BAB IV

RANCANGAN SISTEM JARINGAN USULAN

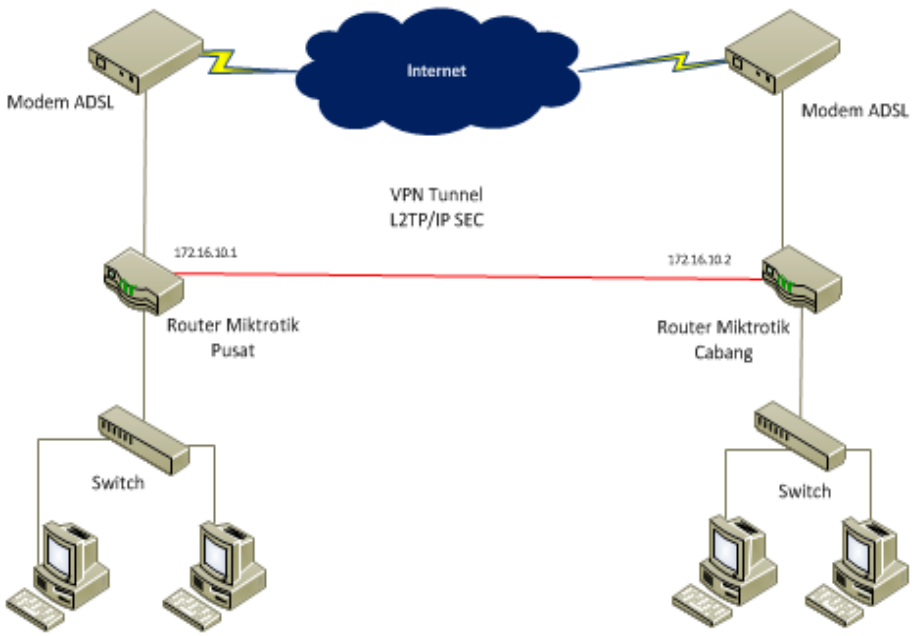
4.1. Manajemen Jaringan Usulan

Setelah penulis menganalisa sistem jaringan berjalan pada PT. Trixten Global internasional, maka penulis mengusulkan sebuah jaringan menggunakan VPN (*Virtual Private Network*) dengan metode L2TP dan IPSec untuk menghubungkan kantor pusat dengan cabang. Dan di fungsikan untuk menjembatani antara kantor dan karyawan-karyawan yang sering bepergian (*mobile workers*) dengan memanfaatkan koneksi *internet* yang dimiliki tersebut.

Dengan menggunakan *router* Mikrotik yang sudah ada, kemudian dikonfigurasi untuk menerapkan sistem jaringan VPN. Untuk kantor pusat dikonfigurasi VPN *server* dengan metode L2TP/IPSec, sedangkan kantor cabang L2TP/IPSec *Client*. Dengan ini antara kantor pusat, kantor cabang dan *remote client* akan lebih mudah untuk melakukan komunikasi, pengiriman data perusahaan serta memonitoring jaringan akan lebih aman.

4.1.1. Topologi Jaringan

Dalam mengusulkan topologi jaringan yang akan diimplementasikan pada perusahaan, penulis tidak akan merubah bentuk topologi yang sudah ada pada PT. Trixten Global Internasional, hal ini karena bentuk topologi yang ada sekarang sudah sangat baik. Topologi jaringan kantor pusat dan cabang menggunakan topologi *star*. Penulis mengusulkan untuk menggunakan VPN (*Virtual Private Network*) untuk berkomunikasi atau pertukaran data antar kantor menjadi lebih aman.

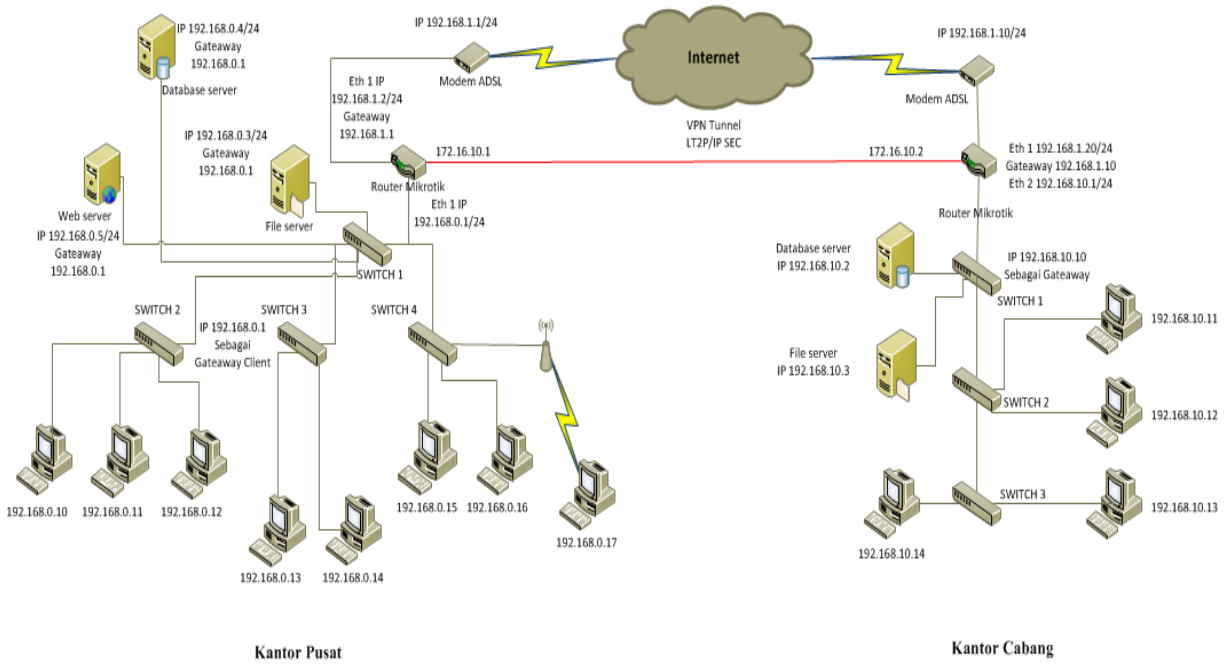


Gambar IV.1

Topologi Jaringan Usulan

4.1.2. Skema Jaringan

Pada skema jaringan usulan ini penulis menggambarkan secara detail dalam *IP Address* hanya tidak meletakkan seluruh perangkat komputer. Untuk simulasi implementasi jaringan penulis menggunakan *software Graphical Network Simulator* dan *VirtualBox*. Karena jaringan pada PT. Trixten Global Internasional menggunakan jenis *router Mikrotik router OS* dan pada kantor cabang *Mikrotik Router Board*. Dalam implementasi ini dibutuhkan sebuah *router* untuk dapat menghubungkan antara kantor pusat, kantor cabang dan akses *remote client* untuk membuat jaringan *virtual private network* (VPN), dimana kantor pusat sebagai *server* dan kantor cabang sebagai *client*. Sedangkan untuk *remote access* atau untuk *client* yang berada di luar kantor dapat melakukan koneksi VPN dengan setingan yang terdapat pada perangkat yang digunakan.



Gambar IV.2

Skema Jaringan Usulan

4.1.3. Keamanan Jaringan

Untuk keamanan jaringan yang diterapkan pada PT. Trixten Global Internasional menurut penulis sudah cukup bagus. Dengan memanfaatkan *software* anti virus dan membangun *firewall* pada konfigurasi *router*.

Sedangkan keamanan dalam jaringan usulan ini dengan sistem VPN L2TP/IPSec. VPN merupakan suatu metode pengamanan dengan membentuk koneksi *logical* antar beberapa *node* dalam jaringan yang bersifat *public*. Koneksi yang dibentuk dalam VPN merupakan koneksi *virtual* dalam bentuk *tunnel* dan bersifat *private* dengan adanya fitur *authentication* serta *policy-policy* yang dibentuk oleh setiap *router* yang terlibat. Dan IPSec (*Internet Protocol Security*) menyediakan layanan-layanan keamanan tersebut dengan menggunakan sebuah metode pengamanan yang bernama *Internet Key Exchange* (IKE). IKE bertugas

untuk menangani protokol yang bernegosiasi dan algoritma pengamanan yang diciptakan berdasarkan dari *policy* yang diterapkan.

