MEMPERLUAS FUNGSI LAN (LOCAL AREA NETWORK) DENGAN VPN (VIRTUAL PRIVATE NETWORK) IMPLEMENTASI PADA ISA SERVER

Toni Wijanarko Adi Putra

Program Studi Teknik Informatika STMIK PROVISI, Semarang
toni@provisi.ac.id

Abstract
Network VPN enables remote access to corporate network resources that should only be available if the user is directly connected to the corporate LAN. VPN connections create "virtual" link point-to-point between the remote VPN users and corporate networks. Applications and services running on the user's computer treats the VPN link as an Ethernet connection. One of the main advantages of using a VPN connection, the client / server web application, is that VPN users in remote locations have the potential to access all the protocols and servers on a corporate network. Users can access various services in their local networks in the same way as they did when they were in the location of the company. VPN remote access users do not need special software to connect to each network services and administrators no longer need to create application specific proxy to connect to these resources.

Keywords: ***VPN, Internet, Intranet, ISA Server.***

1. Pendahuluan

Internet telah menjadi bagian tak terpisahkan dari masyarakat moderen dewasa ini. Bahkan bagi generasi yang lahir setelah tahun 1995, internet telah membentuk sebuah dunia tersendiri seperti layaknya bumi di tempat manusia berada. Dalam dunia maya ini, melalui beraneka ragam peralatan teknologi informasi dan komunikasi, para individu maupun kelompok-kelompok masyarakat saling berinteraksi, bertukar pikiran, dan berkolaborasi untuk melakukan sejumlah aktivitas kehidupan. Dunia yang merupakan titik singgung antara dunia fisik dan dunia abstrak ini[1] semakin lama semakin banyak pengunjungnya.

Tidak banyak orang yang menyangka sebelumnya bahwa internet yang tadinya hanya merupakan jejaring komunikasi antara lembaga riset perguruan tinggi di Amerika Serikat akan menjadi dunia tersendiri tempat berkumpulnya masyarakat dunia untuk melakukan transaksi, interaksi, dan koordinasi secara global seperti sekarang ini. Bahkan keberadaannya telah mampu menciptakan suatu revolusi tersendiri di sektor pemerintahan, industri swasta, komunitas akademik, dan aspek-aspek kehidupan lainnya. Masyarakat internet ini semakin lama semakin meningkat jumlahnya. Bahkan statistik terakhir tahun 2008 memperlihatkan bahwa satu dari lima penduduk dunia telah menjadi pengguna internet dewasa ini. Bukanlah suatu hal yang mustahil bahwa dalam waktu yang tidak lama lagi, seluruh penduduk dunia akan menjadi internet user yang aktif.

Memperhatikan bahwa internet adalah suatu wahana ”dari, oleh, dan untuk” masyarakat dunia maya, maka salah satu isu utama yang mengemuka adalah permasalahan keamanan atau security baik dalam hal keamanan informasi (konten), infrastruktur, dan interaksi; karena dalam konteks arsitektur internet yang demokratis ini akan meningkatkan faktor resiko terjadinya incident keamanan yang tidak diinginkan baik yang dilakukan secara sengaja maupun tidak[2]. Apalagi sangat banyak hasil riset yang memperlihatkan bahwa dari hari ke hari, jumlah serangan dan potensi ancaman di dunia maya secara kualitas maupun kuantitas meningkat secara signifikan. Karena internet merupakan suatu ”rimba tak bertuan”, maka masing-masing pihak yang terhubung di dalamnya harus memperhatikan dan menjamin keamanannya masing-masing. (Indrajit, 2008).

Keamanan jaringan saat ini merupakan prioritas yang utama bagi perusahaan. Perusahaan ingin agar jaringan komputer yang ada di dalam

[1] Istilah ini pertama kali diperkenalkan oleh Basuki Yusuf Iskandar (Direktur Jendral Pos dan Telekomunikasi), ketika mencoba menggambarkan karakteristik dari dunia maya, yang merupakan domain kehidupan antara dunia nyata (bumi tempat manusia berpijak) dan dunia abstrak (panggung sandiwara teater dan sejenisnya).

