BAB II

TINJAUAN PUSTAKA

2.1 *VPN* (*Virtual Private Network)*

VPN merupakan suatu metode pengamanan dengan membentuk koneksi *logical* antar beberapa node dalam jaringan yang bersifat *public*. Koneksi yang dibentuk dalam *VPN* merupakan koneksi *virtual* dalam bentuk *tunnel* dan bersifat *private* dengan adanya fitur *authentication* serta *policy-policy* yang dibentuk oleh setiap *router* yang terlibat. Teknologi *VPN* menyediakan tiga fungsi utama untuk penggunanya. Ketiga fungsi utama tersebut antara lain sebagai berikut:

1. *Confidentially* (Kerahasiaan)

   Dengan digunakannya 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.

2. *Data Intergrity* (Keutuhan Data / Keaslian 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. Teknologi *VPN* akan menjaga keaslian data dengan memastikan isi data yang sampai masih tetap sama seperti ketika dikirimkan.

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.

1.1.1 Tipe - tipe *VPN*

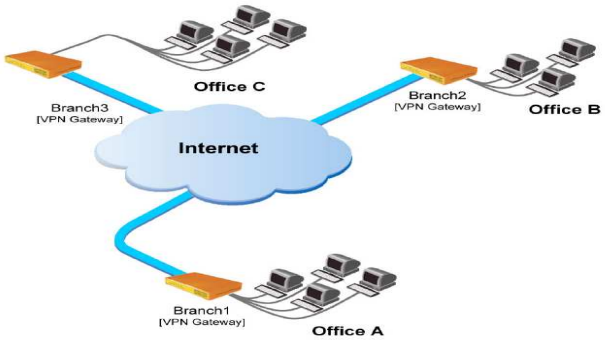
Berikut ini merupakan 2 jenis *VPN* secara garis besar

a) *Remote-Access VPN*

Remote-Access juga dikenal sebagai *Virtual Private Dial-Up Network* (VPDN), merupakan koneksi *user-to*-LAN yang digunakan sebuah perusahaan untuk prara pekerjanya yang membutuhkan koneksi ke jaringan mereka dari berbagai lokasi *remote*. *Remote Access VPN* memungkinkan pekerja untuk mengakses data-data dan segala sumber daya dimanapun mereka berada.

b) *Site-to-Site VPN*

Site-to-Site VPN memungkinkan suatu *private network* diperluas melintasi jaringan *internet* atau layanan *public network* lainnya dengan cara yang aman. *Site-to-Site VPN* merupakan suatu alternatif dari infrastruktur WAN yang bisa menghubungkan kantor-kantor cabang, kantor pusat, maupun *partner* bisnis ke dalam seluruh jaringan yang ada dalam perusahaan.



Gambar 2.1 Jaringan WAN

Sumber : (http://www.checkpoint.com/smb/help/utm1/8.0/1195.htm)

Site-to-Site VPN dibedakan menjadi 2 bagian yaitu *:*

- *Internet VPN*

  Internet VPN biasa digunakan untuk menghubungkan antara kantor pusat dan kantor cabang yang letaknya berjauhan melalui suatu *public* infrastruktur.

- *Extranet VPN*

  Extranet VPN biasanya digunakan untuk menghubungkan suatu perusahaan dengan perusahaan-perusahaan lain misalnya pemasok, penjual, *partner* bisnis, dll. Dengan adanya *Extranet VPN* perusahaan-perusahaan yang terlibat dapat berkomunikasi serta bertukar informasi secara cepat, mudah , tapi dalam sistem keamanan yang terjamin.

2.1.2 Keamanan *VPN*

Seperti yang sudah dijelaskan sebelumnya, *VPN* bukan hanya menjadikan sebuah jaringan bersifat *private* dengan adanya *tunnel logical* tapi juga menjamin setiap *traffic* yang ada di dalamnya. Terdapat beberapa fitur penting yang ada dalam *VPN* :

- Enkripsi

Enkripsi merupakan salah satu metode yang digunakan untuk mengubah data asli menjadi bentuk sandi (*chipper text*) yang mana sandi-sandi tersebut hanya dapat dimengerti oleh pihak pengirim dan penerima data sehingga data tersebut tidak dapat dibaca oleh orang luar yang tidak memiliki hak akses terhadap data tersebut. Untuk mengubah sandi tersebut ke bentuk semula maka digunakan teknik yang dinamakan dekripsi. Terdapat 2 metode enkripsi :

a) *Symetric Key Encryption*

Pada *Symetric Encryption* setiap komputer memiliki 1 kunci rahasia yang akan digunakan untuk mengenkripsi setiap informasi sebelum informasi tersebut dikirimkan melalui suatu jaringan. Kunci tersebut tidak hanya digunakan untuk mengenkripsi tapi juga mendekripsi data. Oleh karena itu, kunci tersebut harus dimiliki oleh kedua komputer sehingga tercapai kesepakatan antara penerima dan pengirim. Karena *key* yang digunakan untuk enkripsi dan dekripsi sama, metode enkripsi ini harus dijaga ketat agar tidak ada pihak luar yang bisa mengambil *key* tersebut dan dengan mudah membaca data yang dikirimkan.

b) *Asymetric Key Encryption*

Pada *Asymetric Encryption* proses enkripsi dan dekripsi masing-masing menggunakan 2 buah *key* yang berbeda, yaitu *private key* dan *public key* yang saling berhubungan secara sistematis. *Private key* dibuat oleh masing-masing komputer. Dari *private key* inilah, sebuah *public key* akan terbentuk. Setiap pengiriman data yang terjadi akan dienkripsi menggunakan *public key*. Ketika informasi itu berhasil diterima, pihak penerima akan melakukan dekripsi menggunakan *key private* mereka. Dikarenakan mempunyai cara kerja yang rumit dan tingkat keamanan yang lebih tinggi, proses ini dapat dikatakan lebih berat.

- *Tunneling*

Teknologi tunneling merupakan teknologi yang bertugas untuk menangani dan menyediakan koneksi *point-to-point* dari sumber ke tujuannya. Disebut tunnel karena koneksi *point-to-point* tersebut sebenarnya terbentuk melewati jaringan umum, namun seolah-olah koneksi tersebut menjadi bersifat *private* karena tidak memperdulikan paket-paket data milik orang lain yang sama-sama menggunakan jalur tersebut.