IPSec mendukung dua buah sesi komunikasi keamanan, yaitu sebagai berikut:

1. Protokol *Authentication Header* (AH), menawarkan *autentikasi* pengguna dan perlindungan dari beberapa serangan (umumnya serangan *man in the middle*), dan juga menyediakan fungsi autentikasi terhadap data serta integritas terhadap data. Protokol ini mengizinkan penerima untuk merasa yakin bahwa identitas pengirim adalah benar adanya, dan data pun tidak dimodifikasi selama transmisi.
2. Protokol *Encapsulating Security Payload* (ESP), Protokol ini melakukan enkapsulasi serta enkripsi terhadap data pengguna untuk meningkatkan kerahasiaan data. ESP juga dapat memiliki skema autentikasi dan perlindungan dari beberapa serangan dan dapat digunakan secara sendirian atau bersamaan dengan *Authentication Header*.

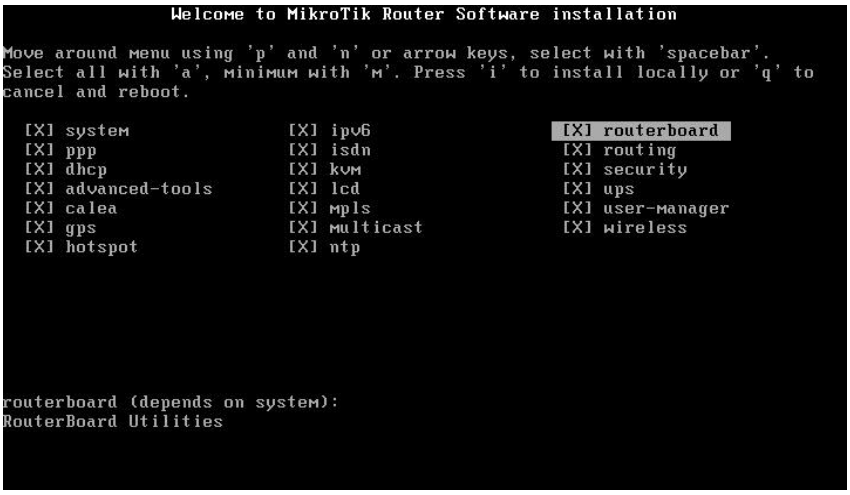
4.1.4. Rancangan Aplikasi

Dalam rancangan aplikasi penulis merancang dan mengimplementasikan suatu jaringan VPN dengan metode L2TP/IPSec untuk menghubungkan antara kantor pusat dan kantor cabang, sehingga dalam pertukaran data akan lebih cepat dan aman.

Tahapan konfigurasi yang harus dilakukan sebagai berikut:

1. Instalasi Mikrotik Router OS

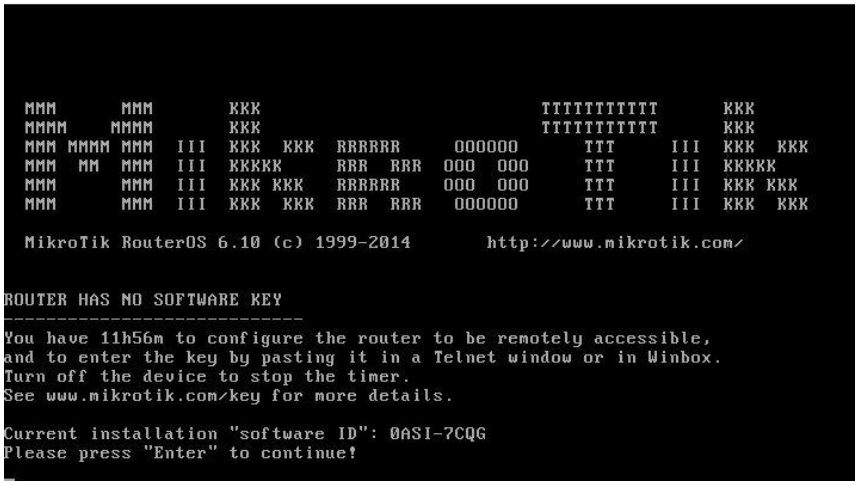
Setting BIOS komputer *server* dan atur booting agar CD/DVD bisa terdeteksi sistem komputer. Kemudian siapkan file instalasi Mikrotik, dan tunggu sampai muncul tampilan seperti dibawah.



Gambar IV.3

Tampilan Instalasi Mikrotik

Lakukan proses instalasi Mikrotik dengan memilih (c*heck*) semua pilihan yang ada dengan tombol **'a'**. Kemudian tekan tombol **'i'** untuk memulai proses instalasi, setelah itu ikuti langkah selanjutnya sampai instalasi selesai dan tekan **'Enter'** untuk *Restart*.



Gambar IV.4

Tampilan Mikrotik

2. Instalasi *Winbox* dan *Login*

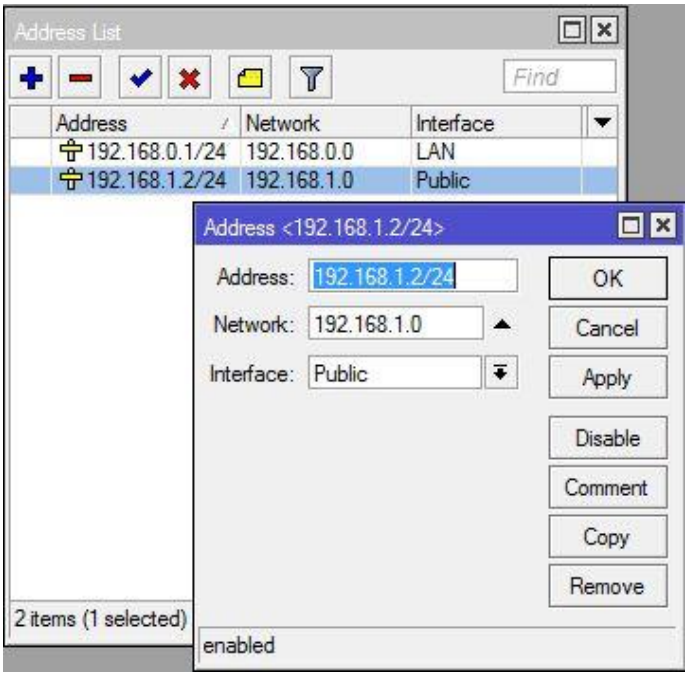
Untuk konfigurasi Mikrotik, penulis menggunakan software Winbox. Setelah Winbox.exe tersimpan di komputer, dapat langsung dijalankan dengan memasukkan *MAC Address* mikrotik, misal 08:00:27:DA:2C:F8, isi juga ***Login*** dengan ***admin*** sedangkan ***password*** kosong saja.

Gambar IV.5

Tampilan Winbox dan Login Mikrotik

3. Pengaturan *IP Address*

Pada *router* ini penulis menggunakan 2 *ether*, *ether* 1 untuk IP *Public* dan *ether* 2 untuk IP *Local*. Langkah memberikan IP *Address* pada masing-masing *interface* dengan klik Menu| IP| Address| pada tampilan Address List klik tombol + warna biru.