[2] “Sengaja” seperti yang dilakukan oleh para hacker, cracker, terrorist, spy, dan sejenisnya; sementara “tidak sengaja” bisa disebabkan karena gangguan infrastruktur (akibat bencana alam) atau masalah teknologi lainnya (malfungsi).

aman baik itu ancaman dari luar maupun dari dalam. ISA server memungkinkan pemakai jaringan di dalam bisa mengakses internet, dan juga memungkinkan orang di internet bisa mengakses server yang berada di jaringan dalam dengan aman.(Sadikin, 2008)

Internet telah sangat mengurangi batasan jarak dan waktu. Kini, seorang karyawan yang sedang berada jauh dari kantornya tidak perlu lagi untuk kembali ke kantor untuk sekedar mengambil data yang tersimpan pada database kantor. Dengan mengkoneksikan database kantor pada internet, karyawan tersebut yang juga terkoneksi dengan internet dapat men*download* data tersebut langsung dari komputernya.

Apabila karyawan tersebut dapat men*download* data dari database kantor tersebut, maka memungkinkan orang lain juga dapat men*download* juga. Oleh karena itu, dibuatlah berbagai macam cara agar orang yang tidak dikehendaki tidak dapat men*download*, merubah ataupun menghapus data penting tersebut. (Thomas, Tom. 2005)

Virtual Private Network (VPN) sendiri merupakan sebuah teknologi komunikasi yang memungkinkan adanya koneksi dari dan ke jaringan publik serta menggunakannya bagaikan menggunakan jaringan lokal dan juga bahkan bergabung dengan jaringan lokal itu sendiri. Dengan menggunakan jaringan publik ini, maka *user* dapat mengakses fitur-fitur yang ada di dalam jaringan lokalnya, mendapatkan hak dan pengaturan yang sama bagaikan secara fisik kita berada di tempat dimana jaringan lokal itu berada. Hal yang perlu diingat adalah sebuah *private network* haruslah berada dalam kondisi diutamakan dan terjaga kerahasiaannya. Keamanan data dan ketertutupan transfer data dari akses ilegal serta skalabilitas jaringan menjadi standar utama dalam *Virtual Private Network* ini.

Pada VPN sendiri terdapat beberapa protokol yang dapat digunakan, antara lain PPTP, L2TP, IPSec, SOCKS, CIPE. Protokol PPTP merupakan protokol awal yang dibangun oleh Microsoft. Selain menjadi dasar dari pengembangan protokol VPN selanjutnya, PPTP juga terdapat pada berbagai versi Windows, diberikan sejak Windows 95 dirilis. VPN dengan Protokol tersebut juga menawarkan solusi biaya yang murah.(Sadikin, 2008).

2. Pengertian Virtual Private Network

Virtual Private Network (VPN) adalah sebuah teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk dapat bergabung dengan jaringan lokal. Dengan cara tersebut maka akan didapatkan hak dan pengaturan yang sama seperti halnya berada di dalam kantor atau LAN itu sendiri, walaupun sebenarnya menggunakan jaringan milik publik.

VPN dapat terjadi antara dua end-system atau dua komputer atau antara dua atau lebih jaringan yang berbeda. VPN dapat dibentuk dengan menggunakan teknologi tunneling dan enkripsi. Koneksi VPN juga dapat terjadi pada semua layer pada protocol OSI, sehingga komunikasi menggunakan VPN dapat digunakan untuk berbagai keperluan. Dengan demikian, VPN juga dapat dikategorikan sebagai infrastruktur WAN alterbatif untuk mendapatkan koneksi point-to-point pribadi antara pengirim dan penerima. Dan dapat dilakukan dengan menggunakan media apa saja, tanpa perlu media leased line atau frame relay.

3. Fungsi Utama Teknologi VPN

Teknologi VPN menyediakan tiga fungsi utama untuk penggunaannya. Ketiga fungsi utama tersebut antara lain sebagai berikut.

3.1 *Confidentially* (Kerahasiaan)

Dengan digunakannnya jaringan publik yang rawan pencurian data, maka teknologi VPN menggunakan sistem kerja dengan cara mengenkripsi semua data yang lewat melauinya. Dengan adanya teknologi enkripsi tersebut, maka kerahasiaan data dapat lebih terjaga. Walaupun ada pihak yang dapat menyadap data yang melewati internet bahkan jalur VPN itu sendiri, namun belum tentu dapat membaca data tersebut, karena data tersebut telah teracak. Dengan menerapkan sistem enkripsi ini, tidak ada satupun orang yang dapat mengakses dan membaca isi jaringan data dengan mudah.

3.2 *Data Intergrity* (Keutuhan data)

Ketika melewati jaringan internet, sebenarnya data telah berjalan sangat jauh melintasi berbagai negara. Pada saat perjalanan tersebut, berbagai gangguan dapat terjadi terhadap isinya, baik hilang, rusak, ataupun dimanipulasi oleh orang yang tidak seharusnya. Pada VPN terdapat teknologi yang dapat menjaga keutuhan data mulai dari data dikirim hingga data sampai di tempat tujuan.

