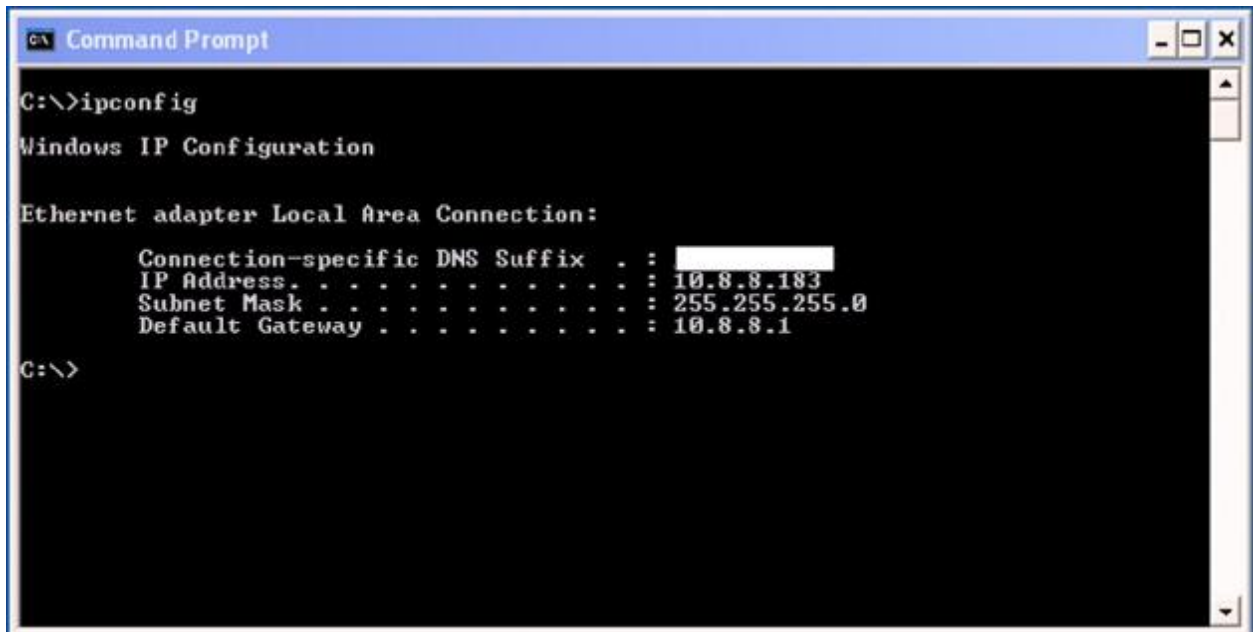


Cisco VPN Client Setup

1. Tampilan IP Address ketika terhubung di LAN



```
C:\>ipconfig

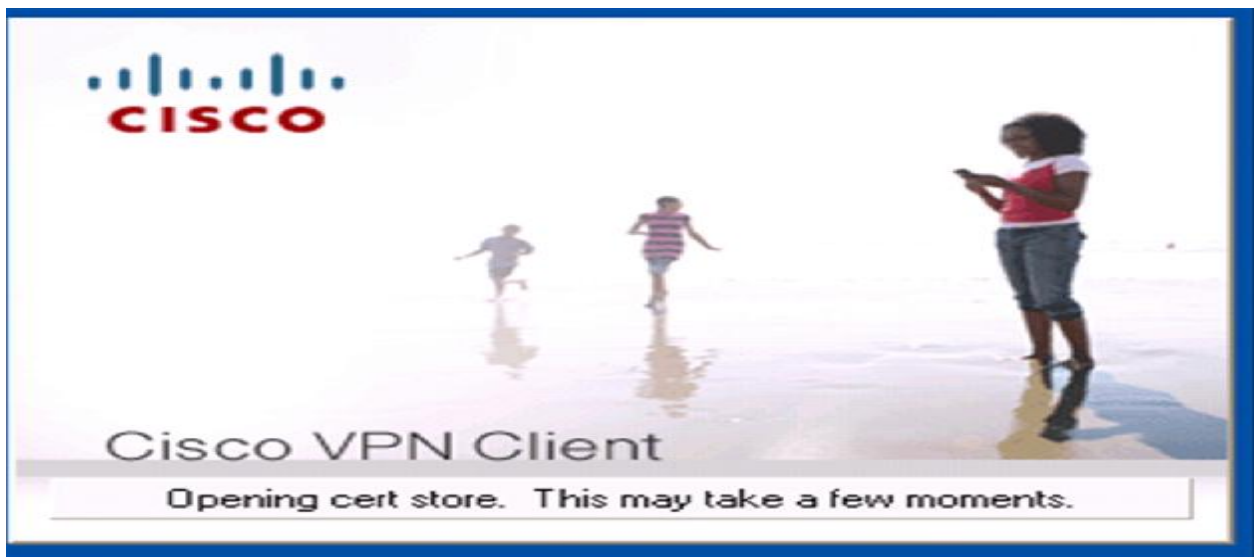
Windows IP Configuration

