BAB IV

DISKRIPSI KERJA PRAKTEK

Dalam kerja praktek ini penulis membuat rancangan jaringan VPN yang dimaksudkan untuk membantu memecahkan masalah pada proses pengiriman data maupun informasi secara aman dan dapat diakses dari manapun dengan kebutuhan semua pihak yang terkait. Dalam merancang jaringan VPN yang baik harus melalui tahap-tahap perancangan jaringan. Cara pengumpulan data jaringan untuk penyelesaian kerja praktek ini baik di dalam memperoleh data, menyelesaikan dan memecahkan permasalahan yang diperlukan dalam menganalisa, merancang dan mengembangan jaringan adalah melakukan observasi pada kantor Dinkominfo Surabaya yaitu dengan mengumpulkan dan mengamati secara langsung terhadap jaringan yang akan digunakan dalam pengoperasiannya.

Setelah mendapatkan data jaringan yang diperlukan, penulis mengadakan tanya jawab dan konsultasi untuk memperoleh informasi mengenai sistem yang berlaku ataupun informasi-informasi lain yang sekiranya dapat membantu pengembangan jaringan.

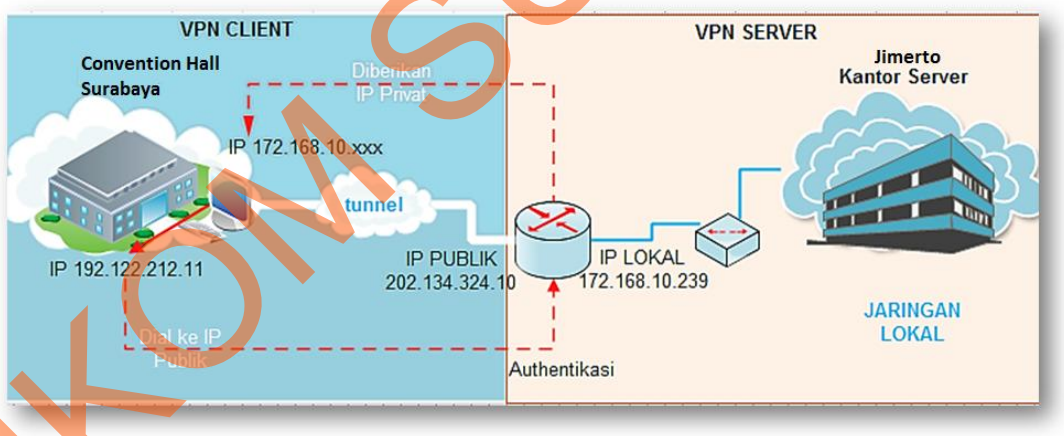
Dalam pengerjaan jaringan VPN ini penulis juga melakukan studi literature untuk mengetahui lebih jelas apa yang akan dikerjakan dan pokok peembahasan penulis mempelajari buku-buku yang terkait dengan pemecahan masalah tentang VPN.

Setelah mendapatkan semua data informasi yang dibutuhkan penulis memasuki tahap pengerjaan untuk mendesain struktur jaringan VPN, mengkonfigurasi VPN client dan server serta melakukan pengujian.

Setelah desain struktur VPN sesuai dengan yang diinginkan, maka penulis akan melakukan implementasi, konfigurasi dan pengujian mengenai tugas kerja praktek ini.

4.1. Rancang dan Konfigurasi VPN

Setelah melakukan desain jaringan VPN, maka penulis dapat mengetahui gambaran dari jaringan yang akan penulis buat. Berikut ini adalah desain jaringan yang penulis buat pada kerja praktek.



Gambar 4.1 Desain jaringan VPN Perijinan Kartu Kuning

Pada gambar 4.1 di atas merupakan gambaran desain jaringan VPN Perijinan Kartu Kuning pada Dinkominfo Surabaya. Di sisi server, akan menggunakan 2 IP, yakni IP Publik dan IP Lokal yang nantinya di-setting di *router* (mikrotik). Fungsi router

mikrotik disini sebagai gateway antara jaringan publik dengan jaringan privat dan VPN Server. Alokasi ip publik yang sudah ditentukan yaitu 202.134.324.10 dan ip lokal 172.168.10.239/24.

Keterangan gambar:

1. IP Publik (router/fe1) : 202.134.324.10
2. IP Lokal (router/fe2): 172.168.10.239/24
3. IP Privat yang diberikan setelah melakukan autentikasi : 172.168.10.10/24
4. IP PC Client yang terhubung modem : 192.122.212.11

Berdasarkan gambar di atas yang pertama kita lakukan adalah membuat desain. Pada gambar desain jaringan VPN, terdapat server yang berada di kantor Jimerto (Dinkominfo) dan client VPN yang berada di Convention Hall Surabaya. Client yang berada di Convention memiliki 2 PC client yang digunakan untuk mengakses aplikasi Perijinan Kartu Kuning yang salah satunya mempunyai ip 172.168.10.250. Setelah desain terbentuk maka yang kita lakukan adalah menentukan IP address yang sudah dialokasikan. Kemudian melakukan konfigurasi pada VPN Server. Konfigurasi yang dilakukan pada VPN Server meliputi pengaturan di router mikrotik sebagai berikut:

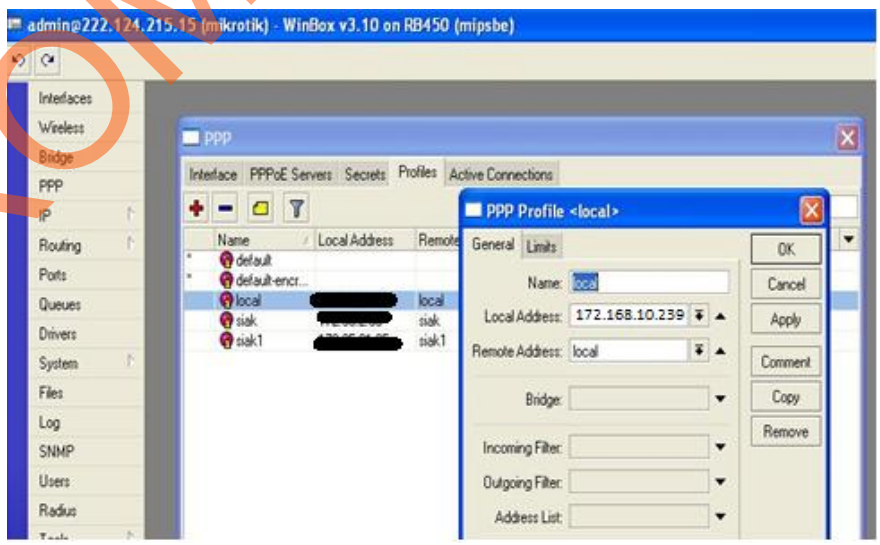
1. Membuat profile local pada Mikrotik RB 450G.
2. Pengaturan secret untuk username dan password yang akan digunakan untuk memverifikasi sebelum VPN Client terhubung ke VPN Server.
3. Membuat PPP (*Point-to-Point Protocol*) interface

