IMPLEMENTASI VIRTUAL PRIVATE NETWORK (VPN) SERVER DENGAN MENGGUNAKAN MIKROTIK OS DI PT.CHARISMA PERSADA NUSANTARA

IMPLEMENTATION OF VIRTUAL PRIVATE NETWORK (VPN) SERVER USING MIKROTIK OS IN PT.CHARISMA PERSADA NUSANTARA

Muhammad Husni Zarkasyi [1], Ir Agus Ganda Permana M.T [2], Heru Christian Dillak, S.Kom. [3]
[1,2,3]Prodi D3 Teknik Telekomunikasi, Universitas Telkom
[1]husnizarkasyi36@gmail.com, [2]agusgandapermana@ymail.com, [3] hdillak@gmail.com

Abstrak

Server sebagai penyedia layanan pada jaringan komputer memiliki peranan penting diperusahaan. Untuk mengatasi permasalahan keamanan didalam jaringan dari kejahatan hackcing yang dapat masuk ke jaringan komputer internal dibutuhkan sebuah teknologi VPN. VPN (Virtual Private Network) merupakan sebuah teknologi komunikasi yang memungkinkan antara satu jaringan yang terkoneksi dengan jaringan lainnya secara private melalui jaringan public. Dengan VPN ini, user dapat terkoneksi kedalam jaringan public dan menggunakannya untuk bergabung dalam jaringan local. Dari hal tersebut dibutuhkan akses IP lokal perusahaan dengan menggunakan jaringan VPN sehingga user dapat tergabung dalam jaringan local dan mendapatkan hak dan pengaturan yang sama seperti ketika user berada di jaringan LAN. Sehingga user tersebut dapat berkomunikasi dengan jaringan local LAN pada sebuah instansi perusahaan.

Pada Proyek Akhir ini telah dibuat dan diimplementasikan sebuah Virtual Private Network (VPN) server dengan menggunakan mikrotik OS yang terinstall di Mikrotik Router Board di PT. Charisma Persada Nusantara.

Hasil dari pengujian fungsional sistem dapat berfungsi dengan baik sesuai dengan yang diinginkan oleh perusahaan yakni pengguna telah mendapatkan hak akses dan dapat terhubung kedalam jaringan local yang luas dengan biaya yang relatif kecil. Kebutuhan VPN server untuk mensharing file sudah dapat diuji coba di PT.Charisma Persada Nusantara sebagai sarana untuk memenuhi syarat kebutuhan teknologi dalam pengimplementasian VPN server dan juga dapat digunakan oleh perusahaan skala kecil hingga menengah yang ingin membangun jaringan private diatas jaringan public.

Kata Kunci : Virtual Private Network, Virtual Private Server, Jaringan Private, Jaringan Public

Abstract

Servers as service providers on computer networks have an important role in the company. To overcome security problems in the network from hacking crimes that can enter internal computer networks, a VPN technology is needed. VPN (Virtual Private Network) is a communication technology that allows private networks to be connected to other networks through a public network. With this VPN, users can connect to a public network and use it to join the local network. From this it requires access to the company's local IP by using a VPN network so that users can join in the local network and get the same rights and settings as when the user is on a LAN network. So that the user can communicate with the local LAN network in a company agency.

This Final Project has been created and implemented a Virtual Private Network (VPN) server by using a proxy OS installed on the Mikrotik Router Board at PT. Charisma Persada Nusantara.

The results of functional testing of the system can function properly as desired by the company, that is, the user has obtained access rights and can be connected to a wide local network at a relatively small cost. The need for a VPN server to share files can be tested at PT. Charisma Persada Nusantara as a means to fulfill the requirements for technology in implementing VPN servers and can also be used by small to medium scale companies that want to build private networks on public networks.

Keyword : Virtual Private Network, Virtual Private Server, Private Network, Public Netwotk

1. Pendahuluan

Dalam perkembangan dunia teknologi informasi dan komunikasi yang semakin pesat sekarang ini informasi menjadi salah satu aspek penting dalam kehidupan. Hal ini dapat dilihat dari mayoritas orang sudah pernah mengakses internet. Pemanfaatan internet sebagai sarana jaringan public untuk mengirimkan suatu informasi mempunyai resiko tersendiri karena internet dibuka secara umum. Agar didalam pertukaran data tetap aman dari aksi hacking di dalam jarigan internet, Maka dari itu dibuat jaringan virtual yang hanya bisa digunakan oleh orang-orang yang mempunyai wewenang untuk mengakses data tersebut yaitu dengan menggunakan VPN (Virtual Private Network).

VPN (Virtual Private Network) adalah sebuah koneksi virtual yang bersifat private karena pada dasarnya jaringan ini tidak ada secara fisik namun hanya berupa jaringan secara virtual, yang tidak semua orang bisa mengaksesnya. Teknologi VPN ini menggunakan sistem operasi Mikrotik merupakan suatu jaringan komunikasi local yang terhubung melalui media jaringan public.

PT. Charisma Persada Nusantara adalah perusahaan Software, Aplikasi Web/Desktop yang menyediakan solusi yang dirancang khusus untuk memenuhi kebutuhan khusunya dibidang teknologi dan informasi [1]. Yang bertempatan di PT. Charisma Persada Nusantara Jl.Pasir Kaliki No.25-27 Paskal Hypersquare Blok B27, Bandung, Jawa Barat.

Pada sebelumnya PT. Charisma Persada Nusantara melakukan pertukaran data perusahaan menggunakan email. Jika menggunakan email perusahaan belum bisa memastikan keamanan data yang dikirim. Dalam kasus tersebut keamanan di dalam pengiriman serta penerimaan data sangatlah penting untuk menjamin bahwa data yang dikirimkan dan diterima telah terlindungi, terutama jika data tersebut bersifat rahasia. Oleh karena itu dari permasalahan dalam mengakses suatu komputer client di PT. Charisma Persada Nusantara akan dibangun suatu VPN server guna untuk menjaga validitas dan keamanan data dari pihak yang tidak berwenang.