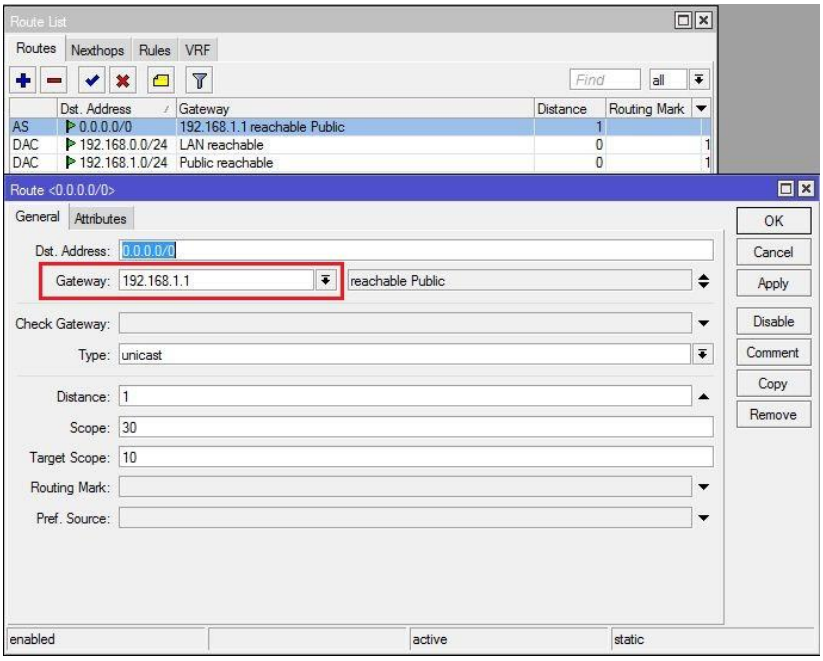


Gambar IV.6

Pengaturan IP Address

4. Pengaturan *Route Table*

Set Route pada Mikrotik Router bertujuan untuk menentukan jalur *gateway* dari jaringan lokal ke jaringan yang terkoneksi *internet*. Dengan cara klik Menu IP| Routes| pada tampilan *Route List* klik tombol + warna biru untuk menambahkan *gateway* seperti gambar:

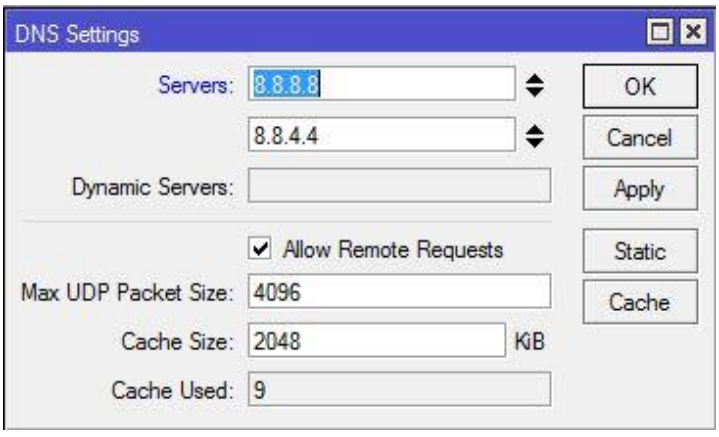


Gambar IV.7

Pengaturan *Route Table*

5. Pengaturan DNS

Pengaturan DNS bertujuan untuk menentukan *network server* dari Mikrotik, dengan cara klik menu IP|DNS.



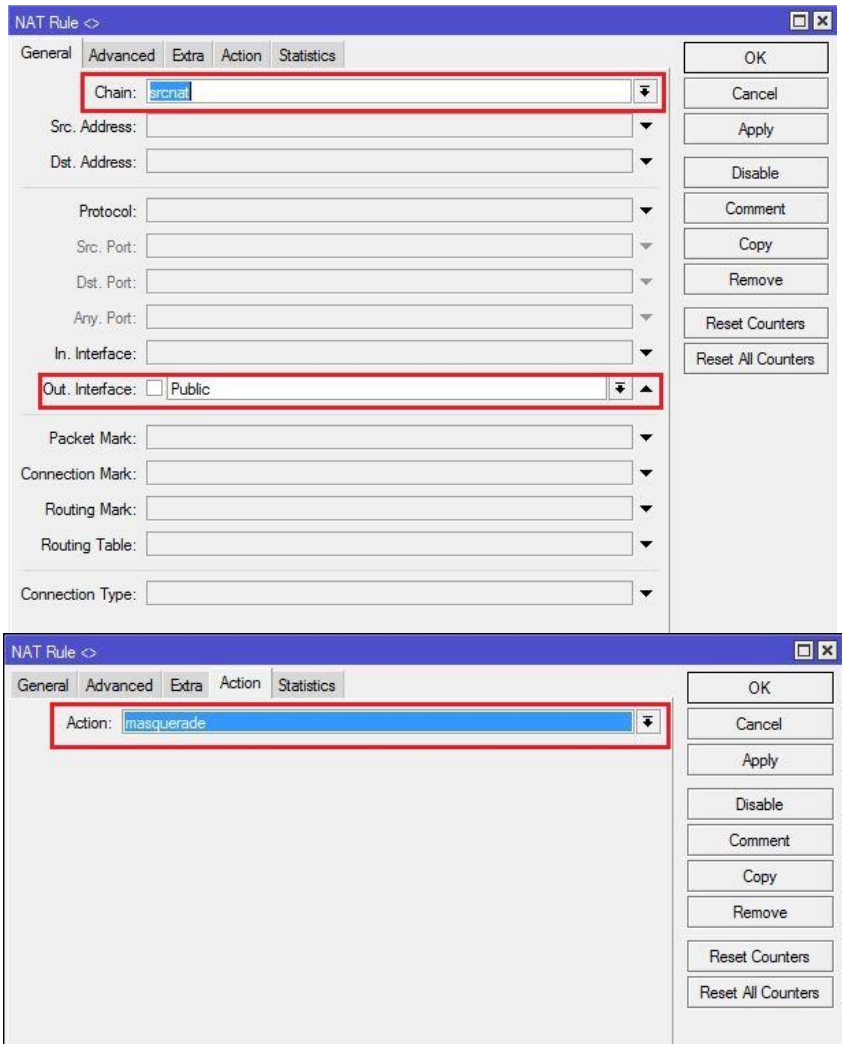
Gambar IV.8

Pengaturan DNS

Isikan *IP address* google apabila settingan DNS nya diarahkan ke google, atau bisa juga ke *IP address speedy* maupun Nawala.

6. Pengaturan *Firewall* NAT

NAT atau disebut juga dengan *Network Address Translation* adalah suatu metode menghubungkan lebih dari satu komputer ke jaringan *internet* dengan menggunakan satu alamat IP. Klik Menu IP| Firewall| NAT. Setting seperti gambar:

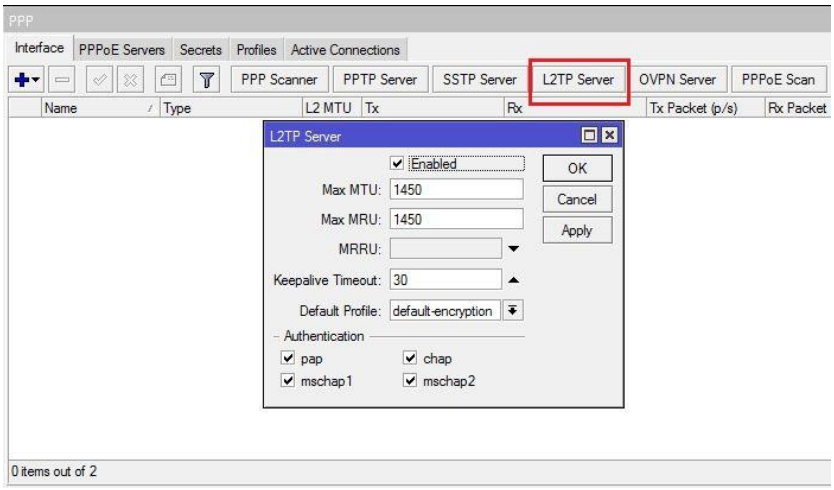


Gambar IV.9

Pengaturan NAT

7. Konfigurasi VPN L2TP Server

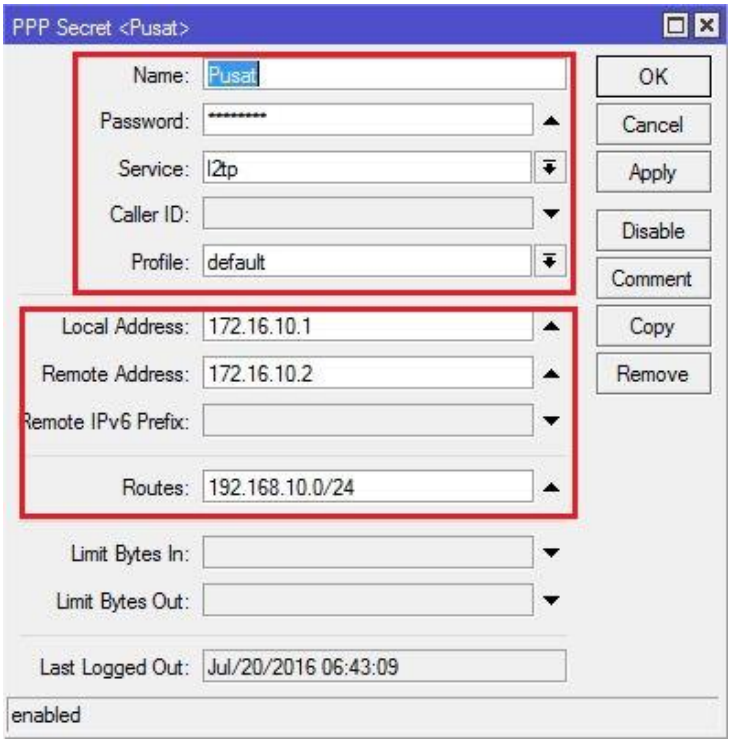
Untuk mengaktifkan *router* sebagai *L2TP server* caranya pun cukup mudah. Pada menu **PPP** | Pilih **L2TP Server.** Kemudian centang opsi '**Enabled**', secara otomatis L2TP Server telah aktif.



