BAB IV

RANCANGAN JARINGAN USULAN

4.1 Jaringan Usulan

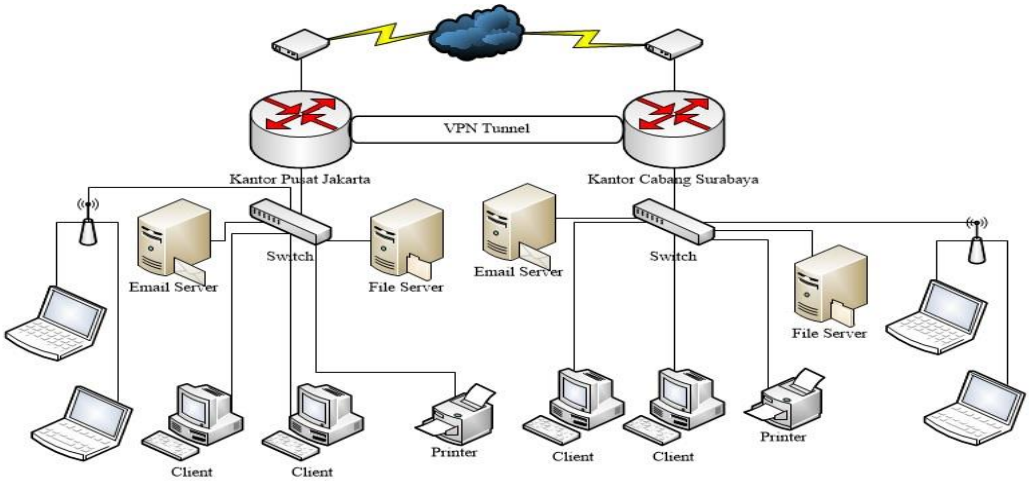
Setelah penulis menganalisa sistem jaringan berjalan pada PT. Global Terminal Marunda, maka penulis mengusulkan sebuah jaringan menggunakan *Virrtual Private Network* (VPN) dengan metode IPSec untuk menghubungkan kantor pusat dengan kantor cabang.

Dengan menggunakan *Router Mikrotik* yang sudah ada kemudian di konfigurasi untuk menerapkan sistem jaringan *Virtual Private Network* (VPN) agar setiap karyawan yang sering bepergian (*Mobile Worker*) dapat memanfaatkan koneksi VPN yang sudah ada serta menambahkan perangkat *access point* agar setiap karyawan yang menggunakan laptop mendapatkan sinyal yang kuat dari *access point*.

4.1.1 Topologi Jaringan Usulan

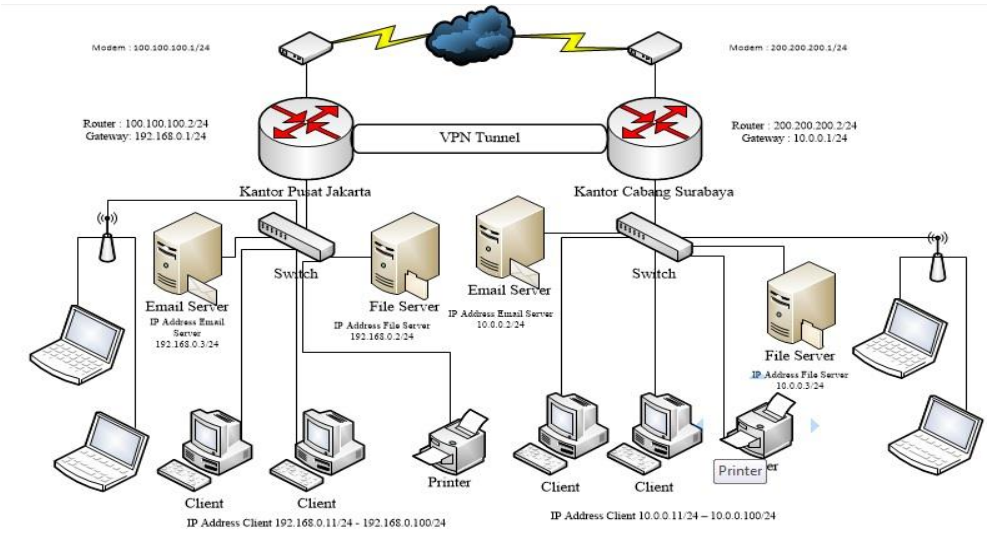
Dalam mengusulkan topologi jaringan yang akan diimplementasikan pada perusahaan, penulis tidak akan merubah bentuk topologi yang sudah ada pada PT. Global Terminal Marunda, hal ini karena bentuk topologi yang ada sekarang sudah sangat baik. Topologi jaringan kantor pusat dan cabang menggunakan topologi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

lebih aman serta menambahkan perangkat *access point* agar setiap karyawan yang menggunakan laptop mendapatkan sinyal yang kuat dari *access point*.



Gambar IV.1 Topologi Jaringan Usulan

4.1.2 Skema Jaringan Usulan



Gambar IV.2 Skema Jaringan Usulan

Pada skema jaringan usulan diatas dapat dilihat bahwa hanya menambahkan *Virtual Private Network* (VPN) pada PT. Global Terminal Marunda yang berfungsi untuk kemudahan karyawan yang bekerja diluar kantor

cabang atau pusat agar dapat berkomunikasi ke jaringan lokal melalui sebuah jaringan publik seperti internet.

4.1.3 Keamanan Jaringan

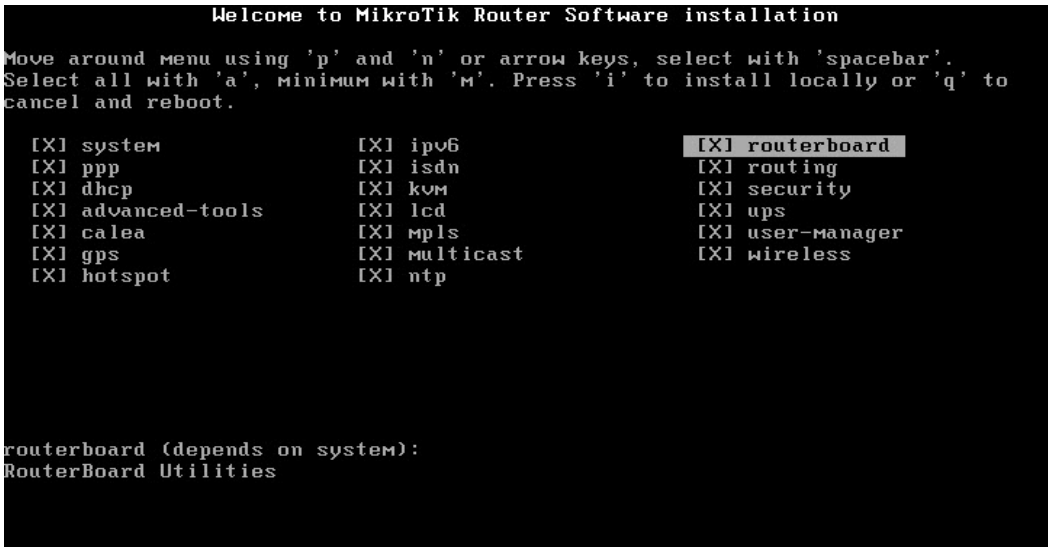
Keamanan jaringan yang ada pada PT. Global Terminal Marunda sudah sangat bagus dengan adanya *firewall* pada konfigurasi *hardware* seperti *router* serta keamanan lainnya menggunakan *software* antivirus. Akan tetapi, penulis mengusulkan jika dalam jaringan PT. Global Terminal Marunda menggunakan *Virtual Private Network* (VPN) dengan metode IP *Security*