Teknologi ini dapat dibuat di atas jaringan dengan pendekatan IP *Addressing* dan IP *Routing* yang sudah berjalan sehingga antara *tunnel* sumber dan tujuan dapat saling berkomunikasi. Apabila komunikasi antar sumber dan tujuan tunnel tidak dapat berjalan dengan baik, maka *tunnel* tersebut tidak akan terbentuk dan *VPN* pun tidak dapat dibangun. Setelah tunnel tersebut terbentuk, maka koneksi *point-to-point* tersebut dapat langsung digunakan untuk mengirim dan menerima data. Dalam penerapannya di *VPN*, tunnel dilengkapi dengan sebuah sistem enkripsi untuk menjaga setiap data yang melewati *tunnel* tersebut. Proses enkripsi dan segala *policy* yang ada dalam *tunnel* tersebut akan dibentuk oleh protokol IPSec. Gabungan antara IPSec dan *Tunneling* inilah yang menjadikan *VPN* menjadi aman dan bersifat pribadi.

- IPSec

IPSec menyediakan layanan *security* dengan mengizinkan sistem untuk memilih protokol keamanan yang diperlukan, memperkirakan algoritma apa yang akan digunakan pada layanan, dan menempatkan *key* yang diperlukan untuk menyediakan layanan yang diminta. Pada IPSec terdapat *negotiation protocol* :

a) AH (*Authentication Header*) menyediakan layanan *Authentication* (menyatakan bahwa data yang dikirim berasal dari pengirim yang benar), *integrity* (keaslian data), dan melakukan pengamanan terhadap IP *Header*.

b) ESP (*Encapsulated Security Payload*) menyediakan layanan *authentication*, *integrity*, *reply protection*, dan *confidentiality* terhadap

data. ESP melakukan pengamanan data terhadap segala sesuatu dalam paket data setelah *header* (enkripsi).

2.2 GET (*Group Encrypted Transport*) *VPN*

Cisco Group Encrypted Transport adalah generasi terbaru dari solusi teknologi *wide access network (*WAN) untuk jaringan *virtual private network* (*VPN*). Kategori dari *VPN* ini tidak menggunakan *tunnel point-to-point*. Untuk pertama kalinya, teknologi *VPN* menghilangkan kebutuhan perangkat untuk melakukan kompromi antara kecerdasan jaringan dan privasi data.

Ini adalah model keamanan baru yang memperkenalkan konsep *router trusted group-member*. Konsep ini menggunakan metodologi keamanan bersama yang independen pada tiap *router* dari hubungan *point-to-point*.

Cisco VPN Group Encrypted Transport dapat melakukan ekspansi suatu jaringan dengan skala lebih besar, yakni dengan mengakomodasi *multicast* dan dapat melakukan hubungan koneksi yang terjalin secara instan pada saat transaksi *branch-to-branch.*

Cisco Group Encrypted Transport *VPN* dibutuhkan untuk :

- Mengamankan koneksi *private WAN*
- Enkripsi data melalui jaringan *MPLS*
- Mengamankan *multicast traffic*
- Menyebarkan suara atau aplikasi kolaboratif yang memerlukan enkripsi hubungan *any-to-any*
- Enkripsi paket IP melalui *link* satelit

Solusi *GETVPN* didasarkan pada *open standards* dan *Cisco patented innovative technology* yang dimana membantu untuk memanfaatkan kekuatan mendasar dari MPLS/*shared* IP *networks*. Selain memanfaatkan *Internet Key Exchange protocol (*IKE) yang ada, IPsec and teknologi *multicast,* solusi *GETVPN* bergantung pada kebutuhan jaringan.

2.2.1 Teknologi – Teknologi Dalam *GETVPN*

GETVPN memiliki beberapa teknologi yang ada di dalamnya. Teknologi - teknologi yang ada di dalamnya saling berhubungan dan bekerja sama untuk menghasilkan suatu sistem jaringan.

1. *GDOI (Group Key Management Protocol)* (RFC 6407)

   GDOI (group key management protocol) digunakan untuk menyediakan sebuah *set* dari *cryptographic keys* dan kebijakan untuk sekelompok perangkat. Dalam jaringan *GETVPN*, *GDOI* digunakan untuk mendistribusi *IPsec keys* untuk sekelompok perusahaan *y*ang harus berkomunikasi dengan aman. *Keys* ini masuk ke dalam proses *refresh* dan *update* yang dilakukan secara periodik pada semua *VPN gateway*. Proses ini bisa disebut dengan proses "*rekey*".

   Protokol *GDOI* ini dilindungi oleh *Phase 1 Internet Key Exchange* (IKE) SA. Semua yang terlibat dalam *VPN gateway* harus melakukan proses otentikasi ke perangkat yang menyediakan *keys* dengan menggunakan IKE. Pada semua metode IKE *authentication*, sebagai contoh, *pre-shared keys* (PSKs) dan *public key infrastructure* (PKI) kedua metode ini didukung untuk otentikasi awal. Setelah *VPN gateways* sudah dikonfirmasi dan dilengkapi dengan kunci keamanan yang tepat melalui IKE SA. Jika proses keamanan IKE SA berakhir, maka *GDOI* akan digunakan untuk melakukan proses *update* terhadap GMs dengan cara yang lebih terukur dan efisien.

   GDOI memperkenalkan dua *encryption keys* berbeda. Satu *key* mengamankan *control plane* pada *GETVPN*; kunci lainnya mengamankan *data traffic*. Kunci yang digunakan untuk mengamankan *control plane* biasanya disebut dengan *Key Encryption Key* (KEK), dan kunci yang digunakan untuk melakukan proses *encrypt data traffic* biasanya disebut dengan *Traffic Encryption Key* (TEK).

2. *Key Server (*KS*)*

Key Server (KS) adalah tanggung jawab IOS *device* untuk membuatnya dan mempertahankan *control plane* pada *GETVPN*. Semua kebijakan enkripsi seperti *interesting traffic, encryption protocols, security association, rekey timers,* dan sebagainya didefinisikan secara terpusat pada *Key Server* dan diberikan kepada semua *Group Member* pada saat proses pendaftaran *Group Member*.

