PERANCANGAN JARINGAN *WIDE AREA NETWORK* PADA PT. VIZTA PRATAMA CABANG JAKARTA DENGAN METODE VPN

Hasan Basri[1], Astriana Mulyani[2], Cahyani Budihartanti[3]
Program Studi Teknik Informatika – STMIK NUSA MANDIRI JAKARTA[1,2]
Program Studi Sistem Informasi – STMIK NUSA MANDIRI JAKARTA[3]
[1]hsbsri@gmail.com, [2]astriana.atm@nusamandiri.ac.id, [3]cahyani.cbh@nusamandiri.ac.id

Abstrak – PT. Vizta Pratama adalah perusahaan yang bergerak di bidang karaoke, yang sudah mempunyai banyak cabang yang tersebar di Indonesia. Area kantornya masih menggunakan sistem jaringan LAN sederhana dan belum adanya jaringan yang menghubungkan kantor pusat dengan kantor cabang. Perusahaan dalam melakukan pertukaran data masih secara manual atau melalui internet, sehingga sistem keamanan jaringan tersebut kurang terjamin. Untuk mengatasi masalah tersebut, maka dibuat sebuah sistem jaringan baru dengan menggunakan teknologi PPTP VPN agar dapat meningkatkan keamanan jaringan melalui metode enkripsi dan mempercepat proses pertukaran data. Perancangan tersebut melalui survei, studi literatur, identifikasi, evaluasi, uji coba yang dilakukan secara simulasi dan sudah berfungsi dengan baik sehingga diharapkan dapat mengatasi masalah yang ada pada perusahaan**.**

Kata Kunci : Jaringan komputer, Metode VPN. WAN

I. PENDAHULUAN

Semakin berkembangnya teknologi informasi sekarang ini, maka kebutuhan akan informasi semakin meningkat pula. 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, Akan tetapi permasalahan keamanan masih menjadi faktor utama. Untuk mengatasi masalah keamanan dalam komunikasi data pada jaringan umum (*public network / internet*) dengan menggunakan *Virtual Private Netork* (VPN).

VPN (*virtual private network*) merupakan salah satu alternatif untuk mengirimkan *voice*, ang bersifat *private* atau aman, karena penggunaan koneksi yang telah terenkripsi serta penggunaan *private keys*, *certificate*, *username* atau *password* untuk *authentikasi* dalam membangun koneksi.

Secara umum VPN merupakan suatu jaringan komunikasi lokal yang terhubung melalui media jaringan publik, insfrasktur publik yang paling banyak digunakan adalah jaringan internet. Didalam VPN terdapat perpaduan teknologi *tunneling* dan *enkripsi* ang membuat VPN menjadi teknologi yang handal untuk mengatasi permasalahan keamanan didalam jaringan.

Dalam implementasinya, VPN terbagi menadi *remote access* VPN dan *site-to-site* VPN. *Site-to-site* VPN digunakan untuk menghubungkan antara dua tempat yang letaknya berajuhan, seperti kantor pusat dengan kantor cabang. *Remote access* jenis VPN ini digunakan oleh pegawai perusahaan yang ingin terhubung ke jaringan lokal perusahaannya dari berbagai lokasi yang jauh.

II. TEKNIK PENGUMPULAN DATA

Metode pengumpulan data dilakukan secara langsung dari sumbernya baik melalui wawancara ataupun observasi pada PT. Vizta Pratama cabang Jakarta. Metode pengumpulan data yang digunakan dalam penelitian ini adalah staff personalia dan staff IT.

a. Observasi
   Observasi yaitu metode pengumpulan data yang dilakukan dengan cara pengamatan secara langsung terhadap suatu kegiatan yang sedang dilakukan. Hal yang penulis lakukan selama melakukan observasi adalah mencatat perangkat keras dan perangkat lunak yang digunakan untuk membangun jaringan di PT.Vizta Pratama Cabang Jakarta.
b. Wawancara
   Wawancara yaitu metode pengumpulan data yang dilakukan dengan cara bertatap muka langsung atau menayakan secara langsung dengan orang –orang yang terlibat didalam objek yang sedang di amati. Dalam hal ini penulis melakukan wawancara dengan karyawan pada perusahaan tersebut selaku staff IT di perusahaan tersebut.
c. Studi Pustaka
   Dalam metode ini penulis menggunakan buku-buku sebagai acuan dan referensi sesuai dengan permasalahan yang ada. Buku yang penulis gunakan sebagai referensi dalam penelitian ini.