4.1.4 Rancangan Aplikasi

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

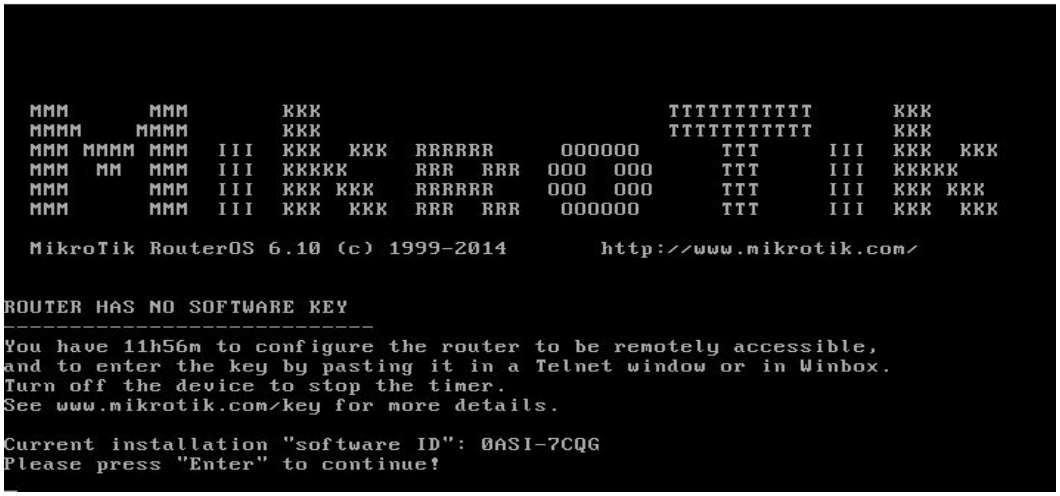
Tahapan konfigurasi yang harus dilakukan sebagai berikut:

1. Hubungkan mikrotik ke komputer yang akan digunakan untuk konfigurasi mikrotik
2. *Setting* BIOS pada komputer *ya*ng digunakan untuk konfigurasi mikrotik 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

