

## BAB V

### HASIL DAN PEMBAHASAN

#### 5.1 Hasil

Berdasarkan hasil riset yang dilakukan penulis dalam melaksanakan penelitian, penulis memberikan solusi untuk mengatasi masalah yang ada pada PT. Palem Baja Palembang yaitu dengan mendesain dan mengimplementasikan teknologi *Virtual Private Network* (VPN) yang bertujuan untuk memberikan keamanan di perusahaan pada saat melakukan komunikasi dengan menggunakan media *internet*.

Solusi yang akan diterapkan oleh penulis dengan menggunakan teknologi *Virtual Private Network* (VPN) pada jaringan perusahaan PT. Palem Baja yang memiliki gedung berbeda lokasi antar gedung cabang dan gedung pusat agar dapat saling berkomunikasi dengan aman, karena pada teknologi *Virtual Private Network* (VPN) memiliki keunggulan dalam mengamankan penggunaannya dari oknum-oknum yang tidak bertanggung jawab untuk melakukan pencurian data atau informasi perusahaan yang bersifat rahasia pada saat gedung pusat dan gedung cabang saling berkomunikasi melalui media *internet*.

Adapun solusi yang akan diterapkan selain dari teknologi *Virtual Private Network* (VPN), penulis juga akan menerapkan media pusat penyimpanan data dan *sharing* data perusahaan atau sering disebut *file*

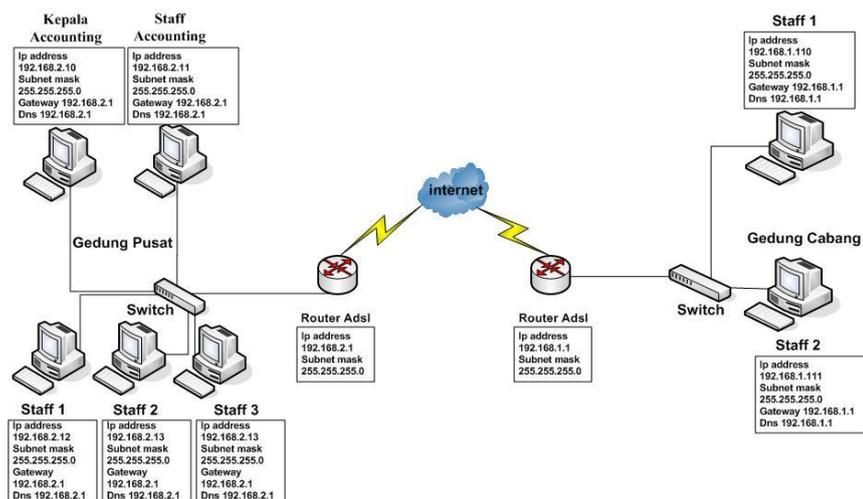
*server*, yang bertujuan untuk manajemen data perusahaan agar lebih tertata pada satu tempat pusat penyimpanan data perusahaan. Dengan adanya *file server* atau pusat data yang akan diterapkan penulis pada perusahaan, semua karyawan yang bertugas menulis atau membuat laporan kegiatan perusahaan baik yang berada di kantor pusat dan di kantor cabang akan memiliki *user* masing-masing untuk melakukan penginputan data ke pusat penyimpanan data.

Dengan adanya pusat penyimpanan data dan *sharing* data, maka setiap karyawan akan memiliki tempat penyimpanan sendiri di satu pusat data perusahaan dan karyawan tidak perlu lagi untuk merasa takut akan kehilangan data atau data yang terhapus secara tidak sengaja oleh karyawan lain, karena data karyawan hanya bisa dihapus atau di tulis oleh karyawan itu sendiri yang telah memiliki *user* dan hak aksesnya masing-masing.

Solusi yang akan diterapkan atau diusulkan diatas yaitu mendesain dan mengimplementasikan *Virtual Private Network* (VPN) dan *file server* pada perusahaan dengan menggunakan sistem operasi *linux* dan aplikasi *open source* yang bersifat gratis namun dapat diterapkan pada perusahaan berskala kecil maupun skala besar.

### 5.1.1 Topologi Jaringan Perusahaan

Berdasarkan hasil dari tinjauan langsung yang dilakukan penulis dalam melaksanakan penelitian, penulis mendapatkan keadaan topologi jaringan yang ada sekarang pada gedung pusat dan gedung cabang PT. Palem Baja Palembang yaitu menggunakan topologi *star* atau bintang, topologi *star* atau bintang yang ada pada kantor pusat dan kantor cabang PT. Palem Baja Palembang dapat dilihat pada gambar di bawah ini :



**Gambar 5.1 Topologi Star Gedung Pusat dan Gedung Cabang PT. Palem Baja Palembang**

Pada gambar diatas topologi jaringan pada gedung pusat dan gedung cabang PT. Palem Baja Palembang menggunakan topologi *star* dan terdapat 5 buah komputer di gedung pusat dan dua buah komputer di gedung cabang dengan menggunakan *Internet Services Provider (ISP) Telkom Speedy*, maka dari topologi diatas pada saat kedua gedung saling berkomunikasi melakukan

pengiriman data menggunakan media *internet* yang terhubung secara langsung ke pengguna internet diseluruh dunia.

### **5.1.2 Pemilihan Perangkat Keras dan Perangkat Lunak**

Adapun dalam melakukan pemilihan perangkat keras dan perangkat lunak yang akan diterapkan pada perusahaan harus di sesuaikan dengan kebutuhan yang diperlukan agar dapat memperkecil pengeluaran dalam pembelian perangkat keras dan perangkat lunak. Adapun penjelasan dalam pemilihan perangkat keras dan perangkat lunak , diantaranya sebagai berikut :

#### **1. Pemilihan Perangkat Keras**

Pemilihan perangkat keras dilakukan penulis yang bertujuan untuk menyesuaikan kebutuhan dalam mendesain dan mengimplementasikan *Virtual Private Network (VPN) server* dan *file server* pada perusahaan, disini penulis menyarankan perusahaan untuk menggunakan satu komputer yang akan digunakan dalam menjalankan *Virtual Private Network (VPN) server* dan *file server*, dikarenakan untuk menghemat pengeluaran perusahaan dalam pembelian perangkat keras yaitu berupa komputer.

Selain dari pertimbangan menghemat pengeluaran penulis akan melihat keadaan mesin *server* setelah selesai di implementasikan dan melakukan pengujian terhadap mesin

*server* dalam menangani *client* yang ada di gedung pusat dan di gedung cabang. Jika dalam melakukan pengujian *server* saat menangani *client* nya tidak dapat berjalan optimal atau *client* membutuhkan waktu lama saat mesin *server* meberikan respon dan kekurangan lainnya, maka penulis akan menyarankan pada perusahaan untuk melakukan penambahan satu komputer lagi guna untuk memisahkan mesin *server* VPN dan mesin *file server*.

Pemilihan perangkat keras yang disarankan oleh penulis untuk membangun *server Virtual Private Network* (VPN) dan *file server*, diantaranya sebagai berikut :

1. *Motherboard* MSI N1996
2. *Processor Intel dual core*
3. *Memory DDR2 Visipro 2 GB*
4. *Keyboard mouse Logitech*
5. *Harddisk Seagete 500 GB*

## **2. Pemilihan Perangkat Lunak**

Pemilihan perangkat lunak yang akan dilakukan untuk menjalankan sistem *Virtual Private Network* (VPN) *server* dan *file server*, diantaranya sebagai berikut :

1. Sistem Operasi Debian *Squeeze* 6.03 i386
2. SSH Server PPTPD 1.3.4-3, PPP
3. Samba Server 3.5.6
4. SSH Server
5. Anti Virus Clamav

Pemilihan perangkat lunak yang dilakukan penulis lebih memilih untuk menggunakan sistem operasi *opensource* dari *linux debian* bertujuan untuk tidak melakukan pembelian sistem operasi yang berbayar dalam mengimplementasikan mesin *server* namun dengan menggunakan sistem operasi *opensource* sebuah *server* dapat mengatasi tugasnya sebagai *server* yang menangani permintaan dari klien baik dalam skala kecil maupun skala besar yang tidak kalah dengan menggunakan perangkat lunak berbayar.

Selain menggunakan sistem operasi *opensource* penulis juga menggunakan aplikasi yang bersifat gratis dan terbuka yaitu aplikasi PPTPD dan PPP sebagai kelengkapan dari aplikasi PPTPD, penggunaan aplikasi PPTPD sebagai *Virtual Private Network (VPN) server* dikarenakan cukup mudah dalam melakukan konfigurasi *server* VPN dan tidak membutuhkan waktu yang lama untuk melakukan konfigurasi *server* VPN, aplikasi PPTPD berjalan pada protokol *Point-to-Point Tunneling Protocol (PPTP)*. Menurut (Wendy,

Ramadhana, 2005:7) *Point-to-Point Tunneling Protocol* (PPTP) memberikan sarana terselubung (*Tunneling*) untuk berkomunikasi melalui internet. Salah satu kelebihan yang membuat PPTP ini terkenal adalah karena protokol ini mendukung protokol *non-IP* seperti IPX/SPX, NetBEUI, *Appletalk* dan sebagainya. Protokol ini merupakan protokol standar pada enkapsulasi VPN yang digunakan oleh *Windows Virtual Private Network*. Protokol ini bekerja berdasarkan PPP protokol yang digunakan pada *dial-up connection*.

Adapun selain menggunakan aplikasi PPTPD penulis menggunakan aplikasi *samba server* sebagai pusat penyimpanan dan *sharing* data atau *file server*. Menurut Wilfridus Bambang Triadi Handayana, dkk (2010:99), *Samba* merupakan salah satu aplikasi di mesin UNIX dan turunannya yang mengimplementasikan protokol SMB atau *Server Message Block*. Pada mayoritas sistem operasi, protokol SMB digunakan dalam jaringan *client-server*, sehingga memungkinkan antar sistem operasi yang berbeda tersebut dapat saling berkomunikasi, seperti misalnya bertukar data, akses *printer* secara bersama, hingga digunakan sebagai jalur *login* ke suatu *server domain*.

Penggunaan aplikasi *samba server* dengan menggunakan *metode Pimary Domain Controller* (PDC),

penulis bermaksud untuk memberikan keamanan pada *server* data yang akan diakses oleh pengguna dikarenakan *samba server* dengan metode *Primary Domain Controller* (PDC) akan melakukan validasi *user* kepada setiap *client* yang akan bergabung dalam satu *domain* tertentu, dengan kata lain hanya *user* yang terdaftar diizinkan masuk ke *domain* tersebut dan mengakses semua fasilitas *domain* yang disediakan.

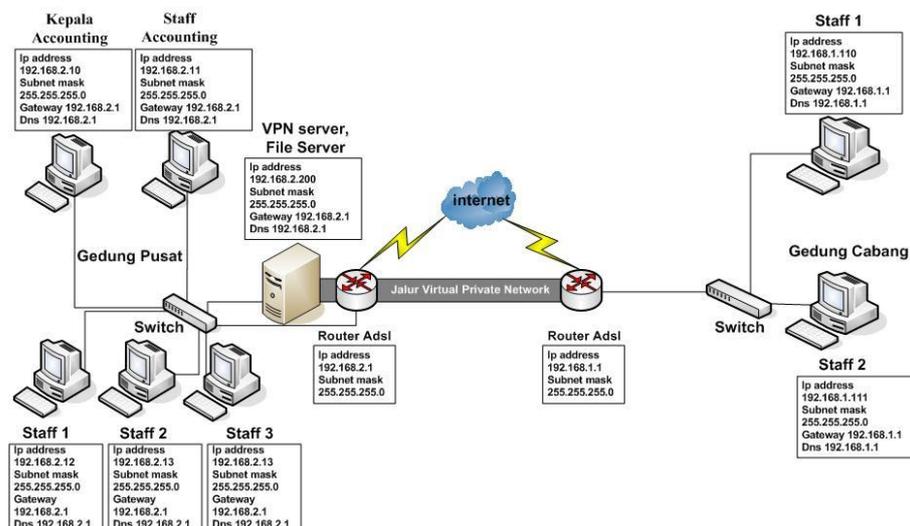
Adapun aplikasi antivirus clamav yang digunakan untuk mengantisipasi data yang berada pada mesin server atau mesin pusat penyimpanan data dari ancaman virus yang dapat merusak data perusahaan, kemudian aplikasi SSH *Server* yang digunakan untuk melakukan *remote* ke komputer *server* sangat membantu penulis saat melakukan konfigurasi pada mesin *server*