Group Member mengotentikasi *Key Server* yang menggunakan IKE *Phase 1 (pre-shared keys or PKI)* dan men-download kebijakan enkripsi dan men-download kunci yang diperlukan untuk operasi *GETVPN*. *Key Server* juga bertanggung jawab untuk melakukan proses *refresh* dan distribusi *keys*.

3. *Cooperative (COOP)* KS *(Key Server)*

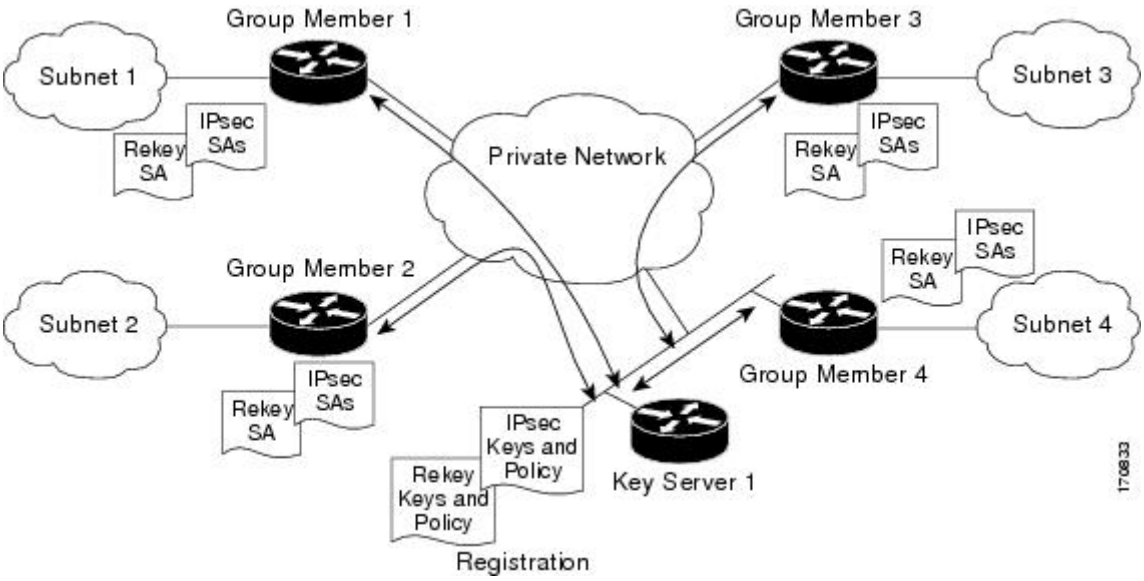
Key Server adalah entitas yang paling penting dalam jaringan *GETVPN,* karena *Key Server* mempertahankan *control plane* Oleh karena itu, *Key Server* tunggal adalah titik kegagalan untuk seluruh jaringan *GETVPN*. Karena redundansi adalah suatu pertimbangan penting untuk *Key Server*, *GETVPN* mendukung beberapa *Key Server,* disebut coorperative (COOP) *Key Server,* untuk memastikan pemulihan kesalahan berjalan baik jika *Key Server* gagal atau menjadi tidak terjangkau.

Sebuah GM dapat dikonfigurasi untuk mendaftar untuk setiap *Key Server* yang tersedia dari daftar semua COOP *Key Server*. Konfigurasi *Group Member* menentukan urutan pendaftaran. Proses penetapan *Key Server* pertama kali oleh *contacted first,* diikuti oleh proses penetapan *Key Server* yang kedua, dan seterusnya.

Proses pengambil alihan (*fail over*) *primary Key Server* terjadi secara langsung begitu *primary Key Server* sebelumnya mengalami putus koneksi. Pengambil alihan ini dilakukan oleh COOP KS. Jika terdapat lebih dari 1 COOP KS, maka akan terjadi proses pemilihan diantara 1 atau lebih COOP KS tersebut. COOP KS dengan *priority* tertinggi akan menggantikan posisi *primary Key Server* sebelumnya.

4. GM (*Group Member*)

Sebuah *Group Member* adalah tanggung jawab IOS *router* untuk melakukan proses enkripsi dan dekripsi. Seperti disebutkan sebelumnya, kebijakan enkripsi didefinisikan terpusat pada *Key Server* dan diunduh ke *Group Member* pada saat pendaftaran. Berdasarkan kebijakan *download*, *Group Member* memutuskan lalu lintas mana yang akan dienkripsi atau didekripsi dan menggunakan kunci apa. Untuk lalu lintas data menggunakan KEK (*Key Encryption Key*) dan untuk lalu lintas *traffic* menggunakan TEK (*Traffic Encryption Key*).



Gambar 2.2 Komunikasi *Key Server* dan *Group Member*

Sumber :

(http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_encrypt_trns_*VPN*.html)

5. IP *Tunnel Header Preservation*

Pada *traditional IPsec*, *tunnel endpoint addresses* digunakan sebagian sumber dan tujuan paket yang baru. Paket tersebut kemudian diarahkan melalui infrastruktur IP, menggunakan alamat IP *gateway source* yang sudah melalui proses *encrypt* dan IP *gateway destination* yang sudah melalui proses *decrypt*. Dalam kasus *GETVPN*, paket *IPsec* melindungi paket data dengan melakukan *encapsulate original source* dan *destination packet addresses* dari *host* di *header* IP luar dengan maksud untuk menjaga alamat asli dari *IP address* tersebut.

Gambar 2.3 *Tunnel Header Preservation*

Sumber :
(http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns165/ns391/images/guide_c07-494660-3.jpg)

Keuntungan terbesar dari *tunnel header preservation* adalah kemampuan untuk melakukan *route encrypted packets* menggunakan infrastruktur *routing* yang mendasarinya. Karena *tunnel header preservation* digabungkan dengan kelompok SAs, replikasi *multicast* dapat diturunkan ke jaringan operator. Karena setiap *Group Member* membagi SA yang sama, *router* IPsec terdekat ke *source multicast* tidak perlu mereplikasi paket ke semua *peers*.

Namun, *GETVPN* sama sekali tidak dianjurkan bila digunakan pada jaringan *internet*, hal ini dikarenakan alamat IP dari *host* tidak dapat disebarkan

ke dalam jaringan dan cara kerja *network address translation* (NAT) mengganggu proses *tunnel header preservation*.