Ethernet adapter Local Area Connection:

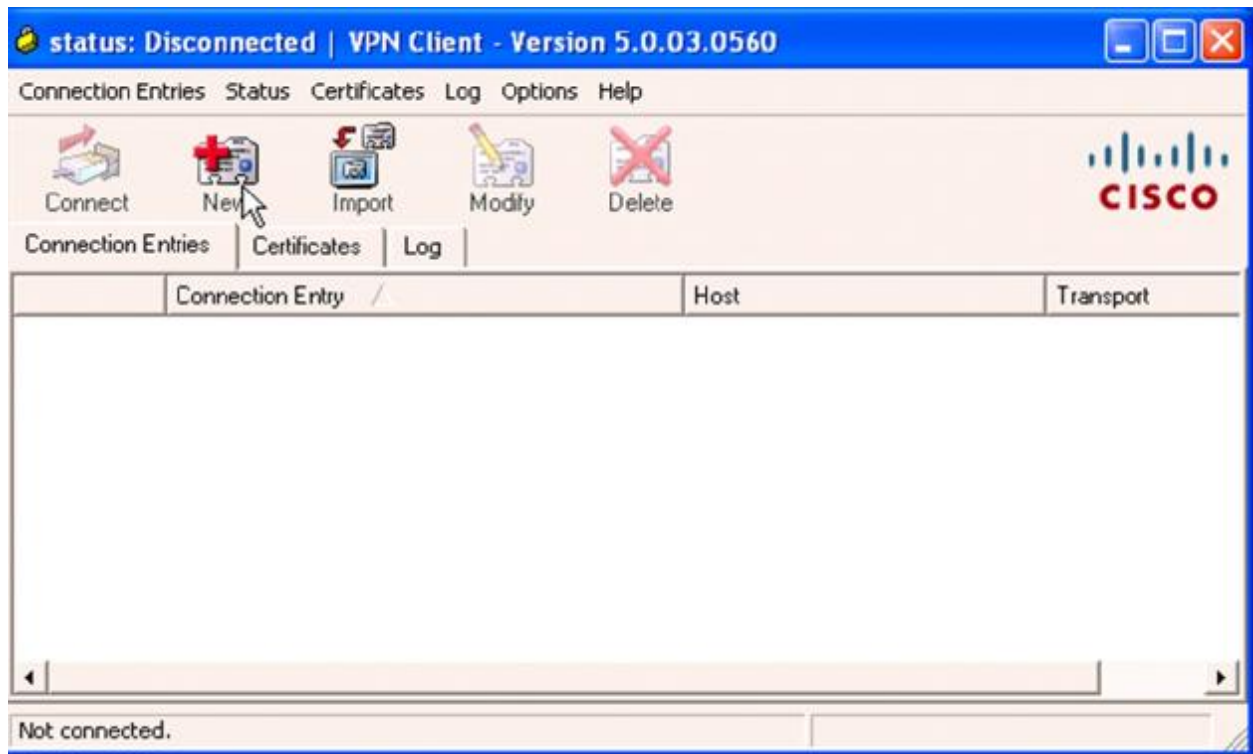
    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 10.8.8.183
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 10.8.8.1

C:\>
```