## **5.2. Pembahasan**

### **5.2.1 Konfigurasi Sistem**

Konfigurasi sistem yang akan dilakukan yaitu melakukan instalasi dan konfigurasi aplikasi VPN server dan *file server*. Sebelum melakukan instalasi dan konfigurasi *server*, penulis akan menentukan topologi jaringan terlebih dahulu yang bertujuan agar sistem yang akan dijalankan dapat berjalan secara optimal sesuai yang diharapkan

penulis. Topologi yang dipilih penulis menggunakan topologi *star* seperti gambar dibawah ini :



**Gambar 5.2 Topologi *Star* yang di Pilih pada Gedung Pusat dan Gedung Cabang PT. Palem Baja Palembang**

Pada gambar topologi *star* di atas akan dijelaskan mengenai mekanisme *server Virtual Private Network* dan *file server* yang akan diterapkan pada perusahaan. Akan dijelaskan pula *user id* dan *IP address* yang akan digunakan *client* pada *file server samba Primary Domain Controller* (PDC), diantaranya sebagai berikut :

### 1. Mekanisme *server Virtual Private Network* (VPN)

Mekanisme *server Virtual Private Network* (VPN) pada gambar topologi *star* diatas yaitu *client VPN* yang berada pada gedung cabang yaitu komputer *staff1* dan *staff2* akan diberikan *user id* dan *password VPN client* dari *server VPN* untuk dapat

melakukan *login* pada saat *server* VPN melakukan autentikasi *user* yang mencoba untuk *login*. Setelah *client* VPN pada gedung cabang mendapatkan *user id* dari VPN *server*, *client* yang berada di gedung cabang akan melakukan pemanggilan atau mengakses ke *server* VPN melalui media *internet* yang ada di gedung cabang untuk diteruskan ke *server* VPN yang ada di gedung pusat, setelah *client* di gedung cabang melakukan pemanggilan ke *server* VPN yang ada di gedung pusat melalui media *internet*, dan pada saat proses pemanggilan telah sampai di *server* VPN yang ada di gedung pusat, maka *server* VPN akan melakukan autentikasi untuk mencocokkan *user id* dari *client* VPN yang sedang melakukan pemanggilan dari gedung cabang.

Setelah proses autentikasi *user id* dan *password* selesai di periksa oleh VPN *server*, dan jika *user id* dan *password* benar pada saat dilakukan autentikasi maka VPN *server* akan memberikan IP *address* lokal atau *private* kepada *client* yang melakukan pemanggilan dari gedung cabang lalu diteruskan kembali ke *client* yang ada di gedung cabang melalui media *internet*, maka pada saat *client* yang ada di gedung cabang telah mendapatkan IP lokal atau *private* yang diberikan oleh VPN *server* yang ada di gedung pusat. Saat itulah terjadi pembuatan jalur *Virtual Private Network* atau jaringan maya yang seolah-olah gedung pusat dan gedung cabang terkoneksi seperti jaringan *local area network*. Apabila pada saat

VPN *server* melakukan autentikasi *user id* dan *password* yang dilakukan *client* tidak cocok, maka proses pemanggilan akan langsung di tolak oleh VPN *server*.

## 2. Mekanisme *File Server*

Mekanisme *file server* yang ada pada gambar topologi jaringan *star* diatas yaitu *file server* yang ada pada kantor pusat menggunakan metode *Primary Domain Controller* (PDC), maka seluruh *client* yang ada di kantor pusat untuk mengakses data atau file yang ada di *file server* atau pusat penyimpanan data dan *sharing* data harus melakukan *login user id* dan *password* ke *domain file server*.

Setelah *client* yang ada di gedung melakukan *login user id* dan *password* ke *domain file server*, maka *server file* akan melakukan autentikasi atas *user* yang mencoba melakukan *login* ke *domain*. Jika pada saat proses autentikasi selesai dilakukan oleh *server file* dan *user id* serta *password* cocok atau benar, maka *client file server* akan mendapatkan *drive* atau direktori masing-masing yang hanya dapat diakses dan dapat dilihat oleh *client* atau *user* itu sendiri dan juga *client* diberikan oleh *server file folder sharing* atau direktori bersama untuk berbagi data dengan *client user file* lainnya baik yang ada di gedung pusat maupun yang ada di gedung cabang. Apabila proses autentikasi gagal atau *user name* dan *password* tidak cocok saat *server file* melakukan autentikasi, maka *client*

yang tidak bisa *login* atau tidak mempunyai *user id* dan *password* tidak bisa untuk melakukan komunikasi pertukaran data.

### **3. *User id* dan *IP Address***

*User id* dan *IP address* yang akan dijelaskan penulis yaitu *user id* yang diberikan oleh *VPN server* dan *file server* ke komputer *client*, serta *IP address* yang digunakan komputer *client* maupun modem ADSL, diantaranya yaitu :

#### **1. *User id* dan *IP Address* di Gedung Cabang**

##### **a. Komputer staff 1**

*User id* *VPN client* hanya diberikan *server* *VPN* untuk *client* *VPN* yang berada di gedung cabang, terdapat 2 *client* yang ada digedung cabang seperti pada gambar topologi jaringan *star* perusahaan diatas maka *user id* yang akan diberikan oleh *VPN server* yaitu *riki\_cabang* dan untuk *password* dirahasiakan.

*User id* untuk *login* ke *server file* yang ada digedung pusat yaitu *riki\_cabang* dan *password* dirahasiakan. *IP address* yang digunakan client komputer staff1 pada gedung cabang yaitu menggunakan *IP address* 192.168.1.110 *subnet mask* 255.255.255.0 *gateway* 192.168.1.1 *dns* 192.168.1.1.

**b. Komputer staff 2**

*User id* VPN untuk komputer staff 2 yang akan diberikan oleh VPN *server* yaitu joni\_cabang dan untuk *password* dirahasiakan. *User id* untuk login ke *server file* yang ada di gedung pusat yaitu joni\_cabang dan *password* dirahasiakan. *IP address* yang digunakan *client* komputer staff2 pada gedung cabang yaitu menggunakan *IP address* 192.168.1.111 *subnet mask* 255.255.255.0 *gateway* 192.168.1.1 *dns* 192.168.1.1.

**c. Router ADSL**

*IP address* yang digunakan router ADSL pada gedung cabang yaitu *IP address* 192.168.1.1 *subnet mask* 255.255.255.0.

**2. User id dan IP Address di Gedung Pusat****a. Komputer Kepala Accounting**

*User id* untuk login ke *domain file server* yang akan diberikan oleh *server file* untuk komputer kepala *accounting* yaitu mujahidi dan *password* dirahasiakan. *IP address* yang digunakan *client* komputer kepala *accounting* yaitu *IP address* 192.168.2.10 *subnet mask* 255.255.255.0 *gateway* 192.168.2.1.

**b. Komputer Staff Accounting**

*User id* untuk *login* ke *domain file server* yang akan diberikan oleh *server file* untuk komputer *staff accounting* yaitu *marina* dan *password* dirahasiakan. *IP address* yang digunakan *client* komputer *staff accounting* yaitu *IP address* 192.168.2.11 *subnet mask* 255.255.255.0 *gateway* 192.168.2.1.

**c. Komputer Staff 1**

*User id* untuk *login* ke *domain file server* yang akan diberikan oleh *server file* untuk komputer *Staff 1* yaitu *kapriansah* dan *password* dirahasiakan. *IP address* yang digunakan *client* komputer *staff 1* yaitu *IP address* 192.168.2.12 *subnet mask* 255.255.255.0 *gateway* 192.168.2.1.

**d. Komputer Staff 2**

*User id* untuk *login* ke *domain file server* yang akan diberikan oleh *server file* untuk komputer *Staff 2* yaitu *ferdinan* dan *password* dirahasiakan. *IP address* yang digunakan *client* komputer *staff 2* yaitu *IP address* 192.168.2.13 *subnet mask* 255.255.255.0 *gateway* 192.168.2.1.

### e. Komputer Staff 3

*User id* untuk *login* ke *domain file server* yang akan diberikan oleh *server file* untuk komputer staff 3 yaitu roni dan *password* dirahasiakan. IP address yang digunakan *client* komputer staff 3 yaitu IP address 192.168.2.14 subnet mask 255.255.255.0 gateway 192.168.2.1.

### f. Router ADSL

IP address yang digunakan router ADSL pada gedung pusat yaitu IP address 192.168.2.1 subnet mask 255.255.255.0.

## 5.2.2 Instalasi dan Konfigurasi Server

Instalasi dan konfigurasi *server* yaitu akan dijelaskan langkah-langkah dalam melakukan instalasi aplikasi dan konfigurasi aplikasi yang akan yang akan di implementasikan pada mesin *server*.

### 5.2.2.1 Instalasi dan Konfigurasi VPN Server

Sebelum melakukan instalasi aplikasi yang dibutuhkan pada komputer *server*, penulis terlebih dahulu melakukan konfigurasi IP address pada komputer *server*. Langkah-langkah melakukan konfigurasi IP address pada komputer *server* yaitu dengan mengedit *file* dengan perintah :

```
#nano /etc/network/interfaces
```

**Gambar 5.3 Perintah Konfigurasi IP Address**

lalu masukkan *IP address* dan sesuaikan dengan kondisi jaringan yang ada seperti gambar dibawah ini :

```
# This file describes the network
interfaces available on your system

# and how to activate them. For more
information, see interfaces(5).

# The loopback network interface

auto lo

iface lo inet loopback

iface eth0 inet static

address 192.168.2.200

netmask 255.255.255.0

gateway 192.168.2.1

auto eth0
```

**Gambar 5.4 Konfigurasi IP Address**

Kemudian masukkan DNS untuk komputer *server* dengan mengedit file */etc/init.d/resolv.conf* seperti gambar dibawah ini :

```
#nano /etc/resolv.conf
```

**Gambar 5.5 Perintah Edit File *Resolv.conf***

Setelah membuka *file /etc/resolv.conf* selanjutnya mengisi *dns* pada komputer *server* dan sesuaikan dengan keadaan jaringan yang ada seperti gambar dibawah ini :

```
nameserver 192.168.2.1
```

**Gambar 5.6 Isi File *Resolv.conf***

Setelah selesai melakukan konfigurasi pada IP *address server* maka lakukan *restart* kartu jaringan agar konfigurasi IP *address* yang dilakukan sebelumnya dijalankan, dengan menggunakan perintah seperti dibawah ini :

```
#/etc/init.d/networking restart
```

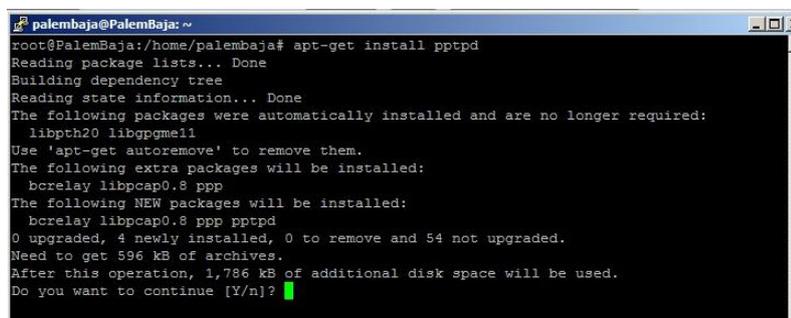
### Gambar 5.7 Perintah *Restart* Kartu Jaringan

Saat proses *restart* kartu jaringan selesai dan pastikan komputer *server* sudah terkoneksi ke *internet*. Maka langkah selanjutnya melakukan *install* aplikasi untuk VPN *server* yaitu aplikasi PPTPD dengan menggunakan *apt-get install pptpd* perintah seperti gambar dibawah ini :

```
#apt-get install pptpd
```

### Gambar 5.8 Perintah Install Aplikasi PPTPD

Saat proses instalasi aplikasi PPTPD berjalan terdapat pilihan apakah akan melanjutkan proses instalasi, seperti gambar dibawah ini :



```
palembaja@Palembaja: ~  
root@Palembaja:/home/palembaja# apt-get install pptpd  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
  libpth20 libpggmell  
Use 'apt-get autoremove' to remove them.  
The following extra packages will be installed:  
  bcrelay libpcap0.8 ppp  
The following NEW packages will be installed:  
  bcrelay libpcap0.8 ppp pptpd  
0 upgraded, 4 newly installed, 0 to remove and 54 not upgraded.  
Need to get 596 kB of archives.  
After this operation, 1,786 kB of additional disk space will be used.  
Do you want to continue [Y/n]?
```

### Gambar 5.9 Proses *Instalasi* PPTPD

Pada gambar di atas dapat dilihat aplikasi untuk kelengkapan PPTPD yaitu *bcrelay* dan PPP terinstall secara bersamaan. Setelah proses instalasi aplikasi PPTPD selesai maka dilanjutkan untuk melakukan konfigurasi pada file */etc/pptpd.conf*. lalu pada bagian isi file */etc/pptpd.conf* tulisan *localip* dan *remoteip*, *localip* adalah IP address untuk komputer server dan *localip* adalah IP address yang akan diberikan kepada *client* VPN dengan range IP address 192.168.2.201 sampai 192.168.2.205 yang ada di gedung cabang, isi file */etc/pptpd.conf* seperti gambar dibawah ini :

```
# IP Address server
localip 192.168.2.200

# IP Address client
remoteip 192.168.2.111-112
```

**Gambar 5.10 Isi File *pptpd.conf***

Setelah selesai melakukan konfigurasi pada file */etc/pptpd.conf* maka langkah selanjutnya dengan melakukan konfigurasi file */etc/ppp/pptpd-options*, kemudian isi file */etc/ppp/pptpd-options* seperti pada gambar di bawah ini :

```

name pptpd
refuse-pap
refuse-chap
refuse-mschap
require-mschap-v2
require-mppe-128
ms-dns 192.168.2.1
proxyarp
nodefaultroute
lock
nobsdcomp

```

**Gambar 5.11** Isi File */etc/ppp/pptpd-options*

Pada gambar di atas di bagian *name pptpd* adalah nama yang dipakai untuk VPN *server* bisa di ganti dengan nama lain selain *pptpd*, lalu pada bagian *ms-dns 192.168.2.1* yaitu *dns* yang akan diberikan untuk *client* VPN.

