# BAB IV

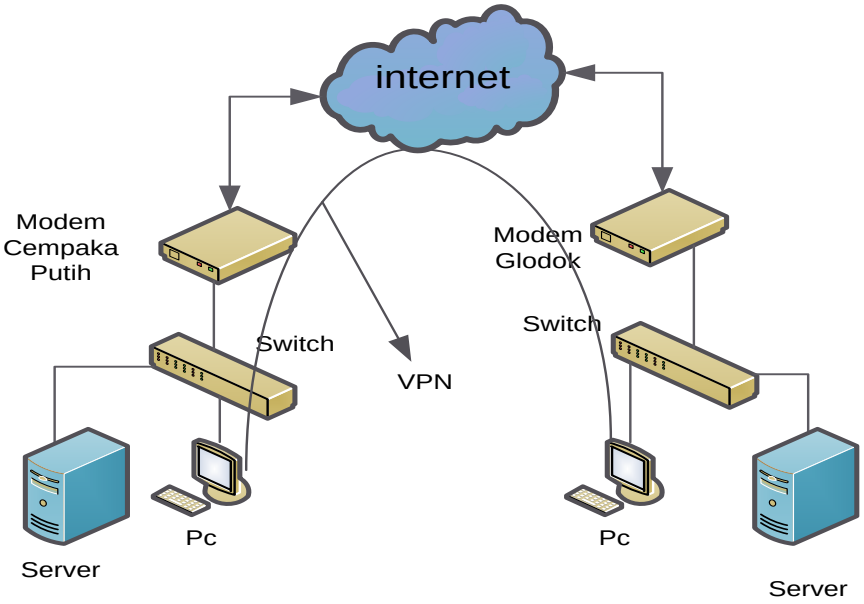
# RANCANGAN JARINGAN USULAN

## 4.1. Jaringan Usulan

### 4.1.1. Topologi Jaringan

Untuk topologi jaringan penulis tidak akan merubah topologi jaringan yang sudah ada pada PT. Citra Selaras Jaya karena topologi yang sekarang digunakan sudah sangat baik dan berjalan sesuai apa yang diharapkan. Jaringan usulan yang penulis usulkan hanya membahkan Virtual Private Network(VPN) untuk dapat mengakses jaringan LAN kantor pusat dan cabang PT. Citra Selaras Jaya dengan membuat jalur yang aman dan rahasia dari jaringan public.

### 4.1.2. Skema Jaringan




Gambar IV.1

Skema Jaringan Usulan

Pada skema jaringan usulan dapat dilihat bahwa menambahkan Virtual Private Network (VPN) yang nantinya akan digunakan untuk kemudahan pengiriman data keserver ataupun monitoring yang dilakukan oleh pihak IT yang akan mengakses jaringan lokal melalui jaringan public seperti internet, dan membuat jalur aman dan rahasia, dengan begitu sistem jaringan PT. Citra Selaras Jaya dengan adanya VPN , pihak IT akan mendapatkan kemudahan untuk mengakses ke jaringan lokal walaupun posisi pegawai tersebut sedang berada di cabang lain.

