BAB IV

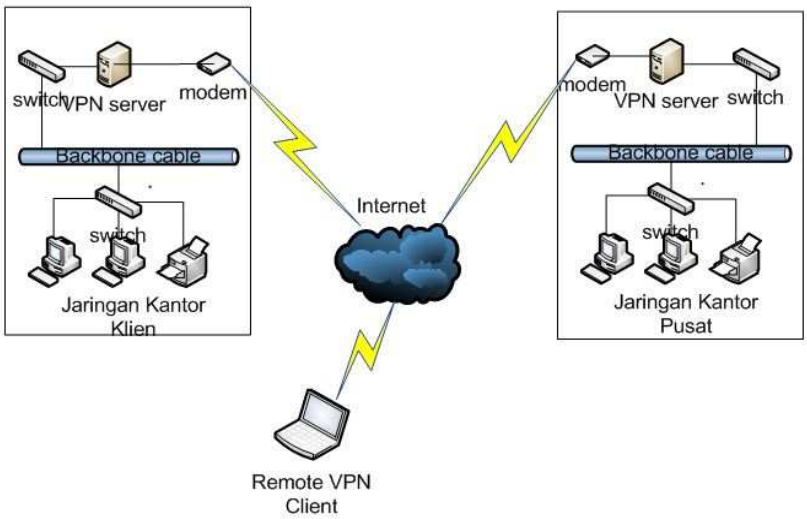
RANCANGAN JARINGAN USULAN

1.1. Jaringan Usulan

Konsep jaringan yang penulis usulkan untuk permasalahan yang ditemukan di PT. Metalogix Infolink Persada adalah dengan penggunaan konsep jaringan VPN dengan metode L2TP/IPsec. Dengan konsep ini diharapkan akan dapat menjadi solusi keamanan jaringan yang diakses dari luar kantor pusat dan untuk mempermudah pekerjaan para pegawai yang memiliki mobilitas tinggi.

1.1.1. Topologi Jaringan

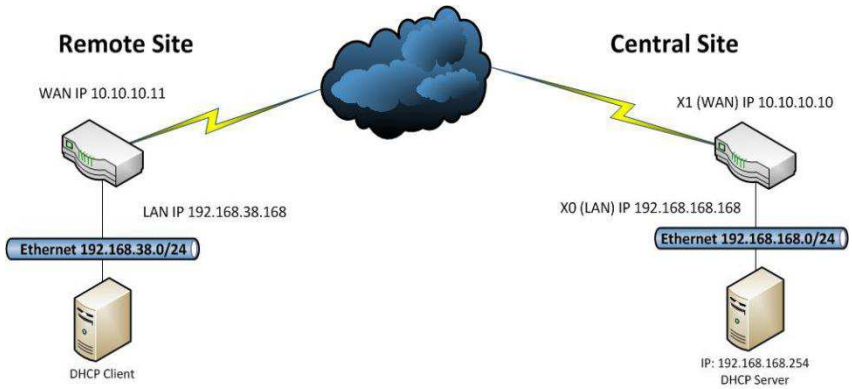
Penggunaan konsep VPN ini tidak banyak merubah topologi LAN kantor pusat yang ada. Dikarenakan konsep ini biasanya digunakan untuk topologi jaringan MAN ataupun WAN. Topologi VPN ini menghubungkan jaringan lokal kantor pusat ke jaringan kantor lainnya melewati jaringan publik.