Setelah selesai konfigurasi pada file */etc/ppp/pptpd-options*, langkah konfigurasi terakhir pada *server* VPN yaitu dengan melakukan konfigurasi pada file */etc/ppp/chap-secret* yang bertujuan untuk mendaftarkan *client* VPN, konfigurasi file */etc/ppp/chap-secrets* dapat dilihat pada gambar di bawah ini :

#client	server	secret	IP Address
joni_cabang	pptpd	*****	192.168.2.111
riki_cabang	pptpd	*****	192.168.2.112

**Gambar 5.12** Isi file */etc/ppp/chap-secrets*

Pada gambar di atas dari isi file */etc/ppp/chap-secrets* yaitu pada bagian client adalah *user id* yang akan diberikan

oleh VPN *server* yang terdapat beberapa *user id client* VPN diantaranya terdapat *user id* joni\_cabang, riki\_cabang, karyawan1, karyawan2 dan karyawan3. Dimana *user id* karyawan1, karyawan2 dan karyawan3 adalah *user id* yang di buat penulis dengan tujuan jika ada penambahan komputer pada gedung cabang ataupun ada karyawan lain yang memiliki tugas untuk bertukar data ke gedung pusat, kemudian pada bagian *secret* yaitu *password* yang diberikan oleh VPN *server* untuk *client* VPN dan *password* tersebut dirahasiakan.

Selanjutnya pada bagian *server* yang terdapat *pptpd* yaitu *client* VPN yang akan melakukan akses ke VPN *server* di arahkan ke *server* pptpd. Adapun pada bagian IP *address* yaitu terdapat IP *address* yang diberikan adalah 192.168.2.111, 192.168.2.112 adalah IP *address static* yang akan diberikan pada user riki\_cabang dan joni\_cabang, pada bagian IP *address* lainnya yang terdapat tanda \* atau bintang adalah IP *address dynamic* yang akan diberikan pada user karyawan1, karyawan2 dan karyawan3 saat melakukan pemanggilan ke *server* VPN.

Setelah melakukan konfigurasi pada *file /etc/ppp/chap-secrets* maka konfigurasi pada *server* VPN telah selesai, langkah berikutnya dengan melakukan *restart* aplikasi PPTPD dengan perintah seperti gambar dibawah ini :

```
#/etc/init.d/pptpd restart
```

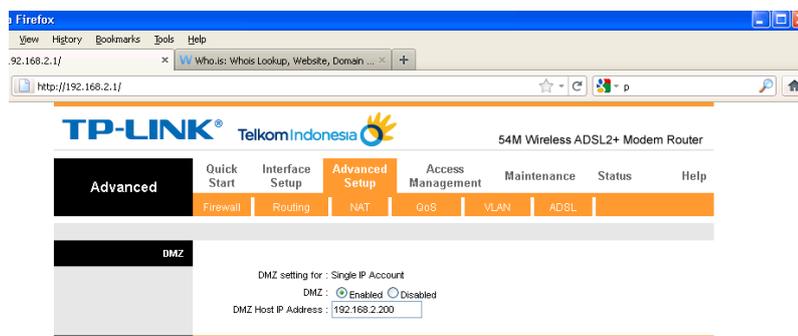
**Gambar 5.13 Perintah *Restart* Aplikasi PPTPD**

Untuk memonitoring atau melihat *log* saat *client* VPN melakukan pemanggilan ke *server* VPN dengan melakukan perintah seperti gambar dibawah ini :

```
#tail -f /var/log/messages
```

**Gambar 5.14 Perintah Melihat *Log Server* VPN**

Setelah selesai melakukan konfigurasi *server* VPN, maka selanjutnya melakukan konfigurasi pada bagian modem ADSL yang ada di gedung pusat. Pada konfigurasi modem ADSL seperti gambar dibawah ini :



**Gambar 5.15 Konfigurasi modem ADSL**

Pada gambar di atas konfigurasi modem ADSL yang dilakukan penulis adalah memasukkan *IP address* komputer *server* pada bagian *DMZ host IP address* dan *IP address* komputer *server* yaitu 192.168.2.200. Tujuan yang dilakukan

pada konfigurasi ini adalah agar komputer *server* yang menggunakan *IP address* lokal atau *private* 192.168.2.200 dapat di akses dari gedung cabang melalui media *internet* dengan menggunakan *IP publik* yang ada di gedung pusat.

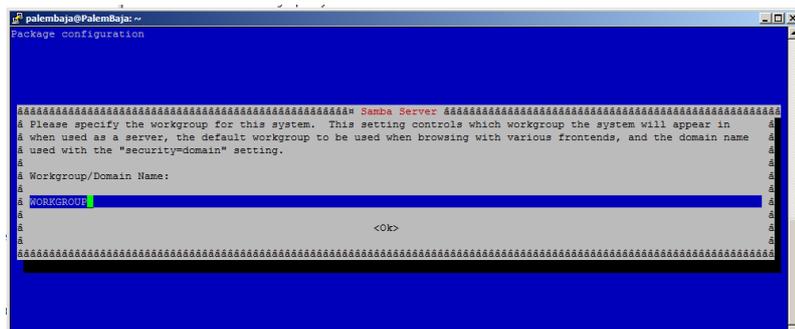
### 5.2.2.2 Instalasi dan Konfigurasi Samba Server

Tahapan Instalasi dan konfigurasi *samba server* dengan metode *Primary Domain Controller* (PDC) yang akan dilakukan pertama kali adalah melakukan instalasi *samba* dengan menggunakan perintah pada terminal seperti pada gambar di bawah ini :

```
#apt-get install samba
```

**Gambar 5.16 Perintah Instalasi Aplikasi Samba**

Setelah melakukan instalasi dengan perintah pada gambar di atas maka saat instalasi akan muncul tampilan untuk membuat nama *workgroup* pada *server samba*. Tampilan tersebut dapat dilihat pada gambar berikut ini :



**Gambar 5.17 Tampilan Nama Workgroup**

Setelah tampilan *workgroup* pada gambar di atas proses instalasi akan dilanjutkan dengan menekan *enter*. Pada saat proses instalasi selesai maka langkah selanjutnya buka *file /etc/samba/smb.conf*. untuk melakukan konfigurasi *file /etc/samba/smb.conf* gunakan perintah seperti gambar di bawah ini :

```
#nano /etc/samba/smb.conf
```

**Gambar 5.18 Perintah Editor *smb.conf***

Langkah selanjutnya dengan memasukkan *script* konfigurasi untuk *file smb.conf*, *script* yang akan digunakan untuk *file smb.conf* seperti pada gambar di bawah ini :

```
[global]
workgroup = PALEMBAJA
netbios name = SERVER
server string = %h server
passdb backend = tdbsam
security = user
username map = /etc/samba/smbusers
name resolve order = wins bcast hosts
domain logons = yes
preferred master = yes
wins support = yes
# Set CUPS for printing
```

```
load printers = yes

printcap name = CUPS

printing = CUPS

# Default logon

logon drive = H:

logon script = scripts/logon.bat

logon path = \\server1\profile\%U

# Useradd scripts

# add user script = /usr/sbin/adduser --quiet
--disabled-password --gecos "" %u

add user script = /usr/sbin/useradd -m '%u' -g
users -G users

delete user script = /usr/sbin/userdel -r %u

add group script = /usr/sbin/groupadd %g

delete group script = /usr/sbin/groupdel %g

add user to group script = /usr/sbin/usermod -
G %g %u

add machine script = /usr/sbin/useradd -s
/bin/false/ -d /var/lib/nobody %u

idmap uid = 15000-20000

idmap gid = 15000-20000

template shell = /bin/bash

# sync smb passwords with linux passwords

passwd program = /usr/bin/passwd %u

passwd chat = *Enter\snew\sUNIX\spassword:*
%n\n *Retype\snew\sUNIX\spassword:*
```

```
%n\n*password\supdated\ssuccessfully* .  
  
passwd chat debug = yes  
unix password sync = yes  
  
# set the loglevel  
  
log level = 3  
  
[public]  
browseable = yes  
public = yes  
  
[homes]comment = Home  
valid users = %S  
read only = no  
browsable = no  
  
[netlogon]  
comment = Network Logon Service  
path = /home/samba/netlogon  
admin users = Administrator  
valid users = %U  
read only = no  
guest ok = yes  
writable = no  
share modes = no  
  
[profile]  
comment = User profiles  
path = /home/samba/profiles  
valid users = %U  
create mode = 0600  
directory mode = 0700
```

```
writable = yes  
browsable = no  
guest ok = no  
[alluser]  
comment = folder sharing  
path = /home/shares/allusers  
valid users = @users  
force group = users  
create mask = 0660  
directory mask = 0771  
writable = yes
```

**Gambar 5.19 File Script *smb.conf***

Setelah melakukan konfigurasi *file smb.conf* seperti gambar di atas, maka langkah selanjutnya membuat direktori baru dan memberikan hak akses pada direktori komputer *server*, direktori baru yang akan dibuat dengan menggunakan perintah seperti gambar dibawah ini :

```
mkdir /home/samba  
mkdir /home/samba/netlogon  
mkdir /home/samba/profiles  
chmod 777 /var/spool/samba/  
chown -R root:users /home/samba/  
chmod -R 771 /home/samba
```

**Gambar 5.20 Membuat Direktori dan Hak Akses**

Selanjutnya setelah membuat direktori dan hak akses pada komputer *server*, langkah yang dilakukan berikutnya

adalah merestart aplikasi *samba server*, dengan menggunakan perintah seperti gambar dibawah ini :

```
#/etc/init.d/samba restart
```

**Gambar 5.21 Restart Aplikasi Samba Server**

Setelah melakukan *restart* aplikasi *samba*, langkah selanjutnya dengan mengedit file */etc/nsswitch.conf* dan tambahkan pada baris *hosts* : *file dns* menjadi *hosts file wins dns*, seperti pada gambar dibawah ini :

```
passwd:          compat
group:           compat
shadow:         compat
hosts:           files wins dns
networks:       files
```

**Gambar 5.22 Edit File nsswitch.conf**

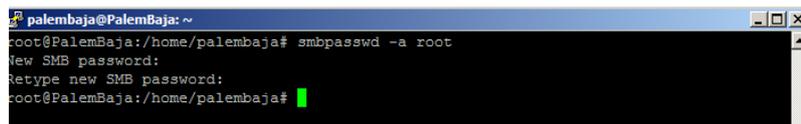
Setelah melakukan konfigurasi pada file *nsswitch.conf*, maka langkah selanjutnya dengan menambahkan *user root* yang ada pada komputer *server* ke database *samba*, langkah menambahkan *user root* ke *database samba* dengan menggunakan perintah seperti pada gambar dibawah ini :

```
#smbpasswd -a root
```