Pada penelitian yang dilakukan sebelumnya oleh Petrus Anton Bagyono, Felix Andreas Sutanto, yaitu Implementasi VPN untuk Akses Server Melalui Perangkat Mobile Pada Jaringan Komputer SMK Triatma Jaya Semarang pada kesimpulannya dikatakan bahwa belum bisa mengakses jaringan local dengan IP public yang diperoleh dari provider pada jaringan SMK Triatma Jaya Semarang masih dinamis, sehingga untuk penyedia layanan untuk bisa mengaksesnya masih membutuhkan penyedia layanan DDNS, dan untuk simulasinya VPN server hanya bisa digunakan dengan menggunakan jaringan LAN (Local Area Network) [12]. Namun, untuk Implementasi VPN server dengan menggunakan Mikrotik OS memiliki pengujian yang lebih baik karena langsung diimplementasikan disebuah perusahaan dengan menggunakan akses jaringan internet penyedia dari ISP (Internet Service Provider) lintasarta dengan akses IP Public static.

Maka dari itu tujuan saya pada proyek akhir ini adalah implementasi Virtual Private Network (VPN) server dengan menggunakan mikrotik OS agar bisa terhubung dengan jaringan local di perusahaan.

2. Dasar Teori

2.1 Konsep *Virtual Private Network*

VPN (Virtual Private Network) adalah suatu koneksi antara satu jaringan dengan jaringan lain secara pribadi melalui jaringan internet atau suatu jaringan pribadi yang dibuat dengan menggunakan jaringan public [16]. VPN biasanya digunakan oleh perusahaan komunitas bisnis yang memerlukan keamanan jaringannya itu sendiri untuk melakukan berbagai kegiatan dilingkungannya sehingga saat pengiriman dan penerimaan data terlindungi oleh enkripsi server VPN [18].

VPN (Virtual Private Network) merupakan sebuah jaringan private yang menghubungkan satu node jaringan lainnya dengan menggunakan jaringan internet [18]. Data yang dilewatkan akan di-encapsulation (dibungkus) dan dienkripsi, supaya data tersebut terjamin kerahasiaannya. Peningkatan penggunaan koneksi VPN dari tahun ke tahun karena murahnya infrastruktur yang dibutuhkan oleh VPN serta mudahnya dalam instalasi, maka koneksi ini lebih efisien dibandingkan dengan metode WAN [6]. Jaringan VPN dikoneksikan oleh ISP lewat router nya ke router-router lain dengan menggunakan jalur internet yang telah dienkripsi antara dua titik, dengan menggunakan leased line untuk hubungan jarak jauh dengan VPN, perusahaan dapat menghemat 20 sampai 40% dari biaya WAN [6].

Selain memakai metode pengamanan enkripsi-deskripsi, VPN masih memakai kriptografi lainnya untuk mendukung pengamanan data. VPN saat ini banyak digunakan untuk diterapkan pada jaringan extranet ataupun intranet perusahaan-perusahaan besar. Sistem keamanan pada VPN dipecah menjadi 3 kategori [18].

1. Trusted VPN : Seorang pelanggan “terpercaya” sirkuit disewakan penyedia layanan dan digunakan untuk berkomunikasi tanpa gangguan. Meskipun “dipercaya “ itu tidak dijamin.
2. Secure VPN : Dengan keamanan menjadi lebih dari sebuah isu bagi pengguna, enkripsi dan enkripsi digunakan pada kedua ujungnya untuk menjaga informasi yang dilewatkan. Hal ini menjamin keamanan yang diperlukan untuk memenuhi perusahaan, pelanggan, dan penyedia.
3. Hybrid VPN : Sebuah campuran dari VPN yang aman dan terpercaya. Seorang pelanggan mengontrol bagian yang dilindungi dari VPN sedangkan penyedia, seperti ISP, menjamin aspek terpercaya.

VPN berkembang dikarenakan adanya perkembangan yang pesat pada perusahaan-perusahaan besar yang ingin tetap memperluas jaringan bisnisnya, namun mereka tetap ingin terhubung ke jaringan local (private) mereka dengan kantor cabang yang dimiliki dan perusahaan mitra kerjanya yang berada di tempat terhubung ke jaringan local milik perusahaan tersebut di manapun mereka berada [6].

VPN (Virtual Private Network) merupakan suatu cara untuk membuat sebuah jaringan yang bersifat "private" dan aman dengan menggunakan jaringan public [16]. VPN juga dapat mengirim data antar dua komputer yang melewati jaringan public sehingga seolah-olah terhubung dengan point-to-point [16]. Data di-enkapsulation (dibungkus) dengan header yang berisi informasi routing untuk mendapatkan koneksi poin to point sehingga data dapat melewati jaringan public dan dapat mencapai tujuan akhir. Sedangkan untuk mendapatkan koneksi bersifat private, data yang dikirimkan harus dienkripsi terlebih dahulu untuk menjaga kerahasiaannya sehingga paket yang yang tertangkap ketika melewati jaringan public tidak terbaca karena harus melewati proses deskripsi. Proses enkapsulasi data sering disebut "tunneling".

2.2 Konsep *Point to Point Tunnel Protocol*

PPTP (Point to Point Tunneling Protocol) adalah protokol yang dikembangkan oleh sebuah konsorsium dimana microsoft adalah salah satu anggotanya, protokol ini dibuat sebagai salah satu implementasi (Virtual Private Network). PPTP mempergunakan model client-server untuk menciptakan koneksi VPN. Sebagian besar sistem operasi microsoft telah dilengkapi dengan PPTP Client, sehingga memudahkan kita untuk mengimplementasikannya (tidak perlu menambah software third party). Selain itu, PPTP juga merupakan protokol jaringan yang memungkinkan pengamanan transfer data dari remote client ke server pribadi perusahaan dengan membuat sebuah VPN melalui TCP/IP [5]. PPTP merupakan protocol jaringan yang mengubah paket PPP menjadi IP datagrams agar dapat ditransmisikan melalui internet [5].
Umumnya terdapat dua komputer yang diperlukan untuk membangun PPTP, yaitu sebagai berikut :

1) Client PPTP
   Komputer yang mndukung PPTP dapat terhubung ke server PPTP dengan dua cara, anara lain sebagai berikut.
   a. Dengan menggunakan Network access server (NAS) milik ISP yang mendukung koneksi PPP.
   b. Dengan menggunakan physical TCP/IP pada LAN sendiri untuk terhubung ke server PPTP.

