REMOTE SITE MIKROTIK VPN DENGAN POINT TO POINT TUNNELING PROTOCOL (PPTP) STUDI KASUS PADA YAYASAN TERATAI GLOBAL JAKARTA

Elly Mufida[1], Dedi Irawan[2], Giatika Chrisnawati[3]
[1,3]Teknik Komputer, AMIK BSI Jakarta
Jl. RS. Fatmawati No. 24, Pondok Labu, Jakarta Selatan
[2]Teknik Informatika, STMIK Nusa Mandiri Jakarta
Jl. Damai No. 8 Warung Jati Barat (Margasatwa) Jakarta Selatan
Email: elly.mufida@gmail.com[1], Dediirawan@gmail.com[2], amira.azzahra@gmail.com[3]

Abstract

Technology VPN (Virtual Private Network) allows everyone to be able to access the local network from outside by using the internet. Through the VPN, the user can access the resources within the local network, gain rights and settings are the same as physically being in a place where the local network is located. Data security and secrecy of data transmission from unauthorized access in transmission on the Internet becomes the main standard in the VPN, so that the VPN is always included will be the main feature is the encryption and tunneling.

Keyword: VPN, *Point-to-point Tunneling Protokol*, PPTP

Abstrak

Teknologi VPN (*Virtual Private Network*)memungkinkan setiap orang untuk dapat mengakses jaringan lokal dari luar dengan menggunakan internet. Melalui VPN, maka user dapat mengakses sumber daya yang berada dalam jaringan lokal, mendapatkan hak dan pengaturan yang sama seperti secara fisik berada di tempat dimana jaringan lokal itu berada. Keamanan data dan ketertutupan transmisi data dari akses yang tidak berhak dalam transmisinya pada internet menjadi standar utama dalam VPN, sehingga dalam VPN selalu disertakan akan fitur utama yaitu enkripsidan *tunneling*.

Kata Kunci: VPN, *Point-to-point Tunneling Protokol*, PPTP

I. PENDAHULUAN

Semakin berkembangnya teknologi informasi sekarang ini, maka kebutuhan akan informasi semakin meningkat. Dimana setiap orang membutuhkan informasi dalam waktu yang cepat, singkat dan akurat, oleh karena itu dibutuhkan suatu sarana yang dapat mendukung hal tersebut . Salah satunya adalah koneksi *internet* yang cepat dan stabil. Namun permasalahan yang sering timbul adalah faktor keamanan yang saat ini menjadi hal yang sangat penting untuk diperhatikan. Maka dibutuhkan suatu cara agar dapat memperoleh suatu informasi data, tukar menukar data, dilakukan dengan aman dan stabil. Oleh karena itu lah VPN diciptakan untuk menyelesaikan permasalahan dalam jaringan yang tidak aman.[1]

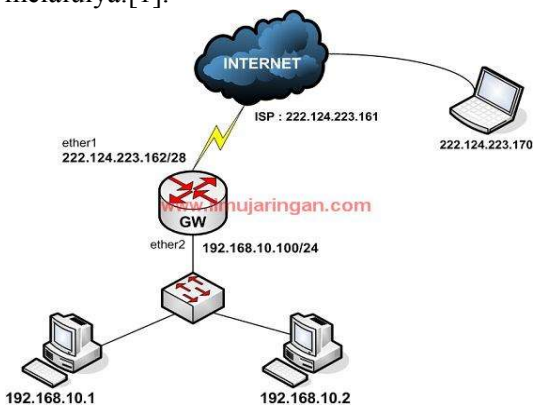
Suatu organisasi atau institusi dalam melangsungkan kegiatannya tidak akan lepas dari pertukaran informasi antar para *stakeholder* yang satu dengan yang lain. Setiap informasi yang dihasilkan oleh salah satu *stakeholder* akan diperlukan oleh *stakeholder* lain. Untuk itu, kebutuhan informasi harus dapat diakses melalui jaringan komputer yang di desain untuk dapat mendapatkan informasi yang diperlukan dengan cepat, mudah, aman dan akurat. Dalam sebuah jaringan komputer, keamanan sewaktu pengiriman dan penerimaan data sangat penting untuk menjamin bahwa data yang dikirim sampai pada yang pihak yang dituju, dan tidak jatuh pada pihak yang tidak berkepentingan, terutama apabila data yang dikirimkan tersebut bersifat rahasia. Untuk itu perlu dilakukan pengamanan data pada jaringan

Yayasan Teratai Putih Global adalah Lembaga yang bergerak di bidang pendidikan yang memiliki 9 (Sembilan) unit sekolah mulai dari PG/TK, SD Islam, SMP Islam, SMA Islam serta SMK yang tersebar di Bekasi dan Jakarta. Dalam proses pendataan terutama berkaitan dengan keuangan siswa, kesembilan unit tersebut memiliki perangkat lunak sistem administrasi sekolah pada unit sekolah masing-masing, kondisi ini menyulitkan pihak yayasan dalam proses konsolidasi data. Proses pengambilan data yang masih manual dengan datang ke lokasi masing-masing sekolah, karena bila data dikirim via email, selain kurang aman juga terkendala batasan kapasitas ukuran file yang dikirim dalam sekali pengiriman menggunakan email.

Dengan memanfaatkan internet, Selain mudah dan cepat, penggunaan internet dapat menekan biaya operasional perusahaan. Tetapi, dengan segala kelebihannya, internet juga memiliki kelemahan. Internet yang dapat diakses oleh semua orang membuatnya menjadi tidak aman untuk mengirimkan informasi yang sifatnya rahasia. Apalagi sudah banyak bermunculan aplikasi-aplikasi yang bisa membobol pesan dengan sangat mudah, yang dilakukan oleh para *hacker* yang tidak beranggung jawab. Oleh karena itu, penggunaan internet di dalam perusahaan juga harus disertai dengan penggunaan sistem keamanan yang terpercaya.Saat ini, Internet juga dapat digunakan untuk menghubungkan jaringan intranet kantor pusat, yaitu sebuah jaringan internal yang berada di dalam perusahaan, dengan 1 atau 2 jaringan intranet di kantor cabang. Teknologi jaringan yang dapat mendukung hal ini adalah teknologi VPN, yaitu teknik yang dapat menghubungkan beberapa jaringan local melalui jaringan publik(internet) dengan teknik VPN komunikasi seakan-akan kedua jaringan tersebut berada di dalam satu jaringan intranet yang besar. Teknologi private network (jaringan pribadi) adalah suatu komunikasi dalam jaringan sendiri yang terpisah dari jaringan umum.

