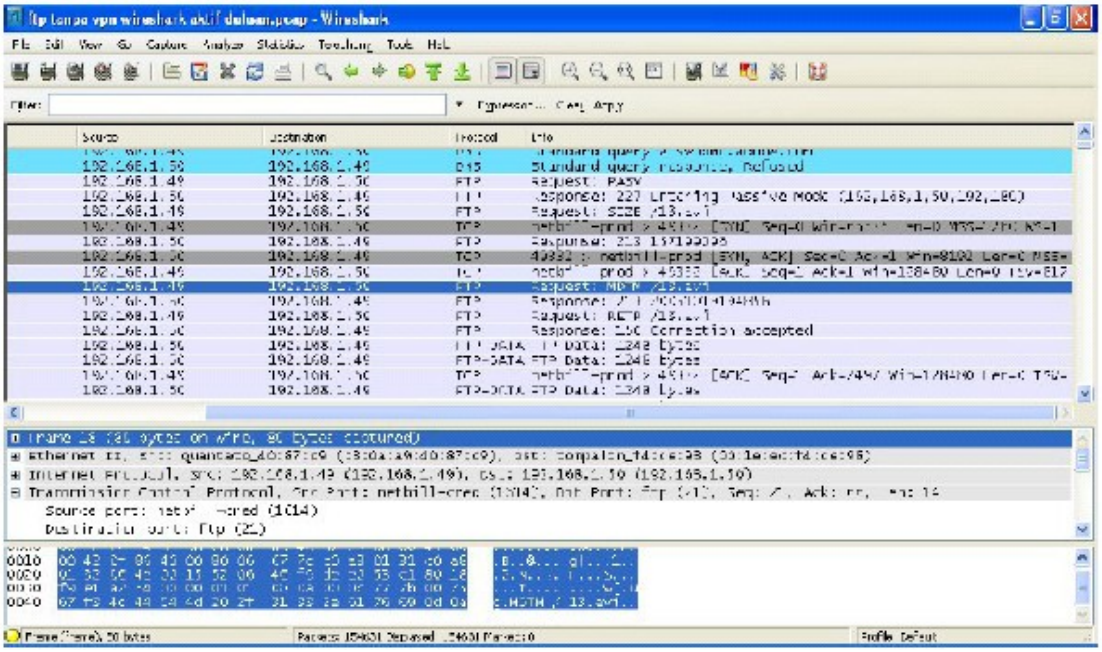
2) Menguji kehandalan VPN:
Untuk dapat menguji kehandalan VPN berbasis IPsec, diperlukan analisa mengenai perbandingan data yang diperoleh dari monitoring FTP *service* melalui VPN dan tanpa VPN.
a. Dibawah ini merupakan gambar monitoring data melalui VPN



Gambar 12. Monitoring data melalui VPN

Hasil monitoring data diatas menyimpulkan bahwa, dengan teknologi VPN, protokol FTP tidak dapat di monitor dan data yang ditransmisikan melalui *tunnel* mengalami kompresi dan file terenkripsi. Dengan demikian VPN terbukti dapat meningkatkan keamanan dalam transmisi data.

b. Dibawah ini merupakan gambar monitoring tanpa melalui VPN



Gambar 13. Monitoring data tanpa melalui VPN

Hasil monitoring data diatas menyimpulkan bahwa, ketika file ditransmisikan tanpa melalui VPN, protokol FTP dapat di monitor dan data yang ditransmisikan dapat dilihat dengan jelas.

4. Kesimpulan

Berdasarkan penelitian yang dilakukan mengenai analisa dan perancangan *site-to-site* VPN berbasis IP Security menggunakan Mikrotik Router Operating System, maka dapat beberapa kesimpulan sebagai berikut:

1. Data yang ditransmisikan melalui VPN akan mengalami kompresi, sehingga transmisi data dapat lebih cepat dan aman.
2. Protokol IPsec yang di implementasikan pada *site-to-site* VPN bekerja dengan mekanisme *network-to-network.*
3. IPSec terbukti sangat baik dalam perlindungan data, karena didalamnya terdapat mekanisme enkripsi data.
4. Dengan IPSec, protokol yang berjalan didalam *tunnel* tidak dapat di *capture* atau di monitoring oleh *protocol analyzer tool.*
5. Kelebihan VPN adalah:
   a. Mempermudah perluasan konektivitas jaringan komputer secara geografis (Skalabilitas).
   b. Peningkatan keamanan dalam komunikasi data.
   c. Menyederhanakan topologi jaringan.

Daftar Pustaka

[1.] Budhi Irawan. 2005. ***Jaringan Komputer***. Graha ilmu. Yogyakarta

[2.] Pendy Aris, Ramadhana Ss Achmad. 2005. ***Membangun VPN Linux Secara Cepat***. Yogyakarta.

[3.] Snader, C Jon. 2005. ***VPNs Illustrated:Tunnels,BPNs,and IPSec***.Addison Wesley Professional.

[4.] William Stallings. 2002. ***Komunikasi data dan komputer: jaringan komputer Jakarta***. salemba teknika.

[5.] Adnan Basalamah, 1999. ***Standar H.323 untuk networking aplikasi multimedia***, *computer Network Research Group (CNRG) ITB*, bandung: Graha Ilmu.