BAB III

ANALISIS DAN PERANCANGAN

3.1 Analisis Sistem

Analisa merupakan suatu tindakan untuk mengetahui lebih jauh tentang obyek yang akan diteliti. Bab ini akan menguraikan proses analisis pembangunan sistem *site-to-site* VPN dan perancangan sistem *site-to-site* VPN. Sebelum dilakukan pengembangan dan perancangan sistem, terlebih dahulu dilaksanakan analisis kebutuhan – kebutuhan pokok sistem *site-to-site* VPN yang akan dibangun.

3.1.1 Analisis Masalah

Keamananan data dalam transmisi sebuah jaringan komputer merupakan faktor yang sangat penting. Dengan adanya *site-to-site* VPN, keamanan menjadi prioritas utama selain fungsi lainnya yaitu untuk menghubungkan antara dua atau lebih tempat yang letaknya berjauhan, seperti halnya kantor pusat dengan kantor cabang yang dimiliki oleh sebuah instansi atau perusahaan.

Kelebihan implementasi *site-to-site* VPN adalah:

1. Peningkatan keamanan dalam komunikasi data
2. Mempermudah dalam perluasan konektivitas jaringan komputer secara geografis (Skalabilitas)

3. Menyederhanakan topologi jaringan

3.1.2 Analisis kebutuhan sistem *site-to-site* VPN

VPN merupakan perpaduan dari teknologi *tunneling* dengan teknologi enkripsi. Teknologi *tunneling* bertugas untuk manangani dan menyediakan koneksi *point-to-point* dari sumber ke tujuannya. Sedangkan teknologi enkripsi menjamin kerahasiaan data yang berjalan di dalam *tunnel*.

Untuk membangun VPN, ada beberapa tahap yang harus dilakukan :

1. Pemilihan jenis implementasi VPN
2. Pemilihan protokol VPN
3. Pemilihan *server* VPN

3.1.3 Jenis implementasi VPN

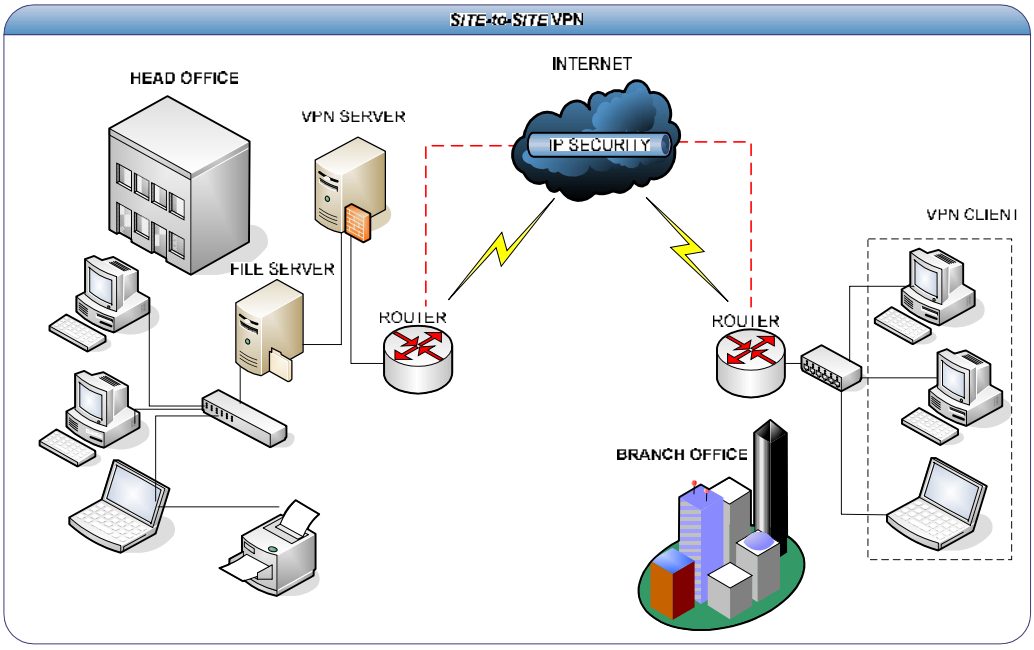
Dilihat dari jenis implementasi VPN yang ada, dalam penelitian ini termasuk dalam kategori *Site-to-site* VPN.

Site-to-site VPN merupakan jenis implementasi VPN yang menghubungkan antara dua tempat atau lebih yang letaknya berjauhan, seperti halnya menghubungkan kantor pusat dengan kantor cabang, baik kantor yang dimiliki perusahaan itu sendiri maupun kantor perusahaan mitra kerjanya.

VPN yang digunakan untuk menghubungkan kantor pusat dengan kantor cabang suatu perusahaan disebut *intranet site-to-site* VPN. Sedangkan bila VPN

digunakan untuk menghubungkan suatu perusahaan dengan perusahaan lain (misalnya mitra kerja, *supplier* atau pelanggan), implementasi ini termasuk jenis *ekstranet*.

Dalam implementasinya, untuk dapat menghubungkan kantor pusat dengan kantor cabang, pada masing-masing kantor dibutuhkan sebuah router (*gateway*), yang dalam penelitian ini digunakan mikrotik versi 2.9.27 sebagai PC router kantor cabang dan PC router sekaligus *server* VPN di kantor pusat. Berikut merupakan gambar topologi jaringan *site-to-site* VPN :



Gambar 3.1 *Site-to-site* VPN

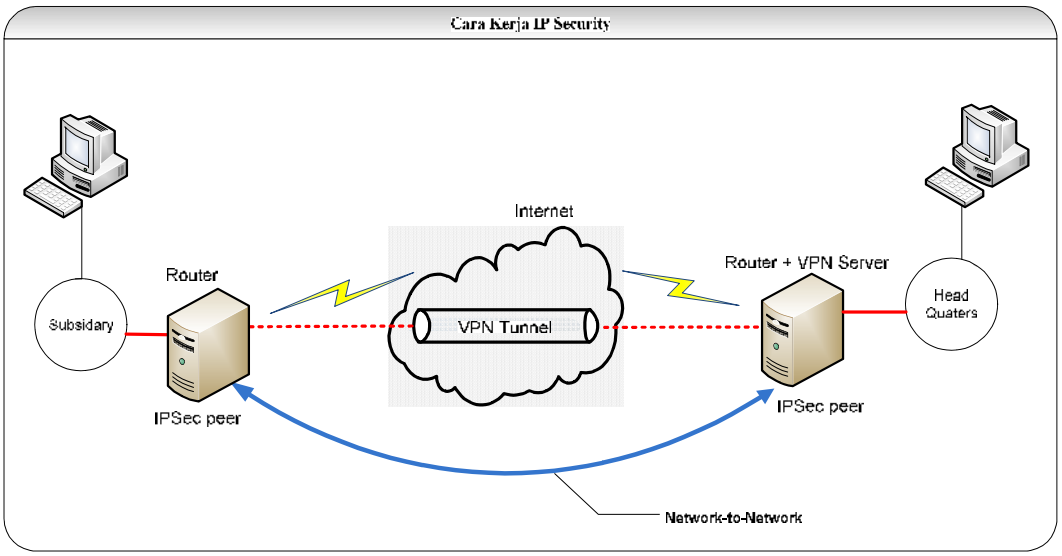
3.1.4 Protokol yang digunakan dalam VPN

Untuk membangun *site-to-site* VPN, dibutuhkan protokol yang berfungsi mengatur komunikasi diantara beberapa komputer di dalam sebuah jaringan, aturan itu termasuk di dalamnya petunjuk yang berlaku bagi cara-cara atau metode mengakses sebuah jaringan, topologi fisik, tipe-tipe kabel dan kecepatan transfer data.