2). Server PPTP
   Server PPTP merupakan server dengan kemampuan routing yang terhubung ke jaringan private dan internet. PPTP di install sebagai protokol jaringan. PPTP server untuk Linux disebut juga dengan PoPToP

Pada saat ini, banyak perusahaan harus mengubah skema pengalamatan jaringan yang ada semua komputer didalam intranet dapat berhubungan dengan dunia luar (internet). Hal itu terjadi khususnya jika perusahaan-prusahaan itu menyusun alamat jaringannya tanpa mematuhi konvensi-konvensi internasional. Selain itu, seorang karyawan yang berada diluar kota juga tidak dapat mengakses alamat-alamat komputer yang berada didalam jaringan intranet perusahaan mereka dengan mudah, karena keterbatasan pada proxy yang menghubungkan jaringan intranet perusahaan dengan internet. Dengan menggunakan PPTP, sebuah perusahaan dapat menciptakan sistem baru dimana para karyawan yang berada diluar kota dapat dengan mudah mengakses komputer-komputer yang berada di intranet perusahaan mereka, tanpa harus mengubah konfigurasi pengalamatan jaringan intranet [5]. Dengan mengunakan tunneling PPP maka administrator LAN perusahaan dimungkinkan untuk secara cepat mengubah akses ke jaringan semua pegawai tanpa diganggu oleh delay, meskipun koneksi kedalam jaringan intranet harus melalui ISP. Dengan kata lain, administrator LAN tetap memegang kendali, kepada siapa akses jaringan intranet perusahaan diberikan, serta dapat mengatur akses ini secara mudah dan efisien.

2.3 Konsep Dasar Layer 2 Tunnel Protokol (L2TP)

L2TP adalah tunneling protocol yang memadukan dan mengkombinasikan dua buah tunneling protokol yang bersifat proprietary, yaitu L2F (Layer 2 Forwarding) milik cisco system dengan PPTP (Point to point tunneling protocol) milik Microsoft. Pada awalnya, semua produk cisco menggunakan L2F untuk mengurus tunnelingnya, sedangkan operating Microsoft yang terdahulu hanya menggunakan PPTP untuk melayani penggunanya yang ingin bermain dengan tunnel. Namun saat ini, Microsoft Windows NT/2000 telah dapat menggunakan PPTP atau L2TP dan teknologi VPNnya [3]. L2TP biasanya digunakan dalam membuat Virtual Private Dial Network (VPDN) yang dapat bekerja membawa semua jenis protokol komunikasi didalamnya. Selain itu, L2TP juga bersifat media independen karena dapat bekerja di atas media apapun. L2TP memungkinkan penggunanya untuk tetap dapat tetap terkoneksi dengan jaringan local milik mereka dengan policy keamanan yang sama dan dari manapun mereka berada, melalui koneksi VPN atau VPDN. Koneksi ini sering kali dianggap sebagai saranana memperpanjang jaringan local milik penggunaanya [3].

Namun, melalui media public teknologi tunneling ini tidak memiliki mekanisme untuk menyediakan fasilitas enkripsi karena benar-benar murni hanya membentuk jaringan tunnel. Selain itu didalam tunnel ini dapat ditangkap dan dimonitor dengan menggunakan protokol analizer [21]. Umunnya L2TP menggunakan port 1702 dengan protocol UDP untuk mengirimkan L2TP encapsulated PPP frames sebagai data yang di tunnel.

Terdapat dua model tunnel yang dikenal, yaitu compulsory dan voluntary. Perbedaan utama keduanya terletak pada endpoint tunnel-nya. Pada compulsory tunnel, ujung tunnel berada pada ISP, sedangkan pada voluntary ujung tunnel berada pada client remote.

Protokol ini menawarkan kapabilitas yang sangat tinggi antar vendor komputer dan jaringan komputer yang bahkan tidak dimiliki oleh protokol tunneling lainnya. Protocol L2TP juga sering juga disebut sebagai protokol dial-up-virtual, karena L2TP memperluas suatu seassion Point to Point Protocol (PPP) dial-up melalui jaringan publik internet [3].

2.4 Konsep Dasar IPSecurity (IPSec)

Ipsec merupakan tunneling protocol yang bekerja pada layer 3. IPSec menyediakan layanan sekuritas pada IPlayer dengan mengizinkan system untuk memilih protocol keamanan yang diperlukan, memperkirakan algoritma apa yang akan digunakan pada layanan, dan menempatkan kunci kriptografi yang diperlukan untuk menyediakan layanan yang diminta. IPSec menyediakan layanan-layanan keamanan tersebut dengan menggunakan sebuah metode pengamanan yang bernama Internet Key Exchange (IKE) [4].

IKE bertugas untuk menangani protokol yang bernegosiasi dan algoritma pengamanan yang diciptakan berdasarkan dari policy yang diterapkan. Dan pada akhirnya IKE akan menghasilkan sebuah system enkripsi dan kunci pengamanannya yang akan digunakan untuk otentikasi yang digunakan pada system IPSec ini.

IPSec bekerja dengan tiga cara, yaitu:

1. Network-to-network
2. Host-to-network
3. Host-to-host

Contoh koneksi network-to-network, misalnya sebuah perusahaan yang memiliki banyak cabang dan ingin berbagi tau share data dengan aman, maka tiap cabang cukup menyediakan sebuah gateway dan kemudian data dikirim melalui infrastruktur jaringan internet yang telah ada. Lalu lintas data antara gateway disebut virtual tunnel [4]. Kedua tunnel tersebut memverifikasi otentikasi pengirim dan penerima dan mengenkripsi sema lalu lintas. Namun lalu lintas di dalam sisi gateway tidak diamankan karena diasumsikan bahwa LAN merupakan segment jaringan yang dapat dipercaya. Koneksi host-to-network, biasanya digunakan oleh seseorang yang menginginkan akses aman terhadap sumberdaya suatu perusahaan. Prinsipnya sama dengan kondisi network-to-network, hanya saja salah satu sisi gateway digantikan oleh client [4].

2.5 Performansi Jaringan QoS (*Quality of Service*)

Quality Of Service (QoS) adalah performansi yang menentukan derajat kepuasan pengguna terhadap service yang diberikan oleh suatu jaringan berdasarkan parameter-parameter [13]. QoS yaitu sebuah metode pengukuran tentang seberapa baik jaringan dan merupakan suatu usaha untuk mendefinisikan karakteristik dan sifat dari satu servis. QoS digunakan untuk mengukur sekumpulan atribut (parameter) kinerja yang telah dispefisikasikan dengan suatu servis [15]. Tujuan dari QoS yaitu untuk memenuhi kebutuhan layanan yang berbeda yang menggunakan infrastruktur yang sama. Parameter dari QoS yaitu *throughput, paket loss, delay,* dan *jitter*

2.4.1 Throughput

Throughput adalah kecepatan (*rate*) *transfer data* efektif, yang diukur dalam bps (bit per *second*). *Throughput* adalah jumlah total ke*data*ngan paket yang sukses, yang diamati pada tujuan selama *interval* waktu tertentu dibagi oleh durasi *interval* waktu tersebut [15].