3.3 *Origin Authentication* (Autentikasi sumber)

Teknologi VPN memiliki kemampuan untuk melakukan autentikasi terhadap sumber-sumber pengirim data yang akan diterimanya. VPN akan melakukan pemeriksaan terhadap semua data yang masuk dan mengambil informasi dari sumber datanya. Kemudian, alamat sumber data tersebut akan disetujui apabila proses autentikasinya berhasil. Dengan demikian, VPN menjamin semua data yang dikirim dan diterima berasal dari sumber yang seharusnya. Tidak ada data yang dipalsukan atau dikirim oleh pihak-pihak lain.

4. Kelebihan VPN Dibandingkan Dengan Teknologi *Leased Line*

Manfaat VPN apabila dibandingkan dengan menggunakan teknologi tradisional seperti leased line antara lain sebagai berikut.

- Biaya lebih murah
  Pembangunan jaringan leased line khusus atau pribadi memerlukan biaya yang sangat mahal. VPN dapat menjadi alternatif yang dapat digunakan untuk dapat mengatasi permasalahan diatas. VPN dibangun dengan menggunakan jaringan internet milik publik tanpa perlu membangun jaringan pribadi. Dengan demikian bila ingin menggunakan VPN hanya diperlukan koneksi internet.
- Fleksibilitas
  Semakin berkembangnya internet, dan makin banyaknya user yang menggunakannya membuat VPN juga ikut berkembang. Setiap user dapat tergabung dalam VPN yang telah dibangun tanpa terbatas jarak dan waktu. Fleksibilitas dapat dicapai apabila user tersebut terkoneksi dengan internet dan mendapat ijin menggunakan VPN.
- Kemudahan pengaturan dan administrasi
  Keseluruhan VPN dapat diatur dalam server VPN sendiri, dan untuk dapat digunakan oleh klien, maka perlu diinstal aplikasi VPN pada klien. Hal ini tentu lebih mudah apabila dibandingkan dengan menggunakan leased line yang masih perlu memonitor modem.
- Mengurangi kerumitan pengaturan dengan teknologi tunneling
  Tunneling atau terowongan merupakan kunci utama pada VPN. Koneksi pribadi dalam VPN dapat terjadi dimana saja selama terdapat tunnel yang menghubungkan pengirim dan penerima data. Dengan adanya tunnel ini, maka tidak diperlukan pengaturan-pengaturan lain yang ada di luar tunnel tersebut, asalkan sumber dari tunnel tersebut dapat menjangkau tujuannya.(Sadikin, Nanang. 2008.)

5. Perangkat VPN

Pada dasarnya, semua perangkat komputer yang dilengkapi dengan fasilitas pengalamatan IP dan diinstal dengan aplikasi pembuat tunnel dan algoritma enkripsi dan dekripsi, dapat dibangun komunikasi VPN di dalamnya. Komunikasi VPN dengan tunneling dan enkripsi ini dapat dibangun antara sebuah router dengan router yang lain, antara sebuah router dengan beberapa router, antara PC dengan server VPN concentrator, antara router atau PC dengan firewall berkemampuan VPN, dan masih banyak lagi.

5.1 Jenis-jenis VPN

VPN memang telah menjadi sebuah teknologi alternatif sejak lama. Dunia bisnis juga telah menggunakan VPN sebagai kunci dari proses bisnisnya. Seperti misalnya dipergunakan untuk melayani pemesanan tiket perjalanan, transaksi perbankan, transaksi informasi keuangan, dan berbagai sektor penting lain juga telah mempercayakan penggunaan VPN. Berdasarkan user yang terkoneksi dengan VPN dan bentuk fasilitas yang diperoleh oleh user yang terkoneksi dengan VPN, maka VPN dapat dibedakan menjadi dua jenis, yaitu sebagai berikut.

5.1.1 *Intranet* VPN

Intranet merupakan koneksi VPN yang membuka jalur komunikasi pribadi menuju ke jarinan lokal yang bersifat pribadi melalui jaringan publik seperti internet. Dengan melalui VPN jenis ini, user dapat langsung mengakses file-file kerja dengan leluasa tanpa terikat tempat dan waktu. Apabila dianalogikan pada sebuah perusahaan, koneksi ke kantor pusat dapat dilakukan dari mana saja, dari kantor pusat menuju ke kantor cabang dapat pula dibuat koneksi pribadi, dan juga dari kantor juga memungkinkan untuk dibuat jalur komunikasi pribadi yang ekonomis.