**Gambar 5.23 Perintah smbpasswd -a root**

Setelah menambah *user root* ke *database samba* dengan menggunakan perintah seperti gambar di atas, maka

*samba server* akan meminta untuk membuat *password* baru di *database samba* untuk *user root* seperti pada gambar dibawah ini :



```
palembaja@PalemBaja: ~
root@PalemBaja:/home/palembaja# smbpasswd -a root
New SMB password:
Retype new SMB password:
root@PalemBaja:/home/palembaja#
```

**Gambar 5.24** Membuat *Password root* di *Samba Server*

Langkah selanjutnya yang akan dilakukan yaitu menambahkan *user root* ke *direktori /etc/samba/smbusers* yang bertujuan untuk membuat *user root* menjadi *user administrator* saat melakukan *join* ke *domain samba Primary Domain Controller (PDC)* pada sistem operasi *windows client*, perintah yang dilakukan untuk menambah *user root* ke *direktori /etc/samba/smbuser* seperti pada gambar dibawah ini :



```
palembaja@PalemBaja: ~
root@PalemBaja:/etc/samba# nano /etc/samba/smbusers
root@PalemBaja:/etc/samba# nano /etc/samba/smbusers
root@PalemBaja:/etc/samba# echo "root = Administrator" > /etc/samba/smbusers
root@PalemBaja:/etc/samba#
```

**Gambar 5.25** Menambah *User root* ke *Direktori smbusers*

Setelah menambah *user root* ke *direktori samba*, langkah selanjutnya melakukan perintah untuk mengatur kelompok *default* pada *client* di sistem operasi *windows*, perintah untuk mengatur kelompok *default* pada *client* di sistem operasi *windows* seperti gambar dibawah ini :

```
#net groupmap add ntgroup="Domain Admins"
unixgroup="root" type=domain -U root

#net groupmap add ntgroup="Domain Users"
unixgroup="users" type=domain -U root

#net groupmap add ntgroup="Domain Guests"
unixgroup="nogroup" type=domain -U root
```

**Gambar 5. 26 Mengatur Kelompok *Default Client* pada *Windows***

Setelah mengatur kelompok *default* pada *client* di sistem operasi *windows* selesai dilakukan, maka langkah selanjutnya menambahkan *user id* dan *password* untuk *client samba Primary Domain Controller (PDC)* di sistem operasi *windows*, dengan melakukan perintah seperti gambar di bawah ini :

```
#net rpc user add roni -U root

#net rpc user password roni "password" -U root

#smbpasswd -e roni
```

**Gambar 5.27 Perintah Menambah *User Client Samba PDC***

Perintah pada gambar diatas yaitu dibaris pertama bertujuan untuk menambah *user roni* dan membuat *password* di baris kedua pada kalimat "*password*" selanjutnya pada baris ketiga melakukan perintah *enable* untuk *user roni*. Untuk menambahkan *user client samba PDC* yang ada pada perusahaan dengan *user mujahidi, marina, kapriansah, ferdinan, riki\_cabang* dan *joni\_cabang* menggunakan perintah

yang sama seperti perintah yang ada pada gambar diatas hanya mengganti nama *user id* dan *password client samba* PDC yang ingin di daftarkan pada server *samba* PDC.

Setelah semua langkah-langkah konfigurasi *server samba* dengan menggunakan metode *Primary Domain Controller* (PDC) diatas telah sudah dilakukan. Langkah terakhir yang dilakukan yaitu dengan melakukan *restart* aplikasi *samba server* dengan menggunakan perintah seperti gambar dibawah ini :

```
#/etc/init.d/samba restart
```

**Gambar 5.28 Perintah *Restart* Aplikasi *Samba***

Selanjutnya untuk melakukan test konfigurasi *samba* yang telah dilakukan yaitu dengan perintah seperti pada gambar dibawah ini :

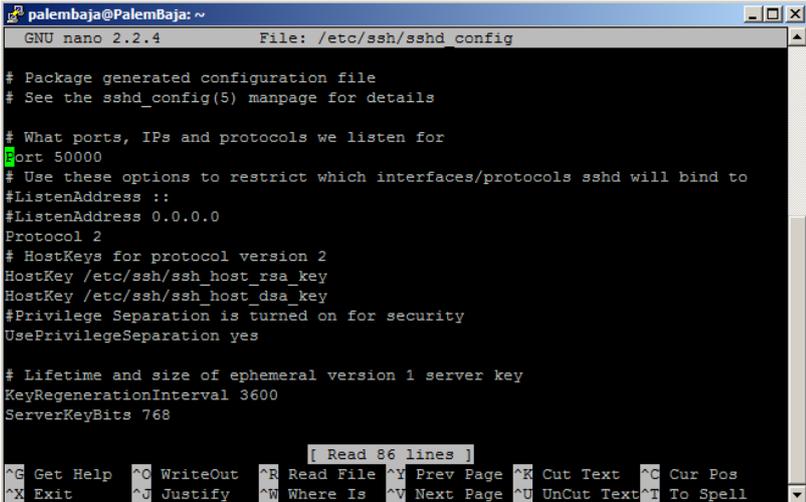
```
#testparm
```

**Gambar 5.29 Perintah *Testparm***

Setelah melakukan perintah yang ada pada gambar diatas maka akan ditampilkan hasil dari konfigurasi dari *file /etc/samba/smb.conf* yang telah dilakukan sebelumnya seperti pada gambar 5.19 *File Script smb.conf*.

### 5.2.2.3 Konfigurasi Keamanan pada Komputer Server

Konfigurasi keamanan pada komputer *server* yang dilakukan penulis yaitu mengganti *port default* SSH *server* yaitu menggunakan *port 22* dan *port 22* tersebut diganti menjadi *port 5000*. Penggantian *port default* tersebut bertujuan untuk mengamankan komputer *server* dari orang yang tidak bertanggung jawab untuk melakukan penyusupan secara langsung ke mesin *server*, karena komputer *server* yang berada di gedung pusat perusahaan sudah bisa diakses dari jaringan luar dengan menggunakan IP *publik* dan langsung diteruskan ke IP *address* lokal pada komputer *server*. Konfigurasi yang dilakukan penulis untuk mengganti *port default* pada SSH *server* dengan mengedit *file /etc/ssh/sshd\_config* seperti gambar dibawah ini :



```
palembaja@PalemBaja: ~
GNU nano 2.2.4 File: /etc/ssh/sshd_config
# Package generated configuration file
# See the sshd_config(5) manpage for details

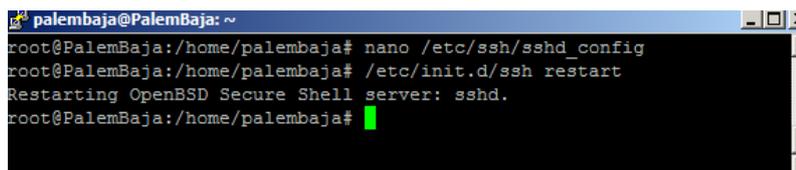
# What ports, IPs and protocols we listen for
Port 50000
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress :
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 768

[ Read 86 lines ]
^G Get Help ^O WriteOut ^R Read File ^V Prev Page ^X Cut Text ^C Cur Pos
^X Exit ^U Justify ^W Where Is ^N Next Page ^_ UnCut Text ^? To Spell
```

**Gambar 5.30 Mengganti Port Default SSH Server**

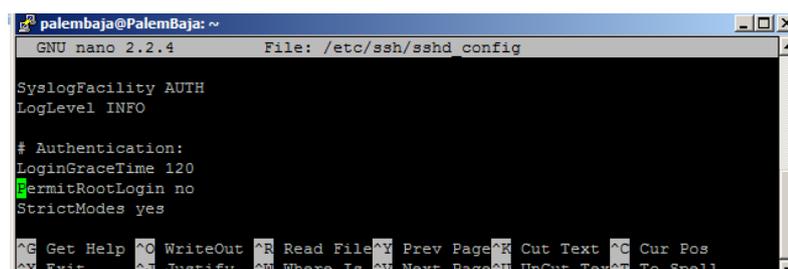
Setelah selesai mengganti *port default* SSH server menjadi 50000, langkah selanjutnya dengan merestart aplikasi SSH server menggunakan perintah seperti gambar dibawah ini :



```
palembaja@Palembaja: ~
root@Palembaja:/home/palembaja# nano /etc/ssh/sshd_config
root@Palembaja:/home/palembaja# /etc/init.d/ssh restart
Restarting OpenBSD Secure Shell server: sshd.
root@Palembaja:/home/palembaja#
```

**Gambar 5.31 Perintah *Restart* SSH Server**

Langkah selanjutnya yang dilakukan penulis adalah untuk tidak mengizinkan *user root* yang ada pada komputer server untuk melakukan *login* melalui SSH server, langkah yang dilakukan yaitu mengedit file */etc/ssh/sshd\_config* dan pada baris *PermitRootLogin yes* ganti menjadi *PermitRootLogin no* seperti pada gambar dibawah ini :



```
palembaja@Palembaja: ~
GNU nano 2.2.4 File: /etc/ssh/sshd_config
SyslogFacility AUTH
LogLevel INFO

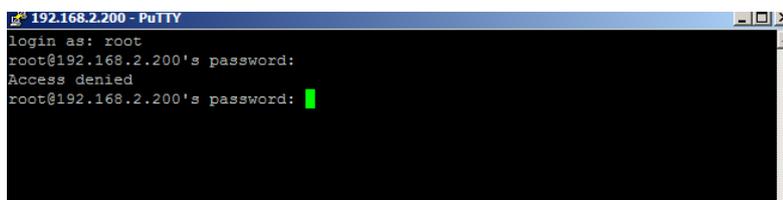
# Authentication:
LoginGraceTime 120
PermitRootLogin no
StrictModes yes

^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
```

**Gambar 5.32 Perintah *Restart* SSH Server**

Selanjutnya *restart* kembali SSH server, kemudian pada saat percobaan untuk *login* melalui SSH server dengan menggunakan *user root* akan terjadi penolakan dari SSH

server, penolakan menggunakan *user root* dapat dilihat pada gambar dibawah ini :



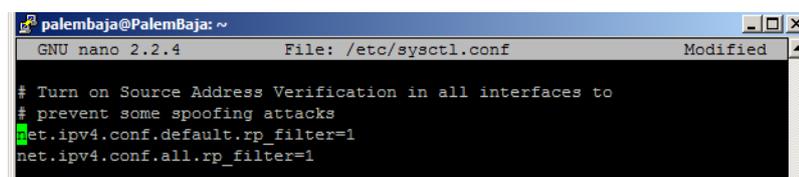
```

192.168.2.200 - PuTTY
login as: root
root@192.168.2.200's password:
Access denied
root@192.168.2.200's password: █

```

**Gambar 5.33 Percobaan Login Menggunakan User root**

Selanjutnya langkah yang dilakukan untuk mengamankan komputer server dari *spoofing attacks*, *spoofing attacks* adalah melakukan pengalihan IP address dan *node source* atau tujuan yang asli dan diganti dengan IP address ke tujuan yang lain. Langkah yang dilakukan untuk mengamankan komputer server dari *spoofing attacks* yaitu dengan mengedit file */etc/ sysctl.conf* kemudian aktifkan dengan cara menghilangkan tanda pagar pada baris isi file yang ada seperti gambar dibawah ini :



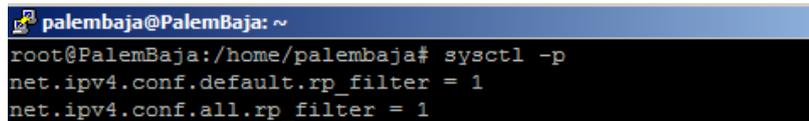
```

palembaja@PalemBaja: ~
GNU nano 2.2.4 File: /etc/sysctl.conf Modified
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
net.ipv4.conf.default.rp_filter=1
net.ipv4.conf.all.rp_filter=1

```

**Gambar 5.34 Mencegah Serangan Spoofing Attacks**

Kemudian simpan konfigurasi diatas dan untuk mengaktifkannya dengan menggunakan perintah *sysctl -p* seperti pada gambar dibawah ini :



```
palem baja@PalemBaja: ~
root@PalemBaja:~/home/palem baja# sysctl -p
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.all.rp_filter = 1
```

**Gambar 5.35 Perintah *sysctl -p***

Selanjutnya melakukan instalasi anti *virus*, anti *virus* yang digunakan yaitu anti *virus clamav* yang bertujuan untuk mengantisipasi data pada mesin *server* dari serangan *virus*. Perintah untuk melakukan instalasi anti *virus clamav* seperti pada gambar dibawah ini :

```
#apt-get install clamav
```

**Gambar 5.36 Perintah Install *Clamav***

Setelah proses instalasi anti *virus clamav* selesai, selanjutnya melakukan update anti *virus clamav* dengan menggunakan perintah seperti pada gambar dibawah ini :

```
#freshclam
```

**Gambar 5.37 Perintah *Update Clamav***

Agar *clamav* melakukan update secara otomatis setiap hari dengan mengetikkan perintah *crontab -e* kemudian tambahkan perintah seperti pada gambar dibawah ini :

```
* * * * /usr/bin/freshclam -l /var/log/clamav/update-
clamav.log
```

**Gambar 5.38 Perintah *Update Otomatis Clamav***

Perintah gambar diatas yaitu perintah untuk menjalankan *update database* anti *virus clamav* pada pukul delapan pagi setiap hari dan log *update clamav* berada pada direktori */var/log/clamav/update-clamav.log*.