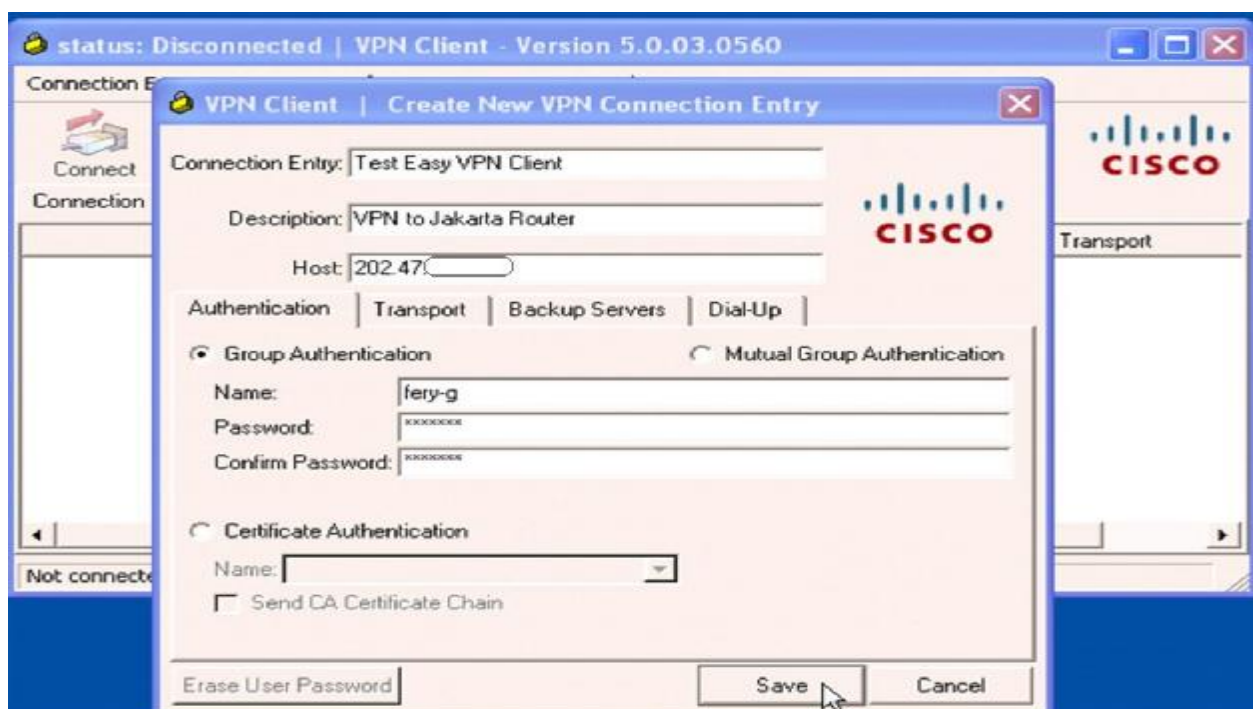
2. Setelah Install, VPN Client Doble Klik. Akan Muncul Proses Loading...