5.1.2 *Ekstranet* VPN

Ekstranet VPN merupakan fasilitas VPN yang diperuntukkan bagi pihak-pihak dari luar anggota organisasi atau perusahaan, tetapi masih memiliki hak dan kepentingan untuk dapat mengakses data dalam kantor. Pada umumnya user dari VPN dari jenis ini merupakan customer, vendor, partnet dan supplier dari suatu perusahaan.

5.1.3 Model *Remote Access* VPN

VPN merupakan sebuah proses remote access yang bertujuan mendapatkan koneksi ke jaringan private tujuannya. Proses remote accsess VPN tersebut dibedakan menjadi dua jenis berdasarkan oleh siapa proses remote access VPN tersebut dilakukan. Kedua jenis tersebut antara lain sebagai berikut.

5.1.4 *Client-initiated*

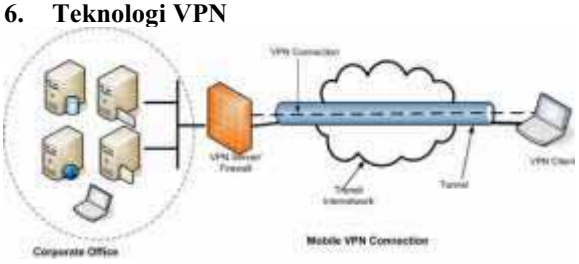
Secara harfiah, client-initiated merupakan pihak klien yang berinisiatif untuk melakukan sesuatu. Pada VPN jenis ini, ketika sebuah komputer ingin membangun koneksi VPN maka PC tersebutlah yang berusaha membangun tunnel dan melakukan proses enkripsi hingga mencapai tujuannya dengan aman. Namun, proses ini tetap mengandalkan jasa dari jaringan Internet Service

Provider (ISP) yang dapat digunakan untuk umum. Clien-initiated digunakan oleh komputer-komputer umum dengan mengandalkan VPN server atau VPN concentrator pada jaringan tujuannya.

5.1.5 *Network Access Server-initiated*

Berbeda dengan clien-initiated, VPN jenis network access server-initiated ini tidak mengharuskan clien untuk membuat tunnel dan melakukan enkrpsi dan dekripsi sendiri. VPN jenis ini hanya mengharuskan user melakukan dial-in ke network access server (NAS) dari ISP. Kemudian, NAS tersebut yang membangun tunnel menuju ke jaringan private yang dituju oleh klien tersebut. Dengan demikian, koneksi VPN dapat dibangun dan dipergunakan oleh banyak klien dari manapun, karena pada umumnya NAS milik ISP tersebut memang dibuka untuk umum.(Dodih. 2004.)

6. Teknologi VPN



Gambar 1 Teknologi VPN

Virtual Private Network merupakan perpaduan dari teknologi tunneling dengan teknologi enkripsi. Berikut penjelasan menganai kedua teknologi tersebut.

6.1 Teknologi *Tunneling*

Teknologi tunneling merupakan teknologi yang bertugas untuk manangani dan menyediakan koneksi point-to-point dari sumber ke tujuannya. Disebut tunnel karena koneksi point-to-point tersebut sebenarnya terbentuk dengan melintasi jaringa umum, namun koneksi tersbut tidak mempedulikan paket-paket data milik orang lain yang sama-sama melintasi jaringan umum tersebut, tetapi koneksi tersebut hanya melayani transportasi data dari pembuatnya. Hal ini sama dengan seperti penggunaan jalur busway yang pada dasarnya menggunakan jalan raya, tetapi dia membuat jalur sendiri untuk dapat dilalui bus khusus.

Koneksi point-to-point ini sesungguhnya tidak benar-benar ada, namun data yang dihantarkannya terlihat seperti benar-benar melewati koneksi pribadi yang bersifat point-to-point.

Teknologi ini dapat dibuat di atas jaringan dengan pengaturan IP Addressing dan IP Routing yang sudah matang. Maksudnya, antara sumber tunnel dengan tujuan tunnel telah dapat saling berkomunikasi melalui jaringan dengan pengalamatan IP. Apabila komunikasi antara sumber dan tujuan dari tunnel tidak dapat berjalan dengan baik, maka tunnel tersebut tidak akan terbentuk dan VPN pun tidak dapat dibangun.