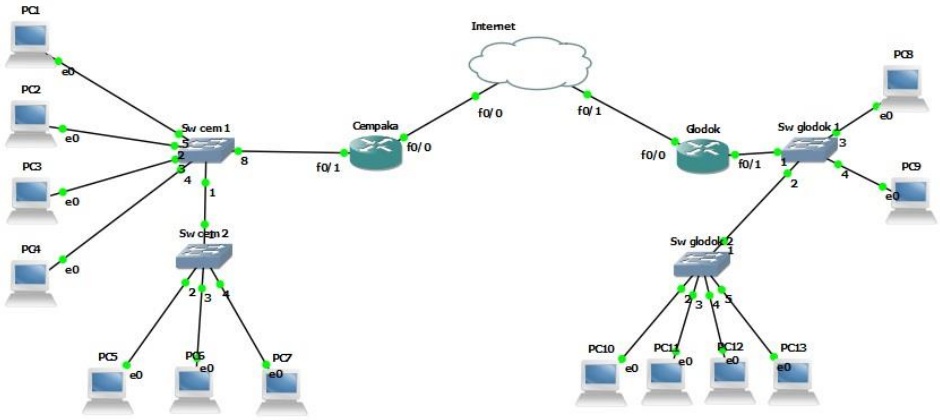
### 4.1.3. Keamanan Jaringan

Keamanan jaringan yang ada di PT. Citra Selaras Jaya sudah sangat bagus dengan membuat firewall pada beberapa konfigurasi hardware seperti router dan mengandalkan software antivirus. Akan tetapi pada saat ini sebaik apapun firewall yang dibuat masih bisa ditembus virus, spam, dan sebagainya. Karena itu penulis memberikan saran jika dalam jaringan Wide Area Network PT. Citra Selaras Jaya ditambah dengan hardware firewall yang memang dirancang untuk melindungi jaringan dari ancaman virus, hacker, dan sebagainya. Ada banyak vendor yang menyediakan hardware firewall diantaranya Cisco Pix Firewall keluaran dari cisco yang terkenal dengan routernya.

### 4.1.4. Rancangan Aplikasi

Pada perancangan aplikasi ini, penulis mencoba menggunakan software simulasi yang digunakan untuk perancangan jaringan VPN, yang berguna untuk menghubungkan kedua jaringan yang ada cempaka putih maupun di glodok

sampai bisa terkoneksi melalui jaringan public seperti internet software yang digunakan sebagai simulasi adalah GNS3 (Graphic Network Simulator).




Gambar IV.2

Desain simulasi jaringan menggunakan GNS

Perfoma jaringan :

a. Sebelum menggunakan VPN, sering terjadi kegagalan komputer client mengirimkan data transaksi ke server dikarenakan banyaknya noise, sehingga data yang diterima oleh server bukan merupakan data Real Time.

b. Sesudah menggunakan VPN, data yang di transmisikan melalui VPN akan mengalami kompresi, sehingga transmisi data dapat berjalan baik dan lancer. Serta adanya peningkatan keamanan dalam komunikasi data.