Setelah melakukan konfigurasi pada VPN Server kemudian kita melakukan konfigurasi pada VPN Client yang berada di Gedung Convention Hall Surabaya. Tahapan yang dilakukan adalah sebagai berikut:

1. Mempersiapkan PC yang akan digunakan sebagai VPN Client.
2. Membuat VPN Connection di setiap PC yang akan digunakan sebagai Client dengan memasukkan IP Publik yang telah disesuaikan dengan VPN Server, jika tidak sama maka tidak akan terbentuk suatu koneksi.
3. Setting username dan password untuk dial-up pertama kali, ini juga harus sesuai dengan VPN Server.
4. Setelah itu mengatur properties pada VPN Connection meliputi, pengaturan security PPTP dan pengaturan data encryption.

4.2. Implementasi VPN Server di Jimerto (Dinkominfo)

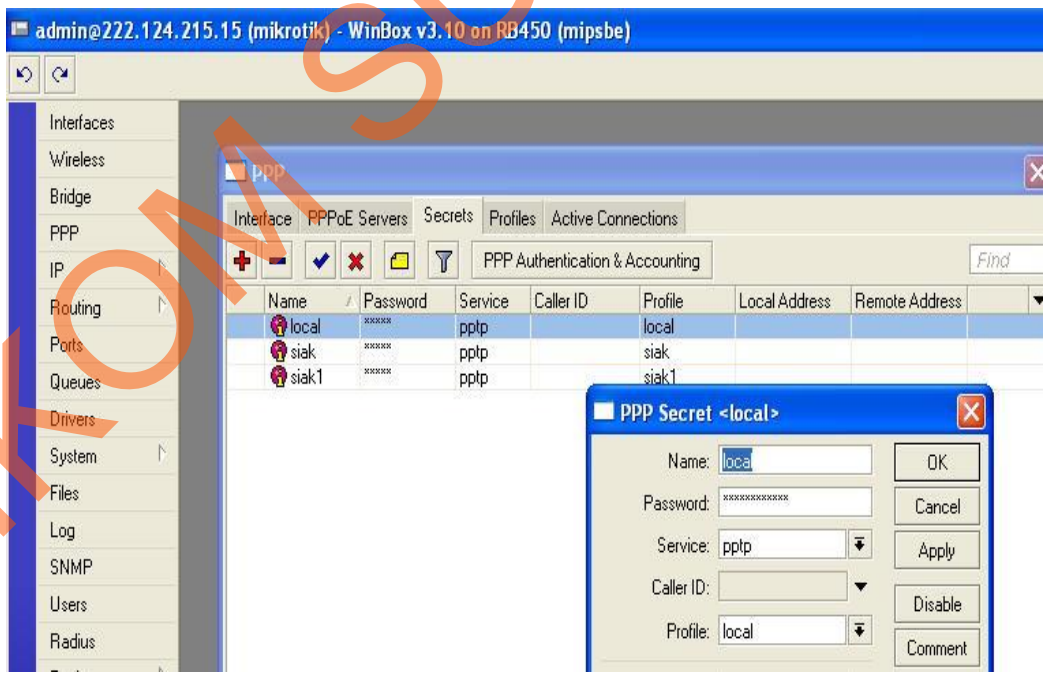
1. Membuat profile dg nama local, address 172.168.10.239



Gambar 4.2 Pembuatan Profile PPP

PPP adalah kepanjangan dari Point to Point Protocol merupakan fitur yang diperlukan untuk komunikasi serial dengan PPP, ISDN PPP, L2TP dan PPTP serta komunikasi PPP on Ethernet (PPPoE). Paket PPP digunakan untk komunikasi Wide Area Network dengan menggunakan komunikasi serial asynchronous maupun mode Synchronous. Fitur PPP ini jika digunakan pada mode synchronous akan memerlukan hardware tambahan tertentu yang didukung oleh driver dalam paket synconous. Sedangkan untuk komunikasi dengan Synchronous dapat menggunakan serial port seperti com1 dan com2.

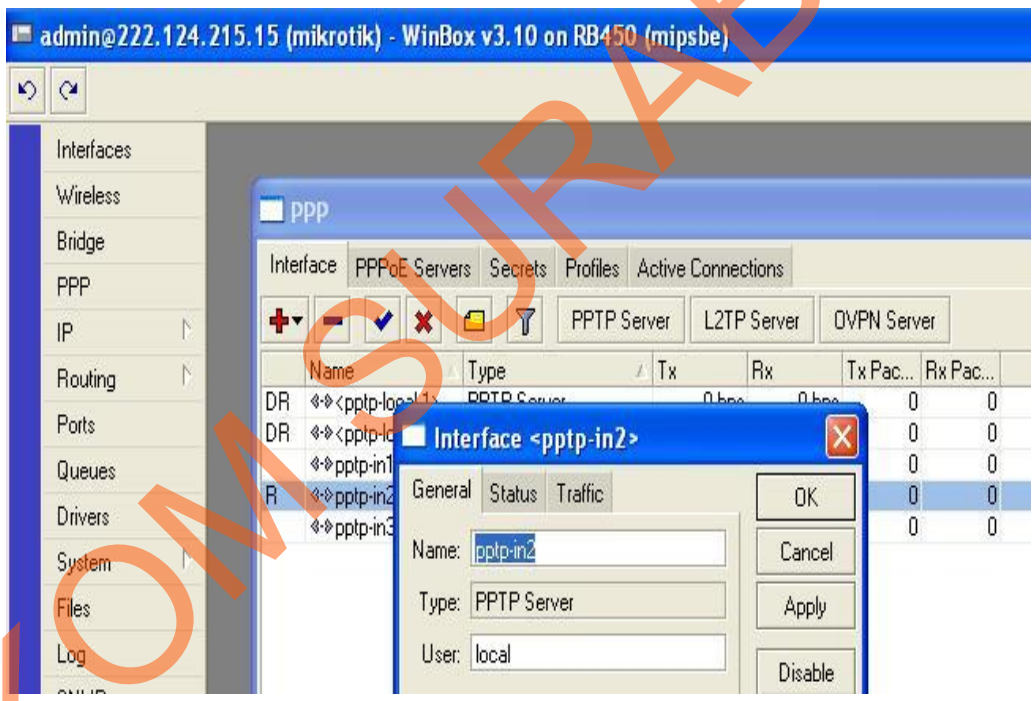
2. Kemudian pilih tab secret dan tambahkan user dan pasword untuk client yang pertama kali masuk ke jaringan VPN.