Internet merupakan sebuah jaringan global dan terbuka, dimana setiap pengguna dapat saling berkomunikasi dan bertukar informasi. Seiring dengan maraknya penggunaan Internet, banyak perusahaan yang kemudian beralih menggunakan Internet sebagai bagian dari jaringan mereka untuk menghemat biaya. Akan tetapi permasalahan keamanan masih menjadi faktor utama. Dalam sebuah jaringan komputer, keamanan didalam pengiriman serta penerimaan data sangat penting untuk menjamin bahwa data yang dikirim tidak jatuh ke pihak ketiga atau pihak yang tidak berkepentingan, terutama jika data tersebut bersifat rahasia atau urgen. Untuk itu perlu dilakukan implementasi metode-metode pengamanan data pada jaringan. Banyak metode yang dapat diimplementasikan, seperti penggunaan tanda tangan digital, enkripsi ataupun pemasangan firewall. Dalam implementasinya, VPN terbagi menjadi remote access VPN dan site-to-site VPN. Site-to-site VPN digunakan untuk menghubungkan antara 2 tempat yang letaknya berjauhan, seperti halnya kantor pusat dengan kantor cabang. VPN yang digunakan untuk menghubungkan suatu perusahaan dengan perusahaan lain (misalnya mitra kerja, supplier atau pelanggan) disebut ekstranet. Sedangkan bila VPN digunakan untuk menghubungkan kantor pusat dengan kantor cabang, implementasi ini termasuk jenis intranet site-to-site VPN[2].

VPN adalah sebuah teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk bergabung dengan jaringan lokal. Dengan cara tersebut maka akan didapatkan hak dan pengaturan yang sama seperti halnya berada didalam kantor atau network itu sendiri, walaupun sebenarnya menggunakan jaringan milik publik.Gambar I.1 menggambarkan konsep dasar dari sebuah jaringan VPN. Secara umum, VPN adalah sebuah proses dimana jaringan umum (*public network* atau *internet)* diamankan kemudian difungsikan menjadi sebuah jarigan privat (*private network*). Sebuah VPN tidak didefinisikan oleh rangkaian khusus atau router, tetapi didefinisikan oleh mekanisme keamanan dan prosedur-prosedur yang hanya mengijinkan penggunanya yang ditunjuk akses ke VPN dan informasi yang mengalir melaluiya.[1].



Gambar 1. Konsep VPN

Suatu organisasi atau institusi dalam melangsungkan kegiatannya tidak akan lepas dari pertukaran informasi antar para *stakeholder* yang satu dengan yang lain. Setiap informasi yang dihasilkan oleh salah satu *stakeholder* akan diperlukan oleh *stakeholder* lain. Untuk itu, kebutuhan informasi harus dapat diakses melalui jaringan komputer yang di desain untuk dapat mendapatkan informasi yang diperlukan dengan cepat, mudah, aman dan akurat. Dalam sebuah jaringan komputer, keamanan sewaktu pengiriman dan penerimaan data sangat penting untuk menjamin bahwa data yang dikirim sampai pada yang pihak yang dituju, dan tidak jatuh pada pihak yang tidak berkepentingan, terutama apabila data yang dikirimkan tersebut bersifat rahasia. Untuk itu perlu dilakukan pengamanan data pada jaringan dengan menggunakan metode-metode tertentu. Salah satu cara untuk mengamankan data pada suatu jaringan adalah dengan mengimplementasikan VPN yang dapat membuat sebuah jaringan bersifat *private* dan aman dengan menggunakan jaringan publik atau internet.

VPN adalah sebuah teknologi jaringan komputer yang dikembangkan oleh perusahaan skala besar yang menghubungkan antar jaringan diatas jaringan lain menggunakan internet yang membutuhkan jalur *privacy* dalam komunikasinya[3]. Sifat pribadi VPN berarti bahwa traffic data VPN yang pada umumnya tidak terlihat, atau di enkapsulasi oleh lalu lintas jaringan yang mendasarinya. Dalam istilah yang lebih teknis, di link lapisan protokol jaringan virtual dikatakan terowongan atau *tunnel* yang melewati jaringan transportasi yang mendasarinya. Istilah VPN dapat digunakan untuk menggambarkan berbagai macam konfigurasi jaringan dan protokol. Tiga fungsi utama VPN (Cisco System Inc., 2003) yaitu: 1. Enkripsi, Pengirim dapat mengenkripsi paket data sebelum dikirim melewati jaringan, sehingga jika paket data disadap tidak akan terbaca, 2. Integritas Data, Penerima dapat memastikan bahwa data dikirimkan melalui jaringan *Internet* tanpa mengalami perubahan, dan 3. Autentikasi Sumber Data, penerima dapat membuktikan keaslian sumber paket data, menjamin sumber informasi.

Jenis Implementasi VPN meliputi [4]:

***a. Remote site* VPN**

*Remote site*yang bisa juga disebut *Virtual Private Dial Up Network* (VPDN), menghubungkan antara pengguna yang *mobile* dengan *Local Area Network* (LAN). Jenis VPN ini digunakan oleh pegawai perusahaan yang ingin terhubung ke jaringan khusus perusahaannya dari berbagai yang jauh (*remote*) dari perusahaan. Skenario *remote access* VPN :

1. *Home User* atau *mobile user* yang telah terkoneksi ke internet melakukan dial ke VPN *gateway* perusahaan.
2. *User diauthenticate* dan akses diizinkan.
3. VPN *gateway* akan memberikan sebuah *IP Private* dari perusahaan kepada *Home user* tersebut, agar seolah-olah *user* tersebut berada dalam satu jaringan lokal.

Selain daripada itu, *remote site*VPN dapat digunakan untuk menghubungkan dua buah jaringan yang berbeda.Topologi ini terdiri satu VPN server dan beberapa VPN *client*. VPN client berupa computer-komputer yang harus menggunakan *username* dan *password* untuk terhubung ke VPN Server[5].