6. *Group Security Association* (SA)

Tidak seperti solusi enkripsi tradisional IPsec, *GETVPN* menggunakan konsep kelompok *security association*. Semua anggota dalam kelompok *GETVPN* dapat berkomunikasi satu sama lain menggunakan kebijakan enkripsi umum dan *shared security association*. Dengan kebijakan enkripsi umum dan *shared security association*, tidak perlu melakukan negosiasi IPsec antar *Group Member*, ini akan mengurangi beban sumber daya pada router IPsec. Traditional *Group Member* scalability (jumlah *tunnel* dan *associated security association*) tidak berlaku untuk *GETVPN Group Member*.

7. *Rekey Mechanism*

Seperti disebutkan di atas, KS tidak hanya bertanggung jawab untuk menciptakan kebijakan enkripsi dan kunci, tetapi juga untuk *refresh key* dan membagikannya kepada GM. Proses mengirimkan kunci baru dilakukan ketika kunci yang ada akan *expire*, proses ini dikenal sebagai proses *rekey*. *GETVPN* mendukung dua jenis pesan *rekey*: *unicast* dan *multicast*. Proses *rekey* terbagi menjadi beberapa macam jenis :

1. *Unicast Rekey*

Dalam proses *unicast rekey*, sebuah *Key Server* menghasilkan sebuah pesan *rekey* dan mengirimkan beberapa salinan pesan untuk setiap *Group Member*. Setelah menerima pesan *rekey*, Sebuah *Group Member* mengirimkan pesan ACK kepada *Key Server*. Mekanisme ACK ini tidak hanya memastikan bahwa daftar *Group Member* aktif di *Key Server* saat ini, tetapi juga memastikan bahwa bahwa pesan *rekey* dikirim hanya sekali untuk *Group Member* yang berhasil menerima *rekey* dan *Key Server* yang hanya untuk *Group Member* aktif.

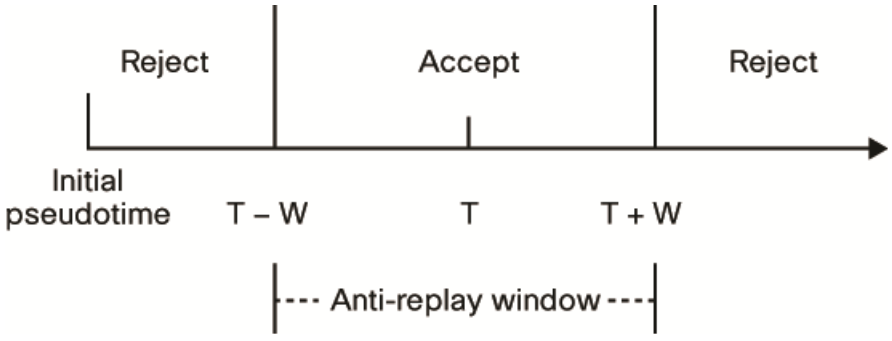
Sebuah *Key Server* dapat dikonfigurasi untuk mengirim ulang paket *rekey*, hal ini digunakan untuk mengatasi *error* sementara di dalam jaringan. Jika *Group Member* tidak mengakui tiga *rekey* secara berturut-turut, *Key Server* akan menghapus *Group Member* dari *database Group Member* aktif dan berhenti mengirim pesan *rekey* dengan *Group Member*.

2. *Multicast Rekey*

Dalam proses *multicast rekey*, *Key Server* menghasilkan pesan rekey dan mengirimkan satu salinan pesan ke alamat *multicast group* yang ditetapkan dalam konfigurasi. Setiap *Group Member* bergabung dengan *multicast group* saat pendaftaran, sehingga masing-masing *Group Member* menerima salinan pesan *rekey*.

Berbeda dengan *unicast rekey*, *multicast rekey* tidak memiliki mekanisme ACK. *Key Server* tidak memelihara daftar *Group Member* aktif. Sama seperti *unicast rekey*, *Key Server* dapat dikonfigurasi untuk mengirim ulang paket *rekey multicast* untuk mengatasi *error* sementara di dalam jaringan.

8. *Time-based anti-replay (TBAR)*



Gambar 2.4 *Time Based Anti-Replay*

Sumber :

(http://www.cisco.com/en/US/i/200001-300000/230001-240000/230001-231000/230078.jpg)

GETVPN biasanya digunakan melalui private WAN (VPLS, MPLS, dan sebagainya). Ketika ancaman serangan anti-replay sangat minim, itu adalah praktek terbaik untuk mengaktifkan *Time-based anti-replay*. *Time-based anti-replay* diaktifkan group wide pada *Key Server*.

2.2.2 Cara Kerja *GETVPN*

Cara kerja teknologi *GETVPN* terbagi menjadi beberapa jenis. Jenis-jenis ini yang membedakan posisi dari terjadinya proses di dalam *GETVPN*.

1. Registrasi *Group Member* (GM) melalui *Group Domain Of Interpretation* (*GDOI*)

   Key Server akan melakukan proses autentikasi dan autorisasi terhadap *Group Member*. Proses yang terjadi ialah penyamaan suatu nama *key* yang digunakan dalam teknologi ini. Jika nama *key* yang digunakan pada KS adalah "key123", maka pada konfigurasi di tiap GM harus menggunakan nama *key* yang sama dengan KS. *Key Server* memberikan satuan IPSec SAs (*Security Associations*) kepada *Group Member*.

   Security Association adalah blok *basic* dari IPSec yang juga merupakan input dari SA database (SADB) yang mengandung informasi tentang *security* yang telah disepakati untuk IKE atau IPSec. Kemudian hasil SA ini diambil oleh GM yang akan dibagikan kepada GM lain. Sehingga membuat setiap GM memiliki informasi SA yang sama dengan KS.

   Jika sudah diterima ke dalam grup, *host* dapat berkomunikasi secara bebas dengan beberapa atau semua *member* dari grup.

2. Enkripsi *Data Plane*

Di saat *Group Member* melakukan komunikasi dengan GM lain, proses pertukaran informasi ini akan terenkripsi menggunakan *Group Keys*. *Group Keys* ini terdapat pada setiap GM. *Key* ini yang mengautorasi secara langsung selama proses komunikasi antar GM di dalam jaringan.