2.4.2 Packet Loss

Packet Loss merupakan suatu parameter yang menggambarkan suatu kondisi yang menunjukan jumlah total paket yang hilang dapat terjadi karena *collision* dan *congestion* pada jaringan [15].

2.4.3 Delay (Latencey)

Delay merupakan waktu yang dibutuhkan *data* untuk menempuh jarak dari asal ke tujuan. *Delay* dapat dipengaruhi oleh jarak, media fisik, *congestion* atau juga waktu proses yang lama [15]. Akibat *delay*, *data* yang kita terima akan mengalami keterlambatan waktu *data*ng sehingga hal ini menyebabkan kita menunggu sejenak *data* tersebut sampai pada tujuan.

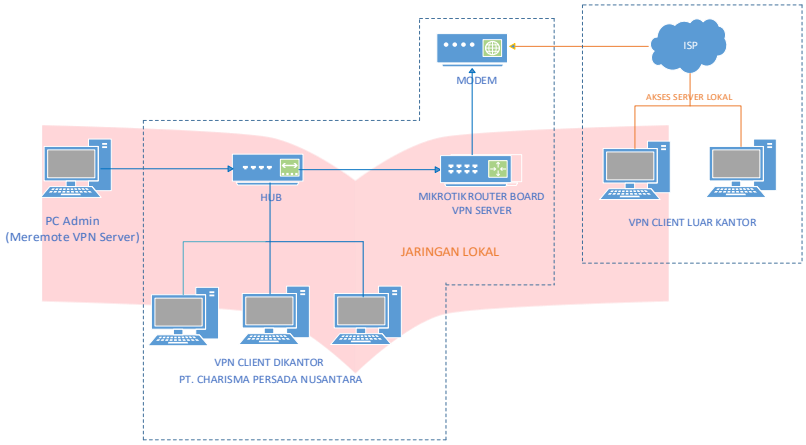
2.4.4 Jitter

Jitter diakibatkan oleh variasi-variasi dalam panjang antrian, dalam waktu pengolahan *data*, dan juga dalam waktu penghimpunan ulang paket-paket diakhir perjalanan *jitter*, disebut juga dengan variasi *delay* [15].

3. Perancangan

3.1 Perancangan Sistem dan Model

Model sistem VPN server diimplementasikan dari sebuah Mikrotik Router Board (VPN Server) dengan menggunakan Mikrotik OS milik perusahaan kemudian dihubungkan dengan beberapa client dengan menggunakan hub lalu menggunakan modem agar bisa terkoneksi ke dalam jaringan internet. Perancangan VPN server ini akan di install-kan di Mikrotik Router Board (VPN Server) agar mendapatkan ip public static tujuannya agar bisa diakses dari luar kantor dan juga sebagai tunnel keamanan saat menggunakan jaringan umum, dimana ketika client ingin berhubungan langsung dengan server yang berbeda jaringan, client tetap bisa terhubung dengan server tanpa mengesampingkan keamanannya. Untuk layanan komunikasi client yang akan dilayani server bisa berupa data, sharing file, FTP server dan sebagainya yang berhubungan dengan akses jaringan local.



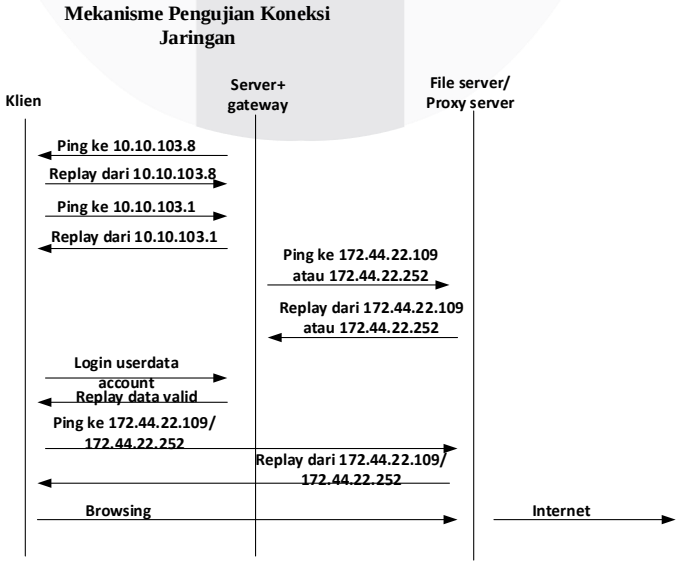
Gambar 3.1. Blok Diagram Sistem Keseluruhan

3.2 Skenario Pengujian

Pada tahap skenario pengujian sistem ini akan di ujicoba di PT Charisma Persada Nusantara dengan jumlah client yang akan diimplementasikan sebanyak 4 user. Untuk Pengujian yang dilakukan terdiri dari 2 macam skenario yaitu :

3.2.1 Pengujian Fungsionalitas Sistem

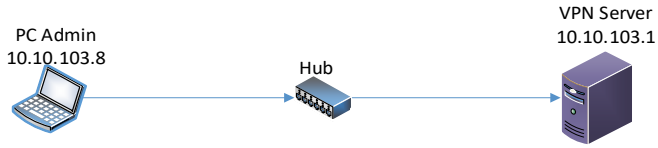
Pada skenario ini akan dilakukan pengujian koneksi yang terjadi antara internet, server, dan client. Pengujian ini, bertujuan untuk mengetahui apakah sistem VPN server yang dibangun telah berfungsi dengan baik atau belum, dan mengetahui komunikasi yang terjadi selama proses pengiriman data. Adapun mekanisme pengujian koneksi jaringan sebagai berikut:



Gambar 3.2. Skenario Pengujian Koneksi Jaringan

3.2.1.1. Koneksi antar Server dengan Client

Meliputi tes *ping*, baik dari sisi *client* ataupun *server* serta tes otentifikasi yang dilakukan dari sisi *client*.