Langkah selanjutnya setelah proses penjadwalan *update* anti *virus clamav* selesai dilakukan, maka dilanjutkan untuk melakukan *scan* komputer *server* agar komputer *server* terhindar dari *virus*. Perintah untuk melakukan scan data seperti pada gambar dibawah ini :

```
# clamscan -r /home
```

**Gambar 5.39 Perintah Scan Clamav**

Langkah yang dilakukan seperti pada gambar diatas yaitu untuk melakukan *scan virus* pada direktori *home*. Jika pada saat selesai melakukan *scan virus* pada direktori *home*, maka untuk menghapus *virus* tersebut dengan melakukan perintah seperti pada gambar dibawah ini :

```
# clamscan --remove
```

**Gambar 5.40 Perintah Menghapus Virus**

Selanjutnya untuk memberi penjadwalan pada anti *virus clamav* agar setiap hari melakukan proses *scan* terhadap data perusahaan secara otomatis yaitu dengan mengeksekusi perintah *crontab -e* kemudian masukkan perintah untuk menjalankan

program yang ingin dijalankan pada komputer *server*, seperti pada gambar dibawah ini :

```
* 10 * * * /usr/bin/clamscan -r --remove /home/ -l  
/var/log/scan-clamav.log
```

**Gambar 5.41 Perintah Penjadwalan Crontab**

Pada gambar diatas adalah perintah untuk melakukan *scan* antivirus *clamav* setiap hari jam sepuluh pagi pada direktori *home*, jika dalam proses *scan* terdeteksi *virus* maka data yang terinfeksi *virus* tersebut akan langsung dihapus oleh anti *virus clamav*.

#### 5.2.2.4 Pengujian VPN Server PPTP

Pengujian VPN *server* PPTP yang telah di implementasikan akan dilakukan pada komputer *client* yang berada di gedung cabang perusahaan, komputer *client* pada gedung cabang menggunakan sistem operasi *windows xp* dan melakukan akses ke VPN *server* PPTP melalui media *internet*, IP *address* yang akan dituju *client* VPN ke *server* VPN PPTP menggunakan IP *publik* yang ada di gedung pusat.

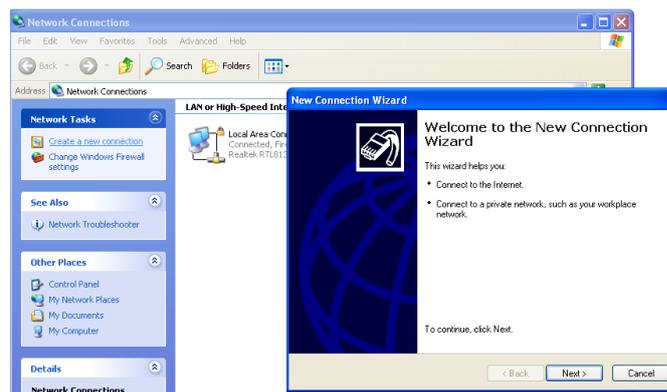
Pengujian pertama menggunakan *user* id *joni\_cabang*, langkah pertama yang dilakukan adalah membuat *network connection* baru untuk melakukan koneksi ke *server* VPN

dengan cara membuka *start menu* pada *windows*, kemudian *network connections* seperti gambar dibawah ini :



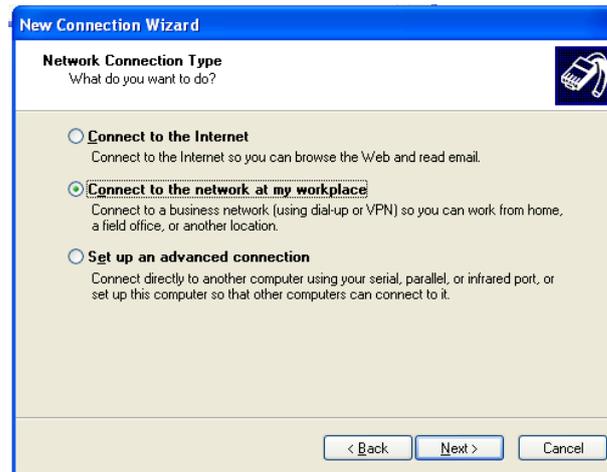
**Gambar 5.42 Network Connection**

Setelah membuka menu *network connections*, langkah selanjutnya yaitu klik pada bagian *create a new connection* dan klik *next* untuk melanjutkan seperti pada gambar dibawah ini :



**Gambar 5.43 Create a New Connection**

Kemudian langkah selanjutnya pilih pada bagian *connect to the network at my workplace* dan klik *next* untuk melanjutkan seperti tampilan gambar dibawah ini :



**Gambar 5.44** *Connect to the Network at My Workplace*

Setelah memilih *connect to the network at my workplace*, selanjutnya pilih *virtual private network connection*, seperti pada tampilan di bawah ini :



**Gambar 5.45** *Virtual Private Network Connection*

Kemudian terdapat menu pilihan untuk membuat *connection name*, maka isi pada kolom tersebut dengan nama perusahaan atau nama *VPN server*, seperti tampilan pada gambar dibawah ini :



**Gambar 5.46 Connection Name**

Setelah selesai pada tahap membuat *connection name*, maka langkah selanjutnya pada bagian *VPN server selection* dengan menginput IP *publik* yang digunakan *server VPN server PPTP* pada gedung pusat dan klik *next*. *Input IP publik VPN server PPTP* seperti pada gambar dibawah ini :



**Gambar 5.47 VPN Server Selection**

Setelah selesai proses penginputan IP *publik* *VPN server PPTP* yang berada di gedung pusat, kemudian pada pilihan *connection availability* terdapat dua pilihan yaitu *anyone's use* dan *my use only*. Pada langkah ini penulis

memilih *opsi anyone's use* dan *next* seperti pada gambar dibawah ini :



**Gambar 5.48** *Conection Availability*

Setelah pada pilihan *conection availability* maka akan keluar pemberitahuan bahwa proses pembuatan koneksi baru yang digunakan untuk mengakses ke *server* VPN PPTP yang ada di gedung cabang telah selesai, selanjutnya centang bagian *add a shortcut to this connection to my desktop* dan klik *finish* seperti pada tampilan dibawah ini :



**Gambar 5.49** *Completing the New Connection Wizard*

Proses pembuatan koneksi baru untuk melakukan koneksi VPN *client* ke VPN *server* PPTP yang berada di gedung cabang telah selesai di konfigurasi.

Selanjutnya pada menu *network connections* atau *shortcut* di *desktop* terdapat *network* koneksi untuk melakukan pemanggilan ke *server* VPN PPTP yang telah dibuat sebelumnya dan jalankan *network connections* yang telah dibuat tersebut maka akan terdapat tampilan untuk melakukan *input user name* dan *password* seperti pada gambar dibawah ini :



**Gambar 5.50** Tampilan *input Username* dan *Password*

Pada gambar diatas masukkan *user name* joni\_cabang dan *password* yang telah didaftarkan ke *server* VPN PPTP yang ada di gedung pusat. Langkah selanjutnya klik *connect* untuk melakukan pemanggilan ke *server* VPN PPTP yang ada di gedung pusat melalui media *internet* yang ada di gedung cabang.

Saat proses pemanggilan ke *server* VPN PPTP akan tampil proses verifikasi *username* dan *password* yang dilakukan oleh *server* VPN PPTP yang ada di gedung pusat, verifikasi *username* dan *password* yang dilakukan *server* VPN PPTP seperti gambar dibawah ini :



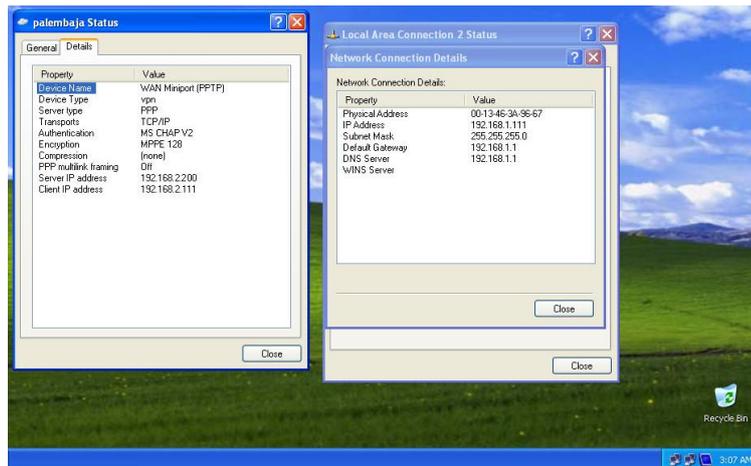
**Gambar 5.51 Verifikasi Username dan Password**

Saat melakukan proses verifikasi *username* dan *password* pada gambar diatas, jika *username* dan *password* benar saat dilakukan verifikasi oleh *server* VPN PPTP yang ada di gedung pusat maka *server* VPN PPTP akan melakukan *registrasi* komputer *client* VPN yang berada di gedung cabang ke jaringan lokal pada gedung pusat.



**Gambar 5.52 Registrasi Komputer Client**

Setelah proses *registrasi* selesai dilakukan maka *server* VPN PPTP akan memberikan *IP address* ke komputer *client* VPN. *IP address* yang diberikan oleh VPN *server* ke komputer *client* VPN dapat dilihat pada gambar berikut ini :



**Gambar 5.53 IP Address VPN dan IP Address LAN**

Selanjutnya *client* VPN joni\_cabang melakukan *ping* ke *IP address server* VPN PPTP yang ada di gedung pusat yaitu dengan melakukan *ping* ke *IP address* 192.168.2.200, seperti pada tampilan gambar berikut ini :

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\joni_cabang>ping 192.168.2.200

Pinging 192.168.2.200 with 32 bytes of data:

Reply from 192.168.2.200: bytes=32 time=76ms TTL=64
Reply from 192.168.2.200: bytes=32 time=79ms TTL=64
Reply from 192.168.2.200: bytes=32 time=81ms TTL=64
Reply from 192.168.2.200: bytes=32 time=81ms TTL=64

Ping statistics for 192.168.2.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\joni_cabang>

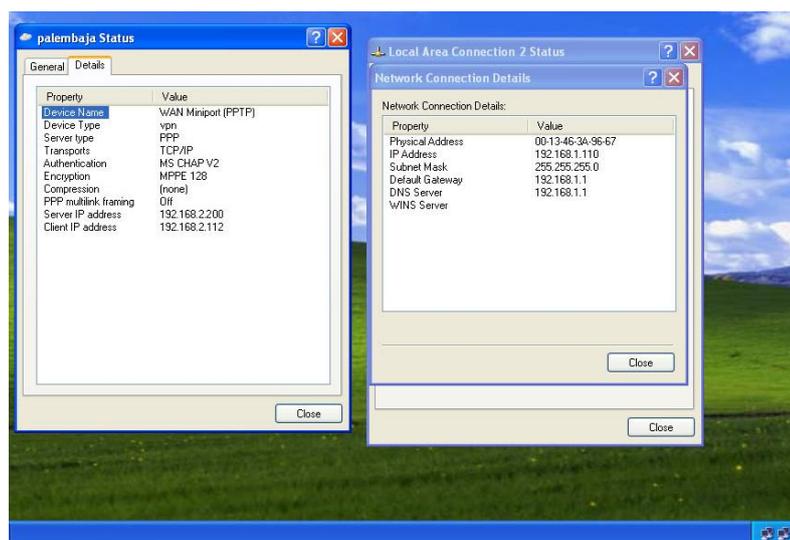
```

**Gambar 5.54 Ping ke IP Address Server VPN**

Pengujian yang dilakukan pada *user VPN client* joni\_cabang yang ada di gedung cabang untuk mengakses ke *server VPN PPTP* di gedung pusat telah berhasil dilakukan.

Pengujian kedua yang dilakukan penulis yaitu pada *client VPN* dengan *username* riki\_cabang tahapan-tahapan atau langkah-langkahnya sama seperti pengujian pada *username* joni\_cabang. Maka pada tahapan pengujian kedua ini hanya dijelaskan dari hasil *IP address* yang diberikan *server VPN PPTP* dan dengan melakukan *ping* ke *IP address server VPN*.

Adapun *IP address* yang diberikan *server VPN PPTP* ke *VPN client* user riki\_cabang yaitu 192.168.2.112, *IP address* yang diberikan *server VPN PPTP* dapat dilihat pada gambar dibawah ini :



**Gambar 5.55 IP Address VPN dan IP Address LAN**

**riki\_cabang**

Setelah IP *address* diberikan *server* VPN PPTP ke *client* VPN, maka pengujian selanjutnya melakukan *ping* dari *client* VPN di gedung cabang ke *server* VPN PPTP di gedung pusat seperti pada gambar dibawah ini :