Apabila tunnel tersebut telah terbentuk, maka koneksi point-to-point palsu tersebut dapat langsung digunakan untuk mengirim dan menerima data. Namun, di dalam teknologi VPN, tunnel tidak dibiarkan begitu saja tanpa diberikan sistem keamanan tambahan. Tunnel dilengkapi dengan sebuah sistem enkripsi untuk menjaga data-data yang melewati tunnel tersebut. Proses enkripsi inilah yang menjadikan teknologi VPN menjadi aman dan bersifat pribadi.

6.2 Teknologi Enkripsi

Teknologi enkripsi menjamin data yang berlalu-lalang di dalam tunnel tidak dapat dibaca dengan mudah oleh orang lain yang bukan merupakan komputer tujuannya. Semakin banyak data yang lewat di dalam tunnel yang terbuka di jaringan publik, maka teknologi enkripsi ini semakin dibutuhkan. Enkripsi akan mengubah informasi yang ada dalam tunnel tersebut menjadi sebuah ciphertext atau teks yang dikacaukan dan tidak ada artinya sama sekali apabila dibaca secara langsung. Untuk dapat membuatnya kembali memiliki arti atau dapat dibaca, maka dibutuhkan proses dekripsi. Proses dekripsi terjadi pada ujung-ujung dari hubungan VPN. Pada kedua ujung ini telah menyepakati sebuah algoritma yang akan digunakan untuk melakukan proses enkripsi dan dekripsinya. Dengan demikian, data yang dikirim aman sampai tempat tujuan, karena orang lain di luar tunnel tidak memiliki algoritma untuk membuka data tersebut.

6.3 *Point to Point Tunneling Protocol* (PPTP)

PPTP merupakan protokol jaringan yang memungkinkan pengamanan transfer data dari remote client ke server pribadi perusahaan dengan membuat sebuah VPN melalui TCP/IP.

Teknologi jaringan PPTP merupakan pengembangan dari remote access Point-to-Point protocol yang dikeluarkan oleh Internet Engineering Task Force (IETF). PPTP merupakan protokol jaringan yang merubah paket PPP menjadi IP datagrams agar dapat ditransmisikan melalui intenet. PPTP juga dapat digunakan pada jaringan private LAN-to-LAN.

PPTP terdapat sejak dalam sistem operasi Windows NT server dan Windows NT Workstation versi 4.0. Komputer yang berjalan dengan sistem operasi tersebut dapat menggunakan protokol PPTP dengan aman untuk terhubung dengan private network sebagai klien dengan remote access melalui internet. PPTP juga dapat digunakan oleh komputer yang terhubung dengan LAN untuk membuat VPN melalui LAN.

Fasilitas utama dari penggunaan PPTP adalah dapat digunakannya public-switched telephone network (PSTNs) untuk membangun VPN. Pembangunan PPTP yang mudah dan berbiaya murah untuk digunakan secara luas, menjadi solusi untuk remote users dan mobile users karena PPTP memberikan keamanan dan enkripsi komunikasi melalui PSTN ataupun internet.

Umumnya terdapat tiga komputer yang diperlukan untuk membangun PPTP, yaitu sebagai berikut.

- Klien PPTP
- Network access server (NAS)
- Server PPTP

Akan tetapi tidak diperlukan network access server dalam membuat PPTP tunnel saat menggunakan klien PPTP yang terhubung dengan LAN untuk dapat terhubung dengan server PPTP yang terhubung pada LAN yang sama.

6.3.1 *Klien* PPTP

Komputer yang mendukung PPTP dapat terhubung ke server PPTP dengan dua cara, antara lain sebagai berikut.

- Dengan menggunakan Network access server (NAS) milik ISP yang mendukung koneksi PPP.
- Dengan menggunakan physical TCP/IP pada LAN sendiri untuk terhubung ke server PPTP.

Klien PPTP yang menggunakan NAS milik ISP harus disetting dengan menggunakan modem dan peralatan VPN untuk membuat koneksi sendiri ke ISP dan server PPTP. Koneksi pertama adalah dial-up menggunakan protokol PPP melalui modem ke ISP. Koneksi kedua adalah VPN dengan menggunakan PPTP, melalui modem dan koneksi ISP, ke tunnel melalui koneksi pertama karena tunnel antar peralatan VPN telah dibangun dengan menggunakan modem dan koneksi PPP ke internet.