Gambar 4.3 Pembuatan PPP Secret

PPP secret merupakan fitur mikrotik yang digunakan untuk memberikan layanan keamanan dalam komunikasi jaringan antara VPN Client dan VPN Server. Di sini VPN Server membuat suatu password yang digunakan untuk verifikasi pertama kali yang dilakukan oleh VPN Client. Sehingga dengan cara ini keamanan dalam komunikasi dapat terjamin.

3. Lalu, membuat interface dg nama: pptp-in2 type: PPTP-Server user: local



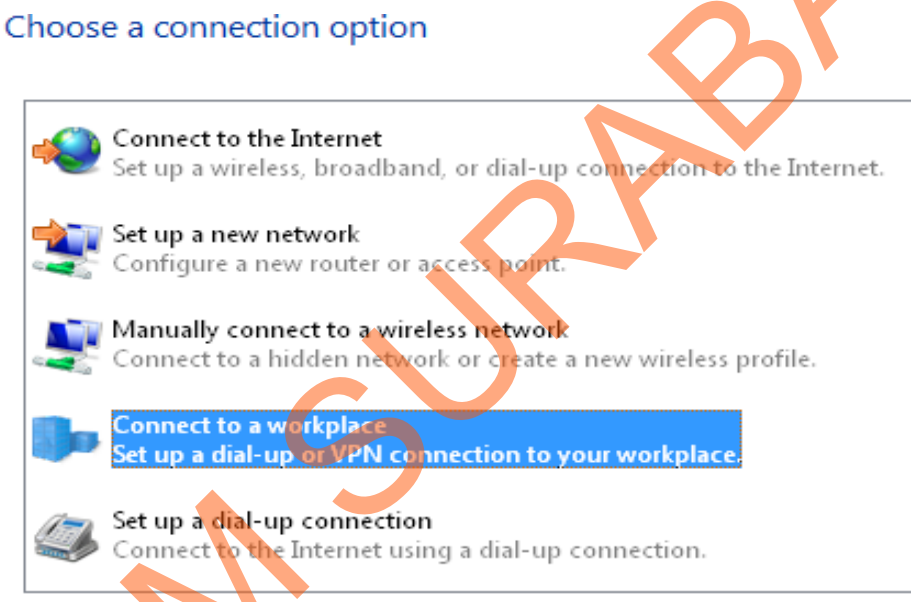
Gambar 4.4 Pembuatan PPP Interface

PPTP atau Point to Point Tunneling Protocol merupakan salah satu model tunneling (terowongan). Artinya adalah terowongan virtual di atas jaringan publik. Selain PPTP terdapat pula *Layer 2 Tunneling Protocol* (L2TP), Generic *Routing Encapsulation* (GRE) atau *IP Sec*. PPTP dan L2TP adalah layer 2 tunneling protocol.

Keduanya melakukan pembungkusan payload pada frame *Point to Point Protocol* (PPP) untuk dilewatkan pada jaringan. IP Sec berada di yang menggunakan packet, yang akan melakukan pembungkusan IP header sebelum dikirim ke jaringan.