Proses pertukaran informasi menggunakan IPSec *Tunnel Mode* dengan "*address preservation*". Dengan adanya *address preservation,* maka alamat asli pengirim suatu paket tidak disamarkan. Hal ini dapat mencegah proses pengiriman paket yang lama dan salah destinasi. Sehingga tidak menghabiskan banyak *bandwidth* dan waktu.

3. *Rekey Key*s Secara Periodik

KS mengganti IPSec *Keys* sebelum IPSec yang dipakai sekarang ini *expire*. Proses ini disebut dengan *Rekey*. Proses ini membuat KS akan selalu *update* dengan jaringan yang di dalam cakupannya.

Sehingga KS dapat selalu terhubung dengan *Group Member* yang masuk di dalam domainnya. Dengan cara ini membuat KS dapat mengetahui jika ada *Group Member* yang sudah tidak aktif.

Proses *rekey* dikenal menjadi dua, yaitu *unicast* dan *multicast*. Jika ada GM yang tidak menerima informasi *rekey* dari KS(sebagai contoh, KS down atau koneksi *internet* terputus), maka GM akan mencoba untuk melakukan re-registrasi ke KS jika waktu yang tersisa hanya 5% dari nilai TEK asli.

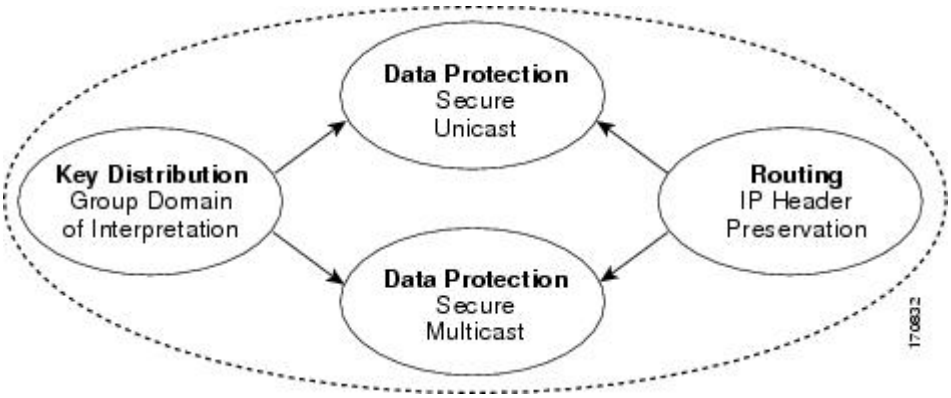
Registrasi harus sudah selesai sebelum masa IPSec SA berakhir dan kemudian GM akan menggunakan IPSec SA yang baru. Namun jika proses re-registrasi berhasil, GM akan menerima SA baru sebagai bagian dari proses re-registrasi dan traffic di dalam alur data plane tanpa adanya gangguan.

Jika proses re-registrasi tidak berhasil, maka GM akan mencoba melakukan proses re-registrasi sampai dengan tiga kali atau lebih pada interval 10 detik untuk membuat suatu hubungan dengan KS.

Tetapi jika semua kesempatan untuk membuat suatu hubungan dengan KS itu tidak berhasil, GM akan melakukan hal yang sama tapi ke KS yang lain, yaitu COOP KS. COOP KS ini merupakan KS lain yang perannya sebagai KS cadangan. Bisa terdapat dua atau lebih KS, ini tergantung dengan suatu kebutuhan di dalam jaringan.

Proses re-registrasi ini dilakukan sampai ke semua KS yang terdapat dalam suatu jaringan. Kemudian GM akan melakukan kembali proses registrasi ke KS pertama (*primary*) sampai proses registrasi berhasil.

2.2.3 Keuntungan *GETVPN*



Gambar 2.5 Keuntungan *GETVPN*

Sumber :

(http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_encrypt_trns_*VPN*.html)

GETVPN memiliki keuntungan sebagai berikut:

- Menyederhanakan komunikasi *branch-to-branch*
  Memastikan *low latency* dan *jitter* dengan mengaktifkan *full-time,* komunikasi langsung antara *sites* tidak membutuhkan *transport* melalui *central hub*.
- Memaksimalkan keamanan
  Menyediakan enkripsi untuk jaringan MPLS dan juga tetap mempertahankan *network intelligence* seperti koneksi *full-mesh, natural routing path*, dan *quality of service* (QoS).
- Sesuai dengan peraturan pemerintah dan undang-undang privasi
  Membantu *user* dalam memenuhi kepatuhan keamanan dan peraturan internal dengan mengenkripsi semua lalu lintas WAN.
- Menawarkan fleksibilitas manajemen
  Menghilangkan manajemen *key peer-to-peer* yang kompleks dengan *group encryption keys.*

2.2.4 Perbandingan Terhadap *VPN* Tunnel

VPN dan *GETVPN* merupakan metode yang berbeda. *GETVPN* merupakan pengembangan dari *VPN*. *GETVPN* memiliki kelebihan dibandingkan dengan *VPN*. Berikut ini adalah tabel perbandingan dari 2 metode tersebut :

Tabel 2.1 Perbandingan *VPN* dan *GETVPN*

VPN	*GETVPN*
Skalabilitas – Tunnel hanya dapat men koneksikan 2 site (point to point).	Arsitektur yang memungkinkan penggunaan topologi yang lebih fleksibel, tidak terbatas pada point-to-point.

Penambahan site baru memerlukan penambahan tunnel baru.	Penambahan site tidak mutlak memerlukan penambahan tunnel baru.
IP *Header* baru ditambahkan ke paket asli, sehingga tidak dapat modifikasi QOS.	IP *header preservation* menyebabkan IP *header* asli pada paket IPsec, sehingga QOS dapat dimodifikasi
Pengiriman packet multicast harus dipecah menjadi beberapa packet unicast, dikarenakan topologi tunnel yang point-to-point.	Pada GetVPN, multicast dapat bekerja sebagaimana mestinya di topologi broadcast/multicast.