Gambar IV.10

Mengaktifkan L2TP

Selanjutnya melakukan setting pada Tab **Secrets.** Pilih Tab **Secrets** | klik **Add [+].** Disini akan mengisi beberapa parameter standar yang utama untuk melakukan koneksi. Seperti '***Name* & *Password***' diisikan untuk dial koneksi L2TP dari *Client*. Kemudian **Service** bisa diisikan dengan '**L2TP**' dan bisa juga dengan '**any**' untuk semua jenis *service* PPP. Dan parameter selanjutnya yang juga penting adalah *setting IP Address* pada *Local Address* dan *Remote Address*. *IP Address* inilah yang nantinya akan ditambahkan secara otomatis ketika koneksi L2TP terbentuk dan sebagai *gateway* komunikasi data. Untuk parameter *Route* bisa juga ditambahkan dengan mengisikan *network* dari kantor cabang, sehingga akan ditambahkan *rule routing* baru secara otomatis.

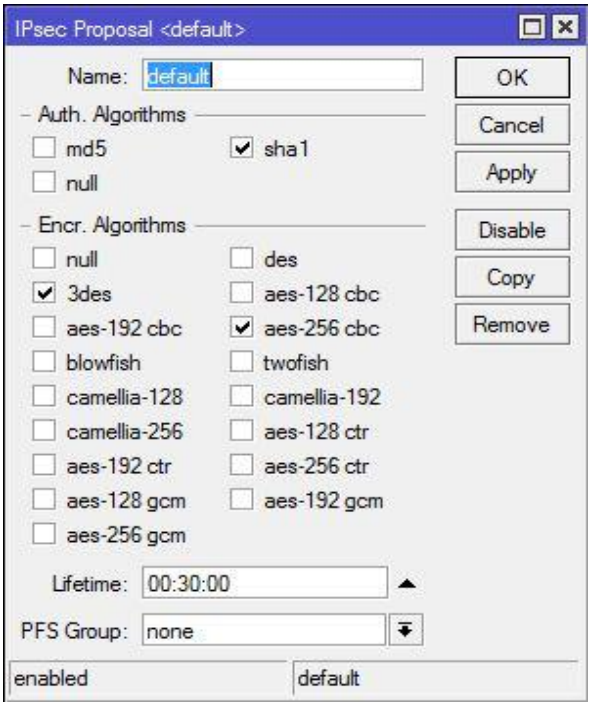


Gambar IV.11

Menambahkan PPP Secret

8. Konfigurasi IPSec untuk L2TP Server

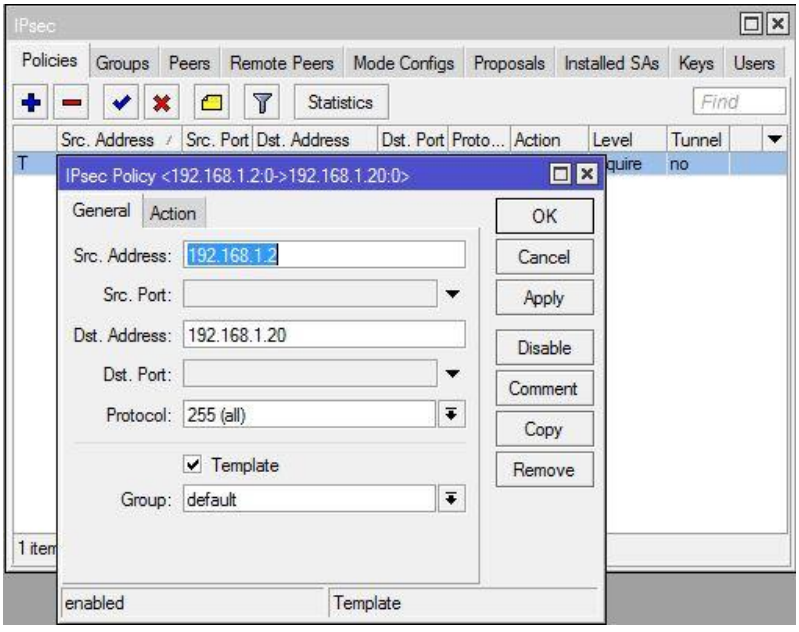
Untuk meningkatkan keamanan akan memadukan L2TP dengan IPSec. Pilih pada menu IP | IPSec. Kemudian penulis akan melakukan setting terlebih dahulu pada Tab **IPsec Proposal**, pada parameter yang tersedia isikan seperti gambar berikut.



Gambar IV.12

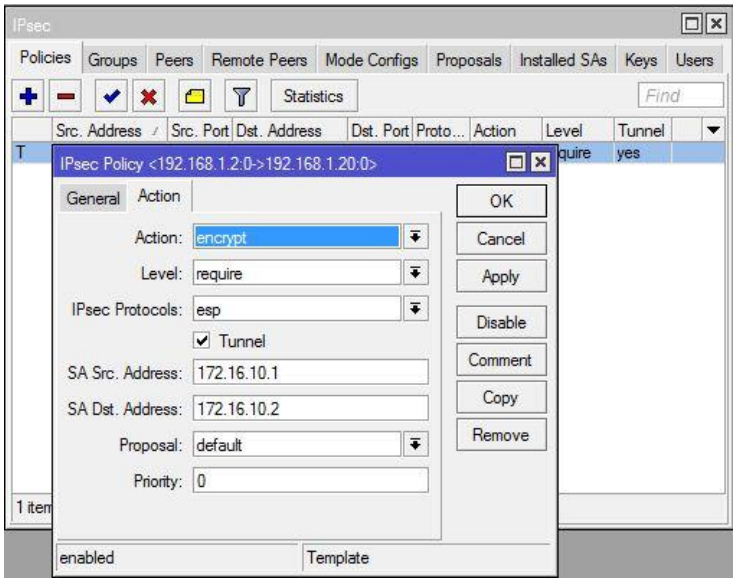
Pengaturan IPsec Proposal

Selanjutnya melakukan setting pada Tab **IPsec Policy,** tambahkan juga parameter pada tampilan berikut.



Gambar IV.13

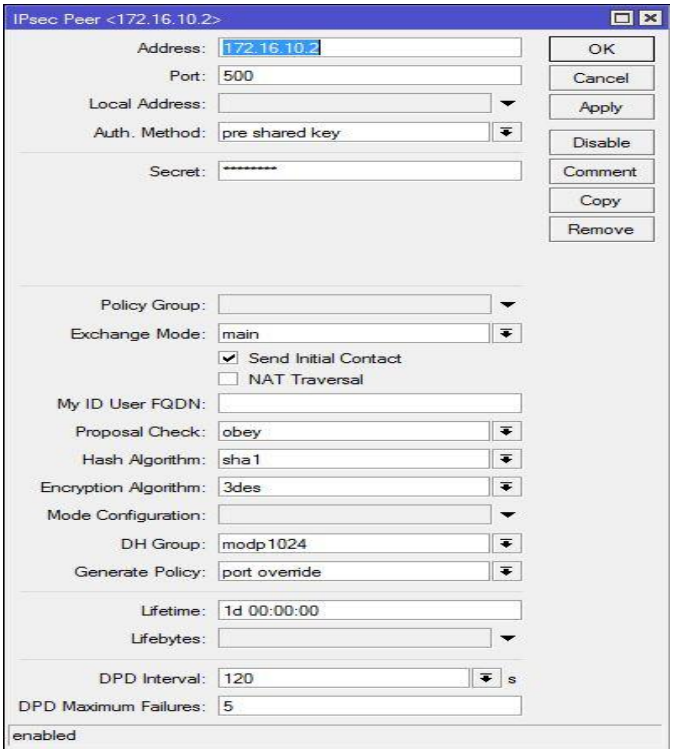
Pengaturan *IPSec Policy* pada tab *General*