4.3. Implementasi VPN Client di Convention Hall Surabaya

1. Membuat VPN connection



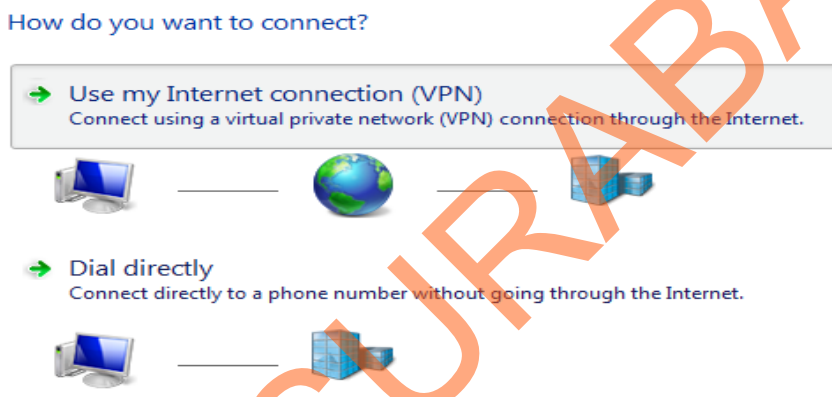
Gambar 4.5 Pembuatan VPN Connection

2. Jika belum ada, pilih No, create a new connection

Gambar 4.6 Pembuatan VPN Connection

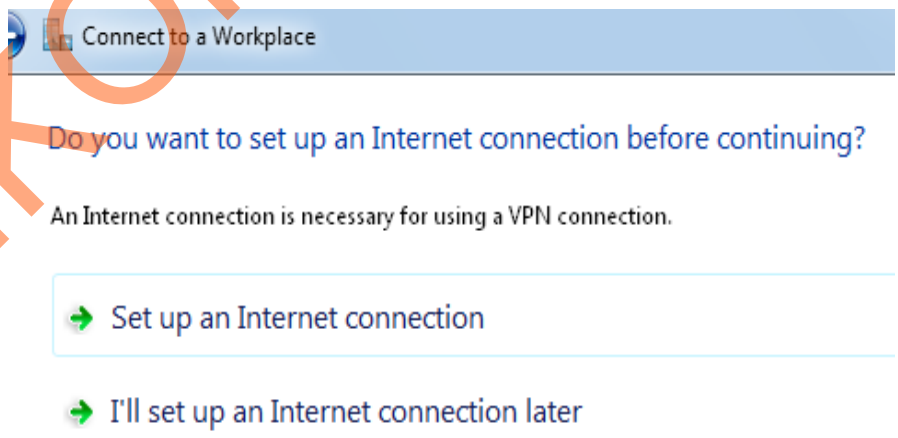
Gambar 4.6 merupakan tahapan pembuatan VPN Connection pertama kali. Jika belum ada VPN Connection yang terdapat di PC client, maka pilih No, create a new connection untuk membuat baru. Jika sudah ada maka pilih Yes, I'll choose an existing connection untuk memilih VPN connection yan sudah dibuat sebelumnya.

3. Kemudian pilih, use my internet connection (VPN)



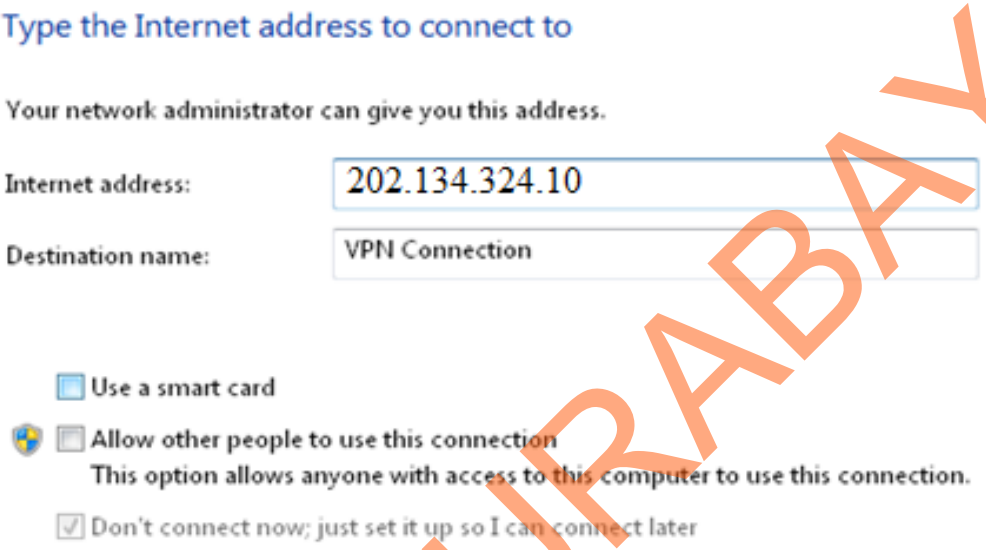
Gambar 4.7 Pemilihan Internet Connection VPN

4. Kemudian pilih set up an internet connection



Gambar 4.8 Connect to Workplace

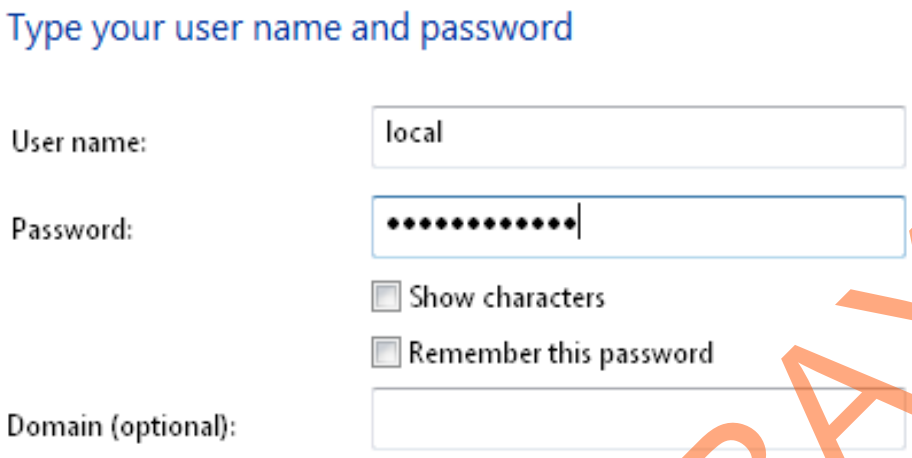
5. Masukkan ip publik dan destination name, ip publik : 202.134.324.10



Gambar 4.9 Memasukkan IP publik

Internet addresss disini adalah ip publik yang diberikan dari sebuah provider tertentu yang telah digunakan pada VPN Server. Internet address ini digunakan saat pertama kali VPN Client melakukan dial-up. Jika internet address tidak sesuai maka VPN Client tidak akan tersambung dengan VPN Server yang dituju.

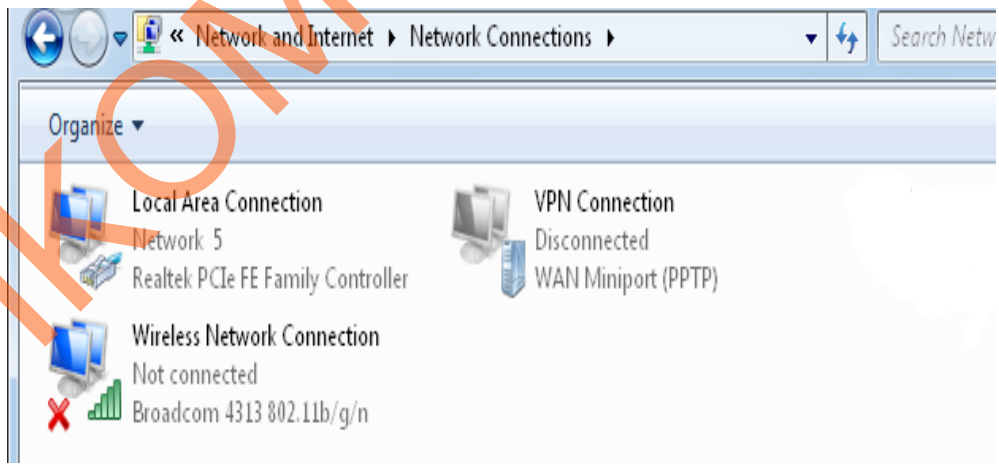
6. Isi username dan password untuk login pertama untuk setiap dial-up ke vpn server dimana harus sama dg sisi server