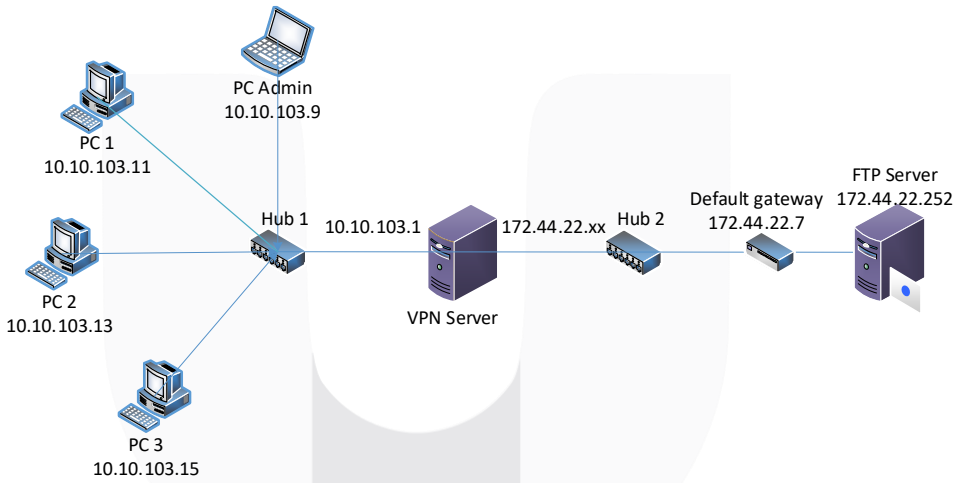


Gambar 3.3. Jaringan Uji Koneksi VPN *Server* dengan *Client*

Adapun mekanisme pengujian skenario untuk kasus ini adalah sebagai berikut:

1. *Server* melakukan tes *ping* /mengirimkan paket icmp melalui terminal / *console* yang dimiliki oleh *Linux CentOS 7*. Apabila *client* memberikan jawaban, maka *server* telah berhasil terkoneksi dengan *client*. Tes ini dilakukan pada kedua buah komputer *client* dengan alamat IP statik (yakni alamat yang tidak akan berubah, memerlukan konfigurasi manual oleh user), hingga kedua buah komputer *client* tersebut, masing-masing memberikan jawabannya.
2. *Client* juga perlu mengetahui apakah ia telah terhubung ke jaringan atau belum, yakni dengan menggunakan bantuan *console* yang dimiliki oleh sistem operasi *Windows* yakni Start → Run → cmd. Sama halnya dengan *server*, *client* juga melakukan proses ping ke alamat *server* yakni 10.10.103.1. Apabila *server* telah memberikan jawabannya, maka *client* berhasil terkoneksi ke *server*.

3.2.1.2. Koneksi antar Server dengan Jaringan Intranet Perusahaan



Gambar 3.4. Jaringan Uji Koneksi VPN *Server* dengan FTP *server*

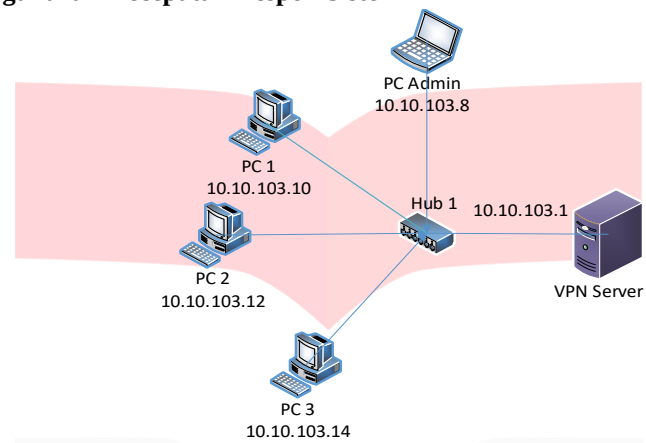
Adapun rincian proses pengujian koneksi antara *VPN server* dengan Jaringan di Perusahaan Charisma Persada Nusantara adalah sebagai berikut:

1. *Client* mengirimkan paket icmp/melakukan tes *ping* ke alamat FTP *server* yakni dari alamat 172.44.22.252 Apabila berhasil terkoneksi *client* bisa mengakses *server* dari luar dengan menggunakan jaringan *local*.
2. Apabila FTP *server* belum memberikan jawaban, maka dapat dilakukan dengan tes *ping* ke default gateway jaringan laboratorium yakni ke 172.44.22.7/24. Apabila gateway berhasil memberikan jawaban, maka kemungkinan FTP *server* yang dituju sedang dalam kondisi *off*, namun apabila yang terjadi adalah sebaliknya maka kemungkinan jaringan laboratorium yang digunakan sedang mengalami gangguan.
3. Proses percobaan di atas akan diulangi hingga FTP *server* memberikan jawabannya kepada VPN *server*.

3.2.2 Pengujian Kehandalan Sistem

Pada tahap pengujian kehandalan sisem ini, ada dua hal yang akan diukur dalam skenario ini, yaitu waktu rata-rata yang dibutuhkan oleh server untuk mengotentifikasi client (dimulai dari client melakukan login/menekan tombol connect) hingga client memperoleh status telah terotentifikasi dari server yakni dengan cara melakukan ”capture” paket-paket data dari sisi server dengan menggunakan bantuan aplikasi Wireshark selama proses otentifikasi berlangsung. Untuk skenario kedua akan dilakukan analisis dan pengukuran pengiriman file/ data pada sisi server dengan client yakni pengkuran sistem men-sharing file mengunakan jaringan VPN, yang bertujuan untuk mengukur kehandalan sistem yang telah dibuat. Kedua metode pengujian ini akan dilakukan secara bertahap mulai dari satu hingga ke-empat komputer client melakukan otentifikasi dan pengiriman data secara simultan. Berikut adalah skema jaringan yang akan digunakan untuk pada masing-masing metode :

3.2.2.1 Proses Pengukuran Kecepatan Respon Sistem



Gambar 3.5. Jaringan Uji Kecepatan Respon Sistem

Pada gambar 3.4. dijelaskan tentang proses pengukuran kecepatan respon sistem untuk menguji kecepatan respon ini akan dilakukan langkah -langkah sebagai berikut :

1. Untuk memperoleh waktu otentifikasi, terlebih dahulu akan dijalankan aplikasi wireshark pada sisi server misalnya selama 30 detik.
2. Selanjutnya, satu orang klien melakukan proses otentifikasi yakni dengan memasukkan serta mengirimkan salah satu nama dan password yang telah terdaftar di dalam database ke VPN server. Proses ini harus dilakukan dalam waktu yang relatif cepat, yakni sebelum waktu yang telah ditetapkan pada wireshark berhenti, sehingga proses komunikasi antar keduanya dapat tercapture dengan baik dan sempurna (mulai dari proses awal hingga proses akhir otentifikasi).
3. Setelah 30 detik, maka proses capture data pada wireshark akan berhenti secara otomatis. Sehingga hasil yang diperoleh dapat disimpan menjadi sebuah file.
4. Apabila proses otentifikasi satu orang klien tersebut telah berhasil dilakukan, maka akan dilanjutkan dengan proses otentifikasi dua orang klien dan seterusnya hingga mencapai 4 orang klien melakukan proses otentifikasi secara simultan yakni dengan melakukan cara yang sama seperti pada langkah 1-3.