Gambar 4.1. Topologi VPN

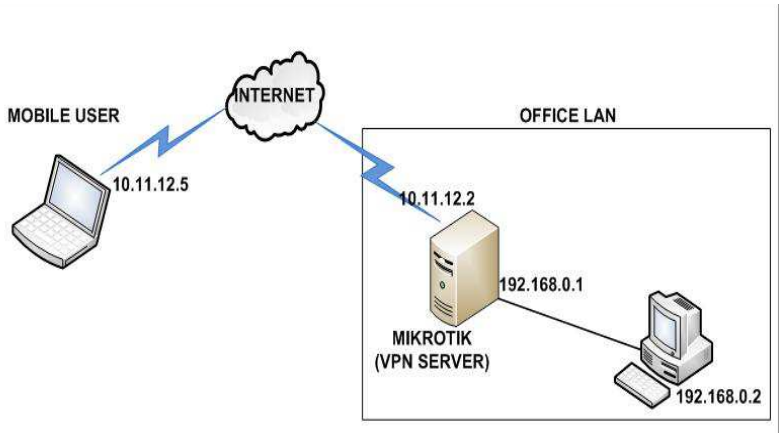
1.1.2. Skema Jaringan

Skema jaringan VPN ini mempunyai dua jenis koneksi. Yang pertama adalah *site-to-site* VPN, yaitu menghubungkan dua buah jaringan lokal yang berjauhan lokasi gedungnya dengan menggunakan jaringan publik sebagai penghubungnya dan menggunakan sebuah VPN *server* pada jaringan lokal kantor pusat dan sebuah VPN *client* pada jaringan kantor cabang.



Gambar 4.2.*site-to-site* VPN

Yang kedua adalah *remote-access* VPN, yaitu menghubungkan sebuah komputer yang berada diluar jaringan lokal kantor pusat yang menggunakan koneksi internet dan aplikasi VPN *client* yang sudah dikonfigurasi pada komputer *remote* yang digunakan.



Gambar 4.3.*remote access* VPN

Tetapi untuk skripsi ini penulis khusus membahas hanya tentang *site-to-site* VPN dengan metode L2TP/IPsec saja.

1.1.3. Keamanan Jaringan

Seperti yang sudah dijelaskan di bab-bab sebelumnya, bahwa keamanan jaringan adalah suatu hal yang penting dalam penggunaan konsep VPN ini. Dikarenakan koneksi yang digunakan untuk menghubungkan antar jaringan adalah koneksi publik yang bisa diakses oleh banyak orang.

Konsep VPN yang ada biasanya sudah memiliki protokol khusus seperti *IPsec* yang dapat mengamankan data saat melewati jaringan publik tersebut.*IPSec* (singkatan dari *IP Security*) adalah sebuah protokol yang digunakan untuk mengamankan transmisi data dalam sebuah *internetwork* berbasis TCP/IP. *IPSec* melakukan enkripsi terhadap data pada lapisan yang sama dengan protokol IP dan menggunakan teknik *tunneling* untuk mengirimkan informasi melalui jaringan internet atau dalam jaringan Intranet secara aman.

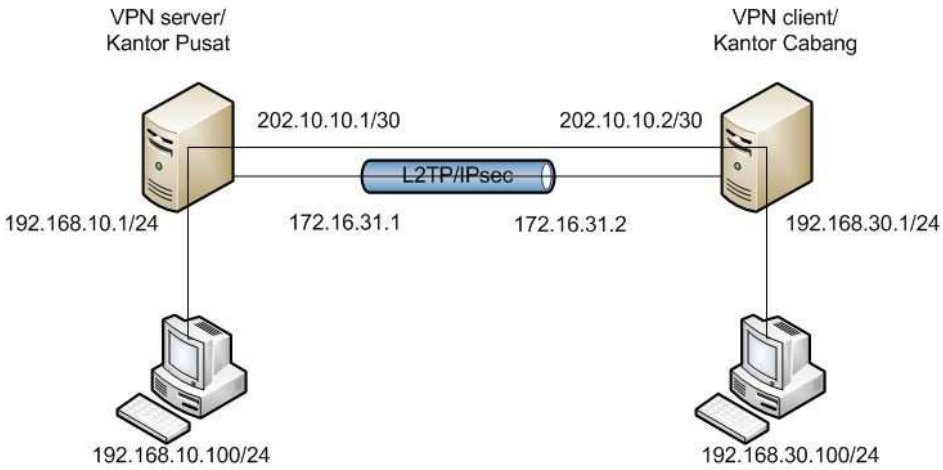
Rancangan VPN yang penulis buat menggunakan metode L2TP/IPsec. Perbedaan dari metode VPN lain adalah keamanan yang cukup baik dengan menggunakan tambahan protokol IPsec pada *layer network.*

1.1.4. Rancangan Aplikasi

Rancangan yang akan penulis terapkan adalah penggunaan *router* mikrotik sebagai VPN *server* dikantor pusat yang dihubungkan ke *switch* utama di jaringan lokal dan terhubung juga ke *modem* untuk koneksi ke internetnya.