***a. Site-to-site* VPN**

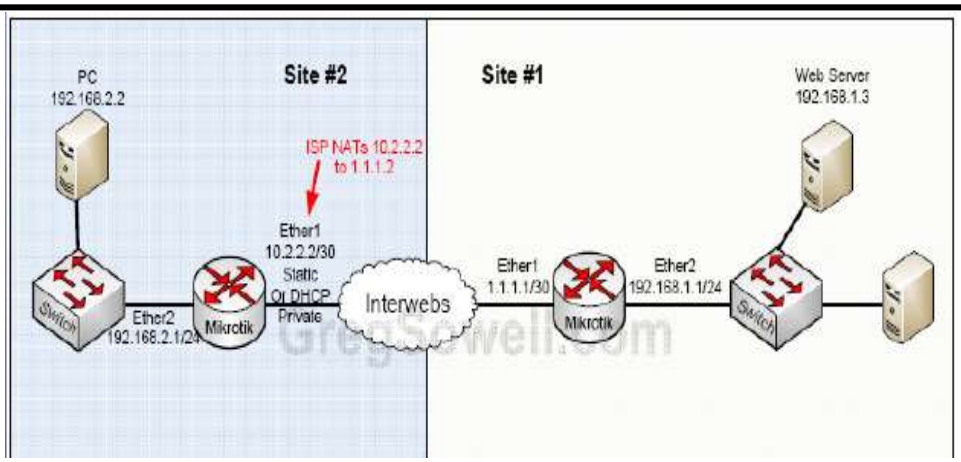
Site-to-site VPN disebut juga sebagai *gateway-togateway* atau *router-to-router.* Implementasi jenis ini menghubungkan dua kantor atau lebih yang memiliki jarak berjauhan, baik kantor pusat, kantor cabang maupun kantor mitranya.

***b. Extranet* VPN**

Extranet VPN digunakan untuk menghubung suatu perusahaan dengan perusahaan lain contohnya mitra bisnis. Sebuah extranet memiliki fungsi *outsourcing help desk* dan *set up* VPN untuk menyediakan koneksi aman dari kantor perusahaan ke perusahaan *outsourcing.*

***c. Intranet* VPN**

Intranet VPN merupakan koneksi VPN yang membuka jalur komunikasi pribadi menuju ke jaringan lokal yang bersifat pribadi melalui jaringan public seperti internet. Malalui VPN jenis ini, biasanya para pengguna VPN dapat langsung mengakses file-file kerja mereka dengan leluasa tanpa terikat dengan tempat dan waktu. Koneksi ke kantor pusat dapat langsung dilakukan dari mana saja, dari kantor pusat menuju kantor cabang kita dapat membuat koneksi pribadi, dan dari kantor cabang juga memungkinkan untuk dibuat jalur komunikasi pribadi yang ekonomis asalkan menggunakan VPN.



Gambar 2. Konsep VPN *site to site*

Pada topologi *site to site,* koneksi VPN yang akan dibangun terdiri dari beberapa router, masing-masing memiliki jaringan lokal, dan pada saat koneksi PPTP terjalin, masing-masing lokal network tersebut akan dapat berkomunikasi.Guna menjamin keamanan oneksi dan data, VPN memiliki tiga metode dan harus dimiliki oleh VPN yaitu sebagai berikut:

a. *Privacy (Confidentiality)*
   Data yang dikirimkan hanya dapat dibuka atau diakses oleh yang berhak.
b. *Reliability (Integrity)*
   Data yang dikirimkan tidak boleh mengalami perubahan dari pengirim data ke penerima data.
c. *Avaibility*
   Data yang dikirimkan harus tersedia ketika dibutuhkan. Semua tujuan ini harus dicapai dengan ditunjang oleh *software, hardware,* ISP, dan pemilihan keamanan yang tepat. Kemanan VPN tidak lepas dari menjaga lalu lintas *(traffic)*, enkripsi yang kuat, teknik otentikasi yang aman dan *firewall* yang mengatur *traffic* ke *tunnel.*

Enkripsi

Enkripsi adalah sebuah proses yang melakukan perubahan sebuah kode dari yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti[4]. Dengan enkripsi, berfungsi mengubah isi dari data yang kita kirim sehingga data tersebut tidak dapat dibaca oleh orang yang tidak berhak mendapatkannya. Informasi yang tidak diacak disebut *clear-text* sedangkan yang diacak disebut *cipher-text.* Di setiap *tunnel* VPN terdapat VPN *gateway* tempat pengiriman data mengenkripsi atau mengubah informasi *clear-text* menjadi *cipher-text* sebelum dikirim melalui *tunnel* ke internet. VPN *gateway* di tempat penerimaan mendeskripsikan atau mengubah *cipher-text* tersebut kembali menjadi *clear-texrt.*

Enkripsi terdiri dari dua jenis, yaitu *symmetric encryption* dan *asymmetric encryption*. *Asymmetric encryption* menggunakan *public* dan *private key* dalam proses enkripsi dan dekripsi, sedangkan *symmetric encryption* menggunakan *key* yang sama dalam proses enkripsi dan dekripsi. Adapun metode *encryption* sebagai berikut:

a. *Symmetric Encryption*
   Metode ini menggunakan *private key* berbagai komputer pengirim dan penerima sama-sama menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi informasi. Karena satu *key* digunakan bersama-sama untuk enkripsi dan dekripsi, maka harus ada pengertian antar kedua pihak untuk menjaga kerahasiaan *key* tersebut.Semua itu mempunyai kunci enkripsi dapat mendekirpsi data yang terdapat dalam lalu lintas VPN. Jika ada *user* yang tidak berwenang memiliki kunci enkripsi, ia dapat mendekripsi data yang ada dan masuk kedalam jaringan yang terhubung melalui VPN. Selain itu kunci enkripsi juga dapat dibuka dengan melakukan *brute force attack.* Hanya masalah waktu sampai seorang *attacker* dapat membuka kunci enkripsi.
b. *Asymmetric Encryption*
   Asymmetric key encryption mengenkripsi informasi dengan satu *key* dan mendekripsi dengan *key* lainnya. Metode ini menggunakan kombinasi dari dua buah *key*, yaitu *private key* yang disimpan untuk diri sendiri, dan *bulic key* yang diberikan untuk *remote-user.*SSLmenggunakan salah satu metode pengenkripsian *asymmetricencryption* ini untuk memastikan

identifikasi dari masing-masing pengguna VPN.

Tunneling

Teknologi *tunneling* merupakan teknologi yang bertugas untuk menangani dan menyediakan koneksi *point-to-point* dari sumber tujuannya. Teknologi ini disebut *tunnel* karena koneksi *point-to-point* tersebut sebenarnya terbentuk dengan melintasi jaringan umum namun tidak memperdulikan paket-paket data milik orang lain yang sama-sama melintasi jaringan umum tersebut, tetapi koneksi tersebut hanya melayani trasnportasi data dari pembuatnya. Koneksi *point-to-point* ini sebenarnya tidak benar-benar ada namun data yang dikirimkannya terlihat seperti benar-benar melewati koneksi pribadi yang bersifat *point-to-point*[6].