Gambar IV.14

Pengaturan *IPSec Policy* pada tab *Action*

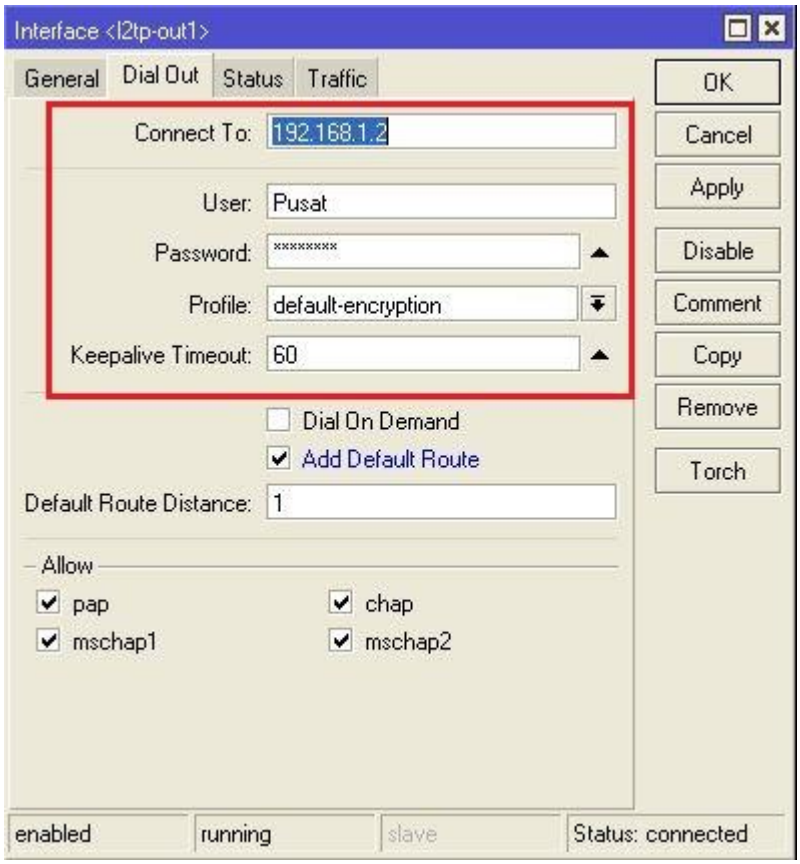
Setelah konfigurasi pada Tab ***IPSec Proposal*** dan ***IPSec Policy*** telah dilakukan, penulis melanjutkan konfigurasi pada Tab ***IPSec Peer.*** Isikan sesuai dengan parameter seperti pada tampilan gambar berikut.



Gambar IV.15
Pengaturan *IPSec Peer*

9. Konfigurasi L2TP Client

Setelah melakukan setting pada sisi L2TP *Server* yang berada pada kantor pusat, kita akan membuat L2TP *Client* yang berada pada kantor cabang. Untuk L2TP Client kita tinggal *dial* ke L2TP *server*. Pilih Menu **PPP** | klik **Add [+]** | pilih **L2TP Client**. Kemudian akan muncul tampilan seperti berikut.



Gambar IV.16

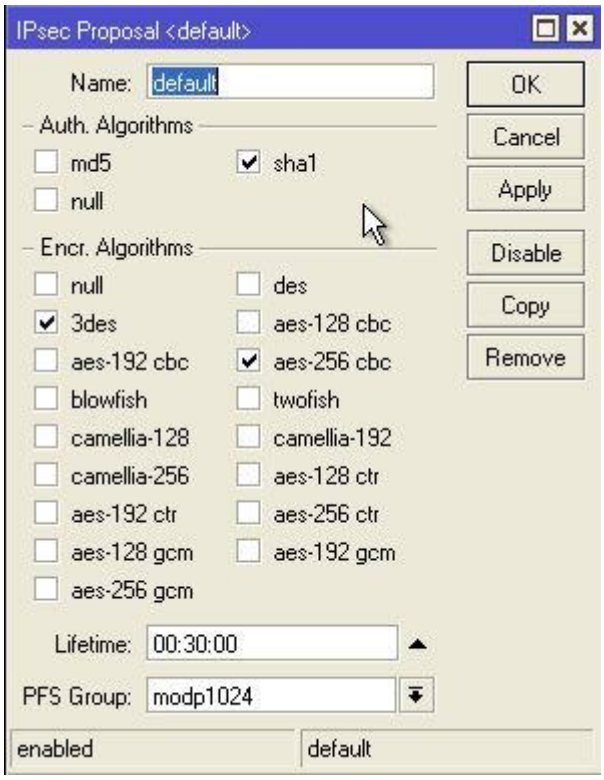
Pengaturan *L2TP Client*

Isikan pada parameter '**Connect to'** dengan IP public dari router di kantor pusat yang menjadi L2TP server. Kemudian parameter '**User & Password**' kita isikan seperti konfigurasi *Secret* di L2TP *server*.

10. Konfigurasi IPSec untuk L2TP Client

Sebelumnya penulis sudah melakukan konfigurasi *IPSec* untuk L2TP *Server*. Dan sekarang penulis juga akan melakukan konfigurasi untuk sisi L2TP *Client*. Pada dasarnya parameter yang digunakan antara *IPSec* baik sisi L2TP *Server* maupun *Client* sama, namun akan sedikit melakukan perubahan pada parameter *IP Address*.

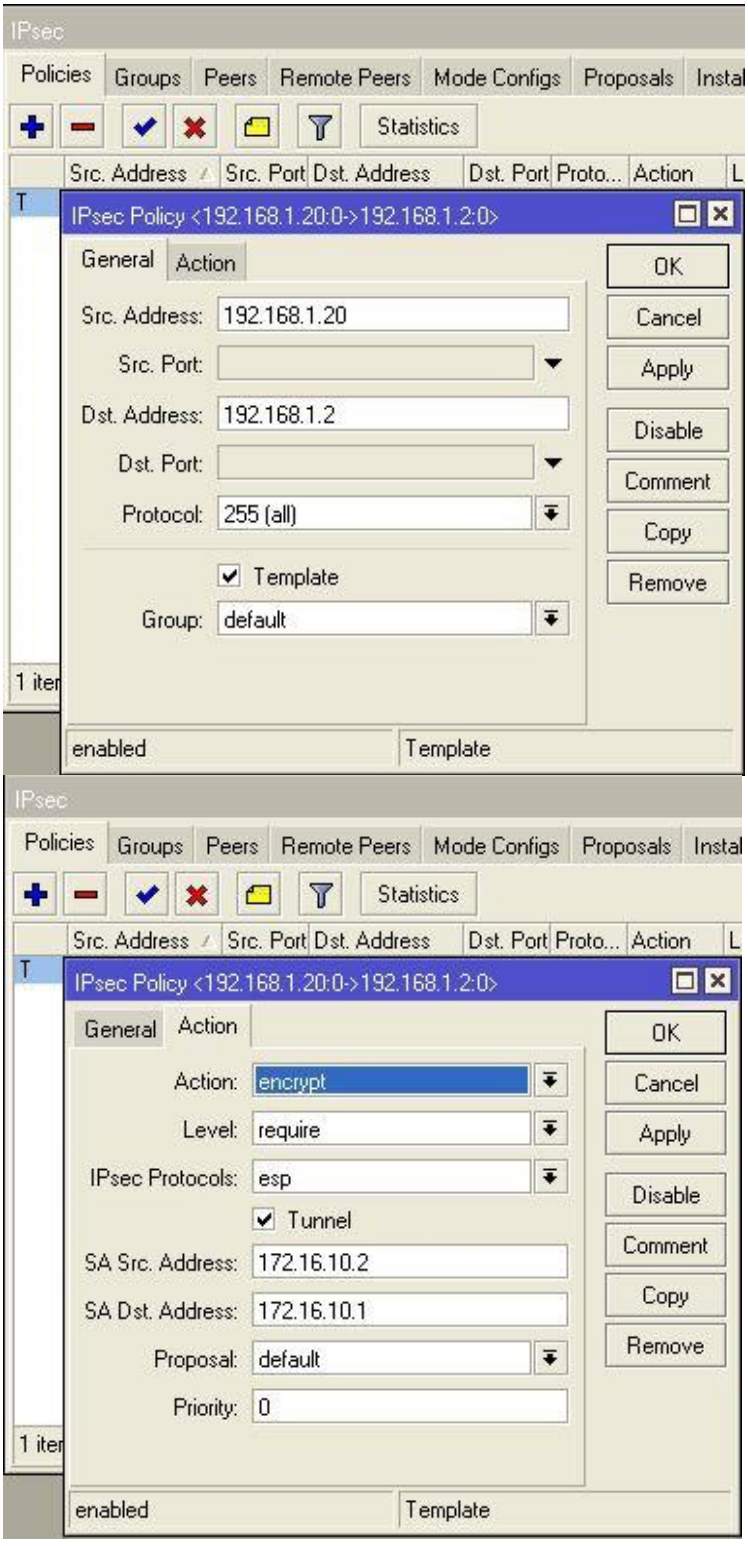
Pada Tab ***IPSec Proposal*** tidak ada perbedaan dengan konfigurasi *IPSec* untuk L2TP *Server*.