```

C:\WINDOWS\system32\cmd.exe - ping 192.168.2.11
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\riki_cabang>ping 192.168.2.200
Pinging 192.168.2.200 with 32 bytes of data:
Reply from 192.168.2.200: bytes=32 time=995ms TTL=127
Reply from 192.168.2.200: bytes=32 time=446ms TTL=127
Reply from 192.168.2.200: bytes=32 time=357ms TTL=127
Reply from 192.168.2.200: bytes=32 time=288ms TTL=127

Ping statistics for 192.168.2.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\riki_cabang>ping 192.168.2.11

```

**Gambar 5.56 Ping User riki\_cabang ke VPN Server**

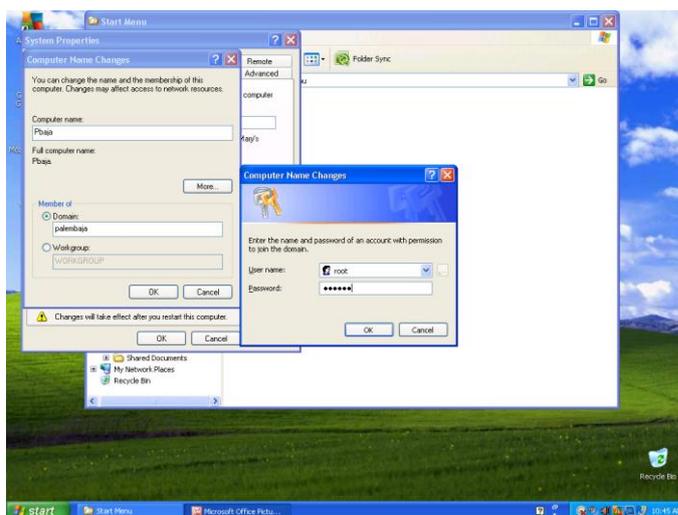
Pengujian kedua dilakukan terhadap *client* VPN PPTP dengan menggunakan user *riki\_cabang* telah selesai dilaksanakan, dan terlihat pada gambar diatas *client* VPN user *riki\_cabang* sudah terkoneksi ke *server* VPN PPTP yang ada di gedung pusat.

#### 5.2.2.5 Pengujian File Server

Pengujian *file server* dengan menggunakan metode *Primary Domain Controller* akan dilakukan pada gedung pusat dan gedung cabang, sistem operasi pada gedung pusat dan gedung cabang menggunakan sistem operasi *windows xp* dan *client file server* yang akan dilakukan pengujian ke *server* pada *client* yang berada di gedung pusat dan di gedung cabang.

Adapun pengujian *file server* yang pertama dilakukan pada gedung pusat yang menggunakan *user* marina, sebelum melakukan pengujian pada *user* marina langkah pertama yang dilakukan yaitu melakukan *join* pada komputer *client* marina ke *domain file server* menggunakan *user root*, *user root* adalah *user* yang di daftarkan di *server file* atau *server samba* sebagai *user administrator* pada *windows*, yang bertujuan untuk mendaftarkan komputer *client* marina ke *domain file server* yaitu Palembang dan pastikan komputer *client* dan komputer *server* sudah saling terkoneksi .

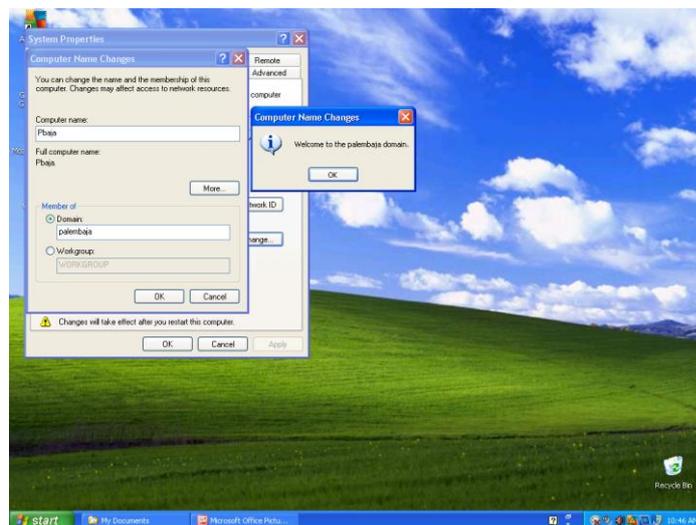
Pada proses untuk melakukan *join* pada komputer *client* marina ke *domain file server* Palembang yaitu dengan membuka *windows explorer*, kemudian klik kanan *properties* keluar tampilan untuk proses melakukan *join* ke *domain file server* seperti pada gambar dibawah ini :



**Gambar 5.57** Proses Melakukan *Join* Komputer  
ke *Domain*

Seperti gambar yang ada diatas, langkah selanjutnya yaitu mencentang bagian *domain* dan masukkan nama *domain file server* yang dituju yaitu *palembaja* kemudian klik ok. Selanjutnya akan keluar *user administrator* pada komputer *windows*, kemudian masukkan *username root* dan *password* selanjutnya klik ok.

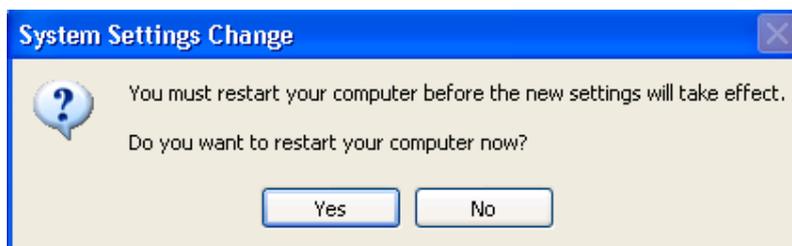
Setelah menginput *username root* dan *password* maka akan keluar tampilan *welcome to the palembaja domain* seperti pada gambar dibawah ini :



**Gambar 5.58 Tampilan *Welcome to The Palembang Domain***

Pada gambar diatas langkah selanjutnya dengan klik ok dan akan terdapat tampilan untuk melakukan *restart* komputer agar proses melakukan *join domain* ke *server* palembaja dapat

dijalankan, tampilan *restart* komputer *client* dapat dilihat pada gambar dibawah ini :



**Gambar 5.59 Tampilan *Restart* Komputer**

Setelah komputer *client* selesai *restart* maka akan keluar tampilan *logon to windows*, kemudian masukkan *username* marina dan *password client file server* atau *client samba Primary Domain Controller (PDC)* yang telah di daftarkan pada komputer *server*, tampilan *logon to windows* dapat dilihat seperti pada gambar dibawah ini :



**Gambar 5.60 Tampilan *Logon to Windows***

Pada gambar diatas dengan menginput *username* dan *password client file server* atau *client samba Primary Domain*

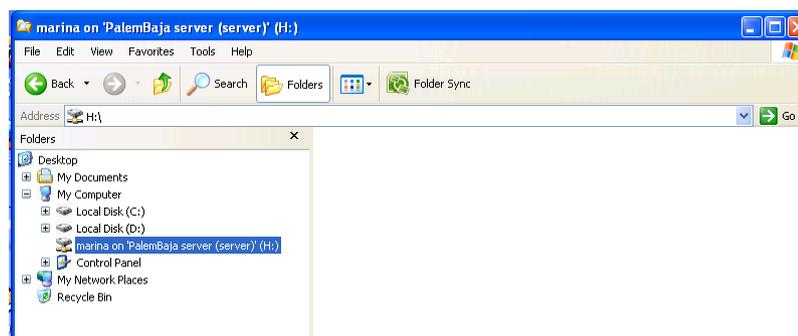
*Controller*, kemudian *samba server Primary Domain Controller* (PDC) akan melakukan pemeriksaan terhadap *username* dan *password* yang mencoba untuk untuk *login* sebagai *client* yang menggunakan *user marina*. jika *password* dan *username* cocok setelah dilakukan pemeriksaan yang dilakukan *samba server Primary Domain Controller* (PDC) maka akan masuk ke *desktop* menggunakan *user marina*. Tampilan *start menu client* yang menggunakan *user marina* dapat dilihat pada gambar dibawah ini :



**Gambar 5.61 Tampilan Start Menu Marina**

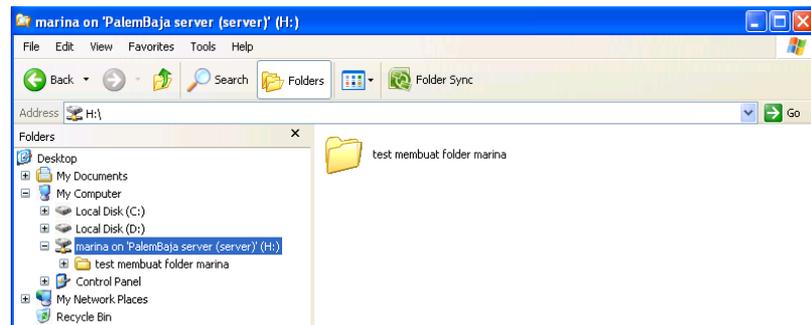
Setelah *client file server* atau *client samba Primary Domain Controller* (PDC) berhasil *login* dengan menggunakan *user marina*, maka *client file server* atau *client samba Primary Domain Controller* (PDC) akan memiliki *local disk* penyimpanan data masing-masing yang hanya bisa di akses atau dilihat oleh *user* itu sendiri. *Local disk* penyimpanan data

tersebut merupakan *local disk* yang diberikan *file server* atau *server samba Primary Domain Controller (PDC)*. *Local disk* penyimpanan data yang diberikan *file server* atau *samba server Primary Domain Controller (PDC)* dapat dilihat pada gambar dibawah ini :



**Gambar 5.62 Local Disk Penyimpanan Data**

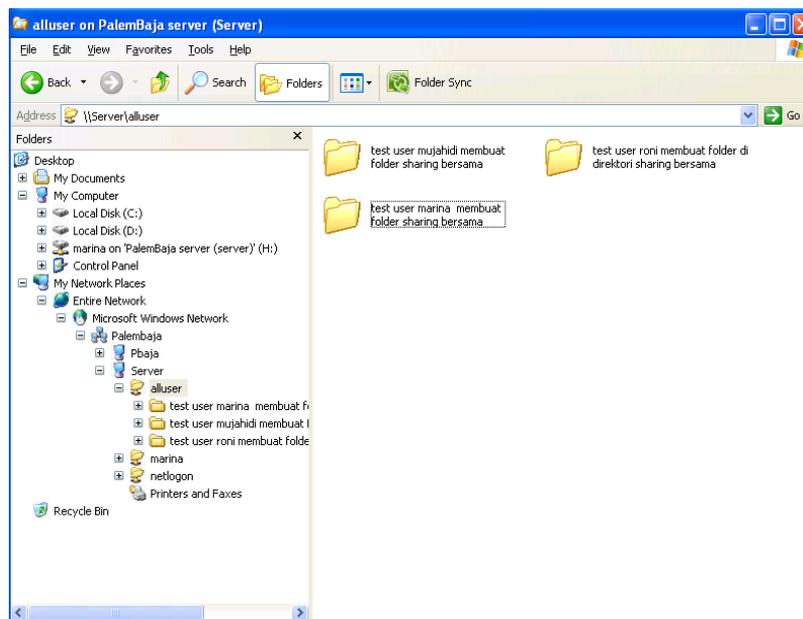
Setelah *client file server* atau *client samba Primary Domain Controller (PDC)* mendapatkan *local disk* penyimpanan data. Selanjutnya melakukan pengujian pembuatan direktori atau pembuatan *folder* pada *local disk* penyimpanan data yang telah diberikan *file server* yang bertujuan untuk memastikan bahwa *local disk* penyimpanan data yang diberikan *server file* diperbolehkan kepada *client* untuk membuat *folder* atau menggunakan *local disk* penyimpanan data tersebut. Pengujian pembuatan direktori atau *folder* tersebut dapat dilihat pada gambar dibawah ini :



**Gambar 5.63** Pengujian Membuat *Folder* atau Direktori

Selain mendapatkan *local disk* penyimpanan data, *client* yang telah memiliki *user* pada *file server* atau *samba server Primary Domain Controller (PDC)* akan diberikan *folder sharing* untuk melakukan pertukaran data antar *client* yang telah memiliki *user* masing-masing.