Gambar 4.10 Memasukkan Username dan Password

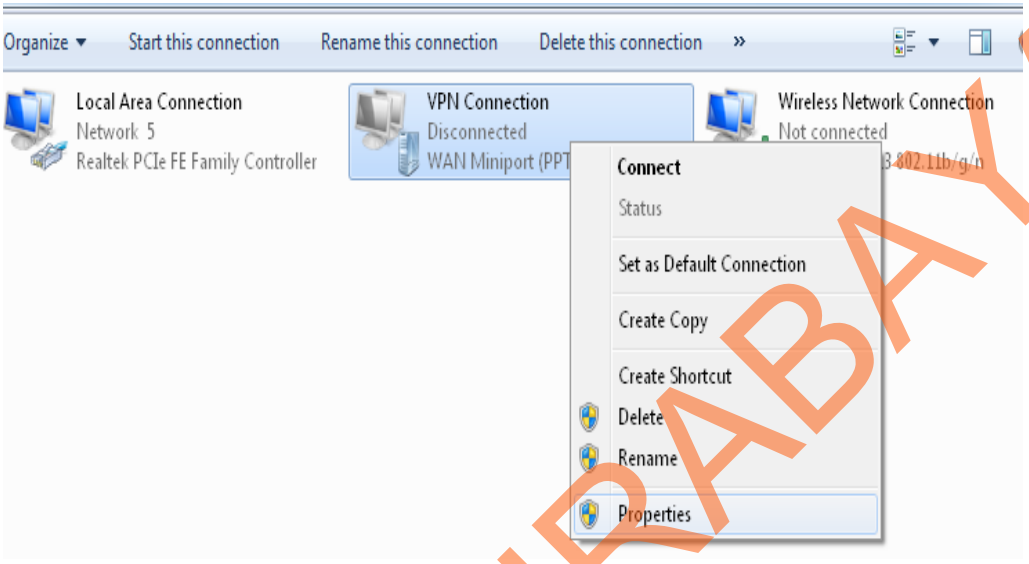
User dan password harus sama dengan yang dikonfigurasi pada VPN Server. User disini diisi local dan password menggunakan perijinankartukuning.

7. Lihat VPN yang kita buat pada network connection : “VPN Connection”



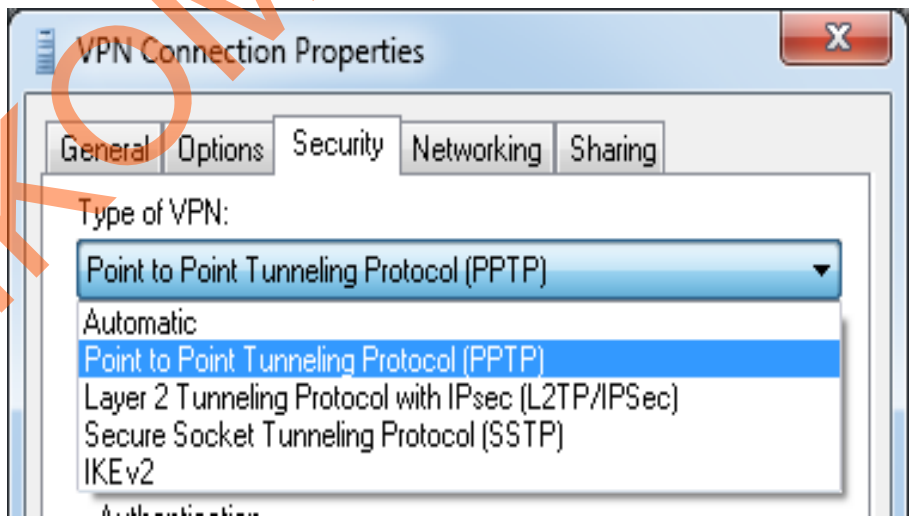
Gambar 4.11 Tampilan VPN Connection yang sudah dibuat

8. Klik kanan kemudian pilih propertis



Gambar 4.12 Pilih Propertis

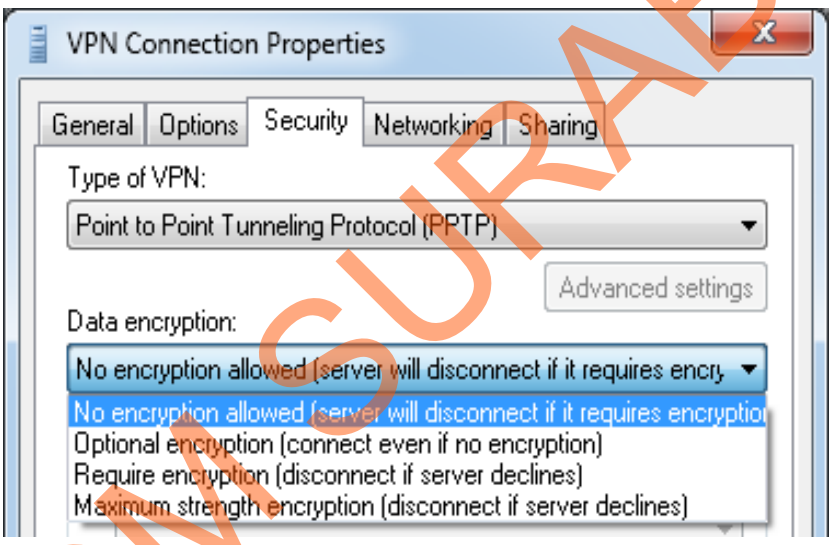
9. Melakukan pengaturan pada Security: pilih Point to Point Tunneling Protocol (PPTP)



Gambar 4.13 Pengaturan Security

PPTP *(Point to Point Tunneling Protocol)* adalah metode tunneling (terowongan) virtual di atas jaringan publik. PPTP bersama L2TP *(Layer 2 Tunneling Protocol)* melakukan pembungkusan payload pada frame *Point to Point Protocol* (PPP) untuk dilewatkan pada jaringan.