Teknologi ini dibuat dengan cara pengaturan *IP Addressing* dan *IP Routing,* sehingga antara sumber *tunnel* dengan tujuan *tunnel* dapat saling berkomunikasi melalui jaringan dengan pengalamatan IP. Apabila komunikasi antar sumber dan tujuan dari *tunnel* tidak dapat berjalan dengan baik, maka *tunnel* tersebut tidak akan terbentuk dan VPN pun tidak dapat terbangun.

Setelah *tunnel* tersebut terbentuk dengan baik, koneksi *point-to-point* tersebut dapat langsung digunakan untuk mengirim dan menerima data. Dalam implementasinya di VPN, *tunnel* tersebut tidak dibiarkan begitu saja tanpa diberikan sistem keamanan tambahan. *Tunnel* dilengkapi dengan sebuah sistem enkripsi untuk menjaga data yang dilewatinya.

Tunneling Protocol

Point-to-point Tunneling Protocol (PPTP) merupakan protocol 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* (PPP) yang dikeluarkan *Internet Engineering Task Force* (IETE). PPTP merupakan protocol jaringan yang merubah paket PPP menjadi IP *datagrams* agar dapat dikirimkan melalui internet. PPTP juga dapat digunakan pada jaringan private LAN to LAN dan komputer yang terhubung dangan LAN untuk membuat VPN melalui LAN.

Keunggulan utama dari penggunaaan PPTP adalah dapat dipergunakannya *Public Switched Telephone Network* (PSTN) dalam membangun VPN. Pembuatan PPTP yang memakan biaya cukup kecil dan mudah untuk digunakan secara luas, menjadi sebuah solusi untuk *remote user* dan *mobile user* karena PPTP memberikan keamanan serta enkripsi komunikasi melalui PSTN ataupun internet.

Umumnya terdapat tiga komputer dipergunakan dalam PPTP, yaitu :

a. Client PPPT. Cara kerja PPTP dimulai dari sebuah remote atau PPTP client mobile yang membutuhkan akses ke sebuah LAN private dari sebuah perusahaan. Pengaksesan dilakukan dengan menggunakan ISP lokal
b. Network Access Server (NAS). Client terhubung ke Network Access Server (NAS) pada fasilitas ISP. NAS di sini bisa berupa prosesor front-end, server dial-in atau server Point-of-Presence (POP). Begitu terhubung, client bisa mengirim dan menerima paket data melalui internet. NAS menggunakan protocol TCP/IP untuk semua trafik yang melalui internet.
c. Server PPTP. Setelah client membuat koneksi PPP ke ISP, panggilan Dial-Up Networking yang kedua dibuat melalui koneksi PPP yang sudah ada. Data dikirimkan menggunakan koneksi yang kedua ini dalam bentuk IP datagram yang berisi paket PPP yang telah ter-enkapsulasi. Panggilan yang kedua tersebut selanjutnya menciptakan koneksi VPN ke server PPTP pada LAN private perusahaan. Koneksi inilah (melalui panggilan kedua) yang di-istilahkan sebagai tunnel

II. METODE PENELITIAN

Dalam penelitian ini, penulismenggunakan metode penelitian sebagai berikut:

1 Analisa Kebutuhan

Tahap awal ini dilakukan analisa kebutuhan, analisa permasalahan yang muncul, analisa keinginan pengguna, dan analisa topologi jaringan yang sudah ada saat ini. Metode yang biasa digunakan pada tahap ini diantaranya:

Wawancara, dilakukan dengan pihak terkait melibatkan dari struktur manajemen atas sampai ke level bawah/operator agar mendapatkan data yang konkrit dan lengkap. Pada kasus di *Computer Engineering* biasanya juga melakukan *brainstorming* juga dari pihak vendor untuk solusi yang ditawarkan dari vendor tersebut karena setiap mempunyai karakteristik yang berbeda; Survey langsung kelapangan, pada tahap analisis juga biasanya dilakukan survey

langsung kelapangan untuk mendapatkan hasil sesungguhnya dan gambaran seutuhnya sebelum masuk ke tahap desain. Survey biasa dilengkapi dengan alat ukur seperti GPS dan alat lain sesuai kebutuhan untuk mengetahui detail yang dilakukan;Membaca buku manual, pada analisis awal ini juga dilakukan dengan mencari informasi dari buku manual dokumentasi yang mungkin pernah dibuat sebelumnya. Sudah menjadi keharusan dalam setiap pengembangan suatu sistem dokumentasi menjadi pendukung akhir dari pengembangan tersebut. Begitu juga pada proyek jaringan, dokumentasi menjadi syarat mutlak setelah sistem selesai dibangun.

Dalam rangka mempelajari setiap data yang didapat dari data-data sebelumnya, maka perlu dilakukan analisa data tersebut untuk masuk ke tahap berikutnya. Adapun yang bisa menjadi pedoman dalam mencari data pada tahap analysis ini adalah:a. *User*/*people*: jumlah user, kegiatan yang sering dilakukan, dan level teknis user;b. Media hardware dan software: peralatan yang ada, status jaringan, ketersedian data yang dapat diakses dari peralatan, aplikasi softwareyang digunakan; c. Data: jumlah pengguna data, jumlah inventaris sistem, sistem keamanan yang sudah ada dalam mengamankan data;d. Network: konfigurasi jaringan, volume trafik jaringan, protokol, *network monitoring* yang ada saat ini, harapan dan rencana pengembangan ke depan;e. Perencanaan fisik: masalah listrik, tata letak, ruang khusus, sistem keamanan yang ada, dan kemungkinan akan pengembangan kedepan.