3.2.2.2 Proses Pengukuran Pengiriman Data

Proses pengukuran *throughput* dalam pengiriman transfer data dari *server* ke *client.* sistem dengan pengukuran ini dibuat untuk mengetahui kemampuan dan mengukur kehandalan sistem kinerja VPN *server* yang telah dibuat. Berikut langkah -langkah yang dilakukan sebagai berikut :

1. Pertama-tama satu komputer *client* melakukan proses otentifikasi terlebih dahulu dengan salah satu komputer *client* yang sudah terkoneksi kedalam jaringan internet/intranet..
2. Setelah proses otentifikasi berhasil dilakukan, maka dapat dilanjutkan dengan melakukan pengiriman paket data dari *client* ke *server* yakni seperti yang telah dipaparkan pada skenario uji fungsionalitas di atas.
3. Proses Pengukuran dibuat skenario dengan menggunakan background trafik dan tanpa menggunakan background trafik selama proses pertukaran data. Tujuannya untuk mengetahui kemampuan VPN *server* saat mengakses data dimana saat VPN *server* yang sedang dilayani dalam kondisi sibuk atau saat kondisi tidak sibuk.
4. Selama proses pengiriman data akan diuji coba dengan mensharing file dari sisi *server* ke client.

4. Pengujian

Pada bab ini dibahas mengenai analisis kebutuhan client serta pengujian dari hasil perancangan yang telah dilakukan. Pengujian yang akan dilakukan terdiri, dari dua macam skenario yakni skenario pengujian fungsionalitas yang meliputi pengujian fungsi VPN server sebagai mesin otentikator dan gateway bagi klien, dan skenario yang kedua yakni pengujian kehandalan sistem guna mengetahui performansi VPN server yang telah dibuat, yakni meliputi pengukuran kecepatan respon VPN server dalam melakukan proses otentifikasi dan pengukuran pengiriman paket data dengan mensharing file ke dalam jaringan local diperusahaan melalui jaringan VPN yang disertai dengan skenario background traffic dan tanpa background traffic. Paramater yang diukur adalah parameter aplikasi data yaitu throughput. Proses pengukuran untuk men-sharing file data dilakukan sebanyak 10 kali yang masing-masing setiap client melakukan sharinga file data selama perioda 30 detik. Tujuan skenario pengukuran ini adalah untuk mengetahui sejauh mana kemampuan sistem VPN server yang telah dibuat dan untuk mengetahui optimalisasi bandwidth pada jaringan saat kondisi traffic tinggi maupun saat kondisi traffic rendah.

4.1 Pengujian Fungsionalitas Sistem

4.1.1 Hasil Pengujian Koneksi antara VPN *server* dan *client*

Analisis hasil simulasi untuk mengetahui keberhasilan antara *client* dan *server*, yakni keduanya dapat melakukan tes ping satu sama lain seperti yang ditampilkan pada gambar berikut.

```
[husni@lMb Lintasarta] > ping 10.10.103.8
HOST                                     SIZE TTL TIME  STATUS
10.10.103.8                                56  64 0ms
10.10.103.8                                56  64 0ms
10.10.103.8                                56  64 0ms
10.10.103.8                                56  64 0ms
10.10.103.8                                56  64 0ms
10.10.103.8                                56  64 0ms
    sent=6 received=6 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms

[husni@lMb Lintasarta] >
```

Gambar 4.1. Hasil Pengujian pada sisi *Server*

```
Microsoft Windows [Version 10.0.17134.165]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\M Husni Zarkasyi>ping 10.10.103.1

Pinging 10.10.103.1 with 32 bytes of data:
Reply from 10.10.103.1: bytes=32 time=77ms TTL=64
Reply from 10.10.103.1: bytes=32 time=48ms TTL=64
Reply from 10.10.103.1: bytes=32 time=73ms TTL=64
Reply from 10.10.103.1: bytes=32 time=70ms TTL=64

Ping statistics for 10.10.103.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 48ms, Maximum = 77ms, Average = 67ms

C:\Users\M Husni Zarkasyi>
```

Gambar 4.2. Hasil Pengujian pada sisi *Client*

4.1.2 Hasil Uji Koneksi VPN *Server* dengan Jaringan Intranet

Sama halnya dengan parameter keberhasilan koneksi *VPN server client*, parameter keberhasilan uji koneksi antara *VPN server* dengan jaringan *Intranet* di sebuah perusahaan Charisma adalah diperolehnya jawaban dari *gateway* jaringan (172.44.22.7) pada saat VPN *server* melakukan *ping* ke jaringan *local* Perusahaan Charisma.

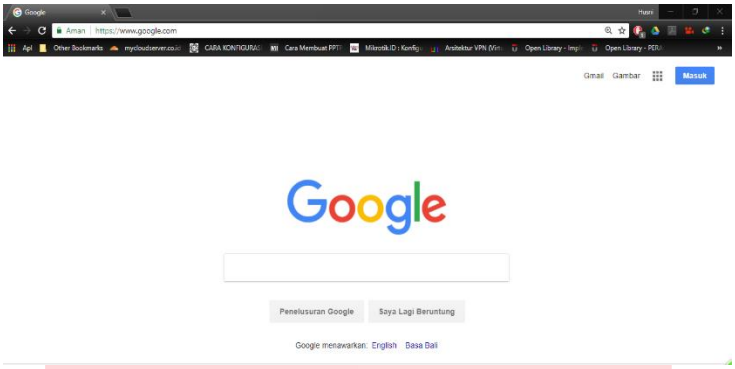
```
[husni@lMb Lintasarta] > ping 172.44.22.7
HOST                                     SIZE TTL TIME  STATUS
172.44.22.7                                56  64 0ms
172.44.22.7                                56  64 0ms
172.44.22.7                                56  64 0ms
172.44.22.7                                56  64 0ms
172.44.22.7                                56  64 0ms
172.44.22.7                                56  64 0ms
172.44.22.7                                56  64 0ms
    sent=7 received=7 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms

[husni@lMb Lintasarta] >
```