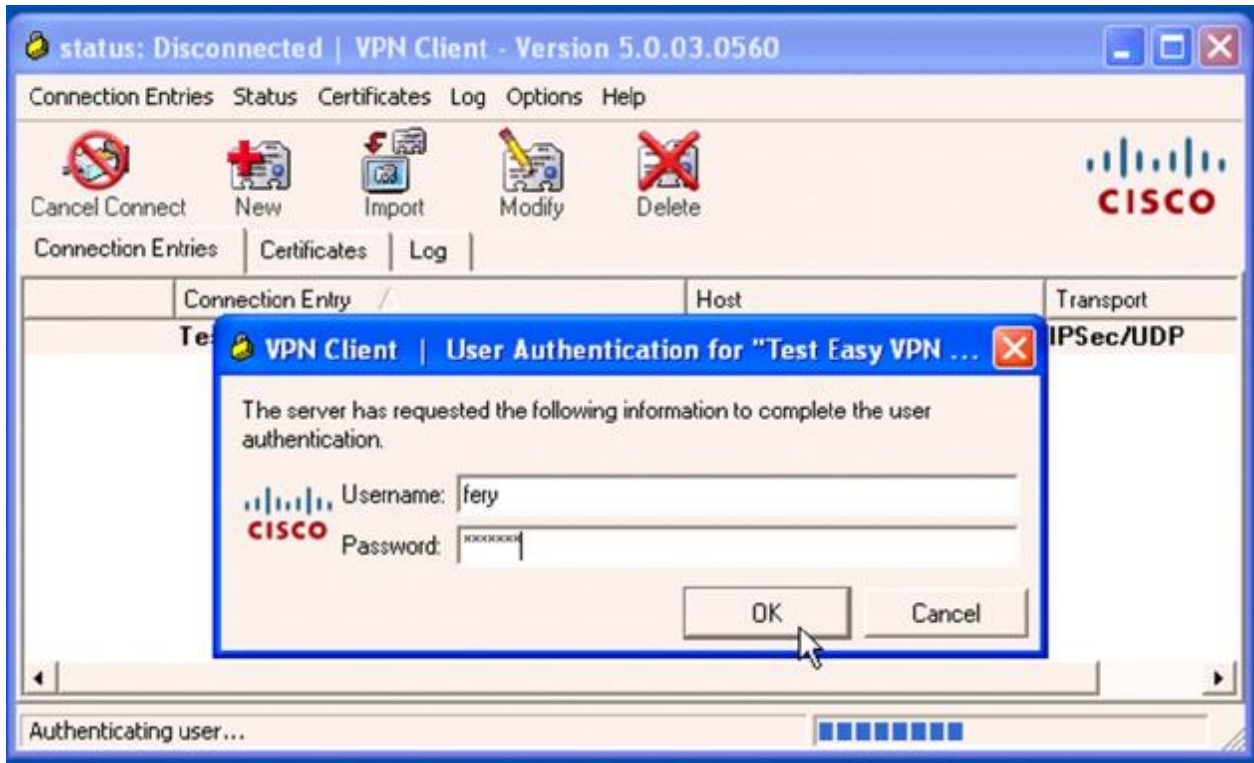
3. Klik New



4. Arahkan Ke IP Address dari VPN Server, dan Isi Group Authentication dengan Username dan Password yang sudah di Define sebelum nya.