2.3 Jurnal Ilmiah

2.3.1 Jurnal 1

Berdasarkan jurnal *International Journal of Advanced Science and Technology* Volume 8, July, 2009 dengan judul "*Vulnerabilities of VPN using IPSec and Defensive Measures*" oleh Byeong-Ho Kang dan Maricel O. Balitanas dijelaskan bahwa *VPN* (*virtual private network*) itu adalah jaringan komputer yang dibawa oleh *virtual circuits* terhubung dengan *internet*. Ide dalam penggunaan internet ke dalam jaringan untuk kebutuhan komunikasi antar cabang pada waktu yang bersamaan memastikan keamanan dan kerahasiaan dari data yang mengalami proses pengiriman. Dengan kata lain *VPN* merupakan jalur komunikasi yang menyediakan koneksi aman antar cabang via *internet.*

Jika memperhatikan akronim secara harafiah dari *VPN*, berarti tidak ada koneksi jaringan langsung antara dua pengguna. Tapi hanya sebuah koneksi virtual yang disediakan oleh *VPN*. Koneksi ini dibilang *private* dikarenakan hanya pengguna terdaftar dengan *software VPN* pada perusahaan itu yang diperbolehkan melakukan transformasi data.

Teknologi *VPN* ini tidak lepas dari teknologi lain di dalamnya. Karena banyak teknologi pendukung yang menjalankan fungsi *VPN* tersebut. Pada jurnal ini dijelaskan kerentanan pemakaian *VPN* menggunakan IPSec dan beberapa tindakan defensif. IPSec sendiri merupakan protokol untuk mengamankan komunikasi IP (*internet protocol*) dengan otentikasi dan mengenkripsi setiap paket IP dari aliran data. IPSec juga mencakup protokol untuk mendirikan otentikasi pada awal sesi komunikasi dan melakukan proses negosiasi kunci kriptografi yang akan digunaka selama sesi.

IPSec dapat digunakan untuk melindungi alur data diantara sepasang *host* (misalnya pengguna komputer atau *server*), antara sepasang *gateway* keamanan (misalnya *router* atau *firewall*), atau antara *gateway* keamanan dan *host*. Sebuah aspek penting dari IPSec adalah tersedianya kunci otomatis saat manajemen yang digunakan untuk bernegosiasi dalam operasi IPSec. Material *key* dan prasyaratan keamanan lainnya didefinisikan ke dalam *policy VPN*.

IPSec mencakup beberapa teknologi menarik seperti IKE (*automatic key management*). IKE merupakan protokol *automatic key management* yang digunakan oleh IPSec. Key utama dari IKE ialah enkripsi dan otentikasi.

Penelitian ini menjelaskan bahwa terdapat kerentanan pada *VPN*. Banyak dari *program client VPN* menawarkan untuk menyimpan data otentikasi untuk beberapa klien, dan ini merupakan pengaturan *default*. Hal ini membuat *VPN* menjadi semakin mudah untuk digunakan dan juga mendekatkan kepada resiko keamanan, terutama jika penggunaan *program client* tidak diawasi dengan baik.

2.3.2 Jurnal 2

Berdasarkan jurnal *International Journal of Scientific Research Engineering & Technology* (IJSRET) June, 2012 dengan judul "*VPN: TO MAKE PRIVATE NETWORKS THROUGH PUBLIC NETWORKS*" oleh Sadhana Pal dan Gyan Prakash Pal sudah dijelaskan dari judul tersebut bahwa *VPN* selain digunakan sebagai jalur komunikasi bersifat *tunnel*, *VPN* juga dapat digunakan untuk membuat hubungan antara *private networks* terhadap *public networks*.

Mengapa *VPN*? Perlu diketahui terlebih dahulu apa kelebihan dari *VPN* ini. Berikut ini ialah kelebihan dari *VPN* :

1. Informasi Perusahaan Aman

   VPN membuat informasi penting perusahaan aman terhadap gangguan yang tak diinginkan.

   - Mengurangi Pengeluaran

     Pengeluaran perusahaan menjadi lebih sedikit. Hal ini dikarenakan penggunaan internet yang menggantikan jaringan WAN. Sehingga perusahaan tidak perlu membiayai WAN. *VPN* juga mengurangi pengeluaran untuk kebutuhan *remote*. Karena proses *remote* dapat dilakukan secara *mobile*, jadi tidak perlu datang ke lokas *site*.

   - Memperluas Pilihan Konektifitas Pengguna

     VPN menyediakan berbagai macam pilihan koneksi. Hal ini memberikan keuntungan bagi penggunaannya. Sehingga dapat menyesuaikan pilihan yang disediakan dengan kebutuhan masing-masing pengguna. Pilihan koneksi itu diantaranya; via kabel, via DSL, via telepon, atau *ethernet*.

   - Meningkatkan Kecepatan Pengembangan

     Jaringan *extranet* dapat dibangun dengan mudah. Karena tidak membutuhkan *engineer* untuk ada di *site* dimana jaringan itu akan dibangun. Proses pembangunan ini dilakukan secara *remote*.

Maka dapat disimpulkan bahwa teknologi ini merupakan teknologi yang sangat memenuhi kebutuhan. Di samping dengan kemampuannya mengurangi pengeluaran suatu perusahaan. *VPN* memberikan solusi komunikasi jaringan yang aman. *VPN* menggunakan internet sebagai media transmisi jaringan. Hal ini juga yang menyebabkan *less cost*. Suatu perusahaan tidak perlu mengeluarkan dana untuk meminjam *data circuit. VPN* mengamankan transaksi dan menjadi media yang dapat diandalkan pada proses *transfer* data. *VPN* yang berbasiskan IP dapat mengembangkan sifat alami dari *intranet*

ke arah yang lebih luas yakni, *remote offices*, *mobile users*, *telecommuters*. Sifat-sifat ini mendukung hubungan jaringan *extranets* yang meghubungkan *business partner*, *customers*, dan *suppliers* untuk memberikan kepuasan *customer* lebih baik lagi dan juga untuk mengurangi biaya produksi.