Protokol yang digunakan pada VPN menekankan pada authentikasi dan enkripsi. Adanya sistem authentikasi akan mengijinkan klien dan *server* untuk menempatkan identitas orang yang berbeda di dalam jaringan secara benar. Enkripsi mengijinkan data yang dikirim dan diterima tersembunyi dari publik saat melewati jaringan publik.

Dalam penelitian ini protokol yang digunakan adalah IP Security. IPsec yang diimplementasikan kedalam *site-to-site* VPN menggunakan mekanisme *network-to-network,* sehingga perlu dilakukan konfigurasi IPsec pada masing-masing *gateway*. Untuk dapat terkoneksi, masing-masing *gateway* melakukan sinkronisasi.

Dibawah ini merupakan gambar dari cara kerja IP Security pada *site-to-site* VPN:



Gambar 3.2 Cara kerja IP Sec *Network-to-Network*

Adapun protokol yang berjalan dibelakang IPSec yaitu:

1. AH (Authentication Header), menyediakan layanan authentication (menyatakan bahwa data yang dikirim berasal dari pengirim yang benar), intregrity (keaslian data), dan replay protection (transaksi hanya dilakukan sekali, kecuali yang berwenang telah mengizinkan), juga melakukan pengamanan terhadap IP header (header compression).
2. ESP (Encapsulated Security Payload), menyediakan layanan authentication, intregity, replay protection, dan confidentiality (keamanan terjaga) terhadap data. ESP melakukan pengamanan data terhadap segala sesuatu dalam paket data setelah header.

Istilah dari IPsec mengacu pada suatu set dari mekanisme yang didesain untuk mengamankan trafik pada level IP atau pada *network layer*. Teknologi dari

IPsec ini didasari oleh teknologi modern dari kriptografi, dimana layanan keamanan yang disediakan antara lain yaitu:

1. ***Confidentiality*** :

   Untuk mejamin kerahasiaan dimana sulit bagi pihak yang tidak berwenang untuk dapat melihat atau mengerti kecuali oleh penerima yang sah bahwa data telah dikirimkan.

2. ***Integrity*** :

   Untuk menjamin bahwa data tidak berubah dalam perjalanan menuju tujuan.

3. ***Authenticity*** :

   Untuk menjamin bahwa data yang dikirimkan memang berasal dari pengirim yang benar.

4. ***Anti Reply*** :

   Untuk menjamin bahwa transaksi hanya dilakukan sekali, kecuali yang berwenang telah mengijinkan untuk mengulang transaksi.

3.1.5 Infrastruktur sistem *site-to-site* VPN

Infrastruktur sistem *site-to-site* terbagi menjadi dua macam, yaitu perangkat keras dan perangkat lunak, yang kedua bagian infrastruktur tersebut saling mendukung satu sama lain.

Dalam pembangunan *site-to-site* VPN, terdapat beberapa kebutuhan *hardware* dan *software* di sisi *server* dan *client* yang harus dipenuhi, yaitu sebagai berikut :

a. Server VPN

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

1. *Hardware*

Simulasi yang dilakukan menggunakan spesifikasi *hardware* 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. 2 buah 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. 2 buah 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

2. *Software*

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

b. *Client* VPN

Adapun spesifikasi *hardware* yang digunakan sebagai komputer *client* VPN dalam simulasi yang dilakukan memiliki spesifikasi sebagai berikut :

1. *Hardware*

Dalam penelitian ini, simulasi yang dilakukan menggunakan spesifikasi *hardware* 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 *client* VPN adalah dengan spesifikasi minimum sebagai berikut :

a. Prosesor : P II 500 MHz

b. Monitor : Flat 15" Resolusi 1024x768

c. RAM : 64 MB

d. VGA : Onboard

e. NIC : 10/100

f. HDD : 40 GB P-ATA atau S-ATA

g. Keyboard

2. *Software*

Spesifikasi perangkat lunak yang digunakan pada komputer pengguna sistem VPN adalah Microsoft Windows 7 Ultimate dan aplikasi VPN *client* yang merupakan fitur dari sistem operasi Windows.

3.1.6 Analisis Pengguna

Sistem *site-to-site* VPN yang di bangun akan digunakan untuk pengguna yang memiliki kualifikasi sebagai berikut :

Tabel 3.1 Karakteristik Pengguna

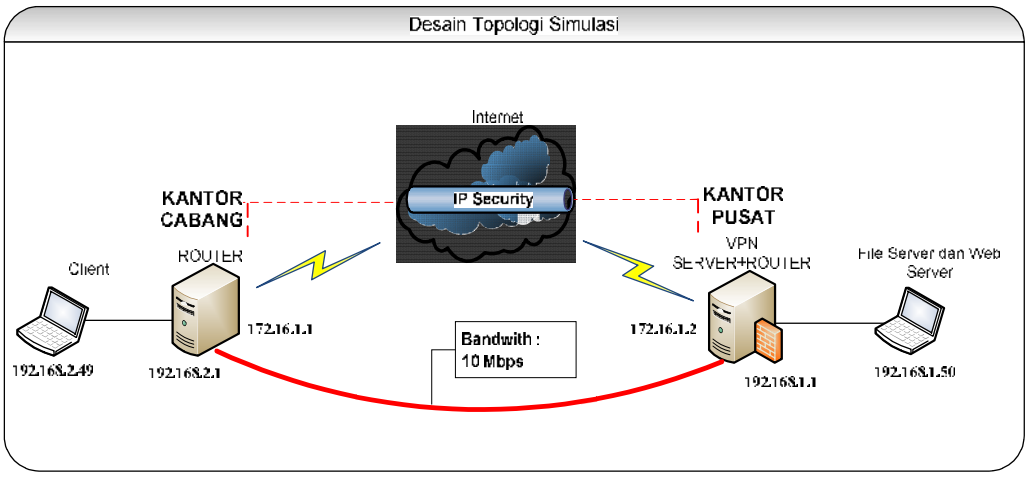
Nama Pengguna	Kualifikasi
Administrator Jaringan	Kualifikasi yang harus dimiliki administrator jaringan yaitu memiliki keahlian di bidang jaringan komputer, menangani LAN, mengkonfigurasi jaringan (khususnya VPN)
Karyawan	Kualifikasi yang harus dimiliki karyawan yaitu memiliki kemampuan dasar di bidang komputer, dapat mengoperasikan Sistem Operasi Windows XP dan pernah menggunakan aplikasi jaringan khususnya yang berkaitan dengan *internet*.

3.2 Perancangan Sistem

Pada bagian ini akan dibahas mengenai perancangan sistem *site-to-site* VPN, yang meliputi perancangan infrastruktur VPN atau topologi jaringan, instalasi dan konfigurasi perangkat lunak.