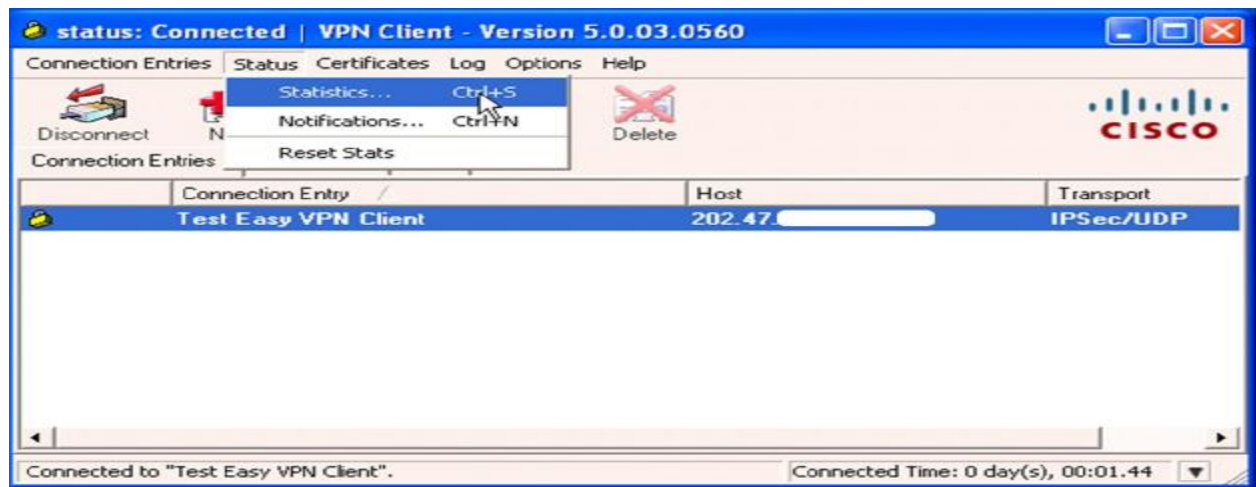
5. Klik Connect, Jika Group Authentication yang anda Masukan benar. Maka akan Muncul Popup Untuk nama dan password AAA yang sudah di define sebelumnya



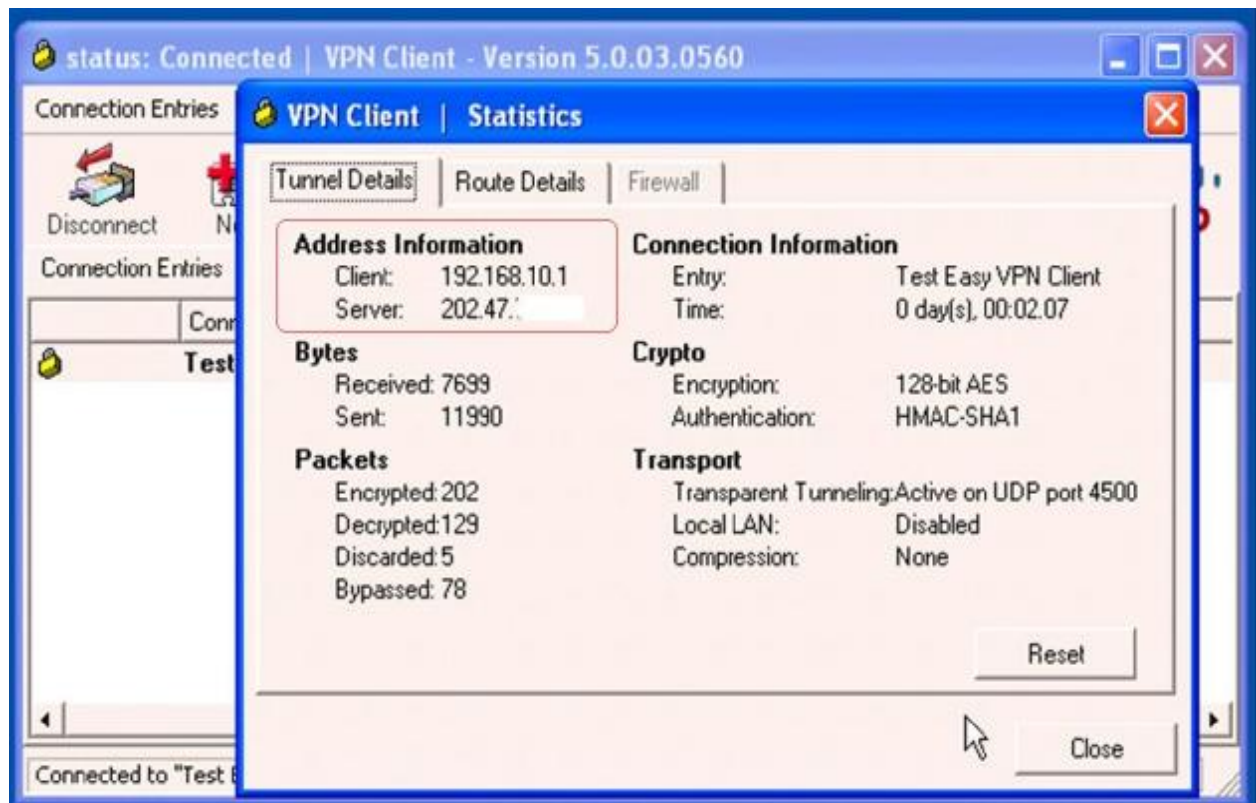
6. Proses Authentikasi dan dan pembentukan link VPN