2. Desain
   Dari data yang didapatkan sebelumnya, tahap *design* ini akan membuat gambar desain topologi jaringan interkoneksi yang akan dibangun. Diharapkan dengan gambar ini akan memberikan gambaran seutuhnya dari kebutuhan yang ada. Desain bisa berupa desain struktur topologi, desain akses data, desain layout perkabelan, dan sebagainya yang akan memberikan gambaran jelas tentang proyek yang akan dibangun. Biasanya hasil dari design berupa:Gambar-gambar topologi (*server farm*, *firewall*, *datacenter*, *storages*, *lastmiles*, perkabelan, titik akses dan sebagainya); Gambar-gambar detail estimasi kebutuhan yang ada.
4. *Testing*
   Beberapa pekerja jaringan akan membuat dalam bentuk simulasi dengan bantuan *tools* khusus di bidang network seperti *Boson*, *Packet Tracer*, *Netsim*, dan sebagainya. Hal ini dimaksudkan untuk melihat kinerja awal dari jaringan yang akan dibangun dan sebagai bahan presentasi dan *sharing* dengan *team work* lainnya. Namun karena keterbatasan perangkat lunak simulasi ini, banyak para pekerja jaringan yang hanya menggunakan alat bantu *tools Visio* untuk membangun topologi yang akan didesain.
5. Implementasi.
   Tahapan implementasi menitik beratkan pada rancang bangun jaringan VPN

Didalam penelitian ini, penulis membutuhkan data-data pendukung yang diperoleh dengan suatu metode pengumpulan data yang relevan. Metode pengumpulan data yang digunakan adalah sebagai berikut: 1). Observasi, yaitu Melakukan observasi atau survei pada jaringan komputer yang saat ini berjalan di perusahaan untuk mengumpulkan data dan informasi yang nantinya akan digunakan untuk pengembangan jaringan perusahaan; 2). Wawancara, yaitu melakukan wawancara dengan pihak-pihak yang bersangkutan, dalam hal ini pihak eksekutif dan staff perusahaan pada divisi yang berkaitan dengan jaringan komputer, untuk mendapatkan gambaran mengenai proses bisnis dan peranan jaringan komputer yang digunakan untuk mendukung proses bisnis tersebut; dan 3) Studi Pustaka, yaitu melakukan studi kepustakaan mengenai teknologi-teknologi jaringan, termasuk didalamnya teknologi *Virtual Private Network* (VPN) sebagai dasar teori, melalui pengumpulan bahan-bahan pustaka baik yang dilakukan di perpustakaan maupun melalui pencarian lewat internet yang dapat membantu memperdalam materi, pembuatan rancangan jaringan dan pengujian sistem jaringan yang dibuat..

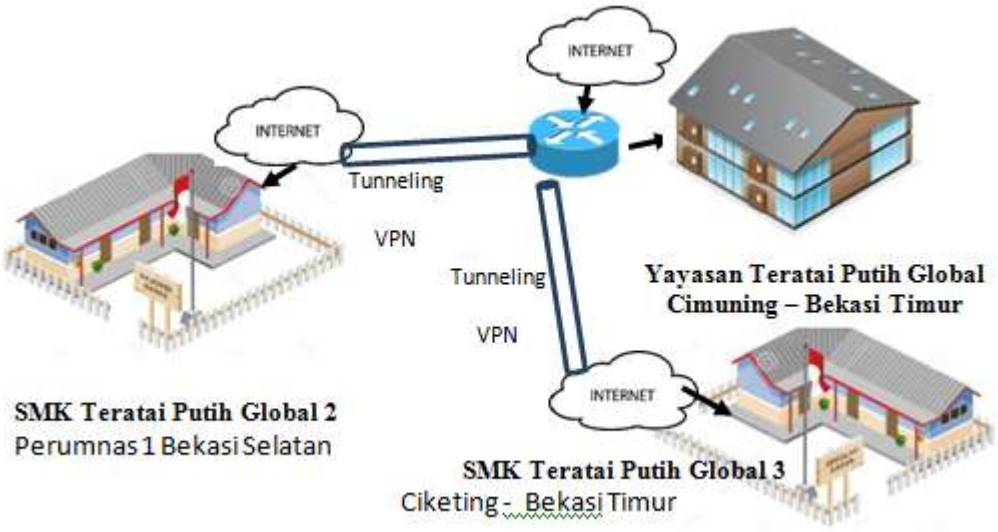
III. HASIL DAN PEMBAHASAN

Pada skema jaringan di smk teratai putih 2, smk teratai putih 3 dan jaringan kantor yayasan teratai putih.terdapat jaringan yang terpisah antara sekolah dan yayasan, masing-masing memiliki koneksi internet dengan ISP yang berbeda. pada yayasan teratai putih menggunakan jasa ISP central Online serta terdapat switch yang mengakomodir jarirngan LAN pada masing-masing lokasi. Dan Pada tiap-tiap sekolah terdapat satu modem, satu *switch* serta PC dengan koneksi internet menggunakan Indihome, semua itu terhubung ke internet

Yayasan memiliki satu buah *IP Public static.* Semua IP komputer *staff* dan karyawan menggunakan konfigurasi IP secara manual.

Semua terkoneksi ke router melalui hub/switch dan terkoneksi ke internet. Server pada yayasan masih menggunakan windows XP yang di dalamnya berjalan aplikasi *Excellent*(aplikasi mengatur keuangan sekolah). Dari komputer server, semuakomputer *client* yang berada di yayasan dapat mengakses data *base Excellent* sehingga dapat dipergunakan untuk transaksi. Sedangkan setiap sekolah hanya bisa menginput data murid, kemudian diberikan ke kantor yayasan untuk di input melalui aplikasi *Excellent.*

Setiap jaringan tidak pernah lepas dari serangan, serangan bisa terjadi kapanpun, yang akan berdampak pada kestabilan dan produktifitas jaringan, Keamanan jaringan yang sedang digunakan pada yayasan teratai putih hanya menggunakan default bawaan perangkat jaringan komputer yang digunakan tanpa ada tambahan, pengamanan instalasi standard mode pengamanan biasa seperti *firewall default* dari router, *password security* WPA2/PSK serta *user login password* yang sangat mudah diretas. Selain itu, Semua perangkat komputer yang digunakan bisa dengan bebas menggunakan koneksi internet, tanpa ada proxy yang diaktifkan untuk menyaring dan memblok sebuah situs yang tidak layak. Selain itu, koneksi antar sekolah juga menggunakan akses langsung, sehingga dapat menimbulkan celah pihak eksternal masuk ke jaringan internal di Yayasan Teratai Putih Global.Secara garis besar permasalahan yang dihadapi oleh Yayasan Teratai Putih Global yaitu dalam penarikan data transaksi kantor pusat ke sekolah-sekolah yang bersifat sangat rahasia.Dari permasalahan tersebut, Jaringan usulan yang akan diterapkan adalah membangun sebuah system jaringan VPN dengan menggunakan *router* Mikrotik, merupakan suatu sistem keamanan yang digunakan untuk mengamankan jaringan komunikasi yang menghubungkan yayasan dengan sekolah-sekolah yang bernaung di bawah Yayasan Teratai Putih Global. Jaringan yang terhubung dan dibentuk dari VPN merupakan suatu pipa *(tunnel)* yang berada dijaringan publik sehingga aliran data yang melewati di dalamnya tidak bisa diakses oleh pihak lain yang tidak memiliki akses ke dalam *tunnel* tersebut.