Adapun langkah-langkah untuk mengakses dan membuat *folder* atau direktori *sharing* antar *client* yang telah memiliki *user* dengan mengakses *my network places*, *entri network*, *microsoft windows network*, *server*, dan *alluser*. Langkah-langkah untuk mengakses *folder* atau direktori *sharing* antar *client* yang telah memiliki *user* masing-masing dapat dilihat seperti pada gambar dibawah ini :



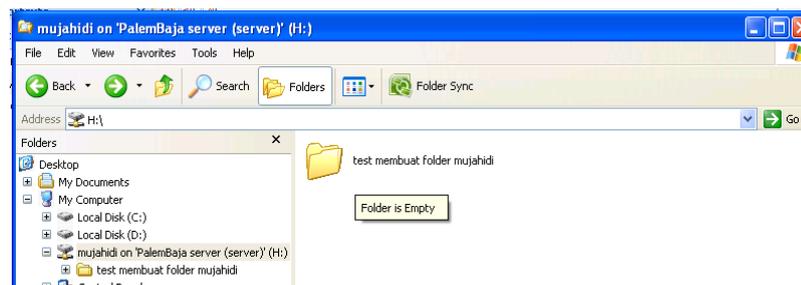
**Gambar 5.64 Mengakses *Folder* atau Direktori *Sharing***

*Folder* atau direktori *alluser* pada gambar diatas adalah direktori yang diberikan *file server* atau *samba server Primary Domain Controller (PDC)* kepada seluruh *user client* untuk saling bertukar data perusahaan. Hasil dari pengujian pertama pada *user* marina telah berhasil dilakukan.

Selanjutnya pengujian yang akan dilakukan pada *user* yang ada di gedung pusat yaitu *user* mujahidi, *user* kapriansah, *user* ferdinan dan *user* roni menggunakan tahapan-tahapan yang sama seperti pengujian pertama yang telah dilakukan pada *user* marina. Maka penulis hanya menjelaskan pembuktian terhadap *client* yang telah memiliki *user* masing-masing saat mengakses atau membuat *folder local disk*

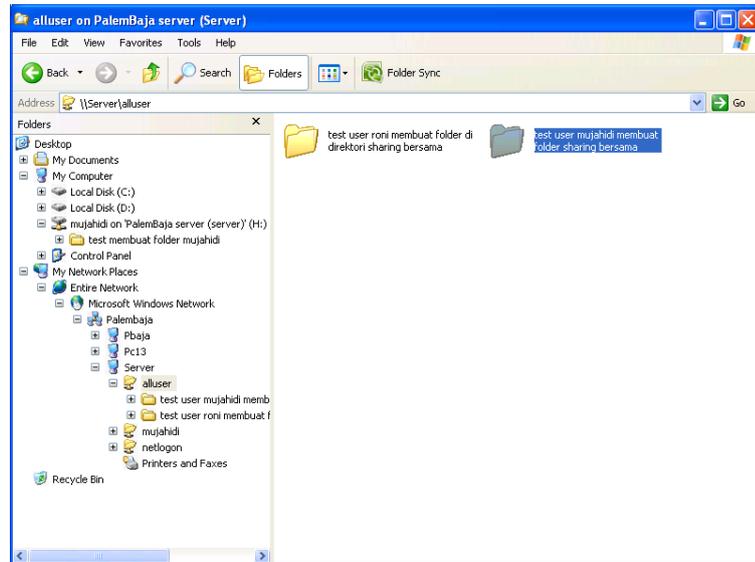
penyimpanan data dan mengakses *folder* atau direktori *sharing*.

Pembuktian pertama dilakukan pada *user* mujahidi saat mengakses atau membuat *folder* di *local disk* penyimpanan data yang diberikan *file server* atau *samba server Primary Domain Controller (PDC)*. Pembuktian pada *user* mujahidi saat mengakses atau membuat *folder* di *local disk* penyimpanan data dapat dilihat seperti pada gambar dibawah ini :



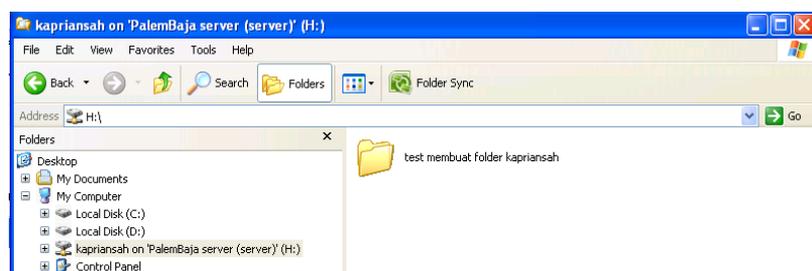
**Gambar 5.65 User Mujahidi Mengakses Local Disk Penyimpanan Data**

Selanjutnya pembuktian *user* mujahidi saat mengakses atau membuat *folder sharing* antar *user* pada direktori atau *folder alluser*, pembuktian *user* mujahidi saat mengakses atau membuat *folder sharing* pada direktori atau *folder alluser* dapat dilihat seperti gambar dibawah ini :



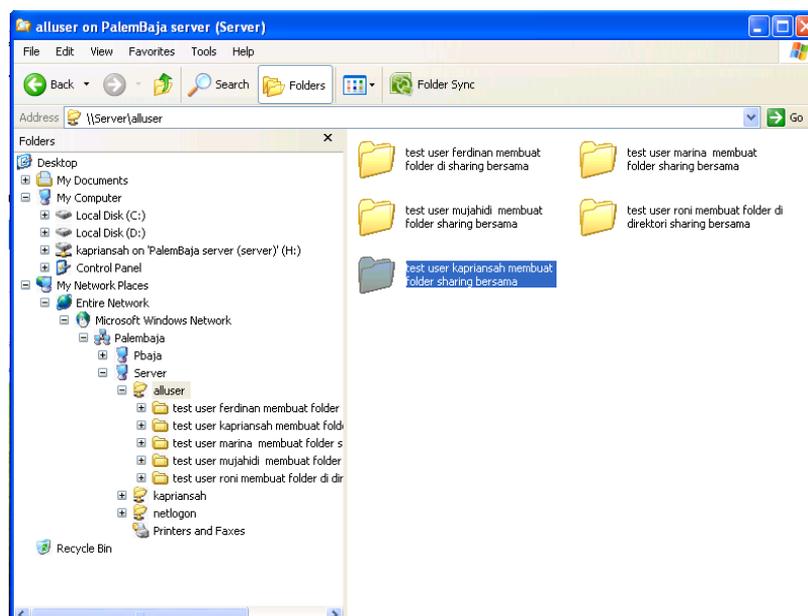
**Gambar 5.66 User Mujahidi Membuat *Folder* di Direktori *Alluser***

Pembuktian kedua dilakukan pada *user* kapriansah saat mengakses atau membuat *folder di local disk* penyimpanan data yang diberikan *file server* atau *samba server Primary Domain Controller (PDC)*. Pembuktian pada *user* kapriansah saat mengakses atau membuat *folder di local disk* penyimpanan data dapat dilihat seperti pada gambar dibawah ini :



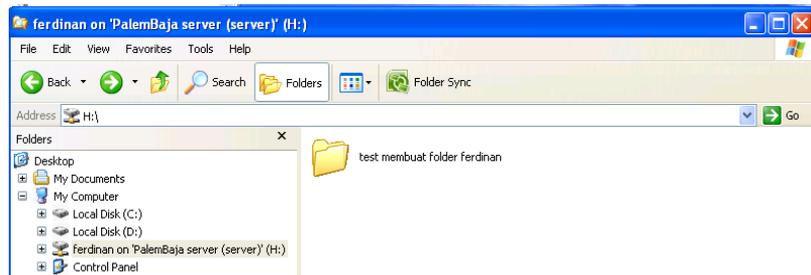
**Gambar 5.67 User Kapriansah Membuat *Folder* di *Local Disk* Penyimpanan Data**

Selanjutnya pembuktian *user* kapriansah saat mengakses atau membuat *folder sharing* antar *user* pada direktori atau *folder alluser*, pembuktian *user* kapriansah saat mengakses atau membuat *folder sharing* pada direktori atau *folder alluser* dapat dilihat seperti gambar dibawah ini :



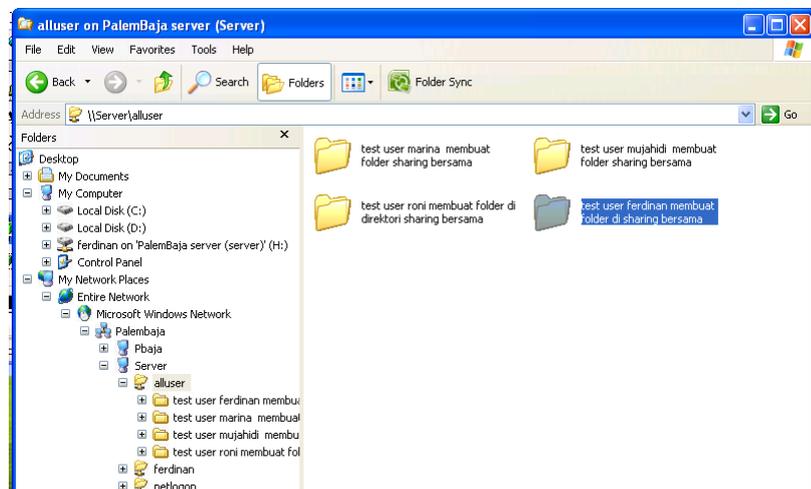
**Gambar 5.68 User Kapriansah Membuat *Folder* di Direktori *Alluser***

Pembuktian ketiga dilakukan pada *user* ferdinan saat mengakses atau membuat *folder* di *local disk* penyimpanan data yang diberikan *file server* atau *samba server Primary Domain Controller (PDC)*. Pembuktian pada *user* ferdinan saat mengakses atau membuat *folder* di *local disk* penyimpanan data dapat dilihat seperti pada gambar dibawah ini :



**Gambar 5.69** User Ferdinan Membuat *Folder* di *Local Disk Penyimpanan Data*

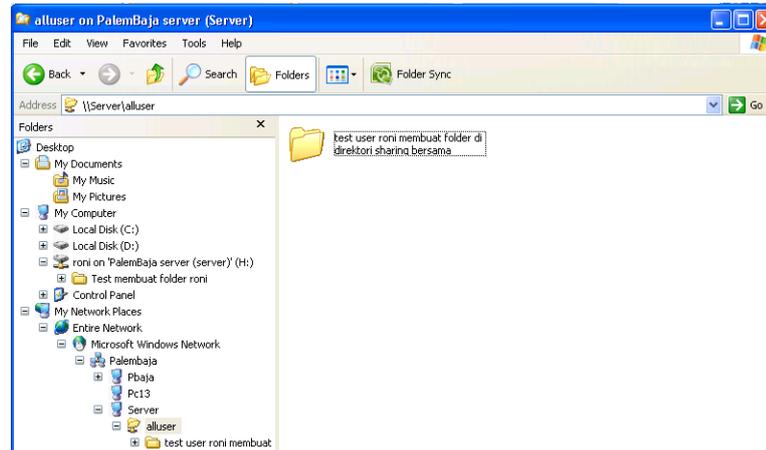
Selanjutnya pembuktian *user* ferdinan saat mengakses atau membuat *folder sharing* antar *user* pada direktori atau *folder alluser*, pembuktian *user* ferdinan saat mengakses atau membuat *folder sharing* pada direktori atau *folder alluser* dapat dilihat seperti gambar dibawah ini :



**Gambar 5.70** User Ferdinan Membuat *Folder* di Direktori *Alluser*

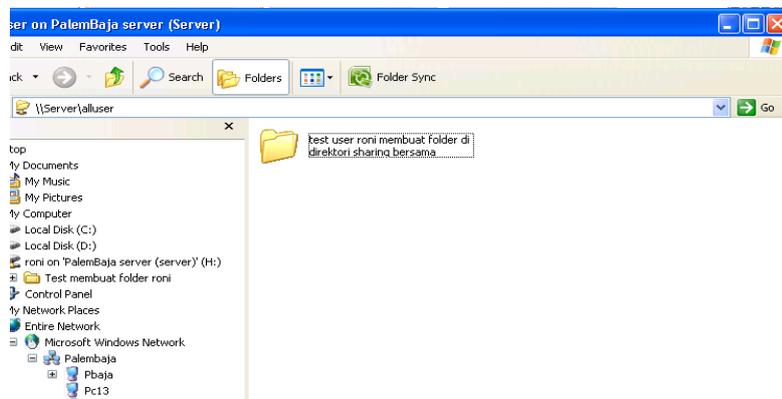
Pembuktian keempat dilakukan pada *user* roni saat mengakses atau membuat *folder* di *local disk* penyimpanan data yang diberikan *file server* atau *samba server Primary*

*Domain Controller (PDC)*. Pembuktian pada *user roni* saat mengakses atau membuat *folder* di *local disk* penyimpanan data dapat dilihat seperti pada gambar dibawah ini :



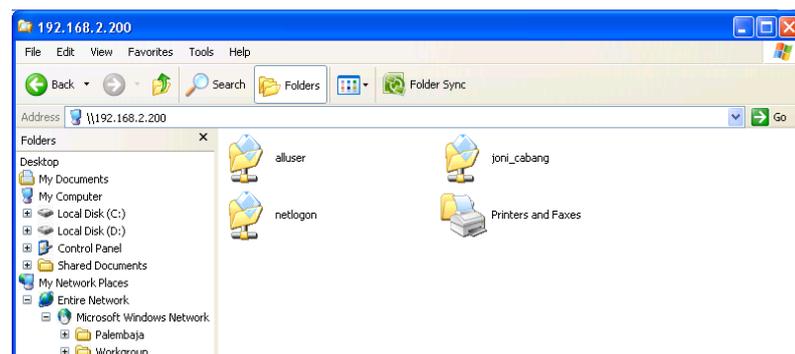
**Gambar 5.71 User Roni Membuat Folder di Local Disk Penyimpanan Data**

Selanjutnya pembuktian *user roni* saat mengakses atau membuat *folder sharing* antar *user* pada direktori atau *folder alluser*, pembuktian *user roni* saat mengakses atau membuat *folder sharing* pada direktori atau *folder alluser* dapat dilihat seperti gambar dibawah ini :



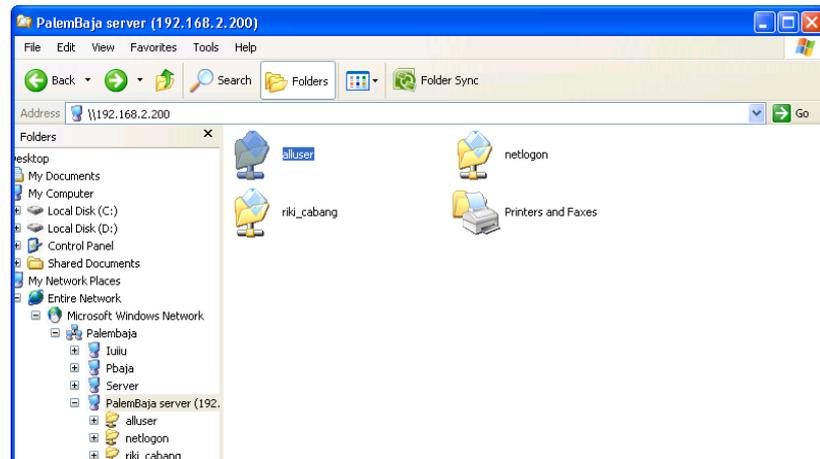
**Gambar 5.72 User Ferdinan Membuat Folder di Direktori Alluser**

Pembuktian *file server* selanjutnya akan dilakukan pada gedung cabang dengan mengakses direktori *alluser*. Pembuktian pertama yang dilakukan yaitu pada pada *user joni\_cabang*, pembuktian *file server* pada gedung cabang seperti pada gambar dibawah ini :



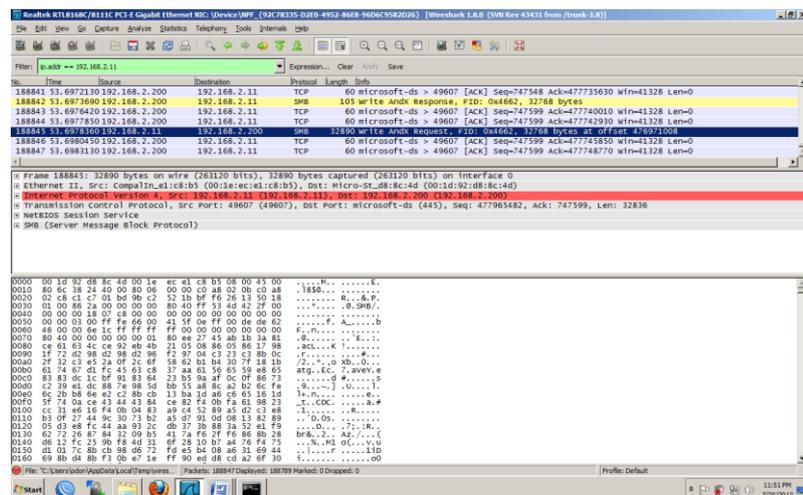
**Gambar 5.73 User joni\_cabang Mengakses Folder di Direktori Alluser**

Pembuktian *file server* yang kedua akan dilakukan pada gedung cabang dengan mengakses direktori *alluser*. Pembuktian kedua dilakukan yaitu pada pada *user riki\_cabang*, pembuktian *file server* pada gedung cabang seperti pada gambar dibawah ini :