3.3 Arsitektur simulasi

Dalam simulasi sistem *site-to-site* VPN akan dilakukan melalui jaringan LAN, dan adapun desain topologi jaringan yang digunakan adalah sebagai berikut :



Gambar 3.3 Desain Topologi Simulasi

Perangkat pendukung pada simulasi *site-to-site* VPN terdiri dari beberapa *hardware* dan *software* yang tertera dalam tabel di bawah ini :

Tabel 3.2 Perangkat pendukung infrastruktur simulasi

Hardware	PC Sebagai *Server* VPN dan Router
	PC Sebagai Router
	Laptop sebagai File S*erver*
	Laptop sebagai *Client* VPN
	Kabel UTP category 5e dan konektor RJ-45.
Software	Mikrotik Router OS v. 2.9.27 sebagai *server* VPN dan Router
	Windows 7 ultimate sebagai *server* dan Windows XP SP 3 sebagai *client*
	Wireshark –win32- 1.2.9 sebagai *protocol analyzer*
	Xampp for windows 1.6.5 (Web *server*)
	File zilla (FTP *Server*)
	RaidenDNSD 1.3.17 (DNS *server*)

Selain kebutuhan *hardware* dan *software* yang tertera pada tabel di atas, terdapat pembagian alokasi IP address yang akan digunakan pada saat simulasi. Pada server VPN telah dilakukan konfigurasi DHCP, sehingga IP Address *client* akan bersifat dinamis. Dibawah ini merupakan tabel alokasi IP Address pada saat simulasi:

Tabel 3.3 Alokasi IP address untuk Router

Device	IP Address	Interface
PC sebagai VPN router	192.168.2.1	Lokal
	172.16.1.1	Publik
Laptop sebagai VPN *client*	192.167.1.50	Lokal

Tabel 3.4 Alokasi IP address untuk *Server* VPN dan File *Server*

Device	IP Address	Interface
PC sebagai VPN *Server* + router	192.168.1.1	Lokal
	172.16.1.2	Publik
Laptop sebagai FTP *server* dan web *server*	192.168.1.50	Lokal

Dikarenakan simulasi ini berjalan pada LAN, maka diperlukan pengaturan bandwidth agar simulasi yang dilakukan dapat merepresentasikan kondisi ideal *internet*. Untuk merepresentasikan kondisi ideal tersebut, dalam penelitian ini digunakan *bandwith limiter* dan bandwidth yang di gunakan adalah sebesar 10 Mbps.

Selanjutnya, untuk skenario pengujian dan analisis perbandingan data dari simulasi *site-to-site* VPN, akan di jelaskan pada bagian pengujian sistem yang tertera pada Bab IV.

3.4 Konfigurasi sistem *site-to-site* VPN

Konfigurasi VPN *server* dan *client* adalah tahap dimana dilakukannya pengaturan-pengaturan parameter yang terdapat pada sebuah perangkat lunak.

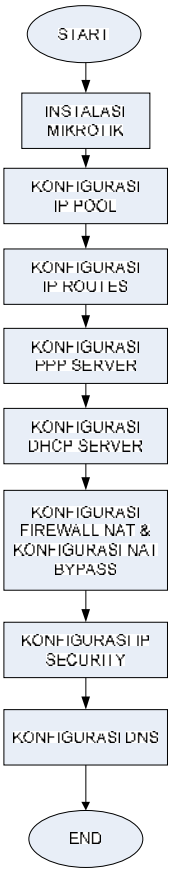
Adapun parameter-parameter yang akan kita setting pada komputer *server,* router dan *client* adalah :

1. Komputer yang digunakan sebagai *server* VPN dan router

   Tahapan konfigurasi yang harus di lakukan 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

   Untuk lebih memperjelas, tahap konfigurasi akan ditampilkan dengan Flowchart seperti pada gambar dibawah ini :



Gambar 3.4 Flowchart Konfigurasi Pada Sisi Server

2. Komputer yang digunakan sebagai router

Tahapan konfigurasi yang harus di lakukan dalam tahap perancangan server adalah:

a. Tahap Instalasi mikrotik

b. Tahap konfigurasi IP Pool

c. Tahap konfigurasi IP Routes

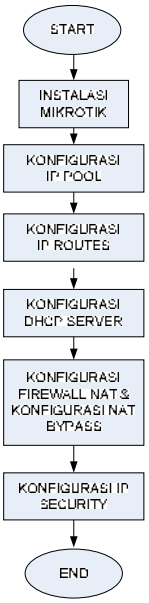
d. Tahap konfigurasi DHCP *server*

e. Tahap konfigurasi firewall NAT Masquerade dan NAT bypass

f. Tahap konfigurasi IP security

g. Tahap konfigurasi DNS

Untuk lebih memperjelas, tahap konfigurasi akan ditampilkan dengan Flowchart seperti pada gambar dibawah ini :



Gambar 3.5 Flowchart Konfigurasi Di Router

3. Komputer *client* VPN

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

a. Tahap konfigurasi akses VPN.

b. Tahap *Connecting* VPN.

3.5 Perancangan dan konfigurasi *Server* VPN

3.5.1 Instalasi Mikrotik V 2.9.27

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.

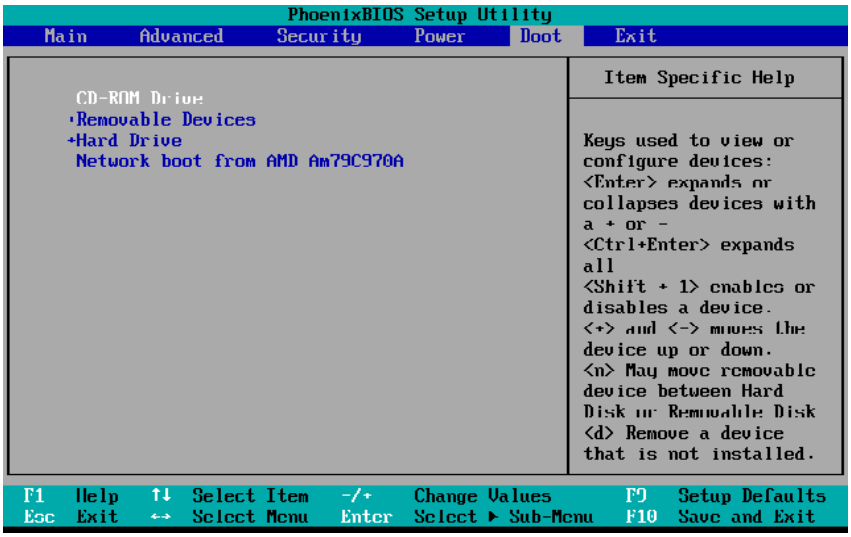
Server VPN yang digunakana adalah mikrotik routerOS versi 2.9.27. Mikrotik routerOS adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer biasa menjadi router network yang mencakup berbagai fitur yang dibuat untuk ip network dan jaringan wireless.

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, dengan spesifikasi seperti yang telah disebutkan di bab sebelummnya
b. Menyiapkan CD instaler Mikrotik yang bootable.

   Menyiapkan CD instaler Mikrotik *Router*OS yang bootable yang file isonya di download dari Internet dan membakarnya kedalam CD dengan aplikasi Nero.
c. Konfigurasi BIOS pada PC.

   Mengatur konfigurasi BIOS agar boot sequence mengarah ke CD,



Gambar 3.6 Konfigurasi BIOS

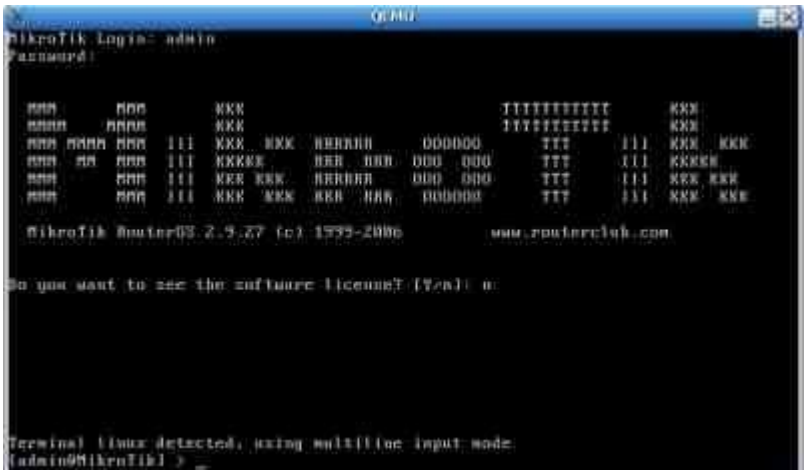
setelah itu menyimpannya dengan menekan F10 lau tekan OK. Sistem akan *restart* unutk melanjutkan proses instalasi sampai muncul layar seperti ni.