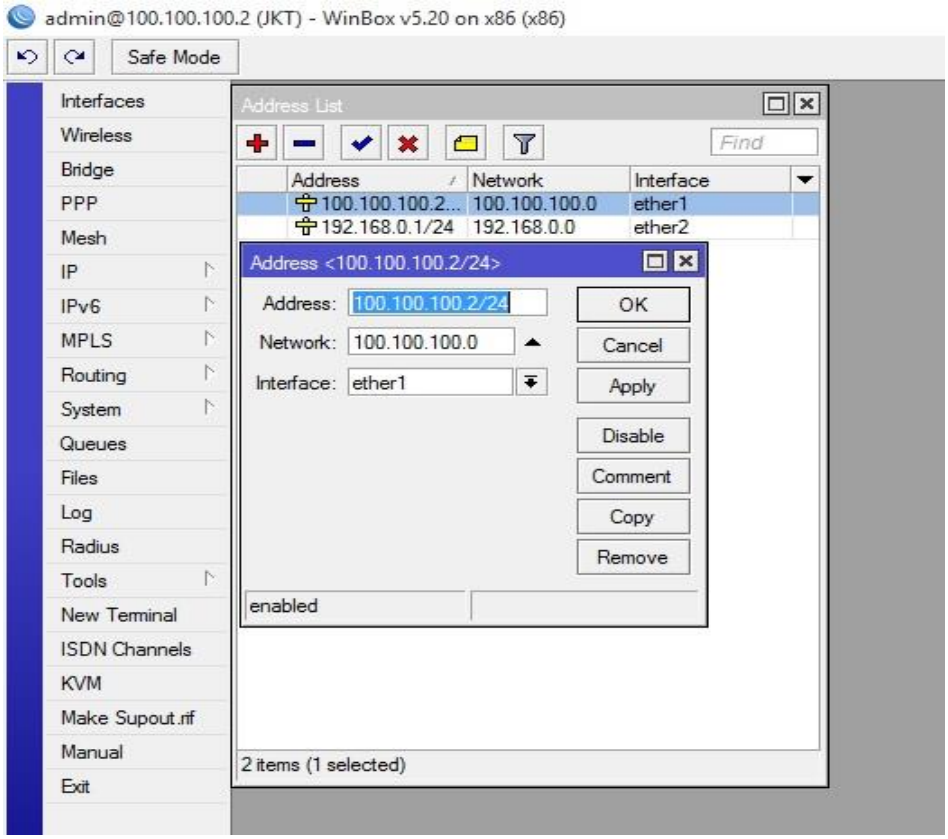
3. Instalasi *Winbox* dan *Login*

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*

4. Pengaturan IP *Address* pada Mikrotik *Router* Kantor Pusat

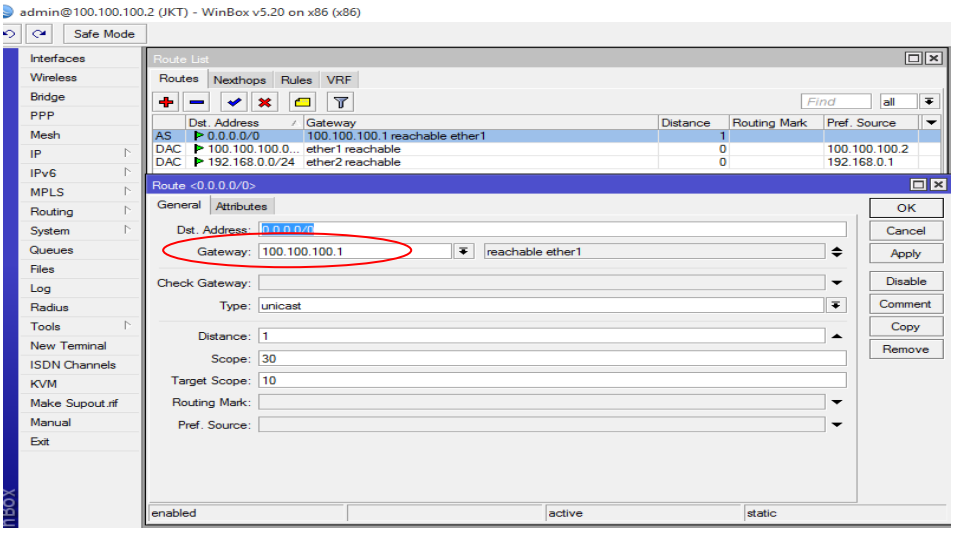
Pada *router* ini penulis menggunakan 2 *ether, ether* 1 untuk IP *Public* dan *ether* 2 untuk IP *Local.* Langkah memberikan IP *Address* pada masing – masing *interface* dengan klik Menu| IP | *Address* | pada tampilan *Address List* klik tombol + warna merah.



Gambar IV.6 Pengaturan IP *Address*

5. Pengaturan *Route Table*

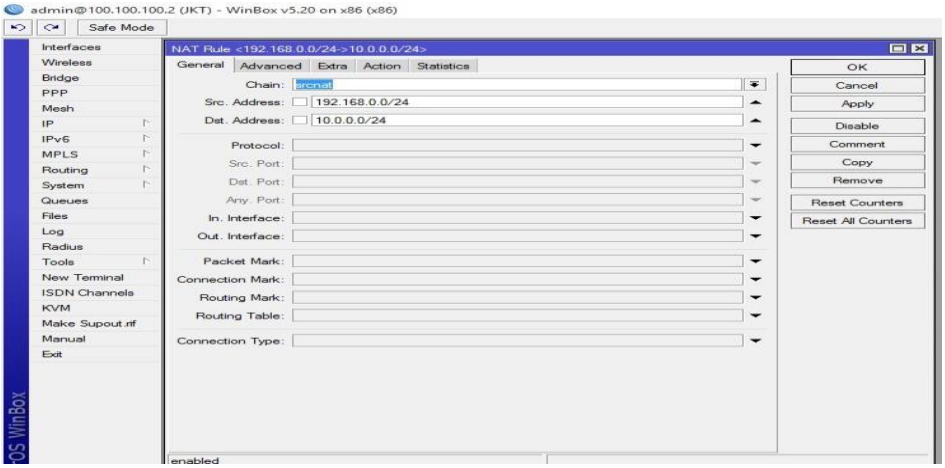
Set Route pada Mikrotik *Router* bertujuan untuk menentukan jalur *gateway* dari jaringan lokal ke jaringan yang terkoneksi internet. Dengan cara klik Menu IP| *Routes*| pada tampilan *Route List* klik tombol + warna merah untuk menambahkan *gateway* seperti gambar:

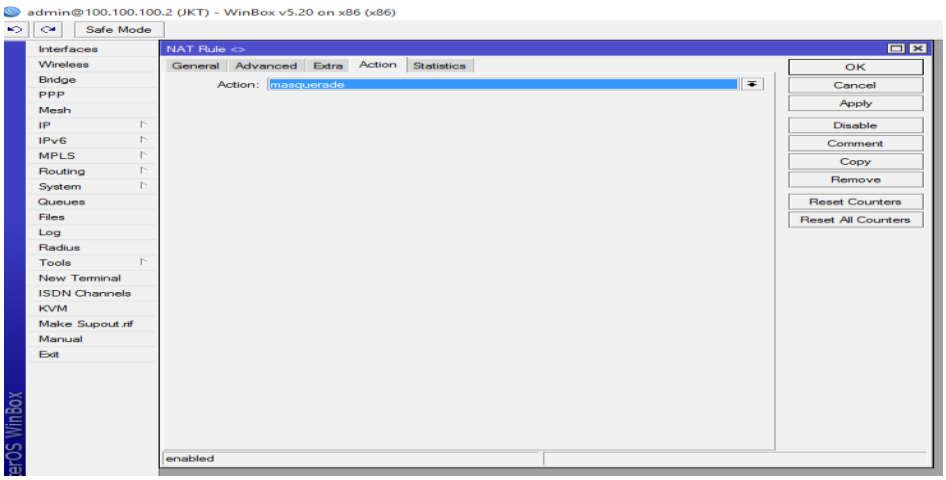


Gambar IV.7 Pengaturan *Route Table*

6. Pengaturan *Firewall* NAT

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

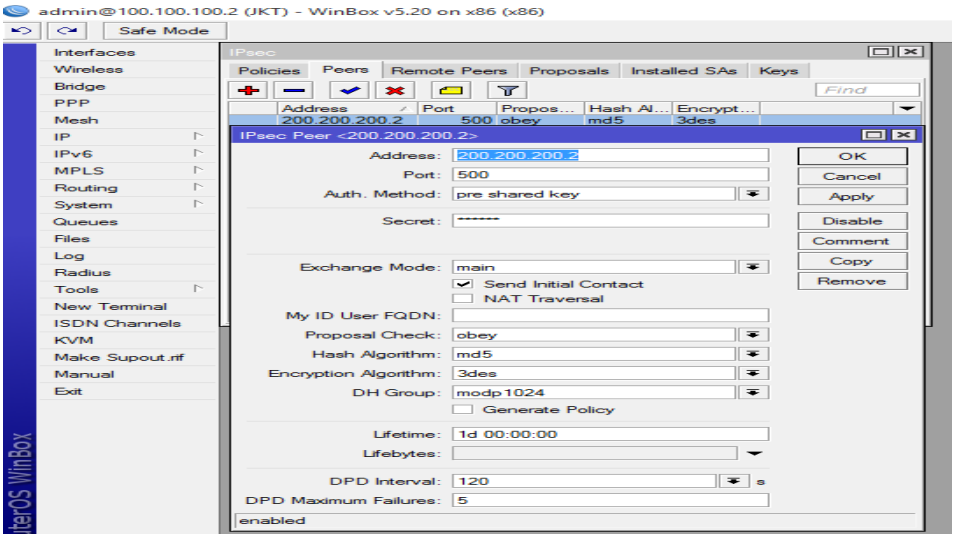




Gambar IV.8 Pengaturan Nat

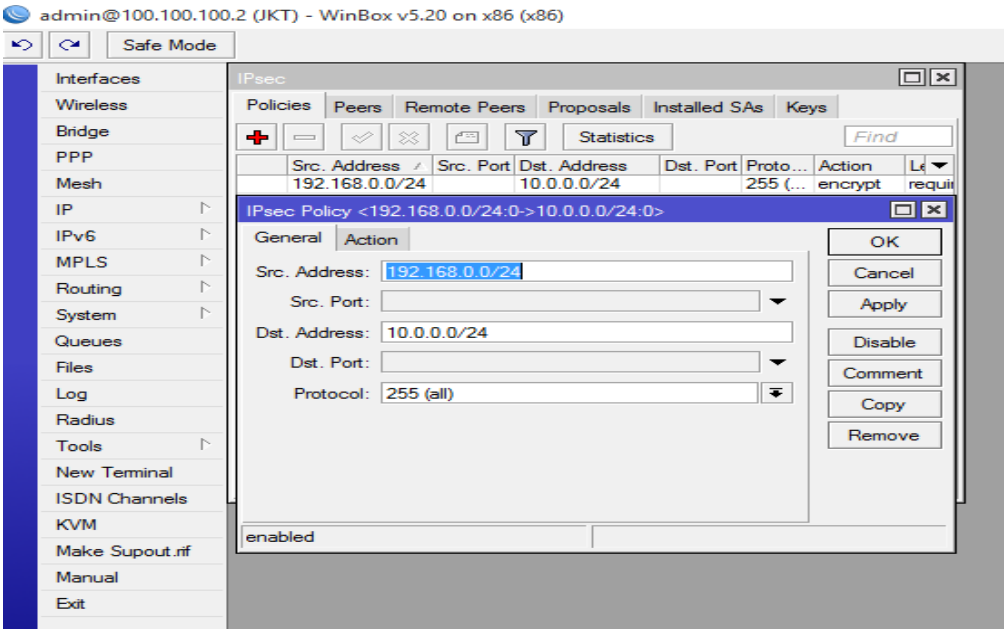
7. Pengaturan IPSec *Peer*

IPSec adalah sebuah protokol yang digunakan untuk mengamankan transmisi *datagram* dalam sebuah *internetwork* berbasis TCP/IP. Klik Menu IP| IPSec|*Peers*. *Setting* seperti gambar :



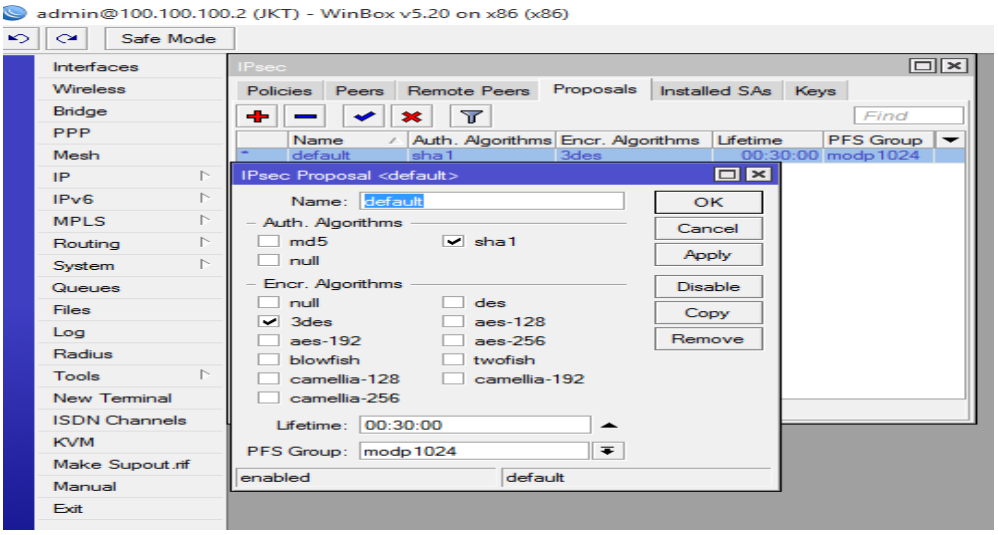
Gambar IV.9 Pengaturan IPSec *Peer*

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



Gambar IV.10 Pengaturan IPSec *Policy*

Selanjutnya setting pada Tab IPSec|Proposal **|,** tambahkan juga parameter pada tampilan berikut :

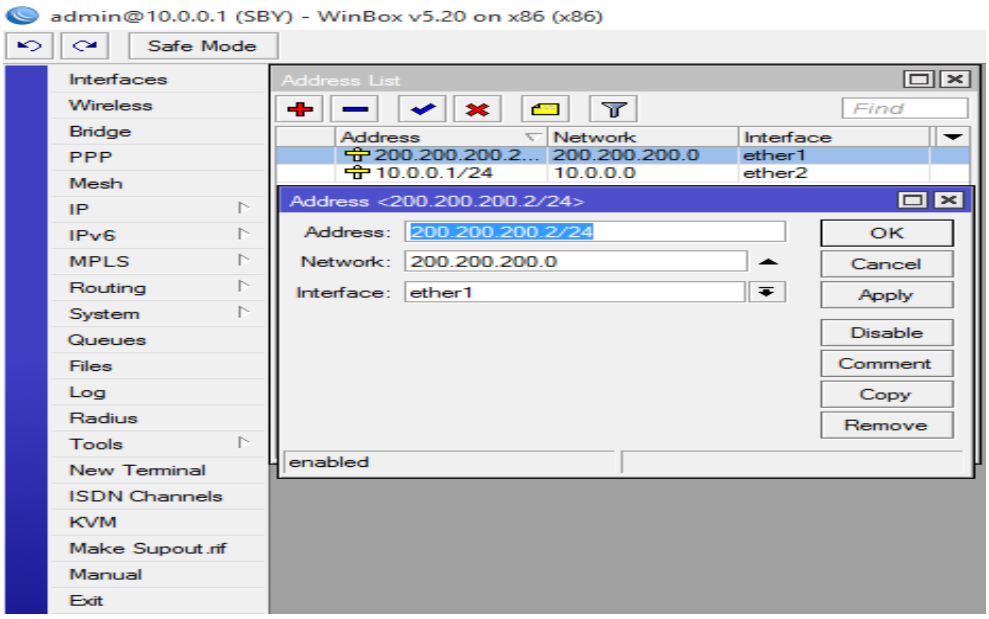


Gambar IV.11 Pengaturan IPSec Proposal

8. Pengaturan IP *Address* pada Mikrotik *Router* Kantor Cabang

   Pada *router* ini penulis menggunakan 2 *ether, ether* 1 untuk IP *Public* dan *ether* 2 untuk IP *Local.* Langkah memberikan IP *Address* pada masing –