**Gambar 5.74** User riki\_cabang Membuat Folder di Direktori Alluser

Setelah melakukan pengujian pengiriman data ke server samba PDC, selanjutnya melihat keamanan data pada saat client saling bertukar data atau mengirim data ke server samba PDC dan data yang dikirim sudah di enkripsi. Pengujian enkripsi data menggunakan aplikasi *wireshark* dapat dilihat pada gambar dibawah ini :



**Gambar 5.75** Pengujian enkripsi data

Pada gambar diatas pada saat *client* melakukan pertukaran data atau melakukan pengiriman data ke *server* samba membuktikan bahwa data telah di enkripsi sehingga hanya *client* yang mempunyai hak akses yang dapat membaca atau melihat data tersebut.

Berdasarkan dari hasil pengujian yang telah dilakukan peneliti diatas, dapat dilihat pada pengujian pertama yaitu pengujian terhadap VPN *client* yang berada di gedung cabang untuk melakukan pemanggilan ke *server* VPN PPTP yang berada di gedung pusat telah berhasil. Maka dengan menggunakan teknologi *Virtual Private Network* (VPN) pada perusahaan PT. Palembang Baja yang ada di gedung pusat dan di gedung cabang sudah saling terkoneksi melalui media *internet* dengan menggunakan IP *publik* perusahaan di gedung pusat. Pada saat VPN *client* di gedung cabang melakukan pemanggilan ke VPN *server* pada gedung pusat, maka VPN *server* melakukan autentikasi terhadap *client* VPN yang melakukan pemanggilan harus memiliki *Username* dan *password* agar tidak sembarang orang dapat mengakses, mengirim ataupun mengambil data yang bersifat *private*.

Selain proses autentikasi yang dilakukan VPN *server* terhadap VPN *client*, VPN *server* juga melakukan *enkripsi* terhadap data-data yang dikirim oleh *client* VPN ke *server*

VPN ataupun sebaliknya, enkripsi merupakan salah satu cara yang dapat digunakan untuk mengubah data asli (sebenarnya) menjadi bentuk sandi (*chipper text*) yang mana sandi-sandi tersebut hanya dapat dimengerti oleh pihak pengirim dan penerima data sehingga data tersebut tidak dapat dibaca oleh orang luar yang tidak mempunyai hak akses untuk melihat data tersebut.

Adapun pada pengujian kedua yang dilakukan peneliti yaitu dengan melakukan pengujian terhadap *file server* yang berada di gedung pusat perusahaan sebagai pusat penyimpanan data dan *sharing data*. *File server* atau pusat penyimpanan data dan *sharing data* pada mesin *server* menggunakan aplikasi *samba server* dengan metode *Primary Domain Controller* (PDC), pada pengujian seperti yang telah dilakukan diatas dapat dilihat *client file server* bisa mengakses tempat penyimpanan data dan *sharing data* berdasarkan *user id* masing-masing karyawan baik di gedung pusat maupun di gedung cabang.

Dengan adanya pusat penyimpanan data dan *sharing data*, maka setiap karyawan akan memiliki tempat penyimpanan sendiri di satu pusat data perusahaan dan karyawan tidak perlu lagi untuk merasa takut akan kehilangan data atau data yang terhapus secara tidak sengaja oleh

karyawan lain, karena data karyawan hanya bisa dihapus atau di tulis oleh karyawan itu sendiri yang telah memiliki *user* dan hak aksesnya masing-masing.

Setelah proses pengujian yang telah dilakukan peneliti dalam membangun jaringan *Virtual Private Network* (VPN) dan *file server* diharapkan dapat membantu perusahaan dalam melakukan komunikasi pertukaran data dan menjaga keamanan data perusahaan dari oknum yang tidak bertanggung jawab untuk melakukan pencurian ataupun merusak data perusahaan yang bersifat rahasia.

#### **5.2.2.6 Kelebihan dan Kekurangan**

Penelitian yang telah diimplementasikan pada perusahaan PT. Palem Baja Palembang dalam membangun teknologi *Virtual Private Network* (VPN) *server* menggunakan PPTP dengan metode *remote access* atau *host to site* dan *file server* sebagai pusat penyimpanan data dan *sharing* data yang menggunakan aplikasi *samba server* dengan metode *Primary Domain Controller* (PDC) terdapat beberapa kelebihan dan kekurangan, kelebihan dan kekurangan tersebut diantaranya yaitu :

## 1. Kelebihan

Mudah dalam konfigurasi VPN *server* yang menggunakan aplikasi PPTPD sehingga tidak memakan waktu lama dalam melakukan implementasi.

Memberikan keamanan pada perusahaan saat perusahaan di gedung cabang dan gedung pusat saling berkomunikasi menggunakan media *internet*.

Biaya relatif murah dalam membangun VPN *server* dikarenakan hanya dengan menggunakan *internet* yang ada sebagai media untuk melakukan komunikasi antar dua gedung yang berbeda lokasi.

Memperkecil ancaman *virus* terhadap pusat penyimpanan data, karena aplikasi *samba server* menggunakan sistem operasi *linux*.

Gedung pusat dan gedung cabang dapat melakukan *Sharing* data dengan menggunakan sistem operasi *linux* ataupun *windows*.

*Client Primary Domain Controller* (PDC) memiliki *drive* penyimpanan data sendiri dan dapat membuka penyimpanan data tersebut dari semua komputer yang terhubung pada jaringan *samba server* dengan menggunakan *user id* masing-masing.

Keamanan data *client* yang berada pada pusat penyimpanan data, hal ini dikarenakan hanya *client* yang memiliki *user id* untuk dapat membuka, menulis, dan menghapus data sesuai *user id* masing-masing.

## 2. Kekurangan

Membutuhkan IP publik *static* pada *server* VPN pada gedung pusat sebagai media untuk melakukan komunikasi antar kedua gedung perusahaan.

Membutuhkan koneksi *internet* yang stabil pada saat kedua gedung perusahaan saling berkomunikasi menggunakan jaringan VPN.

*Client Primary Domain Controller* (PDC) yang menggunakan sistem operasi *windows 7* tidak dapat melakukan *join* ke *domain server Primary Domain Controller* (PDC) dan membutuhkan penelitian lebih lanjut agar *client* yang menggunakan sistem operasi *windows 7* dapat melakukan *join* ke *domain server Primary Domain Controller* (PDC).

Membutuhkan kapasitas *harddisk* yang cukup besar pada komputer *server* karena semua data perusahaan akan di simpan pada komputer *server*.