III. DASAR TEORI

Konsep Dasar Jaringan

Jaringan komputer (*Computer Network*) adalah suatu himpunan interkoneksi sejumlah komputer *automous.* Dalam bahasa populer dapat di jelaskan bahwa jaringan

komputer adalah kumpulan beberapa komputer yang saling berhubungan satu sama lain melalui media perantara. Media perantara ini bisa berupa kabel atau tanpa kabel (*nirkabel*) [1]. Informasi berupa data dapat mengalir dari satu komputer ke komputer lainnya atau dari satu perangkat ke perangkat yang lainnya sehingga masing-masing komputer terhubung tersebut bisa saling bertukar data

VPN

Menurut Athailah mengemukakan bahwa VPN (*Virtual Private Network*) suatu cara untuk membuat sebuah jaringan *private* (pribadi) secara aman dengan menggunakan jaringan publik, VPN dapat melewati jaringan publik seakan akan terhubung secara *point to point*, yang berisi informasi *routing* untuk mendapatkan koneksi *point to point* sehingga dapat melalui jaringan publik sampai ke tujuan [2]. Sedangkan untuk mendapatkan hubungan yang bersifat *private*, data yang dikirim harus dienkripsi terlebih dahulu untuk menjaga kerahasiannya sehingga paket yang tertangkap ketika melewati jaringan publik tidak dapat terbaca karena harus melewati proses *dekripsi*, proses enkapsulasi data ini sering disebut dengan *tunneling.*

Topologi Jaringan

Menurut Herlambang, dkk mengemukakan bahwa *Topologi* atau arsitektur jaringan merupakan pola hubungan antar terminal dalam suatu sistem jaringan computer [3]. *Topologi* ini akan memengaruhi tingkat efektifitas kinerja jaringan. Ada beberapa jenis topologi yang dapat diimplementasikan dalam jaringan. Namun, bentuk topologi yang utama adalah topologi bus, topologi ring, dan topologi star.

Topologi fisik merupakan *layout* aktual dari kabel (media) jaringan. Topologi yang umum digunakan dalam membangun sebuah jaringan adalah sebagai berikut:

a. Topologi *Ring*.
   Sesuai dengan namanya, *ring* atau cicin, seluruh komputer dalam jaringan terhubung pada sebuah jalur data yang menghubungkan komputer satu dengan komputer lainnya secara berkesinambungan sedemikian rupa sehingga menyerupai semacam cicin.
b. Topologi mesh.
   Topologi mesh sering disebut "*pure to peer*", sebab merupakan suatu implementasi suatu jaringan komputer yang menghubungkan seluruh komputer secara langsung. Topologi ini digunakan pada kondisi dimana tidak ada komunikasi terputus secara absolut antar *node* komputer.Topologi ini merefleksikan desain yang memiliki *multi path* ke berbagai lokasi.Saat ini sangat jarang digunakan sebab sangat rumit dan tidak praktis.
c. Topologi *Star*
   Dalam topologi ini masing-masing komputer dalam jaringan dihubungkan ke sebuah konsentrator atau poin sentral. Poin ini umumnya berupa *hub* atau *switch* dihubungkan dengan menggunakan jalur yang berbeda-beda, sehingga jika salah satu komputer mengalami gangguan, maka jaringan tidak terpengaruh. Hal ini juga memungkinkan pengaturan instalasi jaringan yang lebih fleksibel dan kecepatan komunikasi data yang lebih baik dibanding topologi yang lain (*bus*, dan *ring).*
d. Topologi *Tree.*
   Topologi ini disebut juga topologi jaringan bertingkat. Topologi ini biasanya digunakan untuk interkoneksi antar sentral dengan hierarki yang berbeda. Untuk hierarki yang lebih rendah digambarkan pada lokasi yang rendah dan semakin ke atas mempunyai hierarki semakin tinggi.
e. Topologi *Bus.*
   Topologi *Bus* merupakan topologi yang menghubungkan semua terminal ke satu jalur komunikasi yang kedua ujungnya ditutup dengan terminator. Topologi ini menghubungkan komputer secara berantai *(daisy-chain)*, informasi yang dikirim akan melewati semua terminal pada jalur tersebut. Jika alamat yang tercantum atau informasi yang dikirim sesuai dengan alamat terminal yang dilewati, maka data atau informasi tersebut akan diterima dan diproses, jika alamat tersebut tidak sesuai, maka informasi tersebut akan diabaikan oleh terminal yang dilewati.

IP Address

Herlambang, dkk mengemukakan bahwa IP *Address*(*Internet protocol Address)* adalah pengenal yang digunakan untuk memberi alamat pada tiap tiap komputer dalam jaringan. IP *Address* merupakan representasi dari 32 bit bilangan biner yang ditampilkan dalam bentuk desimal, terdiri atas beberapa segmen, dan tiap segmen terdiri atas 8 bit .