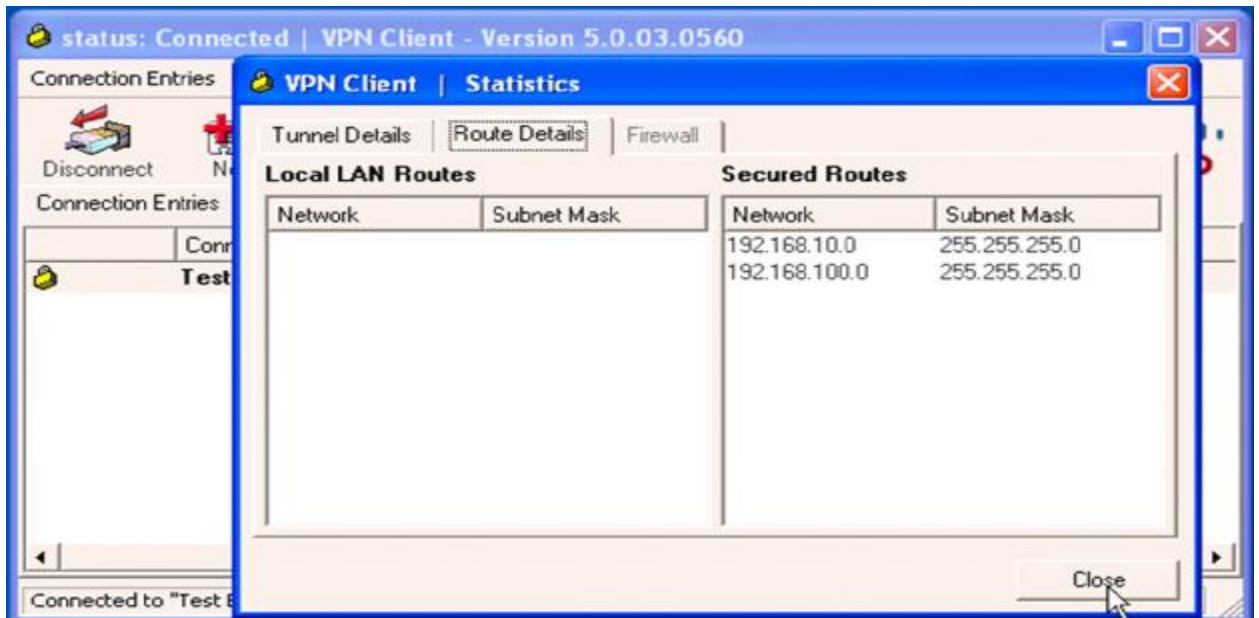
7. Link VPN Connected dan Kita Cek Statictik