Untuk konfigurasi *router* tersebut, penulis menggunakan aplikasi pendukung mikrotik berbasis GUI yaitu *Winbox* yang penulis *install* di perangkat komputer dengan sistem operasi *Windows* 7. Penggunaan *winbox* akan mempermudah dari pengkonfigurasian VPN *server* tersebut.

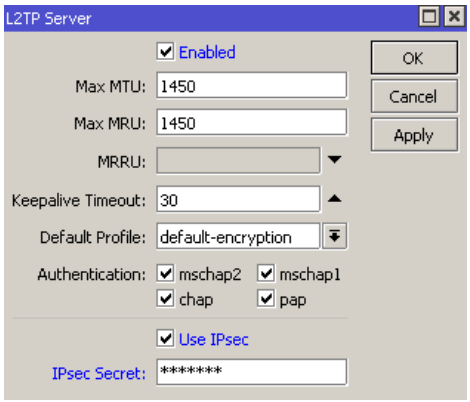
Berikut adalah skema yang penulis buat untuk mensimulasikan teknologi VPN ini pada kantor pusat PT. Metalogix Infolink Persada.



Gambar 4.4. Skema Jaringan Usulan

1. Konfigurasi L2TP VPN *Server*

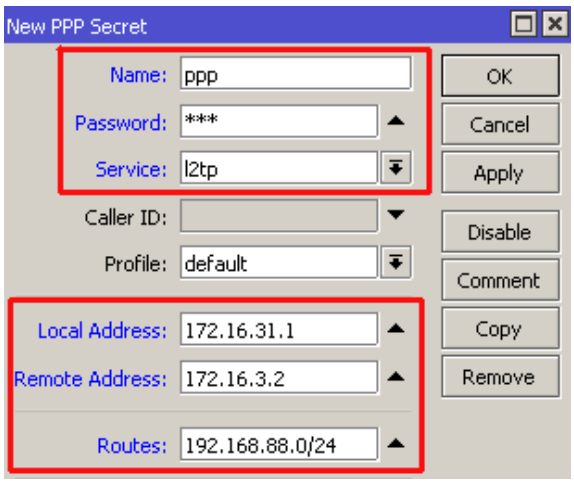
   Pertama kita buka aplikasi *winbox* pada PC yang sudah terhubung ke VPN *server*. Lalu arahkan ke menu **PPP >L2TP *Server*.** Lalu akan muncul tampilan berikut:



Gambar 4.5. Mengaktifkan L2TP *server*

Kita *setting* seperti pada gambar lalu klik tombol OK untuk mengaktifkan L2TP *Server*.

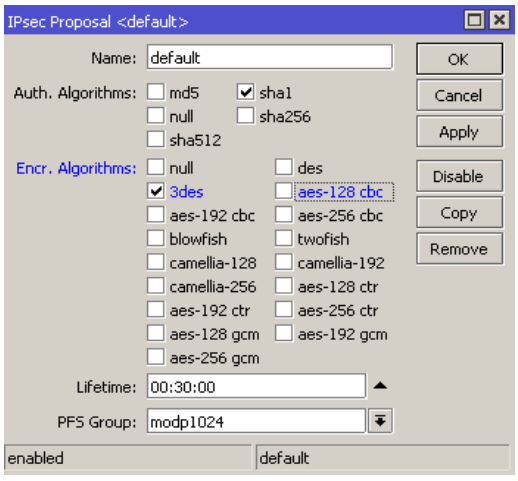
Selanjutnya pilih tab ***Secret*>*Add*** **[+]**. Disini akan kita isi parameter standar seperti *name* dan *password* untuk *dial* koneksi dari VPN *client* dan juga beberapa parameter seperti dalam gambar.