Gambar 3. Rancangan Jaringan Usulan

Dalam infrastruktur jaringan di kantor yayasan teratai putih, khususnya, memiliki Topologi Star yang skala jaringan yang tidak terlalu kompleks. Dan Client Komputer yang digunakan hanya 3 atau 5 untuk beroperasi. Sedangkan untuk yang *meremote* Komputer yayasan dari jarak jauh dan bisa terhubung dengan jaringan lokal yayasan melalui teknologi VPN yaitu sekolah SMK Teratai Putih Global 2 dan SMK Teratai Putih Global 3. Dua sekolah tersebut memiliki inftrasuktur yang standar, dalam rancangan usulan topologi hanya menambahkan router mikrotik untuk membagi network jaringan apabila ada penambahan *client* komputer di setiap ruang Tata Usaha.

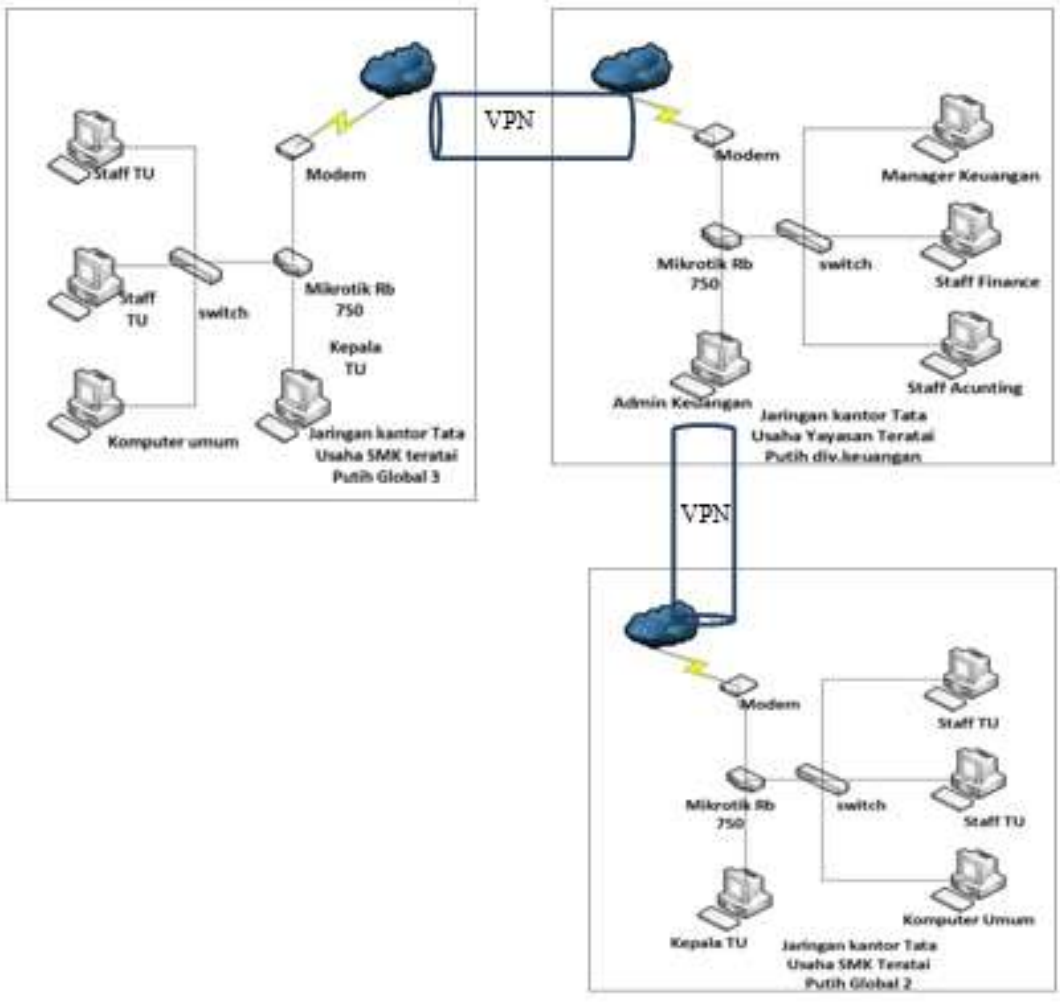
Rancangan Topologi Usulan

Dalam skema jaringan usulan, penulis akan menambahkan teknologi VPN untuk

mengkomunikasikan dan berbagi data dengan Aman. Karena VPN akan menggunakan metode enkripsi(pengacakan) dalam mengirimkan data transaksi dari sekolah ke yayasan. Dengan teknlogi VPN diharapkan mengurangi tindak kecurangan atau penyadapan dari seseorang yang tidak beranggung jawab. Gambar di atas adalah skema jaringan yang akan dibangun dimana terdapat satu *user,* satu *modem,* satu *router,* dan satu switch pada yayasan serta koneksi internet menggunakan jasa ISP. Pada tiap-tiap sekolah terdapat satu modem, satu router, satu switch serta PC, semua itu terhubung ke internet, dan komputer di yayasan akan dihubungkan menggunakan VPN yang menjadi satu jaringan local dengan sekolah melalui jaringan publik.

Dengan menggunakan Teknologi VPN, memungkinkan keamanan dalam transfer data akan aman, walaupun data yang dikirim jauh dari jaringan lokal. Untuk keamanan jaringan dalam teknologi VPN, menggunakan Tipe VPN *remote site* VPN. Karena yang akan dihubungkan dengan menggunakan teknologi VPN adalah jaringan lokal dari kantor yayasan dengan sekolah. Dengan *remote site* VPN, jaringan yang terhubung menjadi jaringan internal yang bersifat *private.*

Remote site VPN yang digunakan bersifat *client-initiated* sehingga computer *client* yang ingin terhubung dengan jaringan kantor yayasan dapat membentuk suatu *tunnel* yang aman sepanjang jaringan internet menuju kantor yayasan. Fungsi *tunnel* ini sendiri melindungi pertukaran data yang terjadi antar *client* dan kantor yayasan dari tindakan pencurian oleh pihak yang tidak bertanggung jawab. Seperti *sniffing.* Karena data yang melalui *tunnel* sudah mengalami proses enkripsi.Enkripsi merupakanmetode yang digunakan untuk mengacak data, sehingga orang lain tidak dapat membaca data yang dikirimkan.