Sebelum proses instalasi dimulai komputer harus memiliki ethernet card minimal dua buah (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 3.7 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. Selanjutanya reboot PC Router mikrotik dan mikrotik telah selesai di install.



Gambar 3.8 Tampilan Log in Mikrotik

3.5.2 Konfigurasi mikrotik sebagai *server* VPN

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

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

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

   Sampai langkah ini kita 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 kita inginkan.

   Dalam simulasi ini, login default kita ganti dengan “server” dan password kita ganti dengan “icky”.

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

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

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

4. Selanjutnya kita 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 kita masuk ke tahap pemberian IP address pada *interface* Mikrotik.

   Adapun parameter-paremeter yang akan kita setting untuk interface :

   a. ether1 IP address: 192.168.1.1

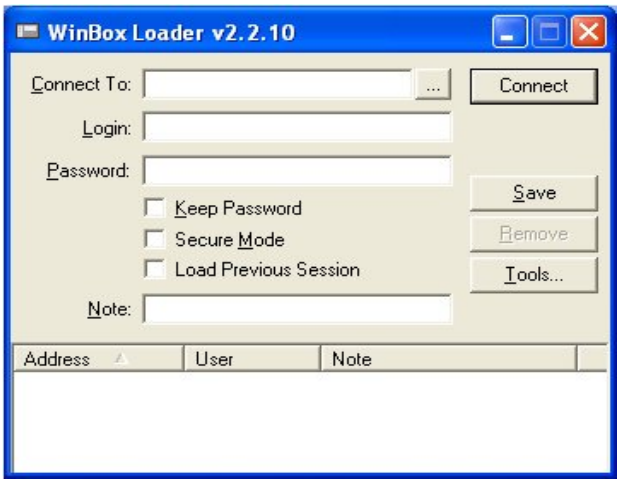
   b. ether2 IP address: 172.16.1.2

```
[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 kita 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*).



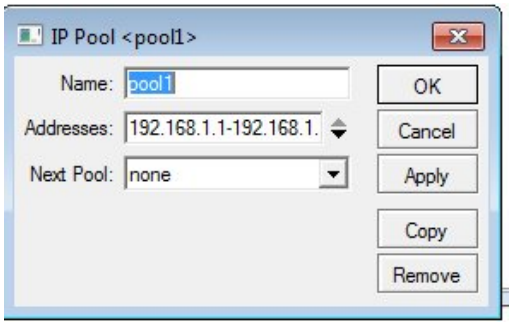
Gambar 3.9 WinBox Loader

Selanjutnya kita akan membuat server VPN dengan menggunakan fitur PPP. Adapun konfigurasi yang dilakukan adalah sebagai berikut :

a. Konfigurasi IP Pool

Untuk mengalokasikan sejumlah IP address yang akan digunakan oleh *Client* VPN digunakan IP Pool. Dengan IP Pool pengalokasian IP address menjadi lebih efisien, karena kita dapat memberi batasan IP yang dapat mengakses *server* VPN.

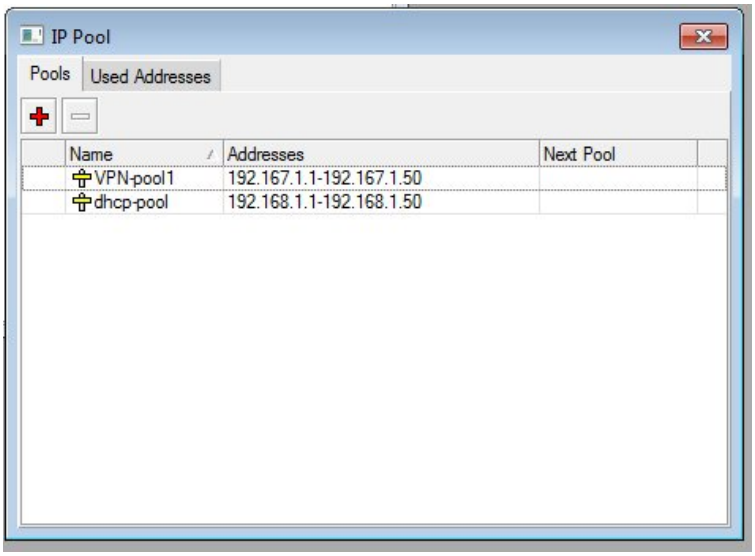
Dalam penelitian ini, *range* IP yang di alokasikan adalah 192.168.1.1-192.168.1.50. Di bawah ini merupakan tampilan dari *interface* IP Pool.



Gambar 3.10 Interface IP Pool

Pembuatan IP Pool menggunakan *console* :

```
[admin@vpn] > ip pool add name=pool1 next-pool=none
ranges=192.168.1.1-192.168.1.50
```



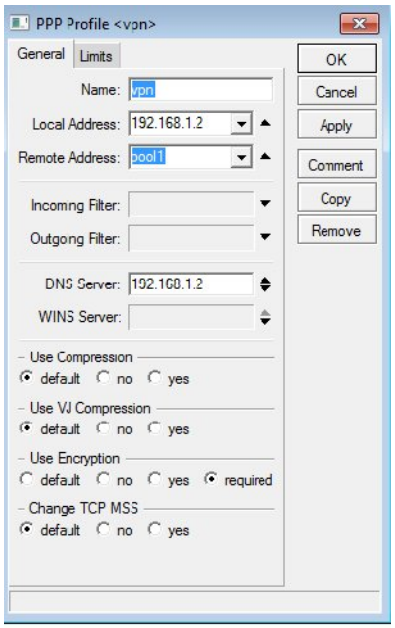
Gambar 3.11 IP address untuk *client* VPN

Menampilkan IP address untuk client di IP Pool menggunakan *console* :

```
[admin@MikroTik] > ip pool print
```

b. Konfigurasi profile PPP

Local Address adalah IP address yang digunakan sebagai VPN Gateway oleh Mikrotik. *Remote Address* adalah IP Address yang akan diberikan kepada masing-masing VPN Client dan IP Address inilah yang dikenali dan berkomunikasi dengan PC yang lain.



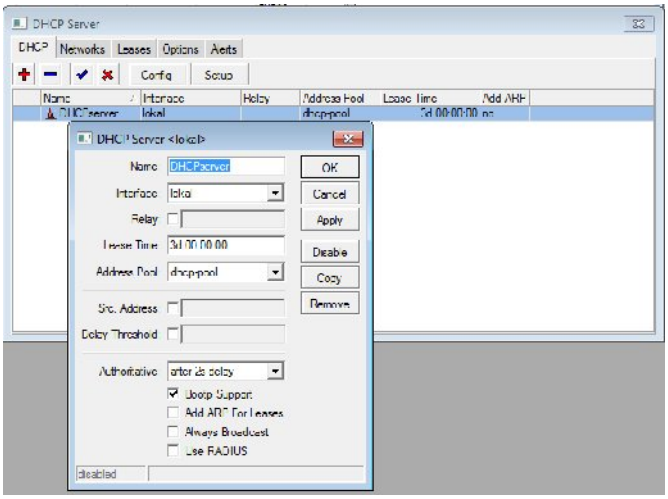
Gambar 3.12 Konfigurasi profile PPTP

Konfigurasi profile PPP menggunakan *console* :