Gambar IV.17

Pengaturan *IPSec Proposal* pada *Client*

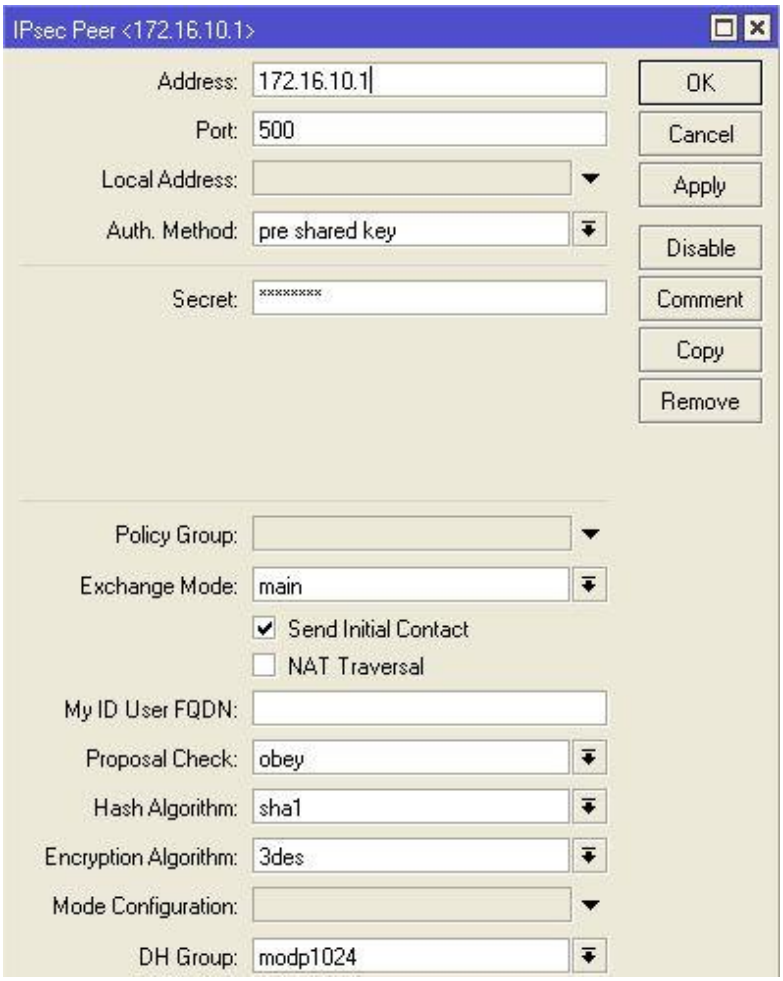
Kemudian untuk selanjutnya pada Tab ***IPSec Policy*** penulis akan mengganti IP Address dan untuk parameter yang lain samakan dengan *IPSec* di sisi L2TP *server*.



Gambar IV.18

Pengaturan *IPSec Policy* pada *Client*

Setelah *setting IPSec Policy* maka kita akan melakukan *setting* juga untuk *IPSec Peer*. Kita juga tinggal mengganti *IP Address* dan set parameter yang lain seperti halnya pada *IPSec* di sisi *L2TP server*.



Gambar IV.19

Pengaturan *IPSec Peer* pada *Client*

Terakhir kita akan memeriksa apakah interkoneksi jaringan L2TP/IPSec telah tersambung atau belum antara kantor pusat dengan kantor cabang. Apabila konfigurasi benar dan tersambung maka akan tercantum pada info Status: *Connected* serta akan muncul sebuah *interface* baru dari L2TP.

4.2. Pengujian Jaringan

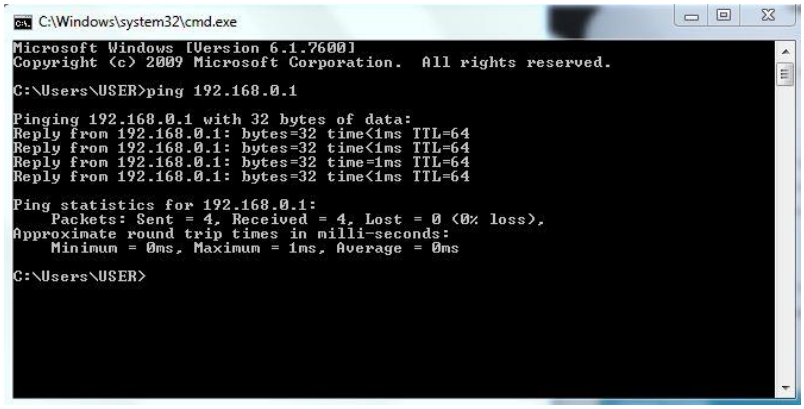
Dalam hal membangun jaringan komputer perlu dilakukan sebuah pengujian terhadap jaringan yang telah dibangun sebelumnya, hal ini berguna untuk memastikan bahwa semua sistem yang telah dibuat berjalan dengan baik dan sesuai dengan yang direncanakan.

4.2.1 Pengujian Jaringan Awal

Pada sub bab ini akan dilakukan beberapa pengujian awal diantaranya tes koneksi dari *client* ke *gateway*, dari *client* ke *router* dengan cara *ping*.

1. *Ping* dari *client* ke *gateway* pada kantor pusat.

Pada pengujian ini penulis mencoba melakukan tes koneksi dari salah satu *client* ke *gateway* dengan cara ping pada kantor pusat.

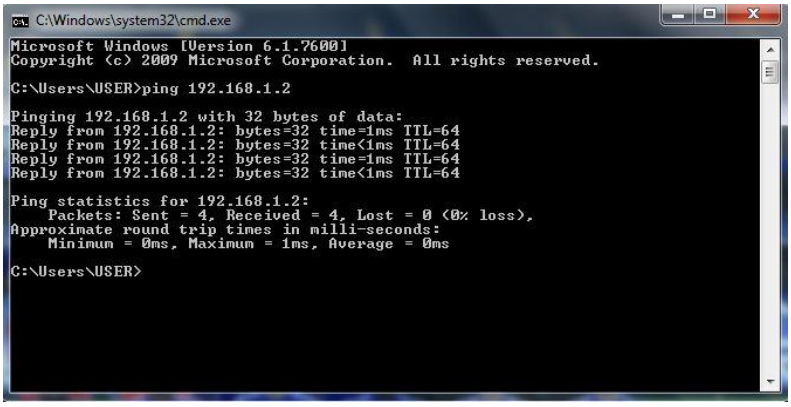


Gambar IV.20

Ping dari *Client* ke *Gateway* pada Kantor Pusat

2. *Ping* dari *client* ke *router* pada kantor pusat

Pada percobaan kali ini penulis akan mencoba menghubungkan atau melakukan tes koneksi antara *client* dengan *router* yang berada pada jaringan lokal.