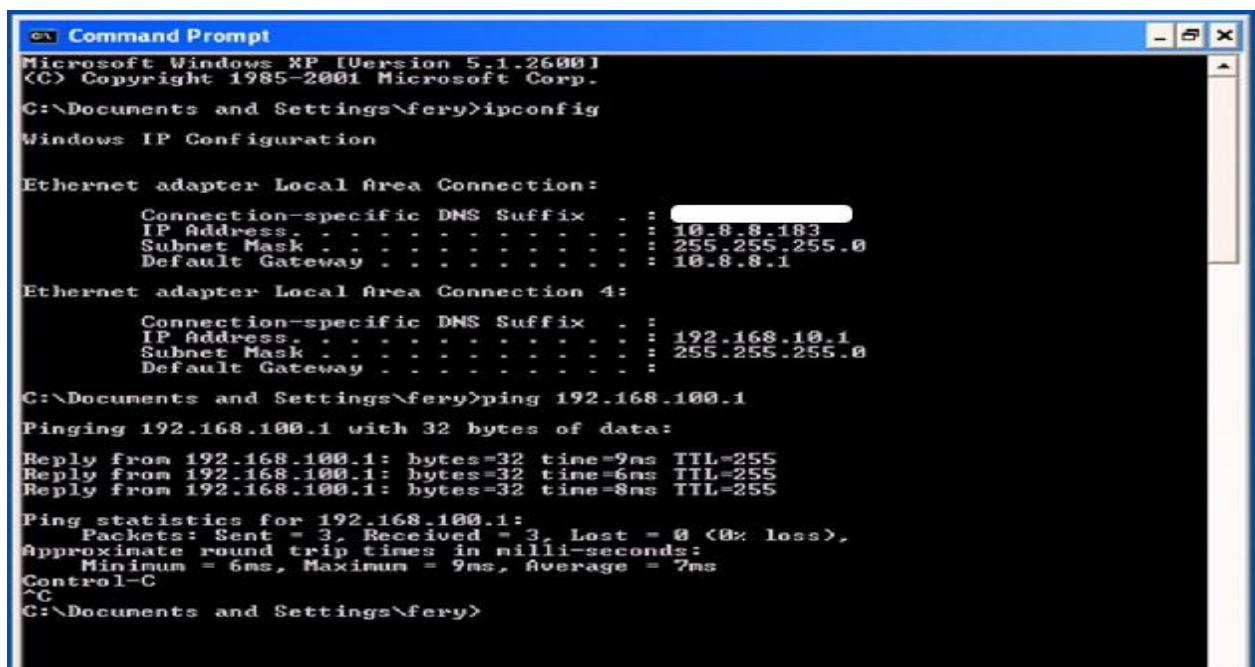
8. Cek Statistik



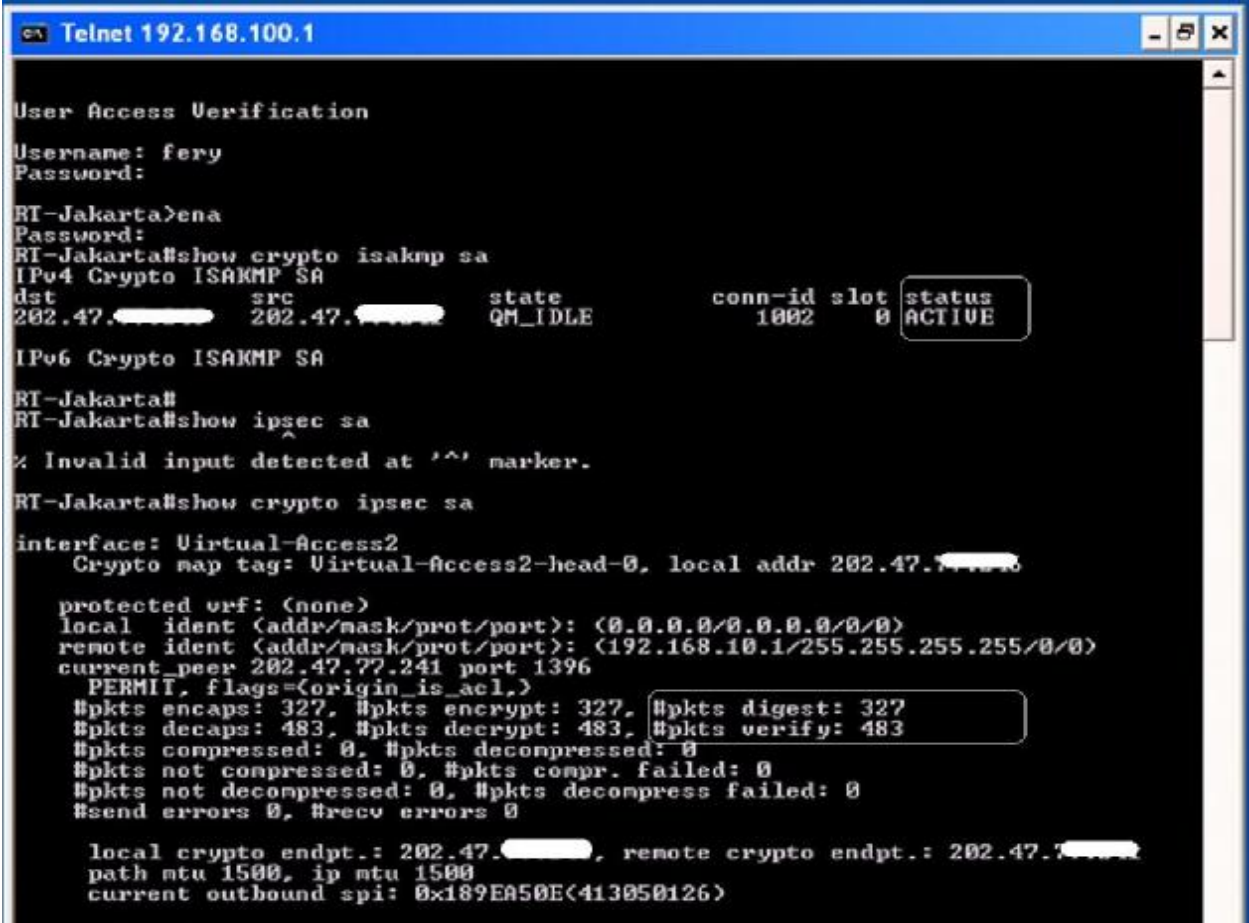
9. Cek Route Detail



10. Cek Perubahan IP Address di sisi Client, Dimana VPN Server akan Men- Injected IP Address ke VPN Client dan Secara Otomatis VPN Client bisa terhubung ke jaringan Di belakang VPN Server, Kita bisa Mencek dengan melakukan Ping.



11. Setelah VPN Connection Terbentuk, Kita bisa meng akses Router VPN Server dengan telnet menggunakan IP Private dari Router VPN Server. Cek Pada VPN Server, Status Active Crypto Isakmp dan paket data yang telah di Encrypt – Decrypt.



```
Telnet 192.168.100.1

User Access Verification
Username: fery
Password:

RT-Jakarta>ena
Password:
RT-Jakarta#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id slot status
202.47.     202.47.     QM_IDLE        1002    0    ACTIVE

IPv6 Crypto ISAKMP SA

RT-Jakarta#
RT-Jakarta#show ipsec sa
% Invalid input detected at '^' marker.
RT-Jakarta#show crypto ipsec sa
interface: Virtual-Access2
  Crypto map tag: Virtual-Access2-head-0, local addr 202.47.

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (192.168.10.1/255.255.255.255/0/0)
current_peer 202.47.77.241 port 1396
  PERMIT, flags=<origin_is_acl,>
  #pkts encaps: 327, #pkts encrypt: 327, #pkts digest: 327
  #pkts decaps: 483, #pkts decrypt: 483, #pkts verify: 483
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

local crypto endpt.: 202.47.
path mtu 1500, ip mtu 1500
current outbound spi: 0x189EA50E(413050126)
```

12. Proses Koneksi Dari VPN Client ke VPN Server Sudah Terbentuk, sekarang Semua Paket data yang lewat dari Client ke Router VPN akan di Encrypted. More Secure....

Thanks,

Fery Junaedi