```
[admin@MikroTik] > ppp profile add name=profile1 local-
address=192.168.1.2 remote-address=pool1 use-
compression=default use-vj-compression=default  use-
encryption=yes change-tcp-mss=default
```

c. Konfigurasi DHCP server

Dynamic Host Configuration Protocol (DCHP) adalah protokol yang berbasis arsitektur *client/server* yang dipakai untuk memudahkan pengalokasian alamat IP dalam satu jaringan. Sebuah jaringan lokal yang tidak menggunakan DHCP harus memberikan alamat IP kepada semua komputer secara manual. Jika DHCP dipasang di jaringan lokal, maka semua komputer yang tersambung di jaringan akan mendapatkan alamat IP secara otomatis dari *server* DHCP. Selain alamat IP, banyak parameter jaringan yang dapat diberikan oleh DHCP, seperti *default gateway* dan DNS server.



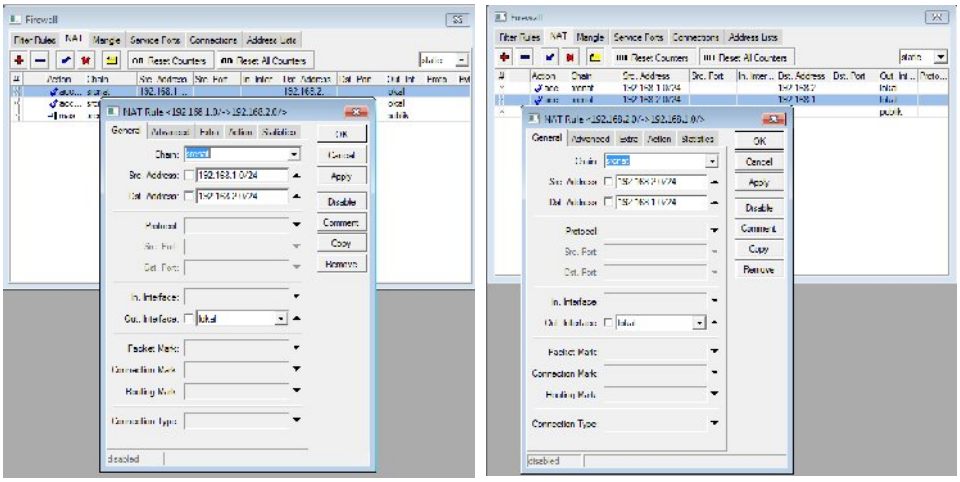
Gambar 3.13 Konfigurasi DHCP server

konfigurasi DHCP *server* menggunakan *console* :

```
 [admin@vpn] > ip dhcp-server add name=DHCPserver
interface=local lease-time=no address-pool=dhcp-pool
authoritative=after-2sec-delay bootp-support=dynamic
```

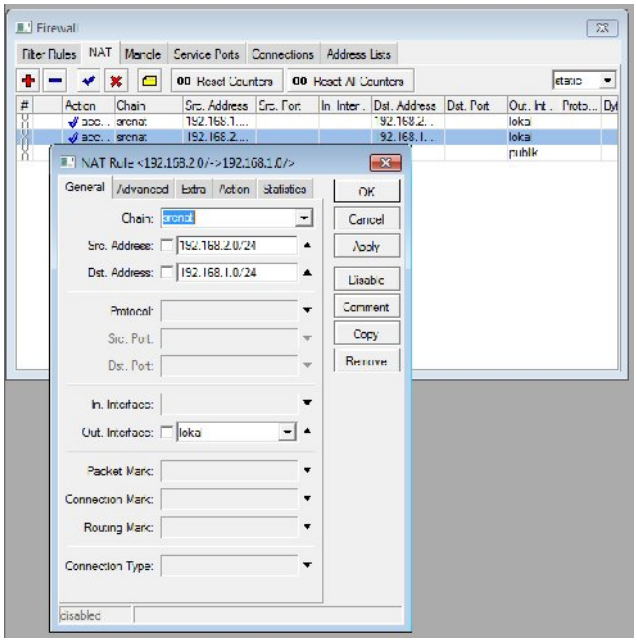
d. Konfigurasi *Firewall* NAT *Masqueurade* dan NAT *Bypass*

Sebelum masuk ke tahap aktivasi IP Sec, terlebih dahulu harus kita melakukan konfigurasi *firewall* NAT *masqueurade*. Didalam konfigurasi NAT *masqueurade* terdapat dua buah kondisi yang harus kita *setting* yaitu NAT masqueurade untuk *server* dan router. Adapun proses konfigurasi dapat dilihat pada gambar dibawah ini :



Gambar 3.14 Konfigurasi Firewall NAT Masqueurade

Setelah melakukan konfigurasi pada *firewall* NAT *masqueurade*, selanjutnya kita akan melakukan konfigurasi untuk NAT bypass yang ditunjukkan pada gambar dibawah ini :



Gambar 3.15 Konfigurasi firewall NAT bypass

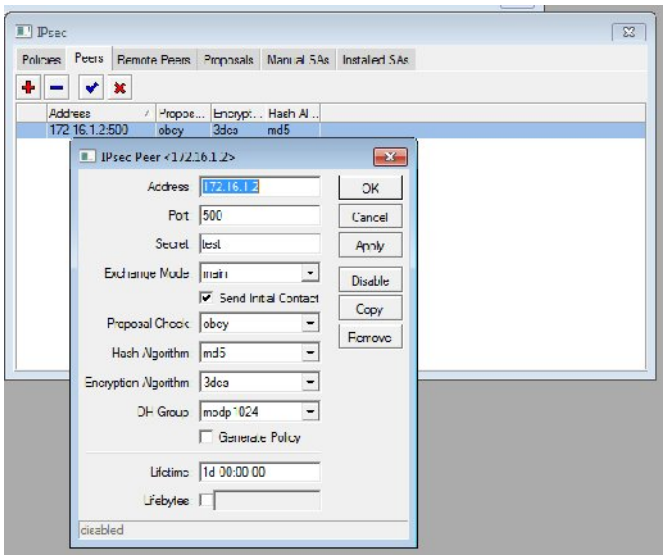
konfigurasi Firewall NAT *Masqueurade* dan NAT *bypass* menggunakan *console* :