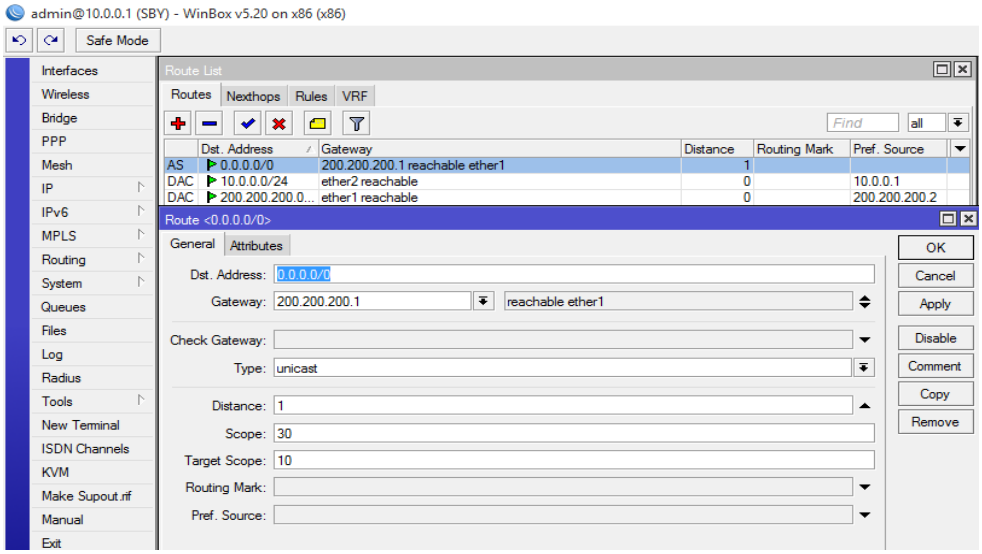
masing *interface* dengan klik Menu| IP | *Address* | pada tampilan *Address List* klik tombol + warna merah.



Gambar IV.12 Pengaturan IP *Address*

9. Pengaturan *Route Table*

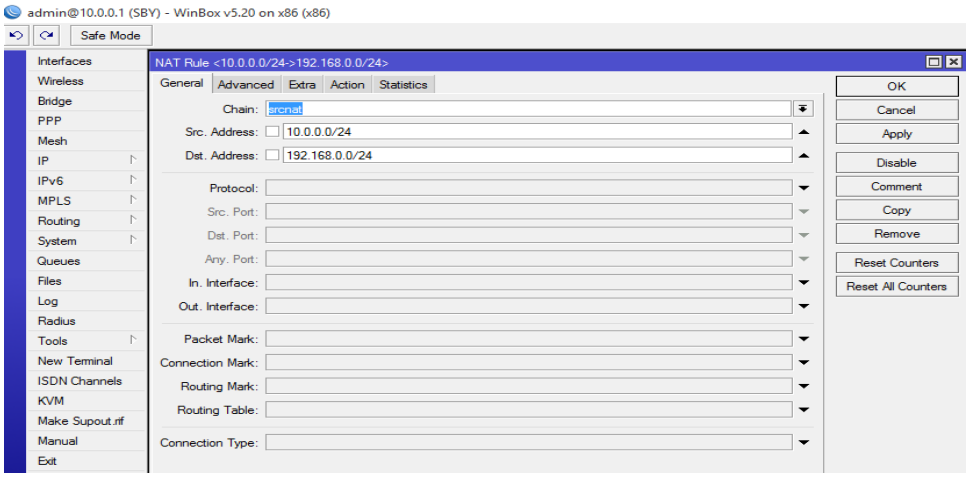
Set Route pada Mikrotik *Router* bertujuan untuk menentukan jalur *gateway* dari jaringan lokal ke jaringan yang terkoneksi internet. Dengan cara klik Menu IP| *Routes*| pada tampilan *Route List* klik tombol + warna merah untuk menambahkan *gateway* seperti gambar:

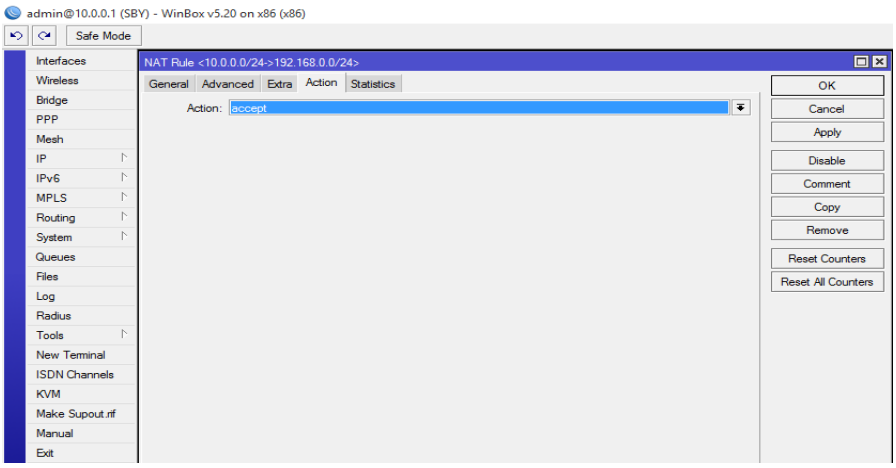


Gambar IV.13 Pengaturan *Route Table*

10. Pengaturan *Firewall* NAT

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

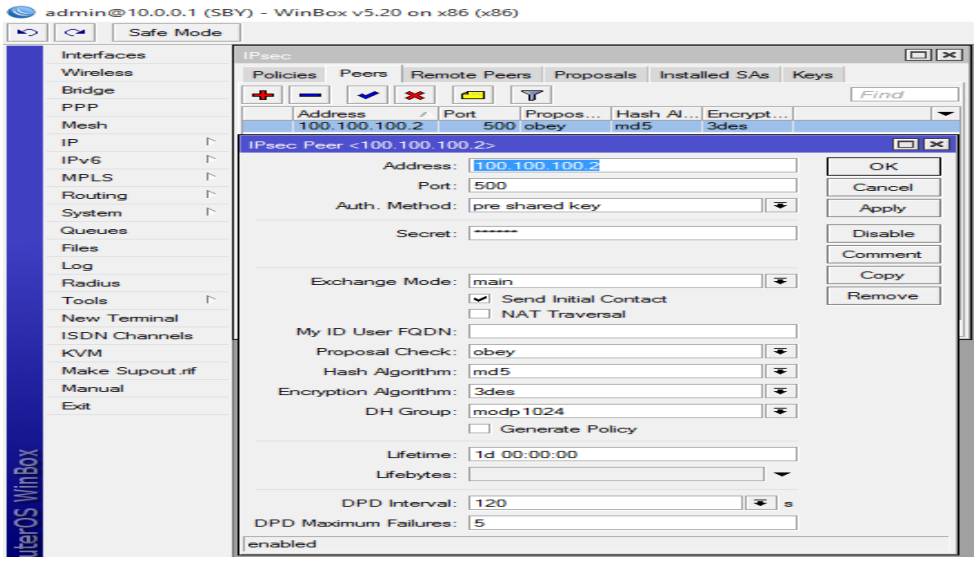




Gambar IV.14 Pengaturan Nat

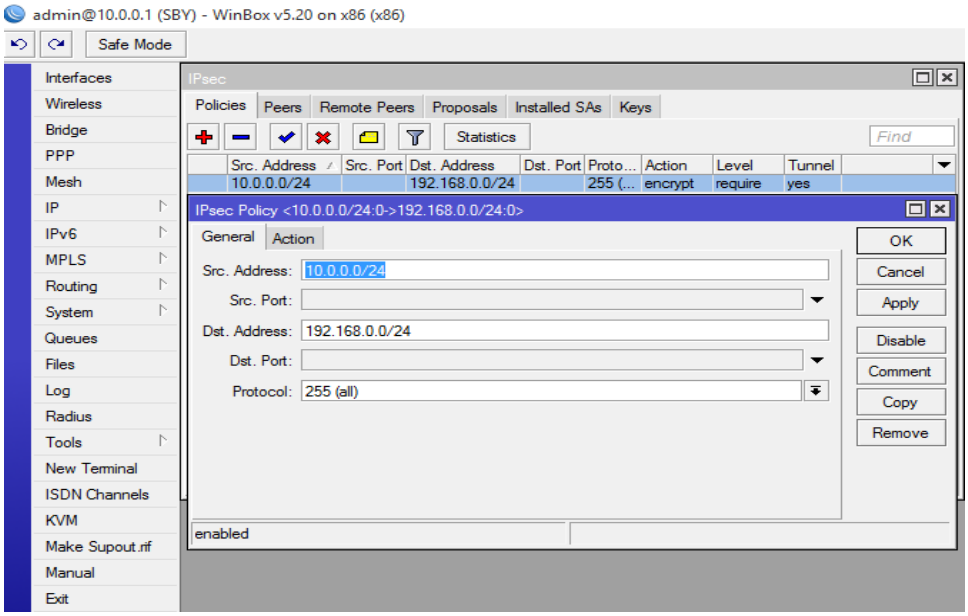
11. Pengaturan *IPSec Peer*

IPSec adalah sebuah protokol yang digunakan untuk mengamankan transmisi *datagram* dalam sebuah *internetwork* berbasis TCP/IP. Klik Menu IP| IPSec|*Peers*. *Setting* seperti gambar :



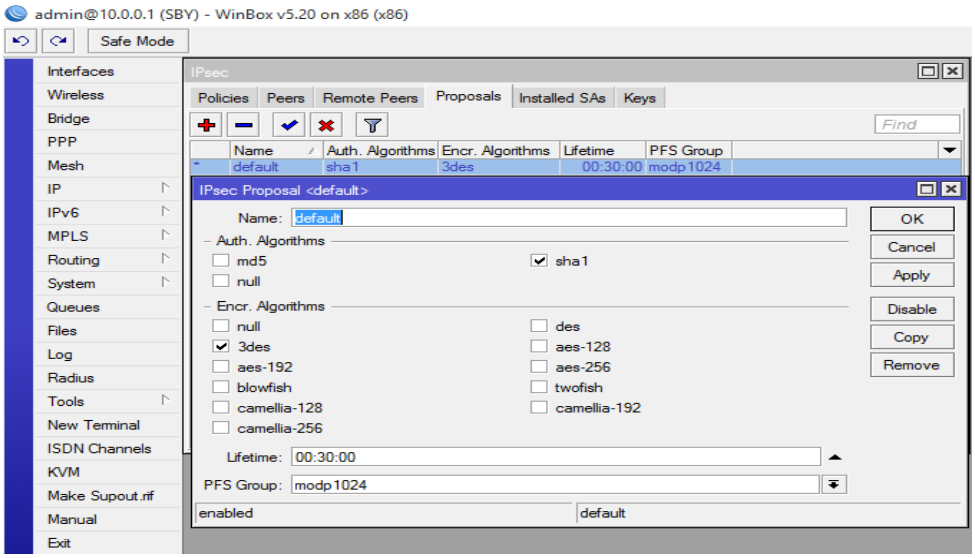
Gambar IV.15 Pengaturan IPSec *Peer*

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



Gambar IV.16 Pengaturan IPSec *Policy*

Selanjutnya setting pada Tab IPSec|Proposal|**,** tambahkan juga parameter pada tampilan berikut :



Gambar IV.17 Pengaturan IPSec Proposal

4.1.5 Manajemen Jaringan

Pada proses ini penulis mengusulkan untuk meningkatkan *Bandwidth* internet agar komunikasi data antara kantor pusat dan cabang berjalan dengan baik. Serta memberikan batasan *Bandwidth* internet pada user yang tidak menggunakan koneksi VPN pada PT. Global Terminal Marunda.

4.2 Pengujian Jaringan

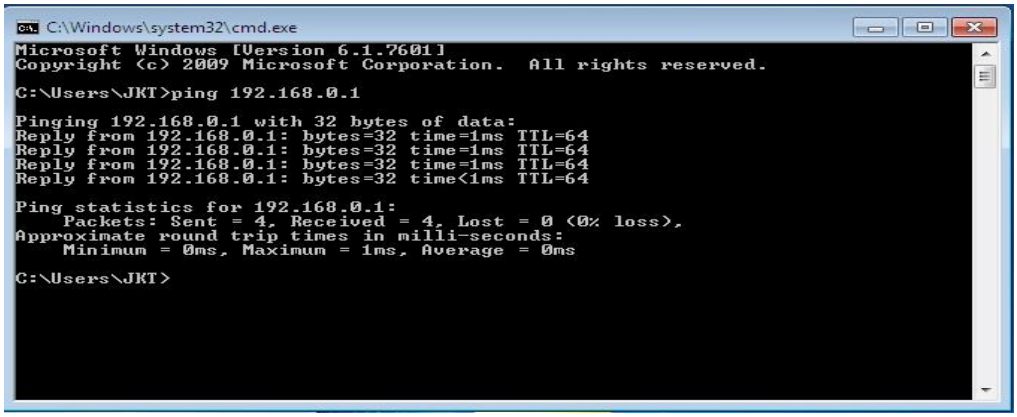
Dalam hal membangun jaringan komputer perlu dilakukan sebuah pengujian terhadap jaringan yang telah dibangun sebelumnya, hal ini berguna untuk memastikan bahwa semua sistem yang telah dibuat berjalan dengan baik dan sesuai dengan yang direncanakan.

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.