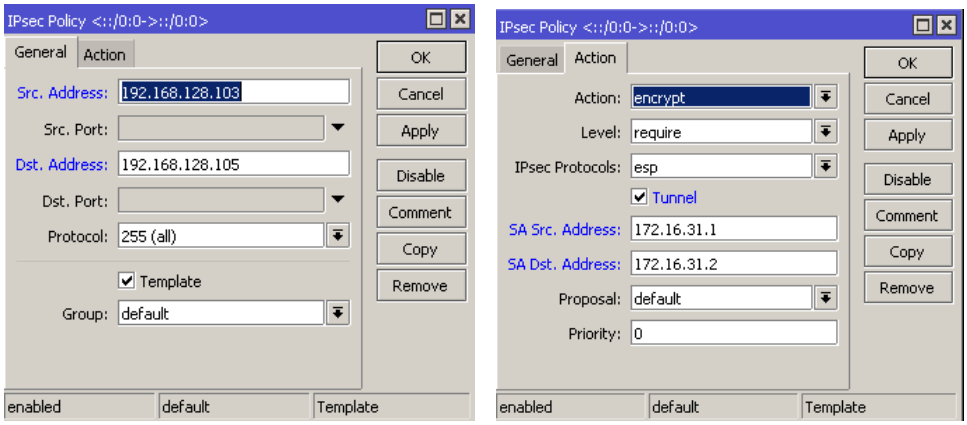
Gambar 4.6. Membuat S*ecret*

2. Konfigurasi *IPsec* VPN *Server*

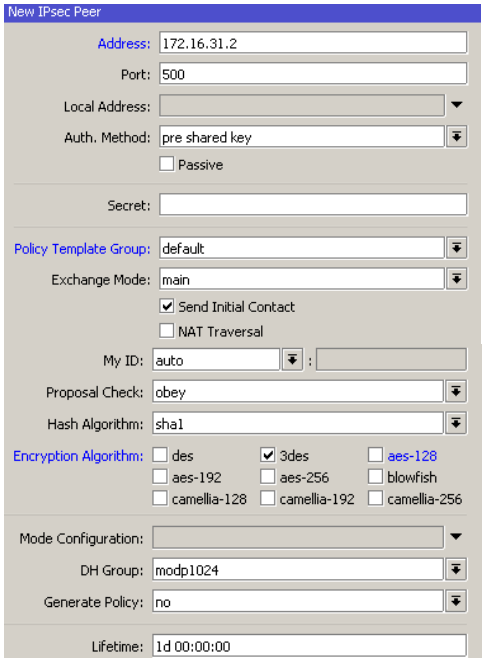
Untuk menambah keamanan, penulis akan memadukan L2TP dengan *IPsec*. Pilih pada menu **IP>IPSec**. Ada beberapa parameter yang dikonfigurasi seperti didalam gambar.



Gambar 4.7.*IPSec Proposal Server*



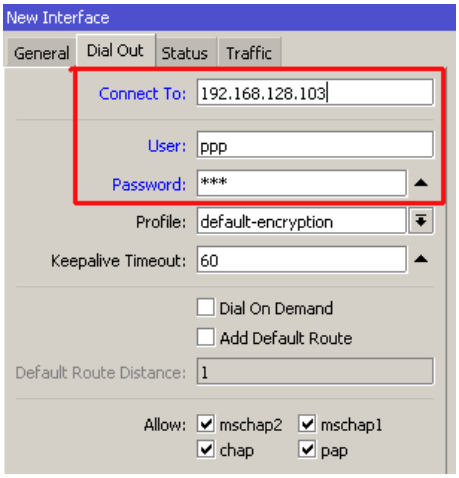
Gambar 4.8.*IPsec Policy Server*



Gambar 4.9.*IPsec Peer Server*

3. Konfigurasi L2TP VPN C*lient*

Selanjutnya setelah selesai mengkonfigurasi VPN *server*, dilanjutkan dengan konfigurasi L2TP di VPN *client*. Kita hanya melakukan *dial* ke L2TP *server*. Buka menu **PPP>*Add* [+]>** pilih **L2TP *client***.



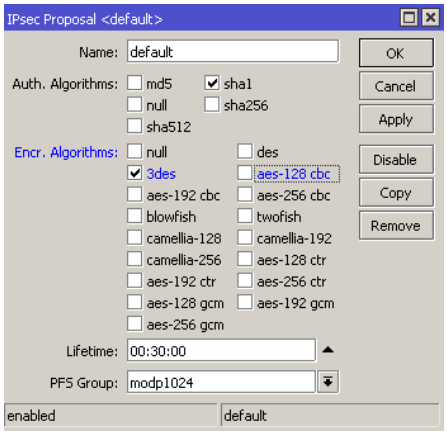
Gambar 4.10.*Setting* L2TP *Client*

Isikan parameter sesuai dengan jaringan yang ada. *Connect* to diisi dengan alamat IP publik *router* kantor pusat. Untuk *user* dan *password* isikan sesuai dengan yang sudah kita buat di VPN *server*.