Persyaratan kedua koneksi diatas tidak dapat dilakukan pada saat komputer menggunakan PPTP untuk membuat VPN diantara komputer yang secara fisik terhubung ke jaringan private perusahaan. Pada skenario tersebut, klien PPTP telah siap untuk terhubung ke jaringan dan hanya menggunakan jaringan dial-up dengan peralatan VPN untuk membuat koneksi ke server PPTP pada LAN.

Paket PPTP dari klien remote access PPTP dan klien lokal LAN PPTP di proses secara berbeda-beda. Paket PPTP dari klien remote access PPTP ditempatkan pada media fisik peralatan komunikasi, saat Paket PPTP dari klien LAN PPTP ditempatkan pada media fisik network adapter seperti dijelaskan pada gambar di bawah ini.

6.3.2 *Network Access Server* (NAS) pada ISP

ISP menggunakan NAS untuk mendukung klien yang dial in menggunakan sebuah protokol, seperti SLIP atau PPP, untuk mendapatkan akses ke internet. Bagaimanapun untuk mendukung PPTP yang dapat digunakan klien, NAS harus memiliki fasilitas PPP.

NAS milik ISP didesain dan dibangun untuk mengakomodasi klien dial in yang sangat banyak. NAS dibuat oleh perusahaan seperti 3Com, Ascend, ECI telematics, dan U.S. Robotics, yang menjadi anggota dari forum PPTP.

ISP yang memberikan pelayanan PPTP dengan memperbolehkan klien menggunakan NAS untuk PPTP dapat mendukung Windows +95, Windows NT versi 3.5 dan 3.51, sama baiknya seperti pada klien PPP, seperti Apple Macintosh atau UNIX. Klien tersebut dapat menggunakan koneksi PPP ke server ISP. Server ISP bertugas sebagai klien PPTP dan terhubung ke server PPTP pada jaringan private, membuat PPTP tunnel dari server ISP ke server PPTP.

6.3.3 *Server* PPTP

Server PPTP merupakan server dengan kemampuan routing yang terhubung ke jaringan private dan internet. Dalam hal ini, server PPTP diartikan sebagai komputer yang menjalankan windows NT server versi 4.0 dan RAS. PPTP diinstall sebagai protokol jaringan. Dengan instalasi tersebut, PPTP disetting dengan menambahkan virtual device layaknya VPN ke RAS dan dial-up networking.

6.4 *Arsitektur* PPTP

Komunikasi yang aman dibuat dengan menggunakan protokol PPTP melewati tiga proses, dimana setiap proses tersebut membutuhkan seleseinya proses yang sebelumnya. Ketiga proses tersebut berjalan dengan cara sebagai berikut.

- *PPTP Connection and Communication*. Klien PPTP menggunakan PPP untuk terhubung ke ISP dengan menggunakan jalur telepon standar atau ISDN line. Koneksi tersebut menggunakan protokol PPP untuk membangun koneksi dan enkripsi paket data.
- *PPTP Control Connection*. Menggunakan koneksi ke internet yang telah dibangun oleh protokol PPP, protokol PPTP membuat sebuah *control connection* dari klien PPTP ke server PPTP di internet. Koneksi tersebut menggunaka TCP untuk membagun koneksi dan ini disebut dengan PPTP *tunnel*.
- *PPTP Data Tunneling*. Akhirnya protokol PPTP membuat IP datagrams yang di dalamnya terdapat enkripsi paket PPP yang kemudian dikirim melalui PPTP *tunnel* ke server PPTP.

Server PPTP membongkar IP datagram dan mendekripsi paket PPP dan kemudian merutekan paket yang telah didekripsi ke jaringan *private*.

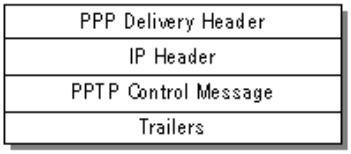
6.4.1 PPTP *Control Connection*

Protokol PPTP menspesifikasikan seri pengiriman dari *control message* antara PPTP-*enabled client* dan server PPTP. *Control message* membangun, memelihara dan mengakhiri PPTP tunnel. Berikut ini merupakan daftar yang dibuat oleh *control message* dasar yang digunakan untuk membuat dan memelihara PPTP *tunnel.*