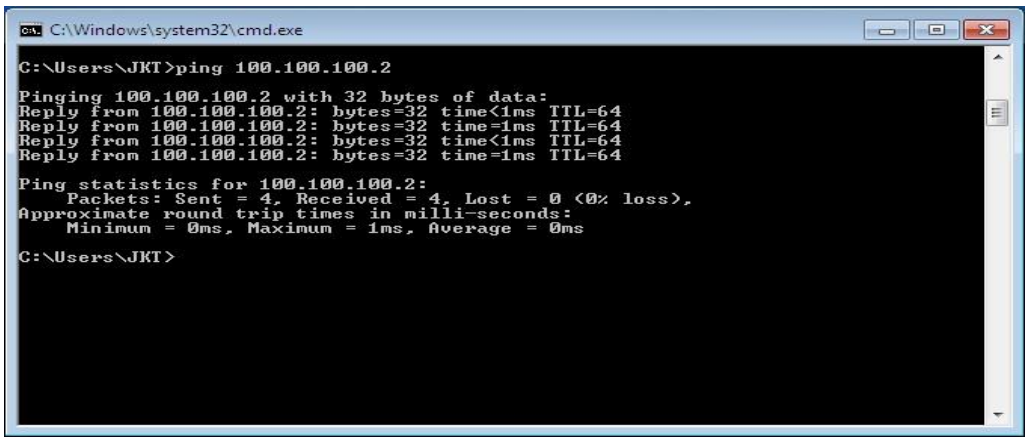
Pada pengujian ini penulis mencoba melakukan tes koneksi dari salah satu *client* ke *gateway* dengan cara *ping* pada kantor pusat.



Gambar IV.18 *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.

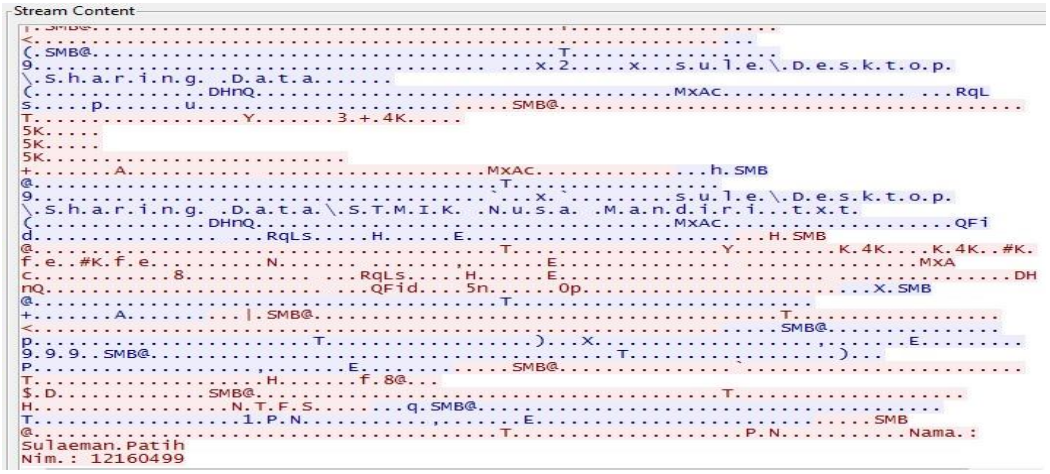


Gambar IV.19 Ping dari *Client* ke *Router* Kantor Pusat

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 menggunakan *wireshark.* Hasil dari paket data sebelum menggunakan VPN dengan aplikasi *wireshark* yaitu terlihat bahwa data yang dikirim bisa terbaca, seperti gambar dibawah ini :

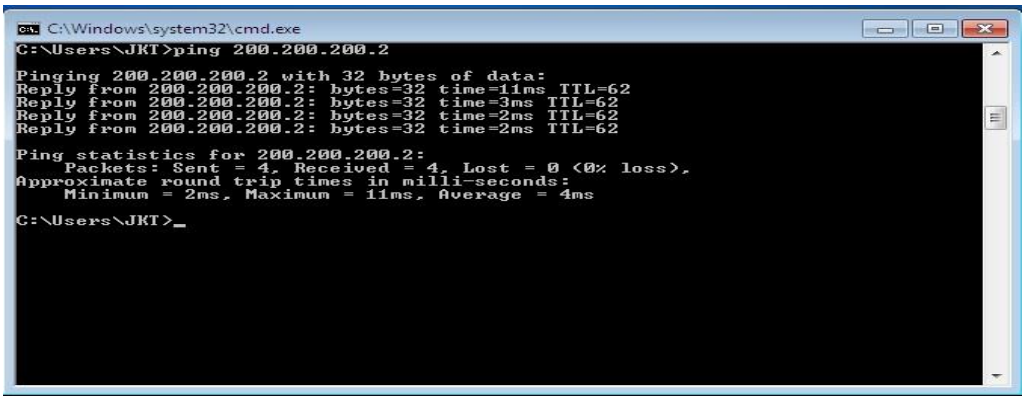


Gambar IV.20 Analisa sebelum menggunakan VPN

4.2.2 Pengujian Jaringan Akhir

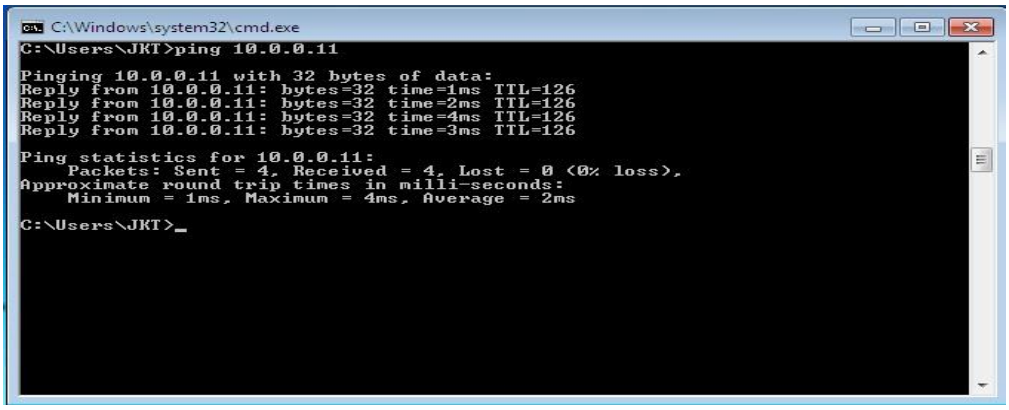
Pada pengujian jaringan akhir penulis akan mencoba melakukan tes koneksi dengan melakukan *ping* dari *client* yang berada di kantor pusat ke *client* kantor cabang, dari *client* kantor pusat ke *router* kantor cabang begitu juga sebaliknya, dan melakukan *tracert* dari kantor pusat ke kantor cabang.