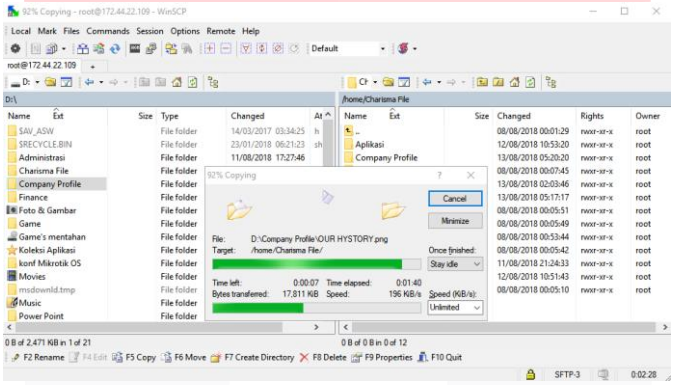
Gambar 4.3. Hasil test ping ke gateway

4.1.3 Hasil Uji Otentifikasi dan Koneksi

Parameter keberhasilan hasil koneksi dan otentifikasi klien adalah berupa klien dapat menampilkan situs *web* yang dituju misalnya www.google.co.id untuk internet dan http://172.44.22.109 untuk mengakses jaringan *local* perusahan. Berikut adalah tampilan dari hasil uji koneksi dan otentifikasi yang telah berhasil dilakukan:



Gambar 4.4 Tampilan Situs Google



Gambar 4.5. Tampilan Uji Coba Akses *Server Local*

Pada gambar 4.5 menunjukan hasil uji coba akses server perusahaan telah berhasil dan bisa digunakan untuk mengirimkan file/ menerima file dari PC server dengan menggunakan jaringan local. Untuk uji coba ini dilakukan dengan menggunakan aplikasi WinSCP untuk me-remote PC server..

4.5 Pengujian Kehandalan Sistem

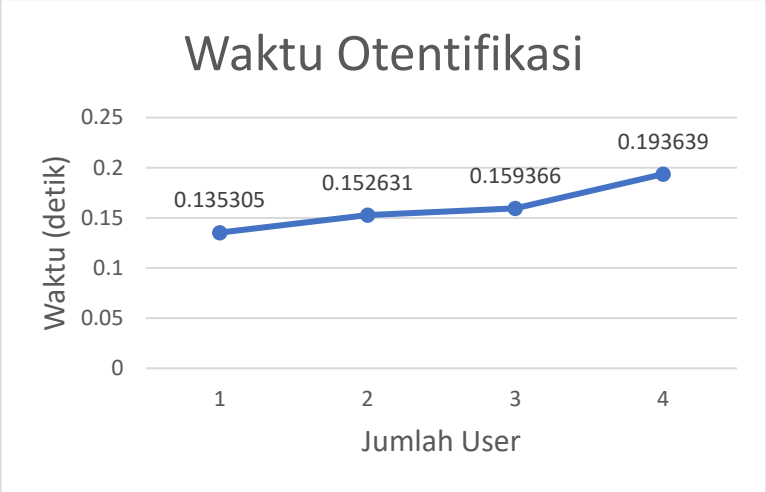
4.5.1 Kecepatan Respon Sistem

parameter yang ingin diketahui adalah waktu otentifikasi klien, yakni waktu yang dibutuhkan oleh *VPN server* untuk merespon permintaan klien agar diperbolehkan menggunakan jaringan *intranet*/*internet*. Waktu otentifikasi ini dihitung mulai dari, klien menekan tombol *connect* pada *login interface*, hingga muncul notifikasi yang terletak pada sisi kanan bagian bawah tampilan menu *wifi* yang menandakan bahwa klien sudah berhasil diotentifikasi oleh *VPN server*.

Tabel 4.1. Tabel Waktu Otentifikasi

Watu Otentifikasi (detik)				
Percobaan	1 Klien	2 Klien	3Klien	4 Klien
1	0,133198	0,157045	0,158206	0,177152
2	0,136649	0,158611	0,160039	0,193633
3	0,136070	0,142237	0,159855	0,210132
Rata - rata	0,135305	0,152631	0,159366	0,193639

Berdasarkan data tersebut, dapat dilihat bahwa dari percobaan satu hingga empat, *VPN server* cenderung lambat dalam merespon klien, Oleh karena itu, dari hasil percobaan ini, belum dapat ditarik suatu kesimpulan yang pasti. Berikut gambar grafik dari pengujian waktu otentifikasi:



Gambar 4.6. Grafik Waktu Otentifikasi

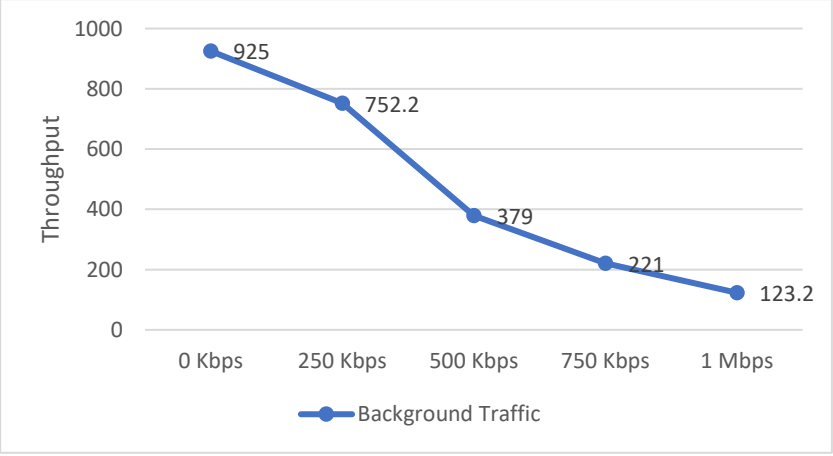
4.5.2 Pengukuran Throughput Dalam Kecepatan (rate) transfer Data

Pengujian skenario ini, dititikberatkan pada proses pengujian perfomansi jaringan VPN yang telah dibangun yakni antara VPN client dengan jaringan local perusahan dengan mengirimkan paket data. Untuk parameter yang diukur adalah throughput yaitu jumlah data (byte) yang dapat diterima dengan baik pada sisi client yang berada dijaringan local dalam selang waktu pengamatan. Dari pengukuran parameter throughput ini diambil nilai rata-rata yang didapat dari proses pengukuran untuk men-sharing file data yang dilakukan sebanyak 10 kali percobaan kemudian dibandingkan antara jaringan tanpa background traffic dengan jaringan yang menggunakan background traffic.