Gambar 4. Skema Jaringan VPN Usulan

Dalam rancangan aplikasi VPN, ada beberapa tahapan yang mesti harus dijalankan, sistem

yang sesuai dengan rancangan, akan mempermudah mengatur konfigurasi jaringan serta tidak membuat seorang administrator tidak bingung dalam memanajemennya

Konfigurasi IP Address

Terdapat pembagian alokasi *IP address* yang akan digunakan pada saat simulasi. *ip public* yang terdapat pada router mikrotik telah dilakukan konfigurasi secara statis, sehingga *IP address* bersifat tetap. Sedangkan ip lokal dilakukan secara DHCP, agar memudahkan untuk mendistribusikan ip kepada *computer client*. Dan ada 2 *client(*komputer sekolah*)* yang akan terhubung dengan jaringan yayasanberfungsi sebagai computer yang dipakai untuk transaksi.

Tabel 1merupakan rancangan tabel alokasi *IP address* yang digunakan pada rancangan jaringan VPN Usulan.

Tabel 1. Alokasi IP Address

No	Lokasi	IP Address	Ket
1	Yayasan Teratai Putih Global	192.168.8.101	*Ip public*
2	Yayasan Teratai Putih Global	192.168.10.1	*Ip local*
2	SMK Teratai Putih Global 2	172.16.20.15	*ip public*
3	SMK Teratai Putih Global 3	217.146.9.6	*ip public*

Konfigurasi *IP Pool*

Pengaturan IP *Pool* untuk DHCP *Server* yang akan diberikan dengan *ranges=192.168.10.5-192.168.10.20*

Konfigurasi *Routes*

Konfigurasi NAT pada Firewall. NAT adalah pemetaan (translasi) alamat IP sehingga banyak IP private dalam sebuah LAN dapat mengakses IP public. Setelah dilakukan penginstalan pada Mikrotik, maka selanjutnya adalah mengkonfigurasi NAT melalui terminal. Setelah terbentuk konfigurasi server untuk bisa terhubung ke internet, langkah selanjutnya membuat konfigurasi mikrotik untuk membuat teknologi VPN, Untuk merancang VPN, maka yang bertindak menjadi VPN Server adalah Router Mikrotik yang berada di yayasan.

Selanjutnya dilakukan konfigurasi VPN server meliputi :

Konfigurasi PPTP *Server*

Hal pertama yang harus dilakukan yaitu membuat PPTP Server yang bertindak sebagai VPN *server* Mikrotik.Pemilihan menu yang pertama yaitu memilih menu PPP berada pada sisi kiri winbox hingga muncul kotak dialog PPP. Pada kotak dialog PPP tersebut pilih menu PPTP *server* hingga muncul kotak dialog PPTP *server.*

Pembuatan PPP *profile*

Untuk memudahkan dalam memanajemen jaringan VPN, maka dibuatlah *profile* baru, agar tidak menggunakan *profile defult* bawaan mikrotik. Dan di dalam *local address,* dan *remote address* di isi IP *pool* yang telah dibuat sebelumnya.

Pembuatan PPTP *secret*

Pada bagian ini pembuatan PPTP *secret* bertujuan pembentukan akun kepada *user* yang akan mengakses jaringan VPN tersebut. Dalam hal ini, ada 2 sekolah yang akan menjadi *remote client.* Sehingga harus membuat 2 PPTP *secret.* Dari kotak dialog PPP, pilih *tab secret* lalu pilih tanda '+' untuk menambahkan PPTP *secret,*dan di menu *profile*, pilih *profile* yang telah dibuat sebelumnya,

Konfigurasi *VPN Client*

Membuat VPN client untuk unit sekolah

Langkah pertama dalam pembuatan VPN client menggunakan fasilitas yang berada di windows 7 yaitu *Network and sharing center*, kemudian dilanjutkan dengan proses *connecting* VPN, Kemudian terbentuk VPN di *remote client*

Manajemen Jaringan

Untuk mempermudah memanajemen jaringan, penulis merancang manejemen *bandwidth* disetiap user agar tidak terjadi bentrok dalam mengakses internet, Fungsi manajemen *bandwidth*adalah agar semua bagian unit komputer mendapatkan *bandwidth*sesuai dengan kebutuhan koneksi internet untuk memaksimalkan *bandwidth*di semua unit komputer. Cara konfigurasinya melalui terminal yaitu:*/queue simple add name="VPN Bandwith" target-address=Lokal interface=Lokal max-limit=2m limit-at=2m parent="VPN"*

Pengujian Jaringan

Dalam hal pengujian jaringan, ada 2 cara untuk mendapatkan hasil yang maksimal. Khususnya dalam merancang teknologi VPN yaitu :

Pengujian Jaringan Awal

Jaringan yang berada di yayasan teratai putih masih menggunakan jaringan konfigurasi dasar, hanya bisa mengakses sebuah internet(*WAN)*, dan mengamankan jaringan dengan *default firewall* bawaan, sehingga mentransfer data dan penarikan transaksi pembayaran siswa disetiap unit sekolah masih menjalankan secara manual. Untuk melihat jaringan awal yang telah terpasang, penulis akan menjelaskan pengujian sebelum rancangan tahapan konfigurasi yang belum terpasang teknologi VPN.Pengujian *Tools*belum terpasangnya teknologi VPN, membuat Penulis hanya memperlihatkan kinerja jaringan yang telahdi rancang, melalui konfigurasi dasar yang dirancang dengan menggunakan simulasi memakai modem Smarftfren yang telah di *dial up* ke mikrotik dan mendapatkan *bandwith* yang telah diatur sebesar 2 Mbps. *Tools* yangdigunakan adalah *Torch* yang ada di aplikasi *winbox.tools* ini dapat digunakan untuk melihat secara *real time* beberapa *bandwith* yang sedang digunakan oleh setiap komputer.