4. Konfigurasi *IPSec* VPN C*lient*

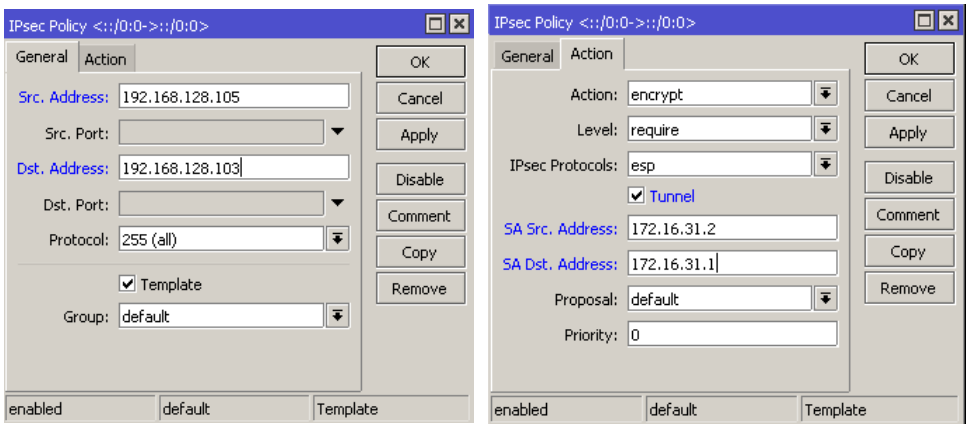
Pada dasarnya parameter yang digunakan untuk *IPSec client* ini tidak jauh berbeda dari yang sudah kita setting di sisi *server*. Hanya ada perbedaan di konfigurasi IP *Address* saja.

Pada tab *IPSec proposal* tidak ada perbedaan dengan konfigurasi di sisi *IPSec server*.



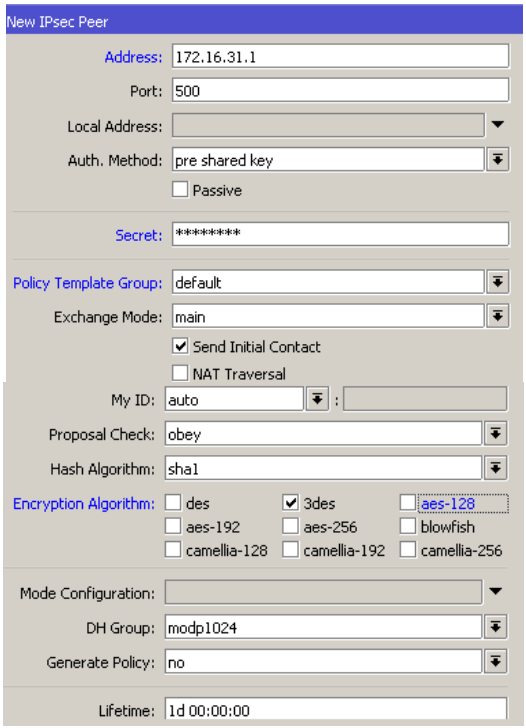
Gambar 4.11. IPsec *Proposal client*

Selanjutnya pada tab *IPSec Policy*. Sesuaikan IP *address* asal dan tujuan yang digunakan.



Gambar 4.12.*IPsec Policy Client*

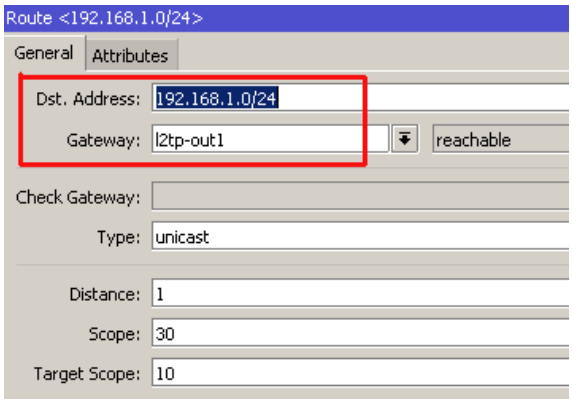
Setelah setting *IPSec Policy*, dilanjutkan dengan setting *IPSec Peer*.