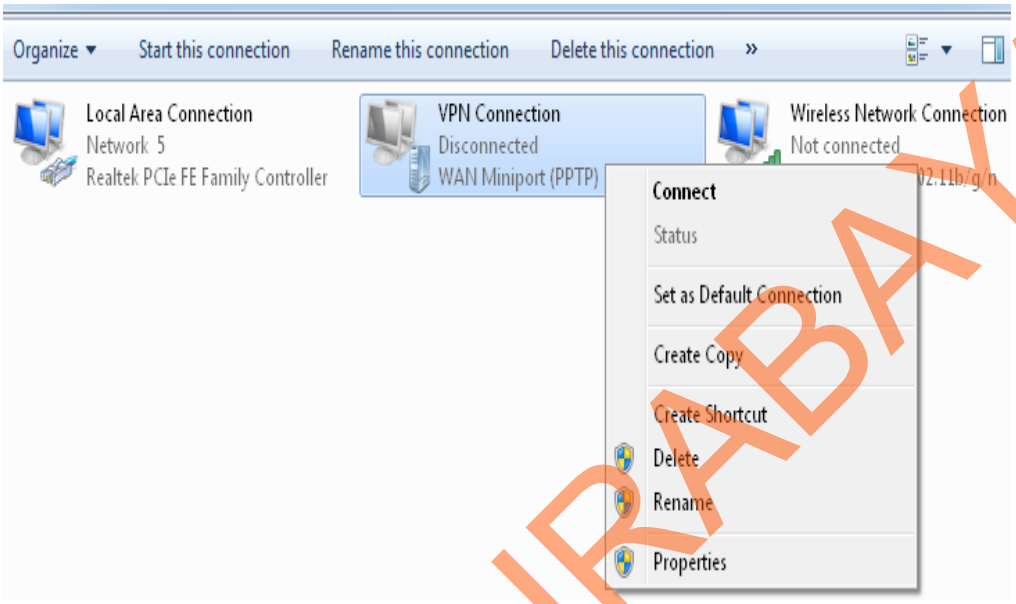
10. Melakukan pengaturan pada Security data encryption : No encryption allowed (server will disconnect if it requires encryption)



Gambar 4.14 Pengaturan Data Encryption

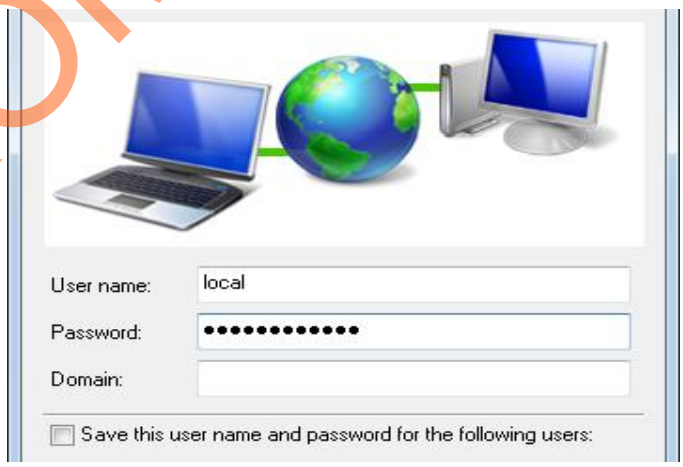
Merupakan metode enkripsi untuk *Encapsulations* (membungkus) paket data yang lewat di dalam tunneling, data yang dilewatkan pada pembungkusan tersebut, data disini akan dirubah dengan metode algoritma *cryptographic* tertentu seperti DES, 3DES atau AES.

11. Kemudian lakukan connect kembali untuk melihat hasil pengaturan yang telah dilakukan.



Gambar 4.15 Pilih Connect

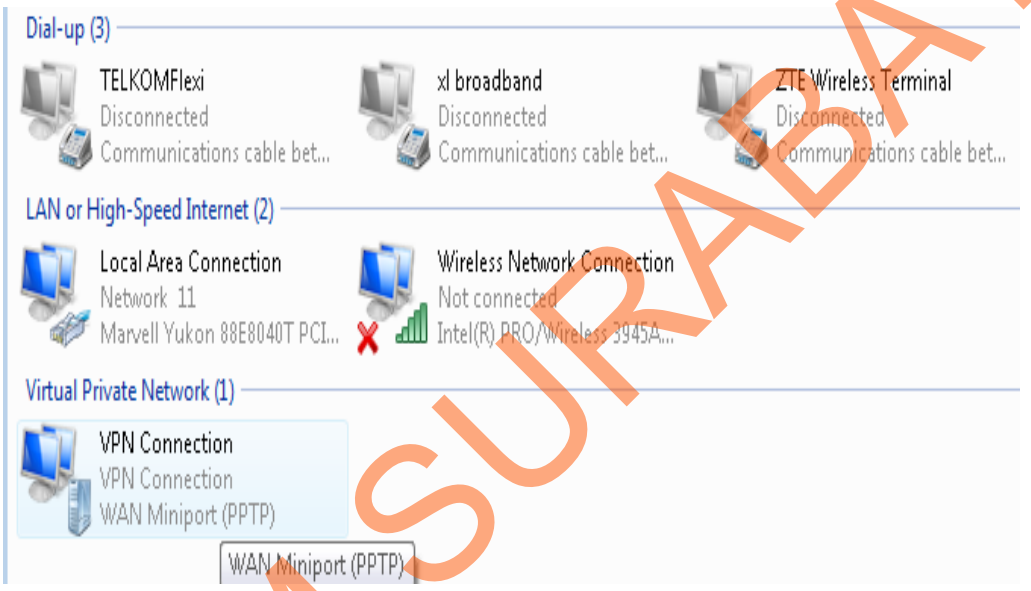
12. Lalu, kita diminta untuk memasukkan username dan password. Isi sesuai dengan yang kita atur tadi.



Gambar 4.16 Dial-up dengan Mengisi Username dan Password

Masukkan username dan password yang telah kita konfigurasi sebelumnya. Username dan password harus sama dengan yang dikonfigurasi pada VPN Server.