1. Router pada kantor pusat (cempaka putih )

   a. Router

      Interface FastEth 0/0 =10.32.152.5

Subnet mask = 255.255.255.252

Interface FastEth 0/1 =192.168.1.1

Subnet mask = 255.255.255.0

b. Server = 192.168.1.10

c. Client

PC1 = 192.168.1.2

PC2 = 192.168.1.3

PC3 = 192.168.1.4

PC4 = 192.168.1.5

PC5 = 192.168.f0.6

PC6 = 192.168.1.7

2. Cara Konfigurasi VPN pada router kantor pusat :

Cempaka (config-if) #aaa new-model

Cempaka (config-if) #aaa authentication login userauthen local

Cempaka (config-if) #aaa authorization network groupauthor local

Cempaka (config-if) #username glodok password 123456

===konfigurasi EzVPN===

Cempaka (config) #crypto isakmp policy 10

Cempaka (config-isakmp) #encr 3des

Cempaka (config-isakmp) #authentication pre-share

Cempaka (config-isakmp) #group 2

Cempaka (config-isakmp) #crypto ipsec transf myset eps-3esp-sha-

Cempaka (config-crypto-transform) #model tunnel

Cempaka (config-crypto-transform) #exit

Cempaka (config) #crypto isakm client config group vpngrp

Cempaka (config-isakmp-group) #key cisco123

Cempaka (config-isakmp-group) #exit

Cempaka (config) #crypto dynamic-map dynmap 10

Cempaka (config-crypto-map) #set transform-set myset

Cempaka (config-crypto-map) #exit

Cempaka (config) #cryp map clientmap client authen list userauthen

Cempaka (config) #cryp map clientmap isakmp autho list groupauthor

Cempaka (config) #cryp map clientmap 10 ipsec-isakmp dynamic dynmap

===apply EzVPN===

Cempaka (config) #int gi0/0

Cempaka (config-if) #crypto map clientmap

=== EzVPN client mode ===

Cempaka (config) #crypto isakmp policy 1

Cempaka (config-crypto-isakmp) #encryption 3des

Cempaka (config-crypto-isakmp) #authentication pre-share

Cempaka (config-crypto-isakmp) #group2

Cempaka (config-crypto-isakmp) #exit

Cempaka (config) #crypto isakmp client config address local mypool

Cempaka (config) #crypto isakmp client config group ezvpn

Cempaka (config-isakmp-group) #key 123456

Cempaka (config-isakmp-group) #pool mypool

Cempaka (config-isakmp-group) #exit

Cempaka (config) #crypto ipsec transf myset esp-3desesp-sha-hmac

Cempaka (config) #crypto dynamic-map mymap1

Cempaka (config-crypto-map) #set transform-set myset

Cempaka (config-crypto-map) #reverse-route

Cempaka (config-crypto-map) #exit

Cempaka (config) #crypto map mymap isakmp author list groupauthor

Cempaka (config) #crypto map mymap client config address respond

Cempaka (config) #crypto map mymap 1 ipsec-isakmp dynamic mymap

Cempaka (config) #int g0/0

Cempaka (config-if) #crypto map mymap

Cempaka (config-if) #exit

Cempaka (config-if) #crypto map mymap

Cempaka (config) #ip local pool mypool 10.10.10.10 10.10.10.11

3. Router pada kantor cabang (glodok )

   a. Router

   Interface FastEth 0/0 =10.32.152.9

   Subnet mask = 255.255.255.252

   Interface FastEth 0/1 =192.168.2.1

   Subnet mask = 255.255.255.0

   b. Server = 192.168.2.2

   c. Client

      PC1 = 192.168.2.10

      PC2 = 192.168.2.11

PC3 = 192.168.2.12

PC4 = 192.168.2.13

PC5 = 192.168.2.14

4. Cara Konfigurasi VPN pada router kantor cabang :

Glodok

=== konfigurasi EzVPN ===

Glodok (config) #crypto ipsec client ezvpn ez

Glodok (config-crypto-ezvpn) #connect auto

Glodok (config-crypto-ezvpn) #group vpngrp key cisco123

Glodok (config-crypto-ezvpn) #mode network-extension

Glodok (config-crypto-ezvpn) #peer 10.32.152.5

Glodok (config-crypto-ezvpn) #xauth userid mode interactive

Glodok (config-crypto-ezvpn) #exit

=== apply EzVPN ===

Glodok (config) # int f0/0

Glodok (config-if) #crypto ipsec client ezvpn ez

Glodok (config-if) #int f0/1

Glodok (config-if) #crypto ipsec client ezvpn ez inside

Glodok (config) #crypto ipsec client ezvpn ezvpn

Glodok (config-crypto-ezvpn) #connect auto

Glodok (config-crypto-ezvpn) #group ezvpn key 123456

Glodok (config-crypto-ezvpn) #mode client

Glodok (config-crypto-ezvpn) #exit

Glodok (config) #int f0/0

Glodok (config-if) #crypto ipsec client ezvpn ezvpn inside

Glodok (config-if) #exit

Glodok (config) #int f0/1

Glodok (config-if) #crypto ipsec client ezvpn ezvpn

### 4.1.5. Manajemen Jaringan

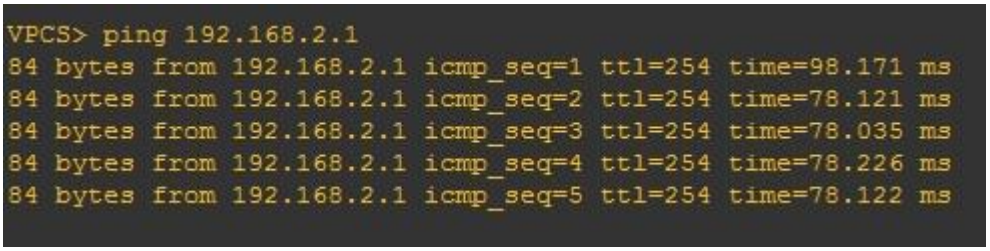
Seperti yang sudah dijelaskan dalam bab sebelumnya yaitu agar setiap toko client bisa mengirimkan paket data transaksi ke server tanpa terputus ataupun gagal, maka penulis mengusulkan untuk menambahkan Virtual Private Network(VPN) pada jaringan PT. Citra Selara Jaya. VPN menghubungkan komponen komponen dari satu jaringan diatas jaringan bersama yang lain melindungi proses pengirimannya. Suatu jaringan private yang dibangun pada suatu infrastruktur jaringan publik yang keamanan datanya terjamin.

## 4.2. Pengujian Jaringan

Dalam membangun sebuah jaringan komputer tentunya perlu dilakukan pengujian terhadap jaringan tersebut untuk memastikan semua sistem berjalan sesuai apa yang diharapkan.