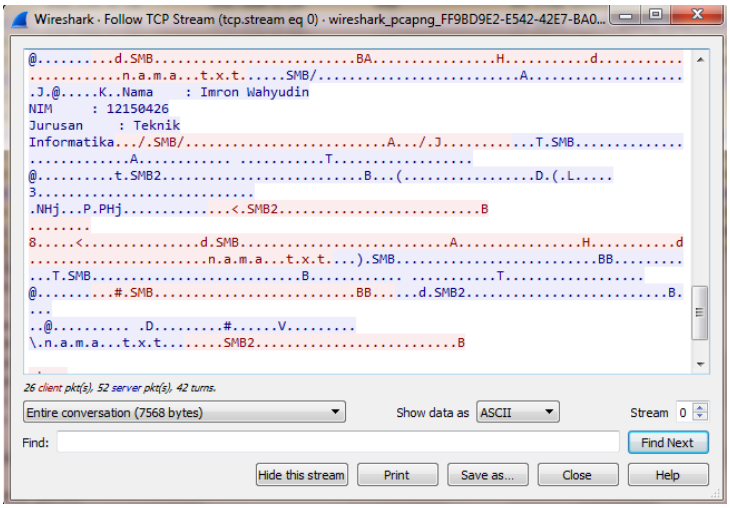
Gambar IV.21

***Ping* dari *Client* ke *Router* Kantor Pusat**

Dari hasil pengujian diatas terlihat bahwa hasil tes koneksi dapat terhubung dengan baik dan tidak ada data yang *lost*.

3. Tes Pengiriman Data

Pada pengujian ini penulis mencoba melakukan pengiriman data dalam jaringan lokal, kemudian dilakukan analisa paket data jaringan mengunakan Wireshark. Hasil dari paket data sebelum menggunakan VPN dengan aplikasi wireshark yaitu terlihat bahwa isi data yang dikirim bisa terbaca, seperti gambar dibawah:



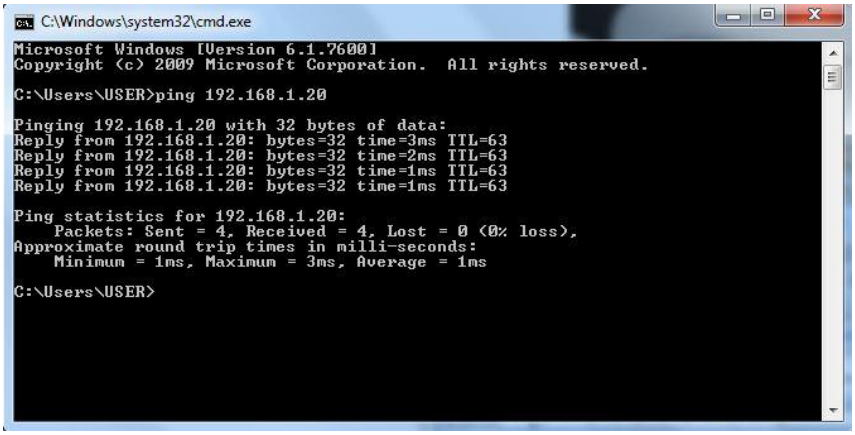
Gambar IV.22

Analisa sebelum menggunakan VPN

4.2.2. Pengujian Jaringan Akhir

Pada pengujian jaringan akhir penulis akan mencoba melakukan tes koneksi dengan melakukan *ping* dari *client* yang berada di kantor pusat ke *client* kantor cabang, dari *client* kantor pusat ke router kantor cabang begitu juga sebaliknya, dan melakukan tracert dari kantor pusat ke kantor cabang.

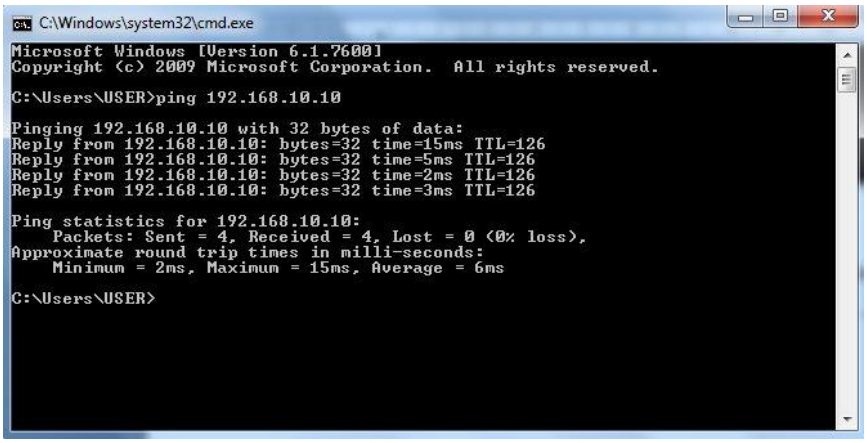
1. *Ping* dari *client* kantor pusat ke *router* kantor cabang



Gambar IV.23

***Ping* dari *client* kantor pusat ke *router* kantor cabang**

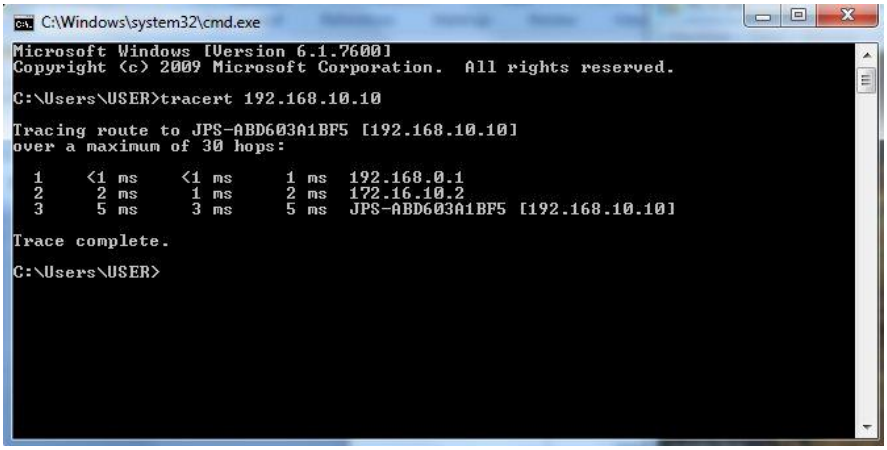
2. *Ping* dari *client* kantor pusat ke *client* kantor cabang