Gambar 4.13.*IPsec Peer Client*

5. Interkoneksi Jaringan

Agar jaringan dari kedua sisi bisa saling terkoneksi. Maka dibuat *routing* statik secara manual di L2TP *client*.



Gambar 4.14.*Routing* Statik C*lient*

Setelah itu baru dipastikan bahwa jaringan kantor sudah saling terkoneksi bisa dengan menggunakan perintah ping dari masing-masing kantor ke kantor lainnya.

1.1.5. Manajemen Jaringan

Manajemen jaringan yang diusulkan tidak jauh berbeda dari manajemen jaringan yang sudah ada. Perbedaannya hanya pada pemberian hak akses untuk karyawan kantor untuk bisa mengakses jaringan lokal kantor pusat dari luar.

Pemberian hak akses tersebut adalah berupa pemberian *username* dan *password* VPN *client* kepada karyawan untuk digunakan saat ingin membuka koneksi ke kantor pusat melalui jaringan VPN.

Tidak semua karyawan yang bisa atau dapat mengakses jaringan dari luar kantor untuk menjaga keamanan data. Hanya beberapa karyawan yang dikira sangat membutuhkan yang akan diberikan hak akses tersebut.

4.2. Pengujian Jaringan

Pada sub-bab ini akan dijelaskan perbedaan yang ditemukan antara jaringan awal sebelum memakai L2TP/IPsec dan jaringan akhir setelah memakai L2TP/IPsec berdasarkan simulasi yang dilakukan oleh penulis.

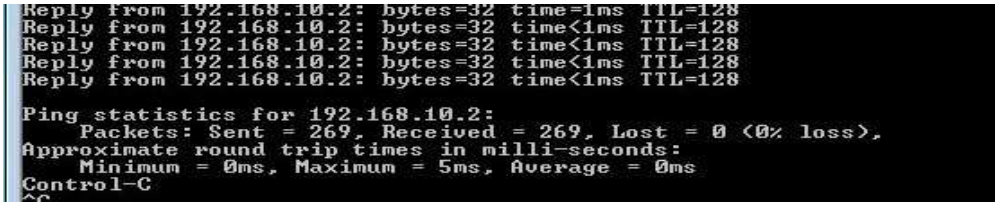
Akan dilakukan beberapa tahap pengujian yaitu *packetloss* dengan menggunakan perintah '*ping'* pada *command prompt*, lalu akan dilakukan *denial of service* menggunakan aplikasi *pingflood.exe* dan terakhir akan dilakukan *sniffing* menggunakan aplikasi *wireshark.*

4.2.1. Pengujian Jaringan Awal

Pada pengujian jaringan awal akan dilakukan tes terhadap jaringan kantor yang sedang berjalan tanpa VPN.

1. *Packet Loss Test*

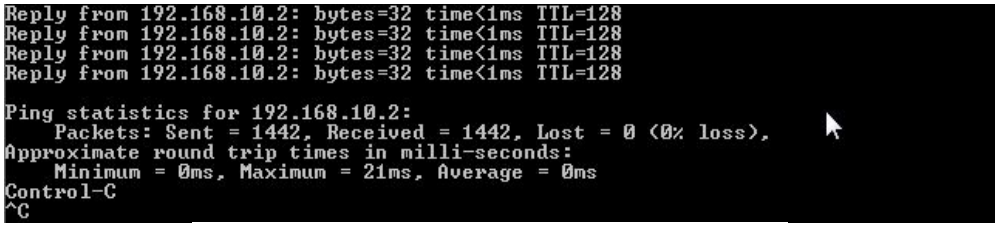
   Pengujian packet *loss* dilakukan beberapa kali tes dengan perintah '*ping'* ke *IP* tujuan menggunakan *command prompt* untuk melihat stabilitas koneksi di jaringan tanpa menggunakan VPN. Dan didapatkan hasil sebagai berikut:



Gambar 4.15 *Packet loss* jaringan awal

2. *Denial of Service Test*

   Pengujian ini untuk mengetahui ketahanan koneksi saat dibanjiri paket. Pengujian dilakukan dengan aplikasi *pingflood.exe*. Setelah dilakukan pengujian didapatkan hasil sebagai berikut:

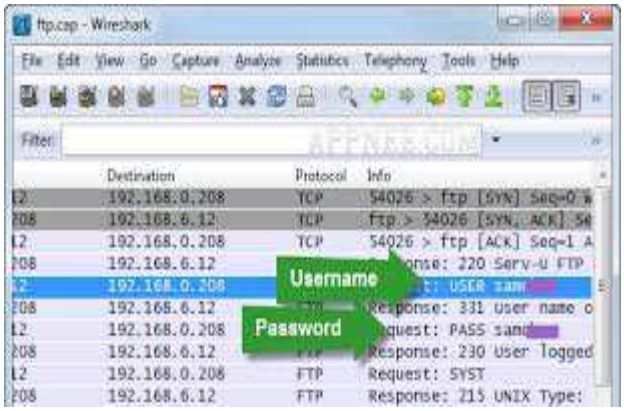


Gambar 4.16 *DoS Attack* jaringan awal

Pengujian dilakukan dengan mengirimkan 10000 paket data sebesar 25kb didapatkan hasil, bahwa jaringan tidak terputus dan maksimum *round trip* sebesar 21ms.

3. *Sniffing Test*

Pada test kali ini akan dilakukan *sniffing* pada *user* dan *password* FTP. Saat salah satu PC mengakses sebuah FTP di dalam kantor. Berikut adalah hasil *sniffing username* dan *password* FTP.



Gambar 4.17. Hasil *sniffing password*

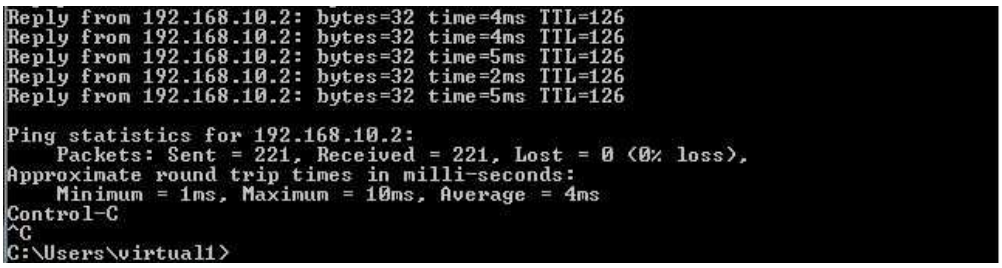
Seperti yang terlihat klien PC dengan IP 192.168.6.12 me*request* koneksi FTP *server* di IP 192.168.0.208 dengan *username* dan *password* dan semuanya bisa terlihat melalui *sniffing* dengan aplikasi Wireshark.

4.2.2. Pengujian Jaringan Akhir

Pada pengujian jaringan akhir ini akan dilakukan beberapa tes seperti yang sudah dilakukan di pengujian jaringan awal tadi. Dengan begitu nanti akan bisa dilihat perbedaan dari kedua jaringan ini anatar yang menggunakan VPN dan yang tidak menggunakannya.

1. *Packet Loss Test*

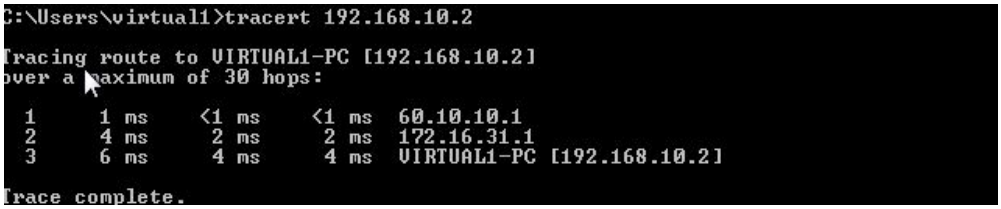
   Pengujian *packet loss* dilakukan beberapa kali tes dengan perintah *'ping'* ke *IP* tujuan menggunakan *command prompt* untuk melihat stabilitas koneksi di jaringan menggunakan L2TP/IPSecVPN. Dan didapatkan hasil sebagai berikut:



Gambar 4.18. *Packet Loss* Jaringan VPN

Dari data diatas dapat kita lihat untuk data max dan *average round trip* suatu paket masih dalam nilai yang wajar. Dari percobaan 221 kiriman paket, max round trip = 10ms dan average round trip = 4ms.