13. VPN telah terkoneksi



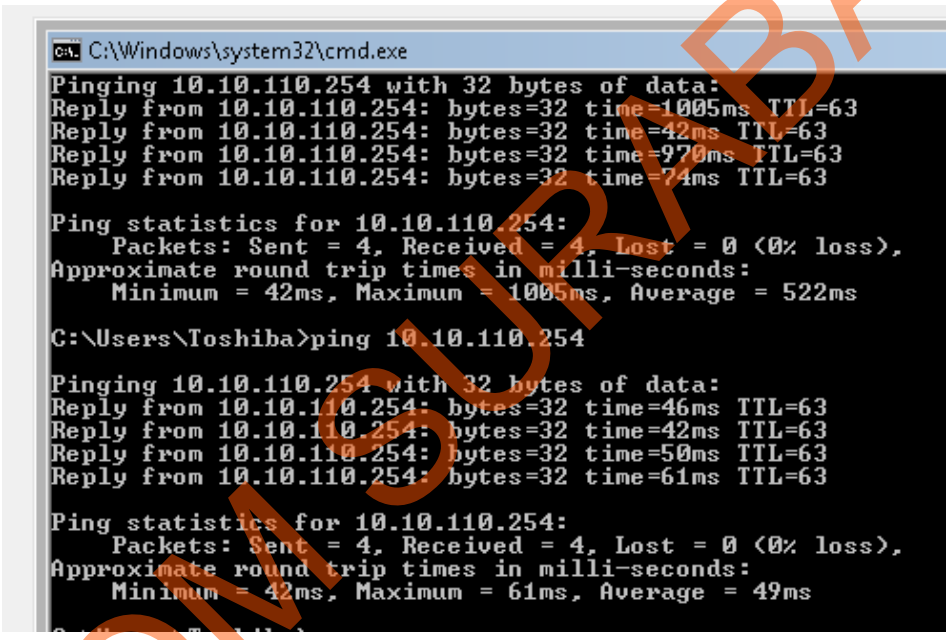
Gambar 4.17 Tampilan VPN yang telah sukses terkoneksi

Setelah VPN Server memverifikasi username dan password dan dinyatakan benar, maka koneksi VPN antara client dan server telah terbentuk.

4.4. Pengujian Koneksi VPN

Pengujian implementasi VPN Kartu Kuning ini berada di Convention Hall dengan menggunakan laptop sebagai client VPN untuk mengakses aplikasi Perijinan Kartu Kuning.

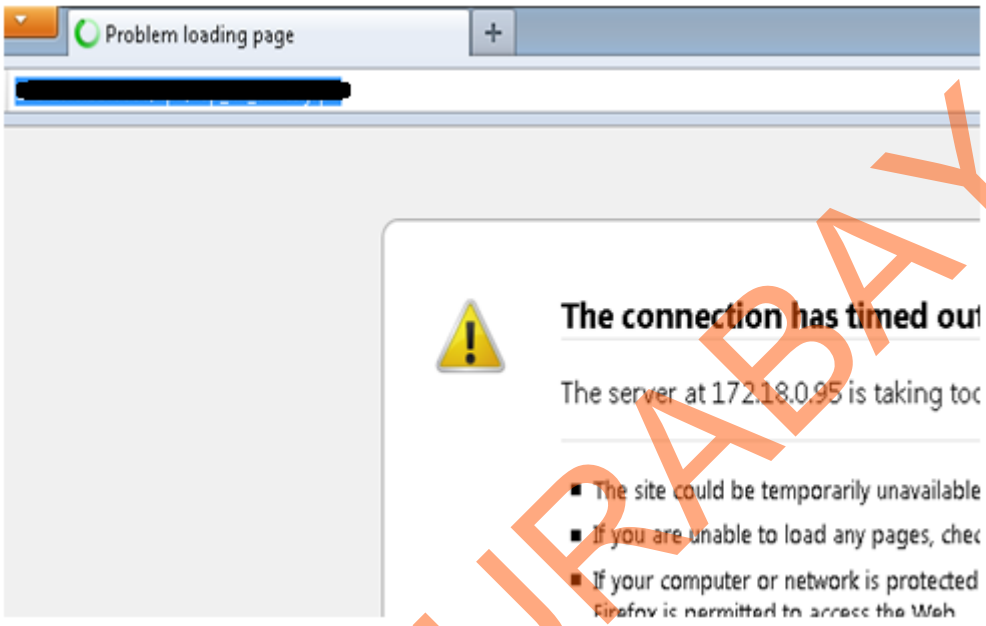
1. Masukkan alamat ip local yang telah diberikan oleh VPN Server.



Gambar 4.18 Tampilan Tes Ping ke IP lokal

Melakukan tes ping pada cmd. IP lokal disini adalah IP yang berada satu network dengan semua IP yang tergabung dalam VPN Server. IP lokal ini bukan merupakan IP aplikasi yang diinginkan. IP lokal ini hanya digunakan untuk melihat apakah sudah masuk ke dalam satu network. Karena yang diinginkan adalah IP aplikasi desktop Perijinan Kartu Kuning. Sehingga VPN Server perlu melakukan routing ke IP aplikasi desktop tersebut.