```
[admin@vpn] > Add chain=scr out interface=lokal action
masqueurade
[admin@vpn] > Add chain=scrnat action=accept src-
address=192.168.2.0/24 dst-address=192.168.1.0/24
```

e. Konfigurasi IP Security

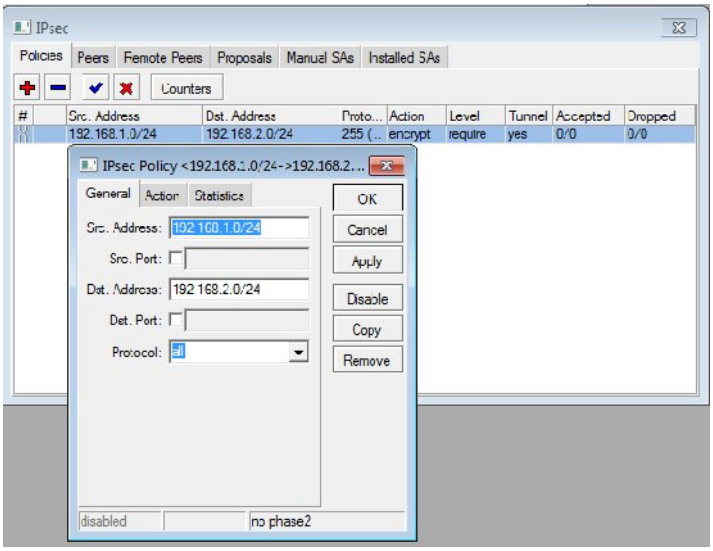
Setelah Tahap konfigurasi IP Routes dan sinkronisasi dengan router selesai, selanjutnya kita akan mengaktifkan modul IPSec. Adapun konfigurasi yang kita lakukan adalah sebagai berikut :

Pilih tab peers kemudian inputkan Ip address: 172.16.1.2 dan pilih algoritma autentikasinya dengan “MD5” serta algoritma enkripsinya dengan “3DES”. Untuk lebih jelasnya dapat dilihat pada gambar dibawah ini :



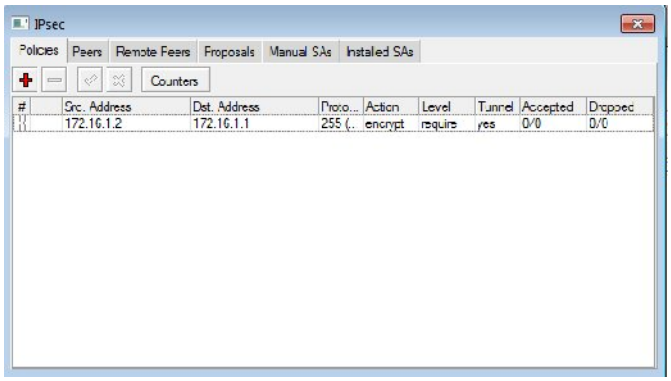
Gambar 3.16 Konfigurasi IPsec peers

Setelah itu pilih tab policies pada menu IPsec dan yang terdapat pada *window* winbox, kemudian inputkan IP Address *source* (sumber) dengan IP lokal : 192.168.1.0/24 dan *destination* (tujuan) dengan IP : 192.168.2.0/24 seperti yang tertera pada gambar di bawah ini :



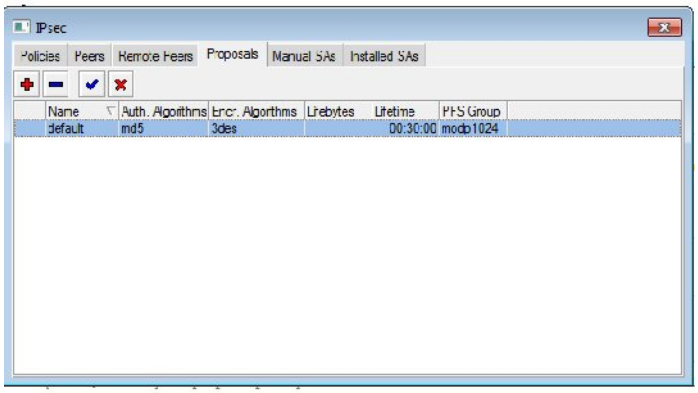
Gambar 3.17 Interface New Ipsec Policy

Setelah kita tekan “OK”, maka akan tampil *interface* IPsec seperti dibawah ini :



Gambar 3.18 Aktivasi modul IP Security pada tab policies

Selanjutnya setelah *setting* policies IP sec, secara otomatis akan terbentuk proposal yang didalamnya berisi algoritma untuk autentikasi enkripsi. Dalam penelitian ini kita menggunakan “MD5” sebagai algoritma autentikasinya dan “3DES” sebagai algoritma enkripsinya.



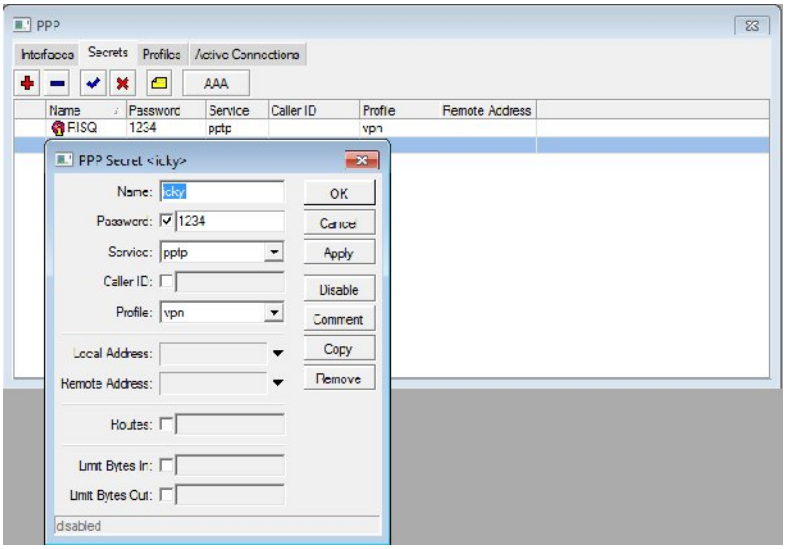
Gambar 3.19 Interface Proposal Ipsec

Di bawah ini merupakan konfigurasi untuk aktivasi modul IPSec melalui *console*:

```
[admin@vpn] /Ip ipsec peer add address = 172.16.1.2/32:500
secret=”test”
[admin@vpn] /Ip ipsec policy add src-address=192.168.1.0/24 dst-
address=192.168.2.0 /24 \sa-src-address=172.16.1.2 sa-dst-
address=172.16.1.1 \ action=encrypt tunnel=yes proposal=default
```

f. Membuat *Authenticated User* / *client* VPN.

Untuk membuat ***Authenticated User*** pilih tab **“SECREET”** pada menu **PPP**. Setting ***Username, Password, Service*** **dan** ***Profile*** seperti gambar dibawah ini :



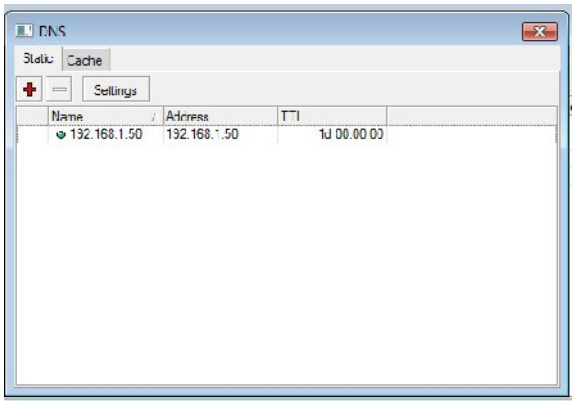
Gambar 3.20 Membuat *Authenticated User*

Membuat *Authenticated User* menggunakan *console* diterminal

```
[admin@MikroTik] > ppp secret add name=icky password=1234
service=pptp profile=vpn disabled=no
```

g. Konfigurasi *Domain Name System* (DNS) untuk *server*

DNS merupakan suatu metode penterjemahan IP menjadi sebuah nama atau sebaliknya. Dibawah ini merupakan konfigurasi DNS pada *server* VPN :



Gambar 3.21 Konfigurasi DNS

Konfigurasi DNS menggunakan *console* diterminal :

```
/ip dns set primary-dns=192.168.1.50
```

3.6 Perancangan dan konfigurasi Router

3.6.1 Instalasi Mikrotik V 2.9.27

Untuk proses instalasi mikrotik, langkah-langkahnya dapat dilihat pada instalasi mikrotik untuk server VPN di bagian yang telah di bahas sebelumnya.

3.6.2 Konfigurasi Mikrotik sebagai router

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

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

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

Sampai langkah ini kita 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 login dengan "router" dan password default sesuai dengan yang kita inginkan.

   Dalam simulasi ini, password default kita ganti dengan "icky".

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

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

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

4. Selanjutnya kita 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 kita masuk ke tahap pemberian IP address pada *interface* Mikrotik.

   Adapun parameter-paremeter yang akan kita setting untuk interface :

   a. ether1 IP address: 192.168.2.1

   b. ether2 IP address: 172.16.1.1