Gambar IV.24

***Ping* dari *client* kantor pusat ke *client* kantor cabang**

3. Tes koneksi dengan *tracert* dari kantor pusat ke kantor cabang



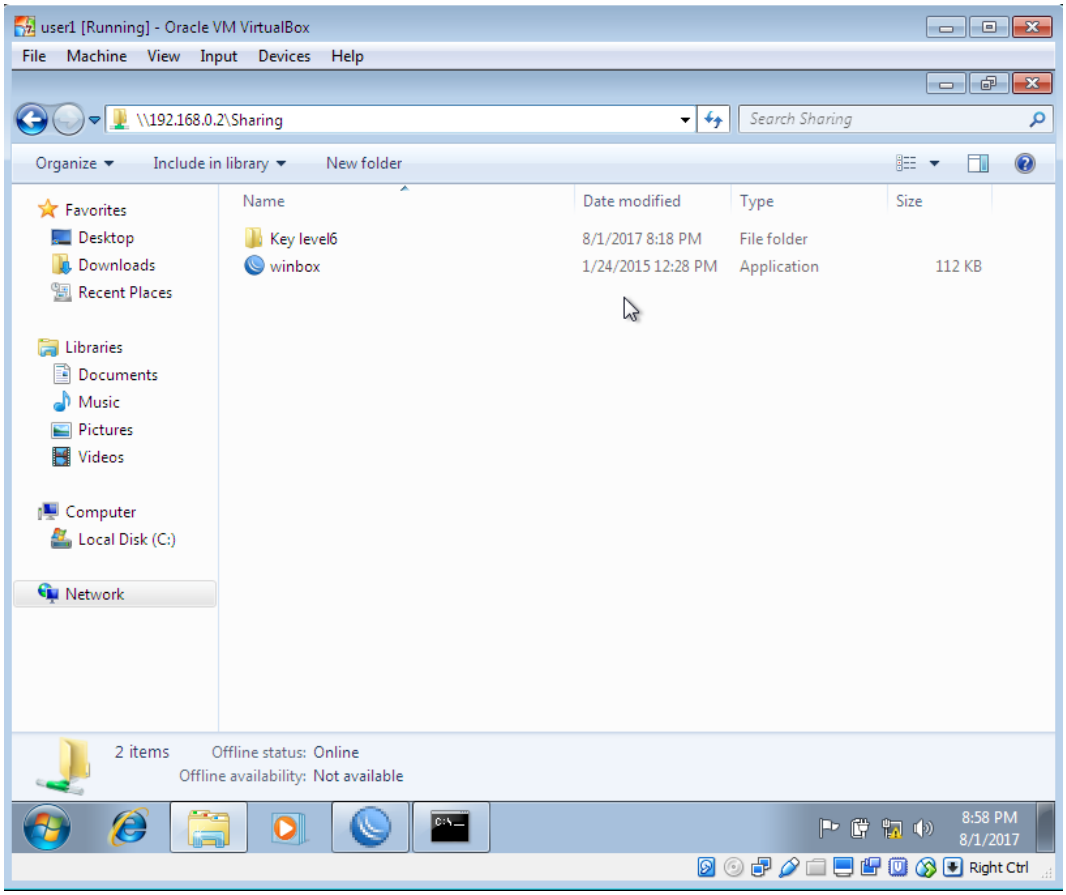
Gambar IV.25

Tes *Trecer*t dari Kantor Pusat ke Kantor Cabang

Pada pengujian diatas telihat bahwa koneksi berjalan dengan baik, dari client kantor pusat bisa terhubung langsung ke kantor cabang, hal ini bisa saling melakukan tukar menukar data. Pengujian dengan *traceroute* untuk melihat rute yang dilewati sebuah data ke tempat tujuan dan ini terlihat bahwa rute melewati *tunnel* yang telah dibuat dengan VPN.

1. Sebelum menggunakan VPN, komputer kantor pusat terkoneksi ke kantor cabang hanya menggunakan e-mail.

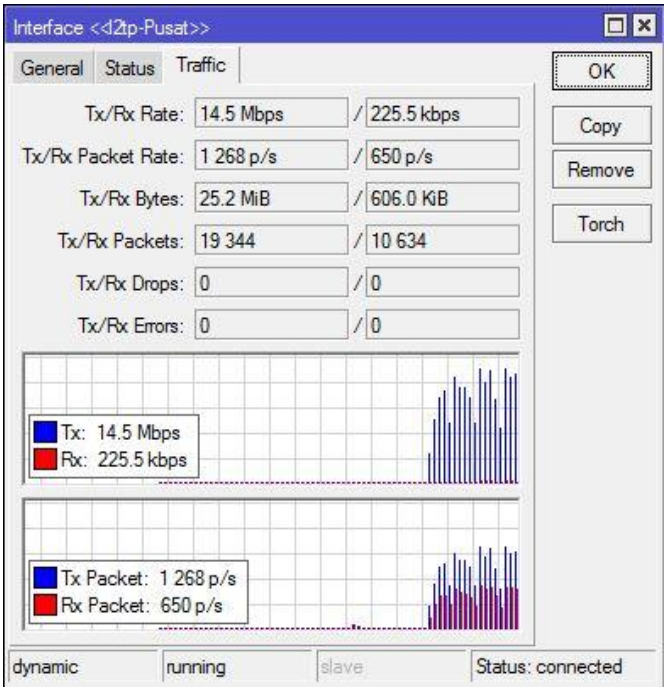
   Yang dimana penerimaan dan pengiriman data tidak terlalu besar dan memerlukan waktu yang cukup lama.
2. Setelah menggunakan VPN, komputer Pusat bisa terkoneksi ke knator cabang dan bisa menerima dan mengirim file dengan waktu yang lebih cepat dan dengan data yang lebih besar.



Gambar IV.26

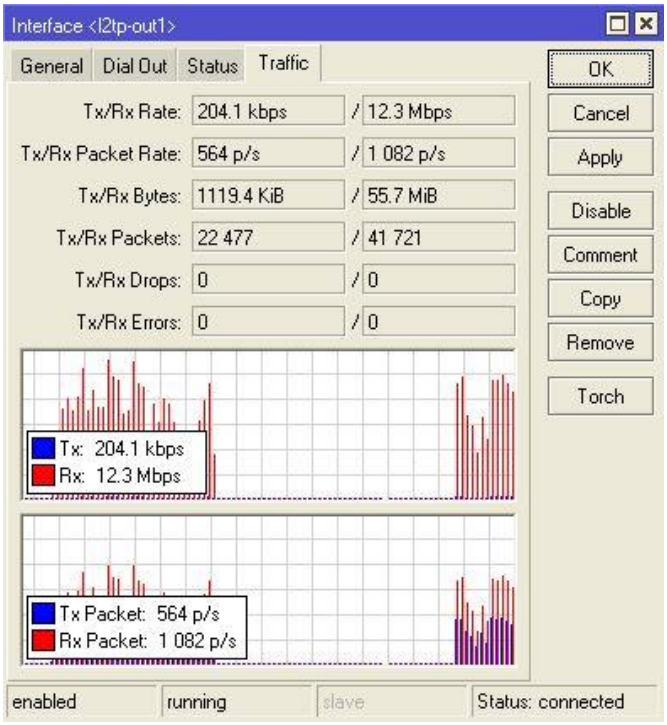
Tampilan Kantor Pusat setelah terkoneksi ke Kantor Cabang

4. Grafik Transer Data



Gambar IV.26

Grafik Transfer Data pada Router Pusat



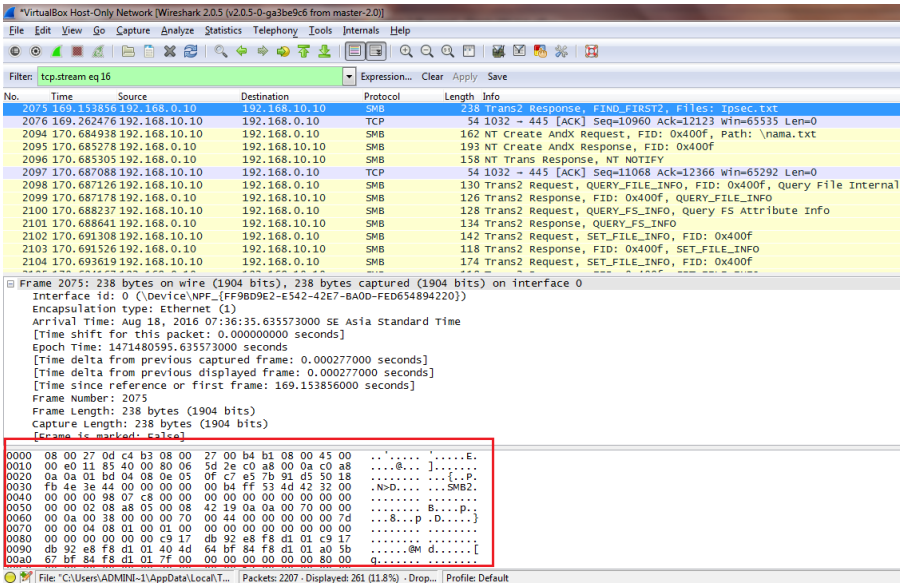
Gambar IV.27

Grafik Transfer Data pada Router Cabang

5. Tes Pengiriman Data

Dalam pengujian ini penulis mencoba melakukan pengiriman data dari PC kantor cabang ke PC kantor Pusat dengan koneksi VPN L2TP/IPSec. Dan setelah dilakukan konfigurasi dengan benar, akhirnya pengiriman berhasil.

Dibawah ini merupakan gambar dari analisa paket data yang melewati jaringan kantor pusat menggunakan wireshark. Dari hasil analisa ini bahwa data yang dikirim telah terenkripsi.



Gambar IV.28

Analisa Paket Data

Tabel IV.1

Tabel Perbandingan Sebelum dan Sesudah Implementasi VPN L2TP/IPSec

Indikator	Sebelum Implementasi VPN	Sesudah Implementasi VPN
Besar data yang dapat diupload	Batas data yang diupload ke email tidak terlalu besar	Tidak ada batasan ukuran file, karena file diletakkan di server file sharing.
Penggunaan bandwidth dan durasi pertukaran data	Bandwidth tidak efisien, karena pengiriman data memerlukan waktu yang lebih lama.	Bandwidth lebih efisien, karena langsung terkoneksi VPN, dan pengiriman lebih cepat.
Keamanan pengiriman data	Pengiriman data masih rentan pembobolan.	Pengiriman data lebih aman, karena VPN telah mengenkripsi data yang dikirim.