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



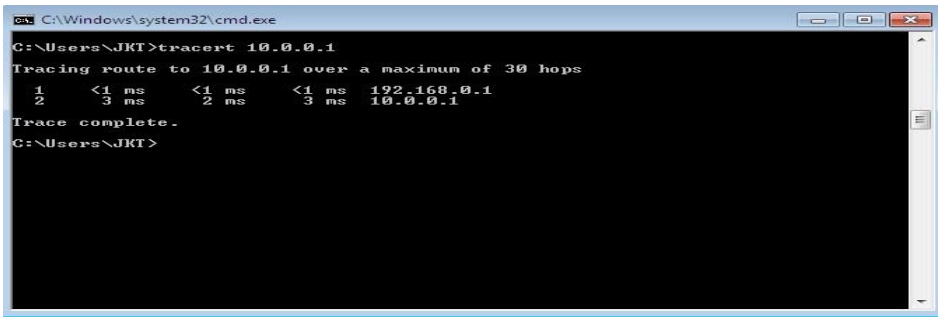
Gambar IV.21 *Ping* dari *client* kantor pusat ke *router* kantor cabang

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



Gambar IV.22 *Ping* dari *client* kantor pusat ke *client* kantor cabang

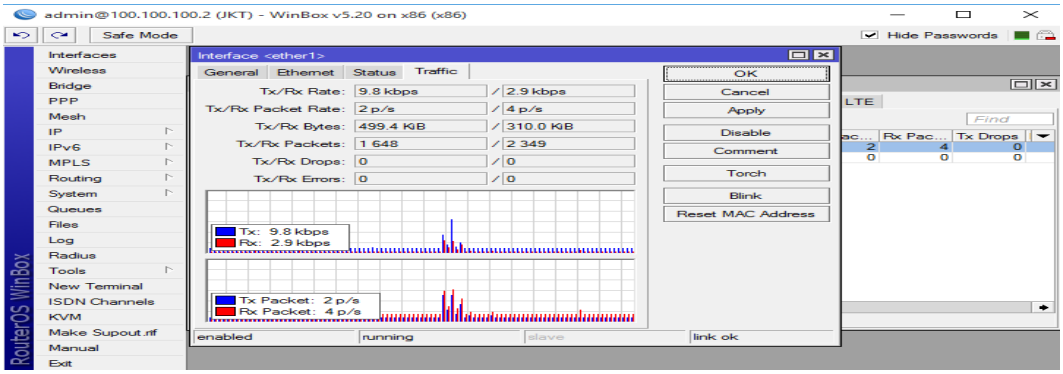
3. Tes koneksi dengan *tracert* dari kantor pusat ke kantor cabang



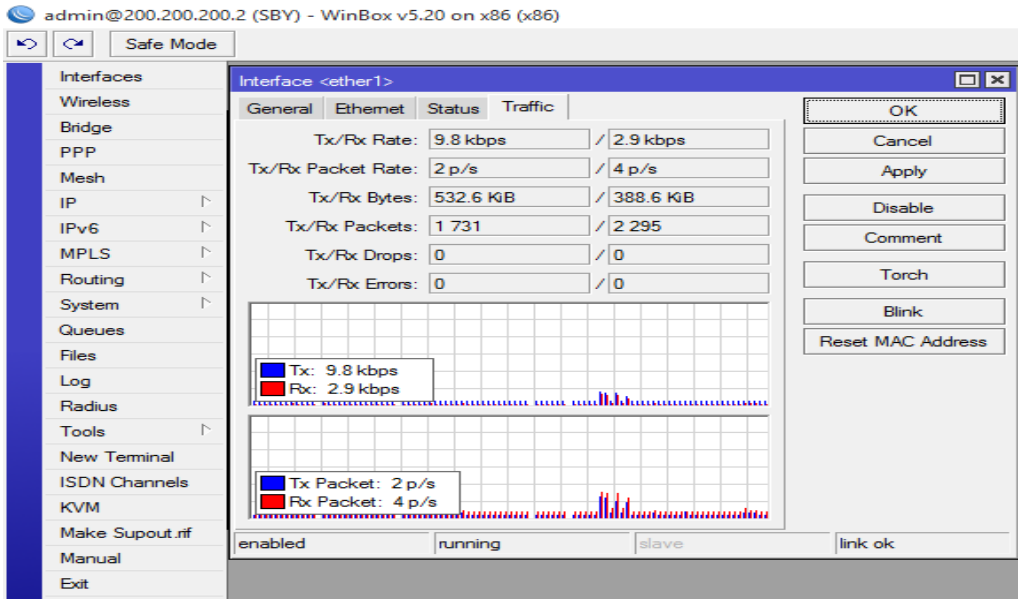
Gambar IV.23 Tes *Tracert* dari kantor pusat ke kantor cabang

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.

4. Grafik *Transfer* Data



Gambar IV.24 Grafik *Transfer* Data pada *Router* Pusat

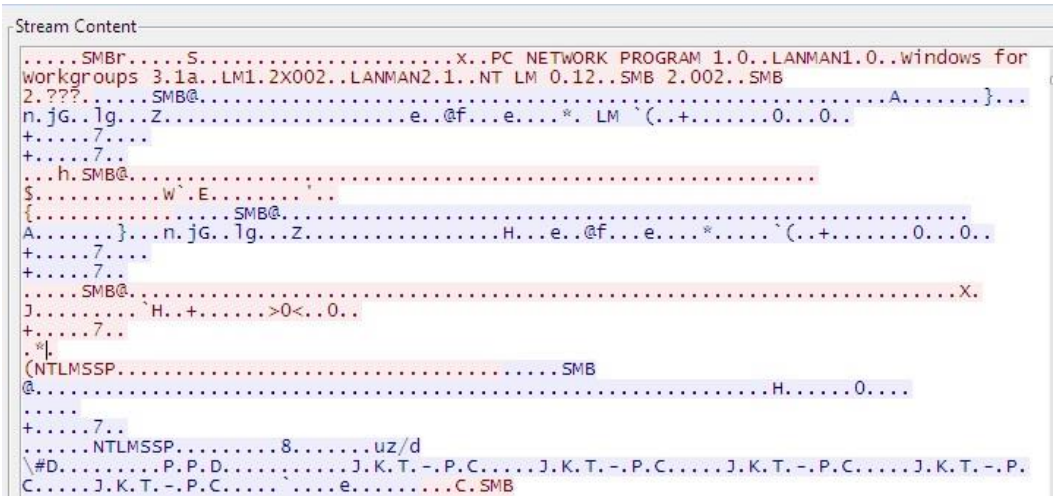


Gambar IV.25 Grafik *Transfer* Data pada *Router* Cabang

5. Tes Pengiriman Data

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

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



Gambar IV.26 Analisa Paket Data