IV. HASIL DAN PEMBAHASAN

Untuk menghadapi permasalahan yang sedang dihadapi oleh PT. Vizta Pratama Cabang Jakarta dengan menggunakan teknologi VPN. Penggunaan teknologi VPN pada jaringan PT. Vizta Pratama Cabang Jakarta akan merubah topologi yang sudah ada pada jaringan tersebut. Perubahan topologi tersebut hanya penambahan router yang nanti akan berfungsi ngsebagai *gateway* (gerbang).

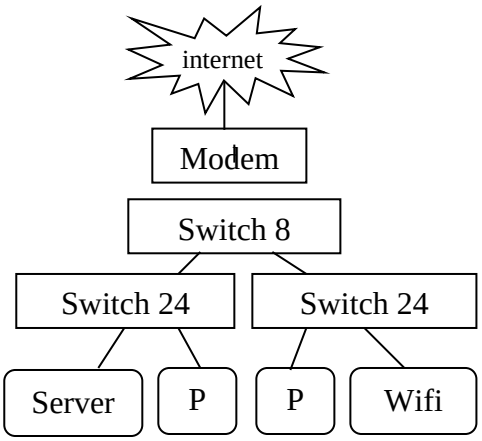
Tipe VPN yang akan digunakan adalah *site-to-site internet* VPN, karena yang akan dihubungkan degan menggunakan teknologi VPN adalah jaringan kantor-kantor cabang dan jaringan kantor pusat, dimana ini merupakan jaringan yang lokasinya tetap, tidak berpindah-pindah. Jaringan-jaringan yang akan dhubungkan hanya merupakan jaringan internal perusahaan saja yaitu kantor pusat dan kantor-kantor cabang, tidak menghubungkan jaringan diluar perusahaan.

Dengan *site-to-site* intranet VPN jaringan pusat dan kantor cabang menjadi satu jaringan internal perusahaan sehingga akan mempermudah untuk *memonitoring* pada jaringan kantor cabang. Untuk mengatasi pengembangan jaringan VPN dalam penambahan kantor cabang, dibutuhkan penambahan router yang berfungsi sebagai

gateway (gerbang) pada kantor cabang untuk menghubungkan dengan kantor pusat.

Topologi Jaringan

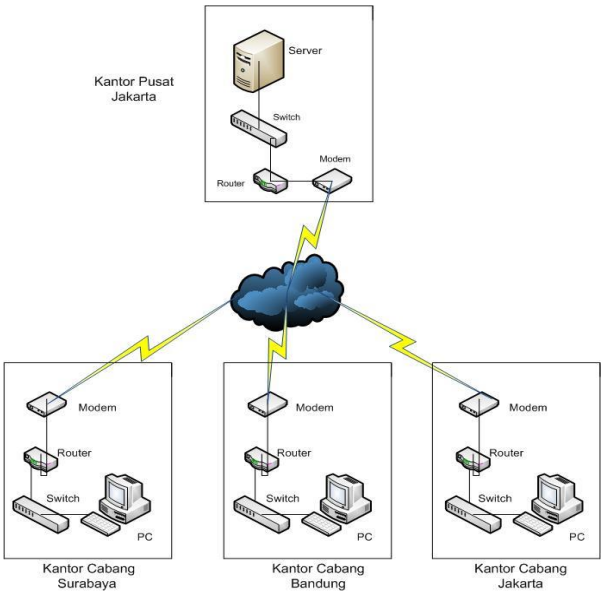
Topologi yang di digunakan pada PT. Vizta Pratama Cabang Jakarta adalah *topologi star* setiap *workstation* harus dihubungkan ke *file server*, jadi terminal pusat bertindak sebagai pengatur dan pengendali semua data komunikasi yang dikirim melalui *server*, terminal pusat akan menyediakan jalur komunikasi khusus pada dua terminal yang akan berkomunikasi. Pada *topologi* ini dibutuhkan *switch* untuk menghubungkan semua komputer supaya menjadi terpusat, berikut ini topologi yang digunakan di PT. Vizta Pratama Cabang Jakarta.