```
[admin@vpn] > ip address add address=192.168.2.1 /
netmask=255.255.255.0 interface=ether1
[admin@vpn] > ip address add address=172.16.1.1 /
netmask=255.255.255.0 interface=ether2
```

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

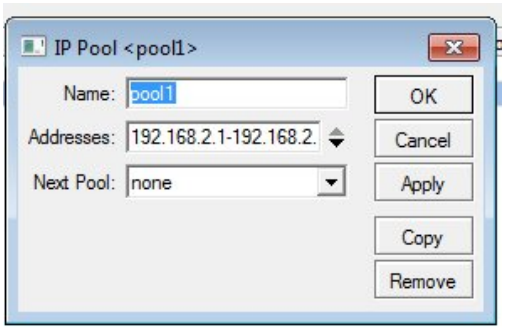
```
[admin@vpn] >ip address print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS  NETWORK  BROADCAST  INTERFACE
0  192.168.2.1/24  192.168.2.0   192.168.2.255  ether1
1  172.16.1.1/24   172.16.1.0    172.16.1.255  ether2
[admin@vpn] >
```

Selanjutnya dikarenakan mikrotik di sisi ini hanya digunakan sebagai router, maka tahapan yang dilakukan adalah :

a. Konfigurasi IP Pool

Untuk mengalokasikan sejumlah IP address yang akan digunakan oleh *Client* VPN digunakan IP Pool. Dengan IP Pool pengalokasian IP address menjadi lebih efisien, karena kita dapat memberi batasan IP yang dapat mengakses *server* VPN.

Dalam penelitian ini, *range* IP yang di alokasikan adalah 192.168.2.1-192.168.2.50. Di bawah ini merupakan tampilan dari interface IP Pool.



Gambar 3.22 Interface IP Pool

Konfigurasi IP Pool menggunakan *console* :

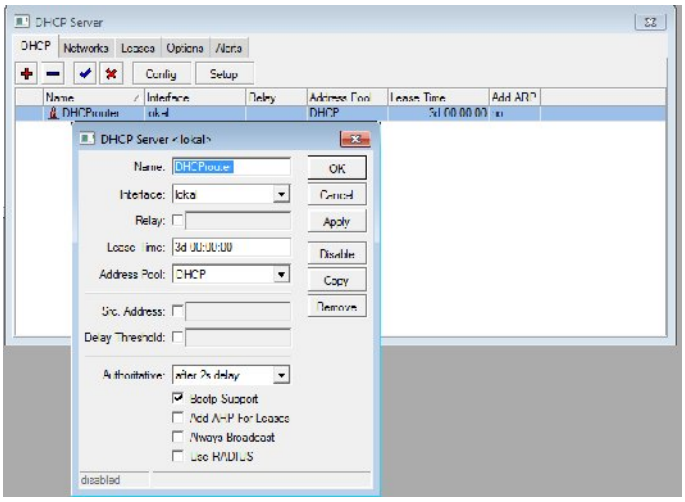
```
[admin@vpn] > ip pool add name=pool1 next-pool=none
ranges=192.168.2.1-192.168.2.50
```

Menampilkan IP address untuk client di IP Pool menggunakan *console* :

```
[admin@MikroTik] > ip pool print
```

b. Konfigurasi DHCP *server*

Dynamic Host Configuration Protocol (DCHP) adalah protokol yang berbasis arsitektur *client/server* yang dipakai untuk memudahkan pengalokasian alamat IP dalam satu jaringan. Sebuah jaringan lokal yang tidak menggunakan DHCP harus memberikan alamat IP kepada semua komputer secara manual. Jika DHCP dipasang di jaringan lokal, maka semua komputer yang tersambung di jaringan akan mendapatkan alamat IP secara otomatis dari *server* DHCP. Selain alamat IP, banyak parameter jaringan yang dapat diberikan oleh DHCP, seperti *default gateway* dan DNS server.



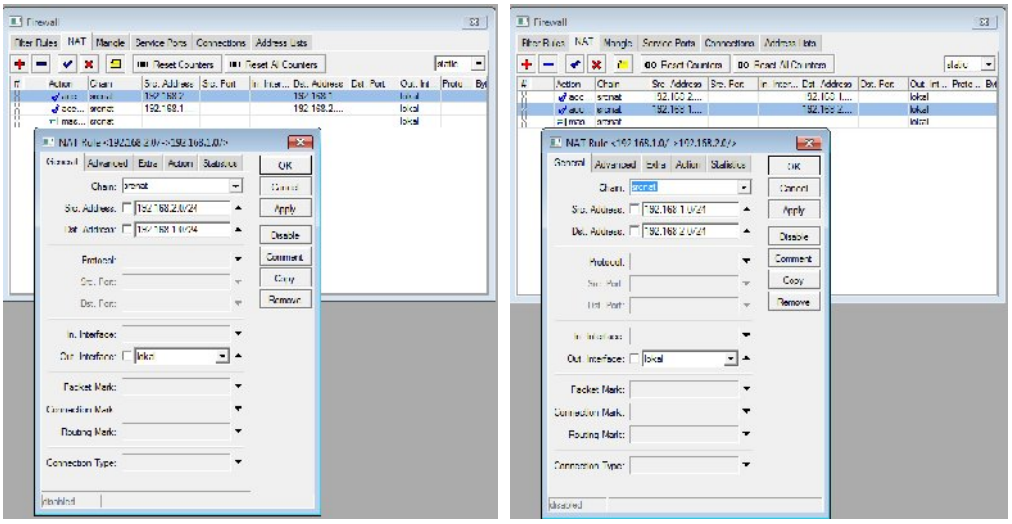
Gambar 3.23 Konfigurasi DHCP *server*

konfigurasi DHCP *server* menggunakan *console* :