2.3.3 Jurnal 3

Berdasarkan jurnal ComTech Volume 01 / Nomor 02 / December 2010 dengan judul *"ANALISA DAN PERANCANGAN JARINGAN BERBASIS VPN"* oleh Johan Muliadi Kerta, David Wennoris, dan Tonny Gunawan menjelaskan bahwa teknologi yang semakin berkembang menimbulkan masalah dari segi keamanan data terutama jika dikirim melalui jaringan *public* seperti *internet*. Dengan masalah tersebut, maka pengguna *internet* berusaha mengamankan apa yang dikirim dimana hanya pihak yang berkepentingan yang dapat mengakses data tersebut misalnya dengan password. Seiring berjalannya waktu, *password* tetap tidak membuat data dan informasi aman berada di jalur *public* tersebut. Dengan permasalahan ini maka dibutuhkan sebuah mekanisme jaringan dimana jaringan tersebut seolah-olah merupakan jaringan *private* atau pribadi namun tetap berjalan pada jaringan *public*. Teknologi tersebut dinamakan *Virtual Private Network* (*VPN*). Dengan menggunakan *VPN* maka data informasi tersebut akan lebih aman berada di jaringan *public* karena disembunyikan atau terenkripsi sehingga *user* lain tidak mengetahui data atau informasi tersebut.

PT. Finroll merupakan perusahaan yang bergerak dalam bidang IT solution yang sedang mengembangkan sayapnya menjadi penyedia jasa informasi mengenai saham maupun finance. Selama ini, untuk melakukan transaksi data dan lainnya ke perusahaan relasinya maupun sebaliknya, PT. Finroll menggunakan email melalui internet. Seperti diketahui, data informasi tersebut kurang aman berada di jalur *public*, apalagi jika data yang bersifat rahasia dan pribadi. Dengan adanya *VPN* maka PT. Finroll dapat menjalankan bisnis dengan pihak relasinya untuk melakukan hubungan secara *private* di dalam jaringan *public*. Ruang Lingkup penelitian ini meliputi analisa jaringan yang saat ini berjalan dan yang akan diusulkan pada PT. Finroll dan relasinya tetapi lebih dikhususkan pada PT. Finroll. Selanjutnya hasil penelitian ini akan memberikan usulan

solusi perancangan *VPN* melalui jalur *tunneling point-to-point* dengan menggunakan protocol PPTP untuk koneksi antar perusahaan. Sedangkan tipe perancangan *VPN* yang akan dibahas berupa *Remote Access VPN*.

Metodologi yang digunakan dalam penelitian ini adalah dengan melakukan studi kepustakaan mengenai teknologi *VPN* dari jenis, keuntungan, kelemahan, dan teori-teori yang mendukung, melakukan wawancara kepada *staff* IT PT. Finroll untuk mendapatkan informasi yang berguna untuk penelitian ini, kemudian melakukan observasi dan survei terhadap jaringan perusahaan pada Millenium Danamata Group (MDG) untuk mendapatkan informasi yang berguna dalam perancangan *remote access VPN*. Setelah itu menetapkan solusi yang dipakai serta menentukan teknologi yang dipakai beserta alasan pemilihan teknologi tersebut. Tahap selanjutnya adalah dengan merancang jaringan *remote access VPN* berdasarkan hasil analisa serta perangkat keras/*hardware* yang dipakai pada masing-masing perusahaan. Dan pada akhirnya mengevaluasi jaringan *remote access VPN* baik itu dari segi *bandwith* yang dipakai, *traffic* antar perusahaan, *encryption* yang dipakai serta proses *tunneling remote access VPN* yang digunakan.

PT. Finroll merupakan salah satu anggota dalam asosiasi Millenium Danatama Group (MDG). Atas pemenuhan kebutuhan dari PT. Finroll yang hanya ingin membentuk jaringan *VPN* dengan relasi bisnisnya yang tertentu saja (tetapi masih dalam lingkup anggota MDG), maka dari itu sistem yang akan dianalisis adalah sistem yang sedang berjalan pada ketujuh anak perusahaan Millenium.

Dimana ketujuh perusahaan tersebut bernaung di dalam satu *group*, yaitu Millenium Danatama Group (MDG). Berikut pertama-tama akan dibahas terlebih dahulu mengenai sejarah MDG lalu kemudian dilanjutkan dengan pembahasan lebih detil mengenai ketujuh anak perusahaan MDG yang menjadi objek utama dalam penelitian ini. Pada ketujuh perusahaan tersebut menggunakan mikrotik sebagai *router*nya. Mikrotik yang dipakai pada ketujuh perusahaan merupakan PC *router* yang diinstal *software* mikrotik. Untuk koneksi *internet* perusahaan di atas menggunakan koneksi *wireless* dimana MPR yang terletak di Gedung Millenium menggunakan jasa ISP PT Jasnita Telekomindo. APERDI, MDI, MPF, serta Gunung Mas terletak di Menara Kebon Sirih. PT. Finroll dan MGL terletak di Graha Millenium.

Keenam perusahaan yang berada pada kedua gedung tersebut menggunakan jasa ISP Biznet Networks. MPF dan APERDI mendapatkan bandwitdh 512 Kbps dan PT. Finroll, MGL, MDI, MPR, Gunung Mas mendapatkan 256 Kbps dari ISP. Selama ini, untuk melakukan transaksi data dan lainnya dari PT. Finroll ke perusahaan relasinya maupun sebaliknya hanya menggunakan jalur *public* yaitu *Internet*. *Internet* memiliki kekurangan dalam segi keamanan yang kurang baik.

Karena PT. Finroll menggunakan jaringan *public* untuk melakukan *transfer* data ke perusahaan relasinya, maka proses *transfer* data antar perusahaan menjadi tidak aman. Banyak alternatif yang ada untuk memecahkan masalah tersebut, salah satunya yaitu menggunakan *encryption email*. Proses ini sama sekali tidak memerlukan biaya Karena *software*nya gratis dan mudah didapat. Tetapi dengan menggunakan *encryption email*, PT. Finroll tidak dapat terhubung dengan jaringan internal perusahaan relasinya sehingga tidak dapat melakukan hubungan misalnya *chatting* antar LAN. Oleh karena itu, disarankan membuat sebuah jalur *private* antara PT. Finroll dengan perusahaan relasinya agar data yang dikirimkan tidak diketahui oleh pihak yang tidak diinginkan.