Tabel 1 PPTP Control Message Type

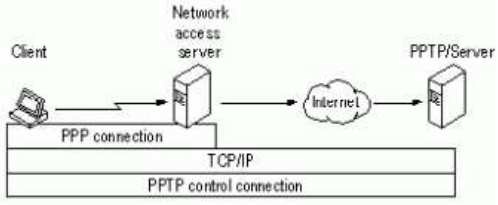
Tipe *Message*	Manfaat
PPTP_START_SESSION_REQUEST	Permintaan untuk memulai Session
PPTP_START_SESSION_REPLY	Untuk menjawab *start session*
PPTP_ECHO_REQUEST	*Maintain session*
PPTP_ECHO_REPLY	Untuk menjawab *Maintain session*
PPTP_WAN_ERROR_NOTIFY	Laporan *error* pada koneksi PPP
PPTP_SET_LINK_INFO	Merubah setting koneksi antara klien dan server PPTP
PPTP_STOP_SESSION_REQUEST	Mengakhiri *session*
PPTP_STOP_SESSION_REPLY	Untuk menjawab *stop session*

Control message ditransmisikan pada paket kontrol pada TCP datagram. Satu koneksi TCP dibangun antara klien PPTP dan server PPTP. Koneksi tersebut digunakan untuk menukar *control message*. *Control messages* dikirim dengan TCP datagram. Datagram terdiri dari PPP *header*, TCP *header*, PPTP *control message* dan *trailer*.



Gambar 2 PPTP TCP Datagram dengan Control Messages

Penukaran *message* antara klien PPTP dan server PPTP melalui koneksi TCP digunakan untuk membuat dan memelihara PPTP *tunnel*.



Gambar 3 PPTP Control Connection ke server PPTP melalui PPP Connection menuju ISP

Catatan pada ilustrasi di atas, *control connection* merupakan skenario dimana klien *remote access* adalah klien PPTP itu sendiri. Pada skenario tersebut dimana klien *remote access* bukanlah PPTP-*enabled* dan tidak menggunakan PPTP-*enabled* NAS milik ISP, PPTP *control connection* dimulai di server ISP.

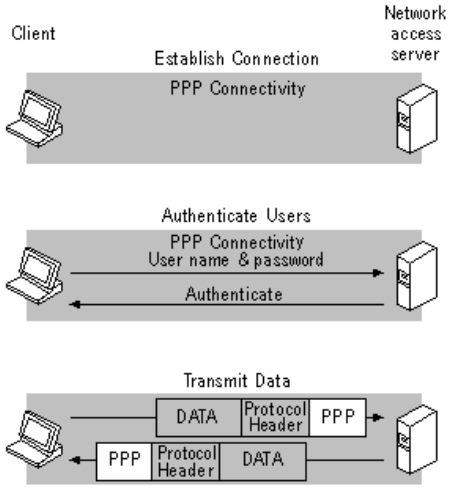
6.4.2 Protokol PPP (*Point to Point Protocol*)

PPP merupakan *remote access protocol* yang digunakan oleh PPTP untuk mengirim *multi-protocol data* melewati TCP/IP. PPP meringkas IP, IPX, dan NetBEUI *packet* antara PPP *frames* dan mengirim ringkasan paket tersebut dengan membuat hubungan *point-to-point* antara komputer pengirim dan penerima.

Umumnya PPTP dimulai saat klien melakukan *dial-up* ke NAS milik ISP. Protokol PPP digunakan untuk membuat koneksi *dial-up* antara klien dan NAS dan memberikan tiga fungsi berikut ini.

- Memulai dan mengakhiri *physical connection*. Protokol PPP menggunakan urutan yang didefinisikan pada RFC 1661 untuk membangun dan menjaga koneksi antar *remote computers*.
- *Authenticates users*. Klien PPTP diautentikasi dengan oleh protokol PPP. Menjelaskan text, mengenkripsi, ataupun *Microsoft encryption authentication* dapat digunakan oleh protokol PPP.
- Membuat PPP datagrams yang terdiri dari enkripsi IPX, NetBEUI, atau TCP/IP packets. PPP membuat datagrams yang terdiri dari satu atau lebih enkripsi, TCP/IP, IPX, atau NetBEUI data packet. Karena paket tersebut terenkripsi, semua trafik antara klien PPP dan NAS akan aman.

Ilustrasinya sepeti gambar berikut ini.



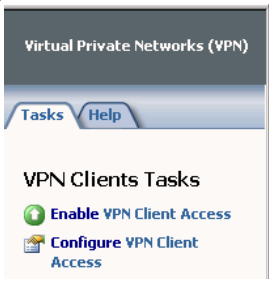
Gambar 4 Dial-Up Networking PPP Connection ke ISP

Untuk beberapa situasi, *remote clients* mungkin memiliki akses langsung ke TCP/IP network, seperti internet. Misalnya, sebuah laptop dengan *network card* dapat menggunakan hotspot internet pada ruang rapat. Dengan koneksi IP secara langsung tersebut, inisial koneksi PPP ke ISP tidak

diperlukan. Klien tersebut dapat menginisialisasikan koneksi ke server PPTP tanmpa membuat koneksi pertama ke ISP.(Thomas, Tom. 2005.)