```
[admin@vpn] > ip dhcp-server add name=DHCProuter interface=local lease-time=no
address-pool=dhcp-pool authoritative=after-2sec-delay bootp-support=dynamic
```

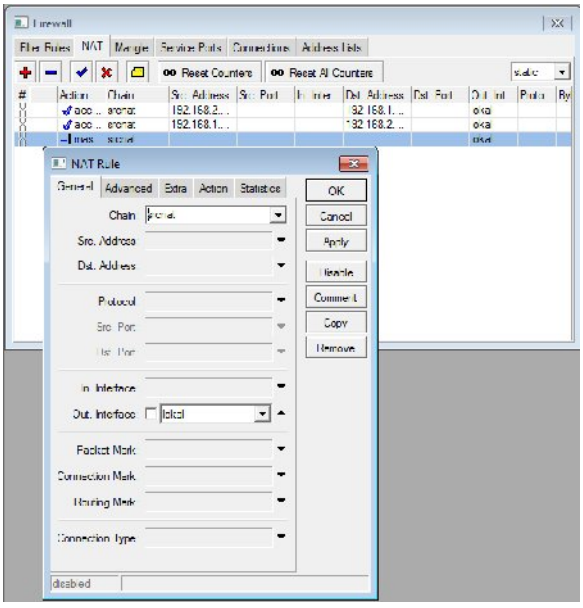
c. Konfigurasi Firewall NAT Masqueurade dan NAT Bypass

Sebelum masuk ke tahap aktivasi IPSec, terlebih dahulu harus kita melakukan konfigurasi *firewall* NAT *masqueurade*. Didalam konfigurasi NAT *masqueurade* terdapat dua buah kondisi yang harus kita *setting* yaitu NAT *masqueurade* untuk *server* dan router. Adapun proses konfigurasi dapat dilihat pada gambar dibawah ini :



Gambar 3.24 Konfigurasi Firewall NAT *Masqueurade*

Setelah melakukan onfigurasi pada *firewall* NAT *masqueurade*, selanjutnya kita akan melakukan konfigurasi untuk NAT *bypass* yang ditunjukkan pada gambar dibawah ini :



Gambar 3.25 Konfigurasi firewall NAT *bypass*

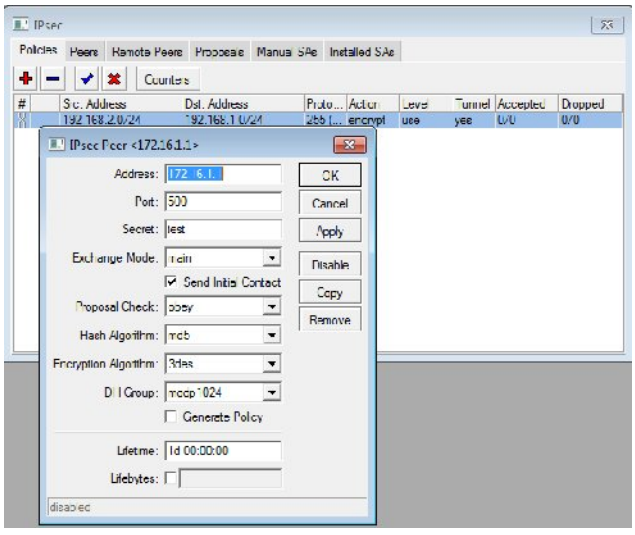
konfigurasi *Firewall* NAT *Masqueurade* dan NAT *bypass* menggunakan *console* :

```
[admin@vpn] > Add chain=scr out interface=lokal action masqueurade
[admin@vpn] > Add chain=scrnat action=accept src-address=192.168.1.0/24 dst-
address=192.168.1.0/24
```

d. Konfigurasi IP Security

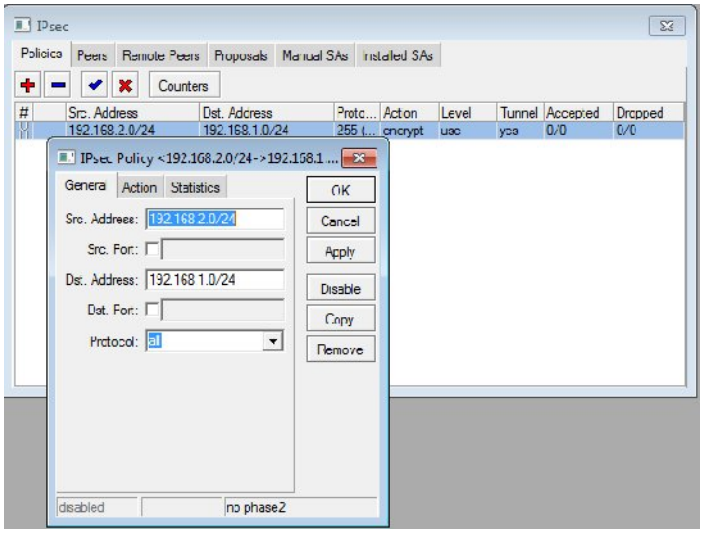
Setelah Tahap konfigurasi IP Routes dan sinkronisasi dengan router selesai, selanjutnya kita akan mengaktifkan modul IP Security. Adapun konfigurasi yang kita lakukan adalah sebagai berikut :

Pilih tab peers kemudian inputkan Ip address: 172.16.1.1 dan pilih algoritma autentikasinya dengan “MD5” serta algoritma enkripsinya dengan “3DES”. Untuk lebih jelasnya dapat dilihat pada gambar dibawah ini :



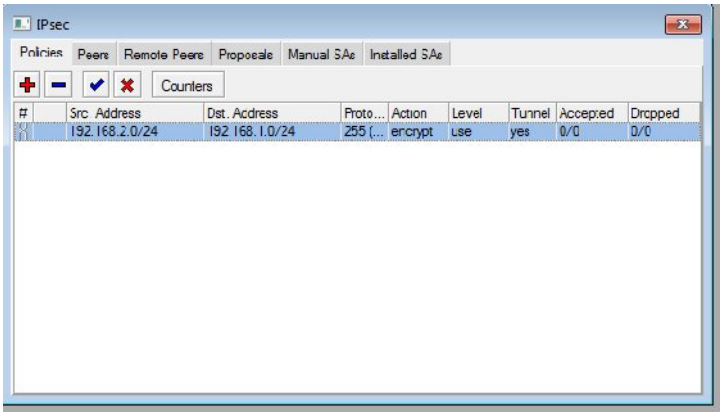
Gambar 3.26 Konfigurasi IPsec *peers*

Setelah itu pilih tab policies pada menu IPsec dan yang terdapat pada *window* winbox, kemudian inputkan IP Address *source* (sumber) dengan IP lokal : 192.168.2.0/24 dan *destination* (tujuan) dengan IP : 192.168.1.0/24 seperti yang tertera pada gambar di bawah ini :



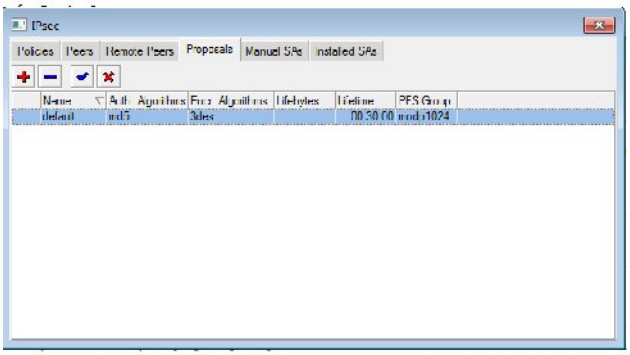
Gambar 3.26 *Interface* New Ipsec Policy

Setelah kita tekan “OK”, maka akan tampil *interface* IPsec seperti dibawah ini :



Gambar 3.28 Aktivasi modul IP Security pada tab policies

Selanjutnya setelah setting policies IP sec, secara otomatis akan terbentuk proposal yang didalamnya berisi algoritma untuk autentikasi enkripsi. Dalam penelitian ini kita menggunakan “MD5” sebagai algoritma autentikasinya dan “3DES” sebagai algoritma enkripsinya.



Gambar 3.29 *Interface* Proposal Ipsec

Di bawah ini merupakan konfigurasi untuk aktivasi modul IPSec melalui *console*:

```
[admin@vpn] /Ip ipsec peer add address = 172.16.1.1/32:500 secret=”test”
[admin@vpn] /Ip ipsec policy add src-address=192.168.2.0/24 dst-address=192.168.1.0 /24
\sa-src-address=172.16.1.1 sa-dst-address=172.16.1.2 \ action=encrypt tunnel=yes
proposal=default
```

Setelah selesai melakukan konfigurasi di sisi *server* dan *router* mikrotik, langkah terakhir adalah melakukan konfigurasi di sisi *client.* Setelah melakukan konfigurasi di sisi *client,* selanjutnya akan masuk 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*
   b. Melakukan *download* file dari file *server* menggunakan FTP *service*
2) Menguji kehandalan VPN:
   a. Melakukan *download* file melalui VPN, kemudian melakukan monitoring data menggunakan wireshark
   b. Melakukan *download* file tanpa VPN, kemudian melakukan monitoring data menggunakan wireshark
   c. Menganalisis perbandingan data layanan VPN dengan tanpa VPN