Pengujian Jaringan Akhir

Dalam pengujian jaringan akhir, Teknologi VPN harus sudah terbentuk. Agar setiap unit sekolah bisa terhubung ke jaringan yayasan Teratai Putih. Dan bisa mengukur tingkat keamanan yang akan digunakan dalam teknologi VPN. Berikut adalah pengujian akhir yang dilakukan adalah:

1). Pengujian file sharing pada jaringan VPN yang sudah terbentuk,
2). Pengujian *Routingd*Dengan melakukan *traceroute* ke sebuah situs internet dari *remote user* saat terhubung ke PPTP *server,* maka hasil *traceroute* akan memperlihatkan bahwa untuk menuju internet, *remote user* tersebut harus melewati IP *lokal* dari router yayasan,
3). Pengujian koneksi antar *client,* Skenario yang dilakukan adalah, *remote user* dari sekolah mencoba mengirimkan paket ICMP(*ping)* ke jaringan ip *public* dan *local* yayasan,
4) Pengujian IP *pool,* Untuk memudahkan seorang administrator dalam pengaturan *ip address* pada jaringan, pada VPN *server* di *setting ip pool* untuk mendistribusikan *ip address ke client* secara otomatis
5) Pengujian *bandwidth*, meliputi pengujian bandwidht pada server dan pada client.

Monitoring user VPN

Untuk monitoring rancangan jaringan VPN menggunakan menu *torch* dengan mengisikan kolom *interface* dengan VPN *remote site* yang telah terbentuk ,

Analisis Parameter QoS

a. *Packet Loss*
Packet Loss dapat disebabkan oleh sejumlah faktor, mencakup penurunan sinyal dalam media jaringan, melebihi batas kemampuan jaringan, paket yang *corrupt* yang menolak untuk transit, kesalahan hardware jaringan. Rumus berikut digunakan untuk menghitung nilai dari Packet Loss.

$$\textbf{Packet Loss} = \frac{\boldsymbol{Packet\_Transmitted - Packet\_Received}}{\boldsymbol{Packet\_Transmitted}} \textbf{100}\%$$

Tabel 2 Perbandingan Packet Loss

Client	Packet Tx	Packet Rx	Packet Loss
192.168.10.14	888 bps	600 bps	31.75 %
192.168.10.13	560 bps	368 bps	-34.28 %

Dari data *packet loss* pada Tabel1dapat disimpulkan bahwa proses pengiriman data sangat baik Karena bernilai dibawah 0%, dimana antrian yang terjadi tidak melebihi kapasitas *buffer* pada setiap *node.*

b. *Delay*
Waktu yang dibutuhkan untuk sebuah paket untuk mencapai tujuan, karena adanya antrian yang panjang, atau mengambil rute yang lain untuk menghindari kemacetan. Delay dapat dicari dengan membagi antara panjang paket (L, *packet length* (bit/s))dibagi dengan link *bandwidth*(R, *link bandwidth*(bit/s)).

Tabel 3 menunjukkan hasil pengujian delay untuk dua buah client.

Tabel 3 Perbandingan Delay

Client	Packet Tx	*Bandwidth*	Delay
192.168.10.14	888 bps	2000 bps	0,004 s
217.146.9.6	1376 bps	2000 bps	0,68 s

Hasil pengujian menujukkan nilai rata-rata delay tidak mencapai 1 detik sehingga data yang dikirim tidak mengalami distosrsi dan redaman yang signifikan.

Hasil analisa dan percobaan

Setelah dilakukan perancangan perangkat jaringan VPN pada yayasan Teratai Putih Global dengan menggunakan *router* Mikrotik untuk penarikan data base transaksi keuangan pada aplikasi *Excellent* diperoleh hasil sebagai berikut :

a. Jaringan kantor yayasan dengan jaringan sekolah dapat terhubung dengan jalur *tunneling* yang memanfaatkan jaringan internet.
b. Proses pengambilan data sudah tidak lagi ditarik secara manual ataupun menggunakan email melainkan sudah menggunakan jaringan VPN yang terintegrasi menjadi sistem jaringan local antara kantor yayasan dengan sekolah.
c. Sistem jaringan VPN jauh lebih aman dan dana yang dibutuhkan dalam pembangunan sistem jaringan VPN dengan *router* mikrotik jauh lebih terjangkau

IV. KESIMPULAN ATAU SARAN

Kesimpulan yang dapat diambil dari rancangan pada tulisan ini adalah:

a. Pengambilan data menjadi lebih efektif karena sudah tidak menggunakan cara manual.
b. Hasil analisa penggunaan *bandwidth*yang telah dilakukan, maka keperluan *bandwidth*yang diperlukan oleh sekolah minimal 2 Mbps.
c. Dengan adanya sistem jaringan VPN, penarikan data data tidak lagi dilakukan secara manual

Berikut adalah saran hasil dari penelitian yang penulis lakukan untuk sistem jaringan VPN Yayasan Teratai Putih Global sebagai berikut :

a. Penambahan *firewall* yang berbentuk *hardware* pada jaringan VPN Yayasan Teratai Putih Global akan memberikan keamanan yang lebih baik.
b. VPN adalah teknologi yang mengandalkan koneksi internet yang stabil tanpa terputus, maka disarankan untuk menggunakan jasa ISP yang sudah terpercaya memiliki kecepatan stabil.
c. Perlu dilakukan *maintenance* sistem jaringan secara berkala dapat menambah kinerja lebih baik pada jaringan VPN

V. REFERENSI

[1] J. Triyono, R. Y. R. K and F. D. Irnawan, "Analisis Perbandingan Kinerja Jaringan VPN Berbasis Mikrotik Menggunakan Protokol PPTP Dan L2TP Sebagai Media Transfer Data," *Jurnal JARKOM,* Vols. Vol. 1, No. 2, pp. 112-121, 2014.

[2] G. Chelara and D. Hermanto2, "Analisis Site to Site Virtual Private Network (VPN) pada PT.Excel Utama Indonesia Palembang," *Seminar Perkembangan dan Hasil Penelitian Ilmu Komputer (SPHP-ILKOM),* pp. 35-44, October 2014.

[3] B. A. Forouzan, "Data communications and networking," New York, McGraw-Hill., 2007.

[4] D. Stiawan, "Sistem Keamanan Komputer," Jakarta, PT. Elex Media Komputindo, 2015.

[5] J. Triyono, R. Y. R. K. and F. D. Irnawan, "Analisis Perbandingan Kinerja Jaringan VPN Bberbasis Mikrotik Menggunakan Protokol PPTP dan L2TP Sebagai Media Transfer Data," *Jurnal JARKOM,* vol. Vol. 1 No. 2, pp. 112-121, Januari 2014.

[6] I. Afrianto and E. B. Setiawan, "Kajian Virtual Private Network (VPN) Sebagai Sistem Pengamanan Data Pada Jaringan Komputer(Studi Kasus Jaringan Komputer Unikom)," *Jurnal Majalah Ilmiah Unikom,* vol. Vol. 12, pp. 43-52, 2014.