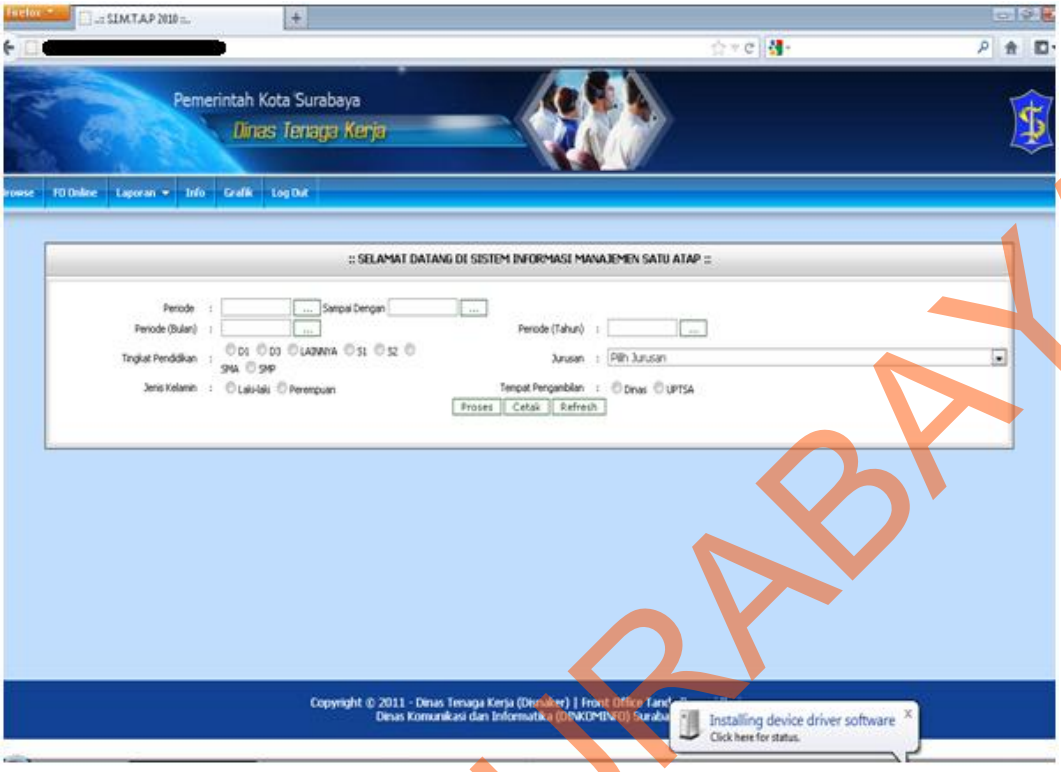
2. Sudah terkoneksi ke jaringan lokal namun belum bias membuka aplikasi.



Gambar 4.19 Tampilan Browser untuk Membuka Aplikasi Perijinan Kartu Kuning

Masih belum bisa membuka aplikasi dikarenakan IP yang digunakan untuk aplikasi masih belum dirouting atau diarahkan ke alamat aplikasi tersebut

3. Setelah ip untuk aplikasi sudah dirouting maka client dapat mengakses dan menggunakan aplikasi tersebut.



Gambar 4.20 Tampilan Aplikasi Perijinan Kartu Kuning yang telah berhasil

Ketika ip aplikasi sudah diroutingkan oleh Server maka ketika VPN Client dengan username dan password yang sesuai, maka client dapat masuk ke jaringan VPN, sehingga VPN Client dapat mengakses aplikasi Perijinan Kartu Kuning tersebut.

4.5 Pembahasan Implementasi

Teknologi ini telah memenuhi kebutuhan Dinkominfo dalam hal:

1. Jaringan dapat terhubung dan berkomunikasi.

Implementasi VPN dapat membantu Dinkominfo dalam menghubungkan aplikasi Perijinan Kartu Kuning di Convention Hall dengan Kantor Dinkominfo Surabaya.

Dengan teknologi VPN maka terhubungnya jaringan antara kantor server aplikasi Perijinan Kartu Kuning di Dinkominfo dengan Gedung Convention Hall dan menghasilkan jaringan yang dapat berkomunikasi secara aman, dapat diakses dimanapun terutama di Convetion Hall serta efisien dan mudah dalam penggunaannya.

2. Dapat diakses dimanapun (di luar Kantor Dinkominfo).

Teknologi VPN yang telah diimplementasikan sangat memudahkan Dinkominfo dalam hal pengaksesannya. Teknologi VPN ini dapat diakses dimana pun VPN Client berada. VPN Client tidak hanya bisa diimplementasikan di Dinkominfo saja namun di Convention Hall juga yang berada jauh dari Kantor Dinkominfo dengan peralatan yang sederhana dan sangat mudah penggunaannya hanya tinggal membuat VPN Connection saja.

3. Komunikasi yang memiliki keamanan yang tinggi.

Dengan menggunakan teknologi VPN, maka tercapai komunikasi yang aman. Aman disini artinya data dieknripsi melalui tunneling yang terdapat pada teknologi

VPN tersebut. VPN mempunyai beberapa konsep yang berhubungan dengan keamanan jaringan diantaranya:

1. Firewall: Firewall pada internet mempunyai fungsi sama dengan firewall pada gedung dan mobil yang memproteksi beberapa bagian agar terhindar dari kebakaran. Dengan menerapkan authentikasi dan enkripsi, VPN sudah cukup *secure* sebagai firewall internet.
2. Authentikasi : Teknik authentikasi sangatlah penting untuk VPN. Dengan authentikasi kita bisa memastikan hanya dengan user dan password yang benarlah hak akses diberikan. Banyak cara melakukan teknik authentikasi mulai dari shared key, algoritma hash, Chalange Handshake Authentikasi Protocol (CHAP) atau bahkan menggunakan algoritma yang umum digunakan, RSA.
3. Enkripsi: Koneksi yang terinkripsi adalah syarat wajib dari VPN. Teknik enkripsi secara garis besar terbagi menjadi dua bagian: *secret (or private) key encryption* dan *public key encryption*. Secret key biasanya menggunakan Data Encryption Standard (DES) yang dishare hanya untuk anggota yang ditentukana saja. Sistem ini sengaja didesain untuk sistem yang tidak untuk dipublikasikan secara umum. Sedangkan Public Key Encryption menggunakan sertifikat (key) yang sudah tersedia dan bebas dipakai untuk kepentingan publik seperti *Pretty Good Privacy* (PGP).
4. Tunneling: VPN juga menggunakan "tunneling" untuk menciptakan koneksi antar host, yakni *Point to Point Tunneling Protocol* (PPTP) dan *Internet Protocol Security* (IP Sec).

4. Efisien dalam implementasi dan penggunaannya.

Dalam hal implementasi dan penggunaannya, teknologi VPN lebih efisien dibanding teknologi lain. Tidak banyak peralatan yang dibutuhkan baik VPN Server maupun VPN Client. VPN Server hanya membutuhkan Router Mikrotik, Mikrotik OS, dan satu IP publik. Di sisi Client hanya membutuhkan PC atau laptop sebagai client dalam mengakses aplikasi yang diinginkan. Dan dalam penggunaannya tinggal membuat VPN Connection pada setiap client dan dengan mudah client dapat mengakses file-file atau fitur-fitur yang dibutuhkan.