Tabel 4.2. Hasil Pengukuran Throughput (Kbps) pada *Data*

Tanpa Background *Traffic*	Dengan Background *Traffic*			
	250 Kbps	500 Kbps	750 Kbps	1 Mbps
925 Kbps	752,2 Kbps	379 Kbps	221 Kbps	123,2 Kbps

Berikut merupakan gambar grafik dari Throughput rata-rata :



Gambar 4.4 Grafik Throughput Pada *Data*

Pada gambar 4.8 menunjukan bahwa pada kondisi tanpa background traffic terlihat perbandingan lebih tinggi dari hasil throughput yang diperoleh jika menggunakan background traffic, maka dapat disimpulkan untuk pengukuran pada skenario transfer data tanpa menggunakan background traffic mampu menstabilkan bandwidth pada jaringan dengan baik. Hal ini dapat disimpulkan bahwa semakin tinggi nilai throughput maka semakin baik untuk parameter kualitasnya.

5. Kesimpulan dan Saran

5.1 Kesimpulan

1. Semakin banyak user yang melakukan akses layanan internet secara simultan maka akan semakin meningkat pula kinerja *VPN server*.
2. VPN *server* memiliki kemampuan yang baik dalam melayani akses data.
3. Pada proyek akhir ini VPN dapat mengakses jaringan local perusahaan dari luar jaringan kantor yang telah di forward ke jaringan internet.
4. Berdasarkan hasil pengukuran *sharing file data* pada skenario yang telah dibuat, *bandwith* lebih efektif apabila digunakan sistem mikrotik sebagai *managemen bandiwth* dengan skenario tanpa menggunakan background *traffic*

5.2 Saran

Saran dari proyek akhir ini yaitu untuk kedepannya pengujian VPN *server* ini dapat diimplementasikan dengan jumlah user yang lebih banyak atau dapat diimplementasikan langsung pada jaringan existing, guna mengetahui kemampuan maksimal *server* yang telah dibuat.

DAFTAR PUSTAKA

[1] About PT.Charisma Persada Nusantara URL: http://charismapersadanusantara.com/

[2] Agnesie Pratiwi Masero, Joko Triyono, Dina Andayati. (2013) "*PERANCANGAN PENGELOLAAN JARINGAN IT PADA INSTITUT SAINS & TEKNOLOGI AKPRIND MENGGUNAKAN TEKNOLOGI* VPN *(VIRTUAL PRIVATE NETWORK)*" ISSN:2338-6312

[3] Achmad Yasher Ramdhani, Priyadi, ST., Anang Sularsa,ST. "*PERANCANGAN DAN IMPLEMENTASI VPN MENGGUNAKAN PROTOKOL PPTP DAN L2TP BERBASIS MIKROTIK*" Program Studi Teknik Komputer Politeknik Bandung (2010)

[4] Ardiyansyah, Bambang. "*IMPLEMENTASI IPSEC PADA VPN*". Palembang : Universitas Sriwijaya

[5] Bruce Schneier, *Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2)*, October 19 1999.

[6] Erma Suryani dan Syamsu Nur Row Honey. (2007) "*IMPLEMENTASI VIRTUAL PRIVATE NETWORK - WAN DALAM DUNIA BISNIS"*

[7] For the K-12 Community of North Carolina "Designing and Building a Campus *Wireless Network*". MCNC. 2012.

[8] Grant, August E & Meadows, Jennifer H. (eds.) (2008). Communication Technology Update and Fundamental, Eleventh Edition. Boston: Focal*"*

[9] Handy Sunjaya, Deny Setiawan, Sandri Pratama. (2013) "*MENINGKATKAN PERFORMA DAN STABILITAS KECEPATAN TRANSFER DATA PADA FREEBSD DENGAN KOSTUMISASI KERNEL*" ISSN 2085-4579

[10] Hallberg, Bruce (2010). *Network*ing: A Beginner's Guide, Fifth Edition. McGraw Hill. pp. 68–69.

[11] Pamungkas, Canggih Ajika. (2016) "*MANAJEMEN BANDWIDTH MENGGUNAKAN MIKROTIK ROUTERBOARD DI POLITEKNIK INDONESIA SURAKARTA"* jurnal informatika.

[12] Petrus Anton Bagyono, Felix Andreas Sutanto. *"IMPLEMENTASI VPN UNTUK AKSES SERVER MELALUI PERANGKAT MOBILE PADA JARINGAN KOMPUTER SMK TRIATMA JAYA SEMARANG"*. Universitas Stikubank Semarang

[13] PressITU-T E.800 (2008) "*Definitions of terms related to quality of service*".

[14] "MikroTik Routers and Wireless: About MikroTik". mikrotik.com. Retrieved 19 November 2015.

[15] Rika Wulandari (2016) "*ANALISIS QoS (QUALITY OF SERVICE) PADA JARINGAN INTERNET (STUDI KASUS : UPT LOKA UJI TEKNIK PENAMBANGAN JAMPANG KULON – LIPI)".*

[16] Siswa Trihadi1; Frenky Budianto2; Wirriyanto Arifin3 (2002) "*PERANCANGAN VIRTUAL PRIVATE NETWORK DENGAN SERVER LINUX PADA PT. DHARMA GUNA SAKTI*

[17] Widiastuti, Asep Mulyana, ST, Sholekan,ST (2008) "*IMPLEMENTASI VPN SERVER PADA JARINGAN PROGRAM PROFESIONAL IT TELKOM BANDUNG"*

[18] Yana Hendriana (2012) "*EVALUASI IMPLEMENTASI KEAMANAN JARINGAN VIRTUAL PRIVATE NETWORK (VPN) (STUDI KASUS PADA CV. PANGESTU JAYA)"* Jurnal Teknologi, Volume 5 Nomor 2, Desember 2012, 132-142