### 4.2.1. Pengujian Jaringan Awal

a. Ping dari client (192168.1.10) ke gateway (192.168.2.1)



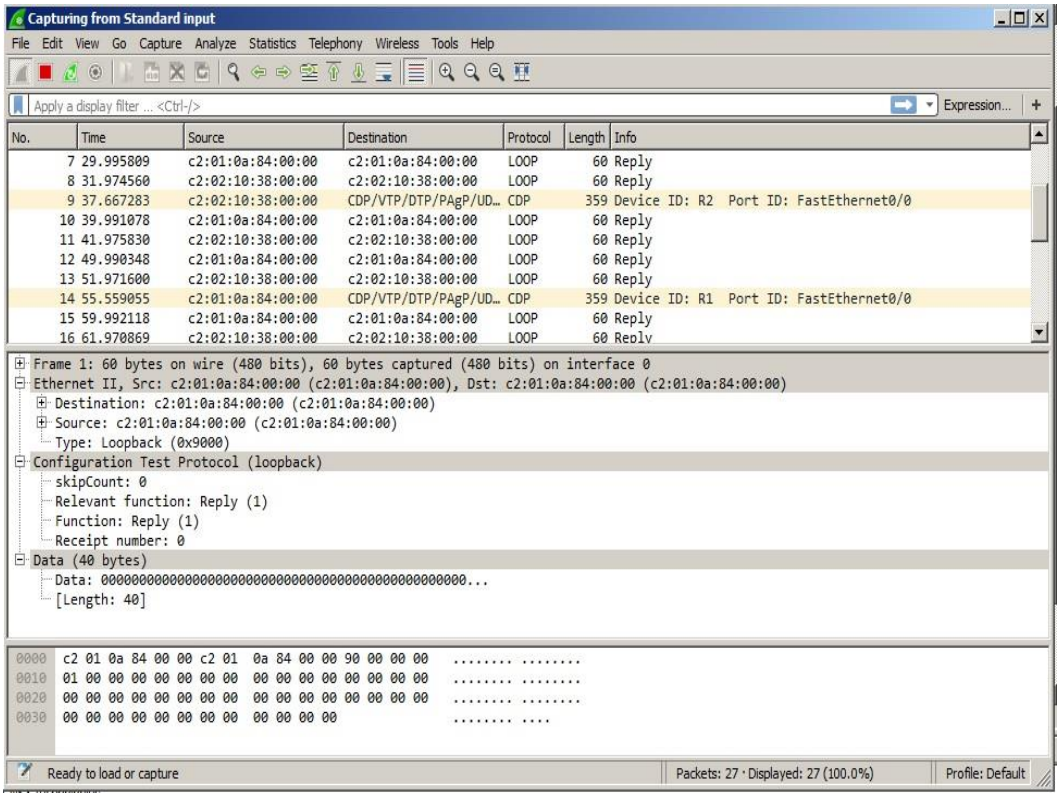
b. Ping dari client (192.168.1.10) ke client (192.168.2.2)

```
VPCS> ping 192.168.2.2
192.168.2.2 icmp_seq=1 timeout
84 bytes from 192.168.2.2 icmp_seq=2 ttl=62 time=93.751 ms
84 bytes from 192.168.2.2 icmp_seq=3 ttl=62 time=93.751 ms
84 bytes from 192.168.2.2 icmp_seq=4 ttl=62 time=93.752 ms
84 bytes from 192.168.2.2 icmp_seq=5 ttl=62 time=93.749 ms
```

c. Ping client (192.168.1.10) ke router (10.32.152.5)

```
VPCS> ping 10.32.152.5
84 bytes from 10.32.152.5 icmp_seq=1 ttl=255 time=15.625 ms
84 bytes from 10.32.152.5 icmp_seq=2 ttl=255 time=15.623 ms
84 bytes from 10.32.152.5 icmp_seq=3 ttl=255 time=15.624 ms
84 bytes from 10.32.152.5 icmp_seq=4 ttl=255 time=15.625 ms
84 bytes from 10.32.152.5 icmp_seq=5 ttl=255 time=15.629 ms
```

d. Capture dengan Wireshark sebelum VPN




### 4.2.2. Pengujian Jaringan Akhir

Pada pengujian jaringan akhir penulis akan coba melakukan test jaringan VPN di router dan memastikan enkripsi data agar data aman.