Dengan adanya jalur *private*, maka proses pengiriman data dapat melalui *file sharing*. Jalur *private* hanya dibuat untuk pengiriman data yang terjadi pada PT. Finroll ke perusahaan relasinya yang berada di gedung yang berbeda sedangkan untuk MGL yang berada di gedung yang sama dengan PT. Finroll, dilakukan proses *routing* biasa. Dengan cara menghubungkan antara jaringan perusahaan dengan *router* masing-masing dengan kabel UTP karena jarak yang antara dua perusahaan tersebut masih bisa ditempuh oleh kabel UTP.

Walaupun jaringan *VPN* ini memiliki kekurangan dari segi kecepatan pengiriman data dibandingkan alternative lainnya seperti WAN. Biasanya PT. Finroll melakukan proses pengiriman data seperti file-file dokumen, program-program, poster-poster dalam bentuk JPEG sebesar ±10 MB via *email*.

Karena data yang dikirimkan dari PT. Finroll relatif kecil ukurannya, maka PT. Finroll memerlukan *bandwidth* 128 Kbps dimana *bandwidth* tersebut dibagikan untuk lima jalur *tunneling*. PT. Finroll mendapatkan *bandwidth* 256 Kbps dari ISP maka

bandwidth untuk proses *VPN* disarankan tidak dibuat *dedicated* sehingga jika proses pengiriman data melewati jalur *tunneling* membutuhkan kapasitas *bandwidth* kurang dari 128 Kbps maka sisa *bandwidth* dapat dipakai untuk kebutuhan yang lain.

Selain itu *VPN* juga menggunakan *authentication*, *encapsulation*, dan *encryption* untuk memastikan keamanan dan integritas dari pengiriman data. Kemudahan untuk melakukan hubungan antara jaringan PT. Finroll dan perusahaan relasinya baik itu melalui *software-software* yang mendukung seperti pony chat, vpress chat. Namun *remote access VPN* memiliki kekurangan dalam hal *bandwidth* karena ada *bandwidth* yang terpakai untuk proses pembentukan jalur *tunnel*. Jalur *tunnel* akan selalu terbentuk baik ada atau tidaknya pengiriman data yang berlangsung antar PT. Finroll dengan relasinya.

Dalam perancangan ini, dipilih PPTP sebagai *protocol* yang digunakan untuk perancangan jaringan *remote access VPN* pada PT. Finroll. PPTP menggunakan *protocol* GRE (*Generic Routing Encapsulation*) untuk proses *encapsulation*, *protocol* MPPE (*Microsoft Point-to-Point Encryption*) untuk proses *encryption*, dan menggunakan *protocol* MS-CHAP2 (*Microsoft Challenge-Handshake Authentication Protocol* 2) untuk proses *authentication*.

Untuk menghubungkan jaringan PT. Finroll dan perusahaan relasinya maka perlu adanya proses *tunneling* antar perusahaan tersebut. Karena proses PPTP merupakan proses client-server maka proses tunneling hanya terjadi antara dua perusahaan saja. Karena ada lima perusahaan yang akan dihubungkan dengan PT. Finroll, maka diperlukan adanya lima proses *tunnel*. Topologi jaringan *VPN* yang ditinjau dari PT. Finroll dapat dilihat pada halaman berikut, dimana pada gambar terdapat lima proses *tunneling* yang bersumber dari PT. Finroll menuju ke perusahaan relasinya. Pertama-tama, kelima perusahaan relasi akan melakukan proses *dial-up* ke PT. Finroll untuk membentuk *tunnel*. Setelah tunnelnya terbentuk, proses *dial-up* yang dilakukan perusahaan lain itu akan bersifat permanen.

Dalam penelitian ini belum dilakukan implementasi secara langsung pada jaringan PT. Finroll dan relasinya, maka dibuat sebuah rancangan simulasi jaringan *VPN*

untuk melihat perbedaan *bandwidth* dan proses *encrypt* data yang terjadi. Beberapa peralatan yang dibutuhkan untuk menjalankan simulasi *VPN* ini antara lain :

1. Lima buah komputer yang terdiri dari :
    - 2 buah PC router yang diinstal Operating System Mikrotik
    - 1 buah PC router yang diinstal Operating System Windows Server 2003.
    - 2 buah komputer client yang Operating System Windows XP service pack 2.
2. Lima buah LAN Card yang terdiri dari :
    - 2 buah LAN card masing-masing pada 2 PC router yang diinstal MikrotikOS.
    - 2 buah LAN card masing-masing pada 1 PC router yang diinstal Windows Server 2003.

Simpulan yang dapat diambil dari penelitian ini adalah *Remote access VPN* dapat membantu PT. Finroll untuk membuat jalur dan komunikasi yang lebih aman dengan kelima perusahaan relasinya dengan proses *encrypt* pada setiap pengiriman datanya. Penggunaan *internet* sebagai media pembuatan jalur *tunnel* merupakan cara yang efisien karena tidak memerlukan biaya tambahan untuk proses pembuatan jalur *tunnel* dan pengiriman datanya.

PT. Finroll menggunakan mikrotik untuk proses routing pada jaringan internalnya, baik untuk mendapatkan internet dan *management bandwidth* sehingga tidak memerlukan *device* tambahan untuk *VPN* gateway maka lebih hemat dalam pengeluaran biaya untuk proses pembuatan *tunnel* antara PT. Finroll dan relasinya. Proses jalur tunnel tidak memerlukan *transfer rate* yang besar sehingga pemakaian *transfer rate* pada PT Finroll relative kecil untuk proses *tunnel* tersebut.

Semakin berkembangnya teknologi informasi maka otomatis sebuah jaringan pun semakin lama akan semakin besar. Oleh sebab itu diperlukan hardware *upgrade* pada PC router sehingga dapat menjalankan proses dengan sebagaimana mestinya.

Perlu dibuat sebuah domain server untuk menampung data-data yang dikirimkan baik dari PT. Finroll sendiri maupun relasinya sehingga dapat mempermudah komunikasi. Adanya penambahan aplikasi LAN *messenger* pada PT. Finroll dan relasinya dapat mempermudah komunikasi. Disarankan membuat sebuah jalur *alternative* baik itu dengan PC router ataupun dengan *router* karena apabila PC *router* utama sedang dilakukan *maintainance*, maka koneksi internet dan jalur *tunnel* pada PT. Finroll dapat terus berjalan