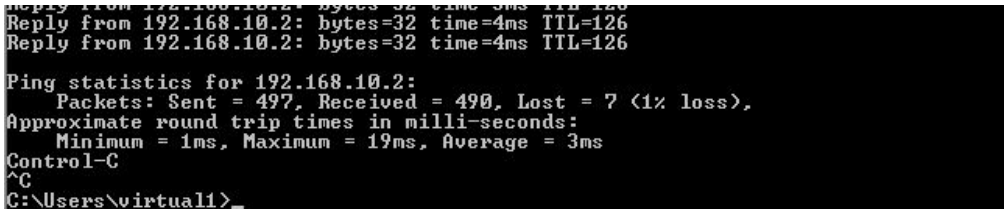
Penulis juga melakukan *trace route* untuk melihat apakah paket yang dikirim sudah melewati jaringan L2TP yang dibuat. Dan seperti gambar dibawah, hasilnya adalah paket dikirim melalui *gateway* kantor cabang IP 60.10.10.1 dan diteruskan ke IP VPN *server* 172.16.31.1.



Gambar 4.19. *Trace Route* VPN

2. *Denial of Service Test*

Pengujian ini untuk mengetahui ketahanan koneksi saat dibanjiri paket. Pengujian dilakukan dengan aplikasi *pingflood.exe*. Setelah dilakukan pengujian didapatkan hasil sebagai berikut:



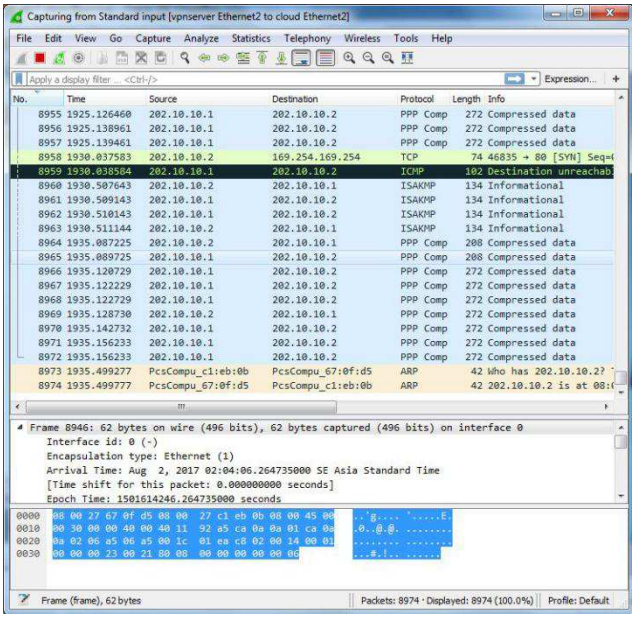
Gambar 4.20. *Pingflood* Jaringan VPN

Data diatas adalah hasil dari pengujian dengan membanjiri VPN *server* dengan 10,000 paket data sebesar 25kb. Hasilnya menunjukan bahwa hanya terjadi beberapa kali *timeout* tetapi tidak sampai mematikan *service* VPN.

3. *Sniffing Test*

Pada kesempatan ini dilakukan pengetesan menggunakan aplikasi Wireshark. Dengan cara meng*capture traffic* pada jaringan antara kantor pusat dengan kantor cabang.

Setelah itu dilakukan pengaksesan FTP *server* pada kantor pusat dari komputer di kantor cabang. Hasilnya *traffic* protokol FTP berupa *username* dan *password* tidak terbaca pada aplikasi wireshark seperti yang ada pada pengujian jaringan awal.



Gambar 4.21. *Sniffing* Jaringan VPN