a. Pengujian untuk memastikan EzVPN sudah aktif

```
cempaka#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
10.32.152.5     10.32.152.9     QM_IDLE           1001    0 ACTIVE

IPv6 Crypto ISAKMP SA
```

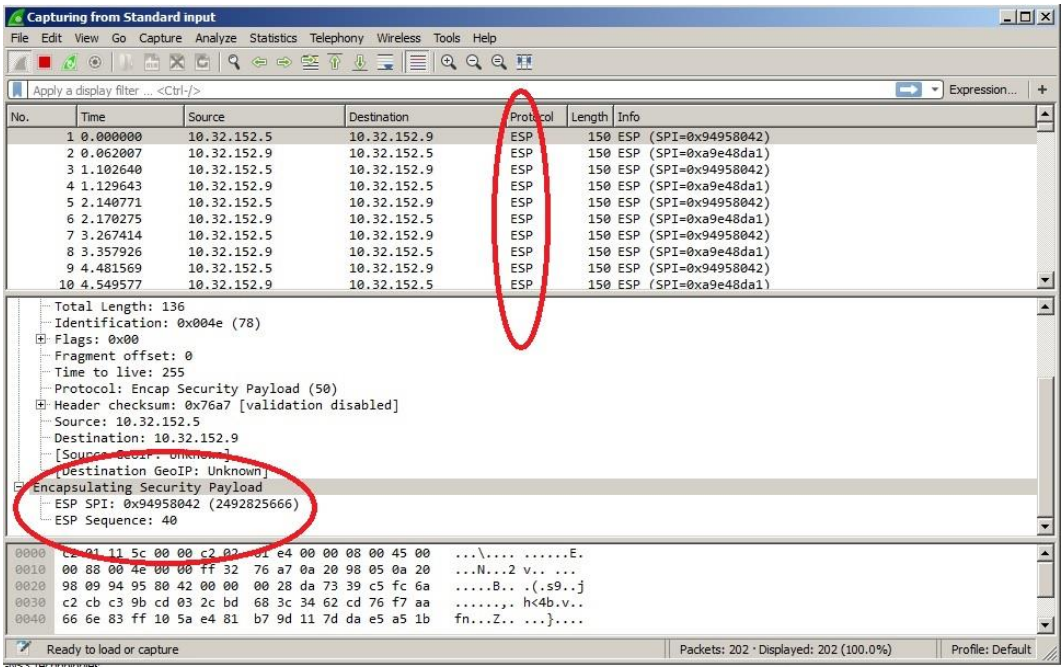
b. Pengujian melihat konfigurasi EzVPN

```
glodok#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
10.32.152.5     10.32.152.9     QM_IDLE           1001    0 ACTIVE

IPv6 Crypto ISAKMP SA

glodok#sh crypto ipsec client ezvpn
Easy VPN Remote Phase: 6

Tunnel name : ez
Inside interface list: FastEthernet0/1
Outside interface: FastEthernet0/0
Current State: IPSEC_ACTIVE
Last Event: MTU_CHANGED
Save Password: Disallowed
Current EzVPN Peer: 10.32.152.5
```

c. Pengujian data yang terenkripsi melalui IPSec

```
cempaka#sh crypto ipsec sa

interface: FastEthernet0/0
    Crypto map tag: mymap, local addr 10.32.152.5

   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): (192.168.2.0/255.255.255.0/0/0)
   current_peer 10.32.152.9 port 500
     PERMIT, flags={}
    #pkts encaps: 15, #pkts encrypt: 15, #pkts digest: 15
    #pkts decaps: 14, #pkts decrypt: 14, #pkts verify: 14
    #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.: 10.32.152.5, remote crypto endpt.: 10.32.152.9
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0x29107822(688945186)

     inbound esp sas:
      spi: 0x815098EB(2169542891)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 1, flow_id: SW:1, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4416208/3523)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE
```

d. Capture dengan Wireshark sesudah VPN




Jadi dengan VPN data menjadi aman karena setiap lalu lintas data terbungkus dengan aman sehingga data tidak disalah gunakan oleh orang yang tidak bertanggung jawab.