7. Konfigurasi VPN pada ISA Server 2004

Secara default, komponen server VPN belum aktif, langkah pertama untuk mengaktifkan fitur server VPN adalah buka Microsoft Internet Security dan Acceleration Server 2004, lalu pilih pada bagian Enable (VPN) Virtual Private Networks.



Gambar 5 Enable VPN

Kemudian langkah selanjutnya adalah pilih Configure VPN Client Access, dan kita tentukan jumlah maximum client yang akan diijinkan mengakses VPN tersebut.

Gambar 6 Setting jumlah maksimum client VPN

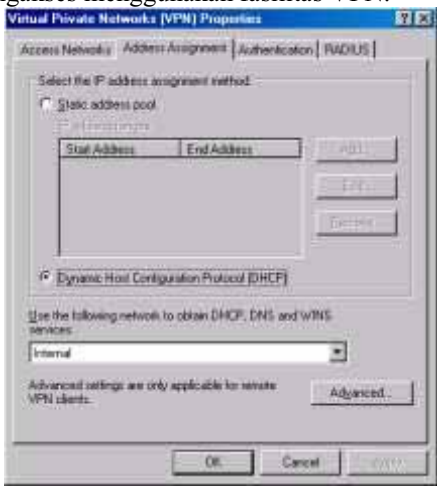
Kita juga bisa menentukan client yang bisa mengakses VPN berdasarkan group.

Gambar 7 Group akses VPN

Kemudian kita tentukan protokol yang akan kita gunakan.

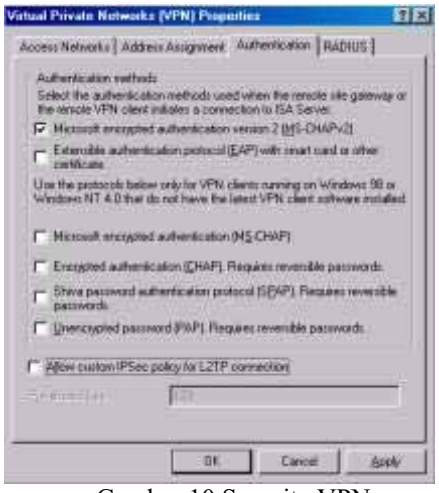
Gambar 8 Protokol VPN

Range ip yang akan digunakan oleh client yang mengakses menggunakan fasilitas VPN.



Gambar 9 Range IP Address VPN

Penempatan Security yang akan kita gunakan.



Gambar 10 Security VPN

5. Kesimpulan

Bahwa dengan jaringan VPN akan kita dapatkan beberapa keuntungan diantaranya adalah

- Biaya lebih murah
- Fleksibilitas
- Kemudahan pengaturan dan administrasi

Pemilihan produk VPN yang tepat, akan membuat jaringan dapat dihandalkan dan dapat digunakan dengan maksimal, dengan tidak menyebabkan terjadinya penurunan kinerja yang berarti. Kebijakan manajemen dan monitoring system jaringan juga menjadi faktor yang mempengaruhi dalam kehandalan dan keamanan sistem VPN. Dengan memilih strategi alternative yang tepat, solusi VPN ini dapat membantu mencapai sasaran.

Daftar Pustaka:

Indrajit, Prof. Richardus Eko. 2008. *Indonesia Security Incident Response Team On Internet Infrastructure.* Penerbit ID-SIRTII.

Dodih. 2004. *Menjadi Administrator & Teknisi LAN yang andal berbasis Windows (Server-Client).* Yogyakarta : Penerbit Gava Media.

Sadikin, Nanang. 2008. Solusi VPN Client Access Di Windows Server 2003. Penerbit Elex Media Komputindo.
Sadikin, Nanang. 2009. Mastering VPN Client Access Di Windows Server 2008. Penerbit Elex Media Komputindo.

Thomas, Tom. 2005. Network Security First step, Penerbit ANDI.

Thomas, Tom. 2005. Computer Networking First-step, Computer Networking First-step. Penerbit ANDI.

Berry Kercheval. 2002. DHCP TCP/IP. Terjemah Dwi Prabantini. Yogyakarta Penerbit ANDI