Gambar 1. Topologi Jaringan Sebelum VPN

Topologi Jaringan Usulan

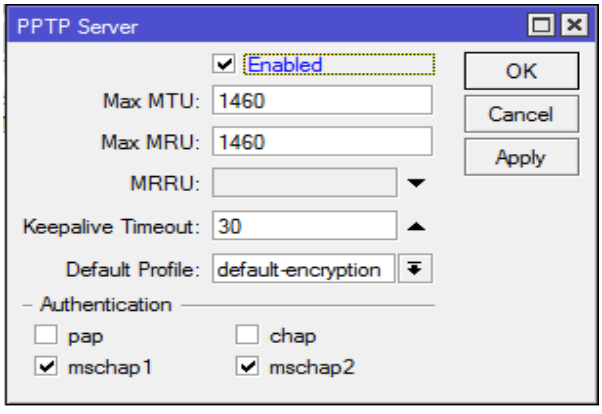
Topologi VPN yang penulis usulkan adalah topologi *hub and spokes.* Karena dari proses cara kerja jaringan pada PT. Vizta Pratama Cabang Jakarta, pertukaran data hanya diperlukan antar kantor pusat dan kantor-kantor cabang, walaupun kadang bisa terjadi pertukaran data antara kantor-kantor cabang, itu dikarenakan kantor cabang tidak mempunyai data yang selalu ter-*update* dari kantor pusat. Setelah kantor pusat dan kantor-kantor cabang dapat mendapatkan data yang ter-*update* dan tidak diperlukan lagi adanya pertukaran data antara kantor-kantor cabang. Ini menjadikan kantor pusat sebagai cetral *site (hub)* dan kantor-kantor cabang sebagai *remote office (spokes). Topologi hub and spokes* juga mudah untuk dikembangkan jika terdapat kantor cabang yang baru dari berbagai kota yang ingin dihubungkan dengan kantor pusat.



Gambar 2. Topologi Jaringan Usulan Menggunakan VPN

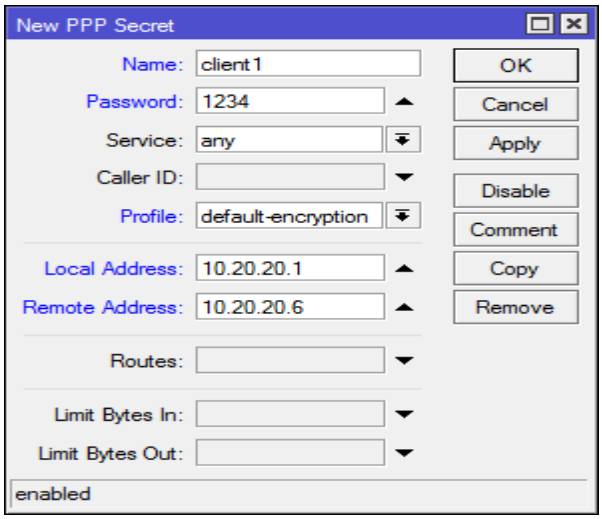
a. Konfigurasi PPTP Server

Berdasar *topologi* di atas, yang menjadi pusat dari *link* PPTP adalah *router* pada kantor pusat, maka harus melakukan *setting* PPTP *server* pada *router* tersebut. Langkah pertama yang harus dilakukan adalah mengaktifkan PPTP *server*. Masuk pada menu PPP, Interface, PPTP *server*. Gunakan *profile Default-encryption* agar jalur VPN terenkripsi. Pada tahap ini, untuk mengaktipkan *secret* agar bisa menentukan *username* dan *password* untuk proses *autentikasi client* yang akan terkoneksi ke PPTP *server*.



Gambar 3. Mengaktifkan PPTP *Server*

Penggunaan huruf besar dan kecil akan berpengaruh. *Local Address* adalah alamat IP yang akan terpasang pada *router* itu sendiri (Router kantor pusat / PPTP *server*) setelah *link* PPTP terbentuk *Remote Address* adalah alamat IP yang akan diberikan ke *client* setelah *link* PPTP terbentuk. Contoh konfigurasi sebagai berikut, arahkan agar menggunakan *profile Default-Encryption.*

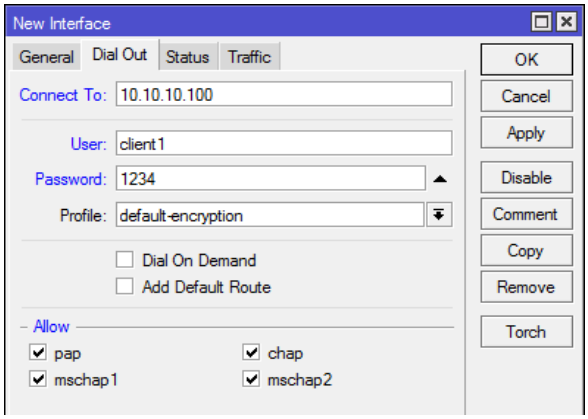


Gambar 4. Konfigurasi Mengaktifkan *Secret*

Sampai disini, konfigurasi *router* kantor pusat (PPTP *Server*) sudah selesai. Berikutnya sekarang kita lakukan konfigurasi pada sisi client Router Bandung, Jakarta, Surabaya.

b. Konfigurasi PPTP *Cilent*

Langkah-langkah untuk melakukan konfigurasi *client* PPTP pada *router* mikrotik adalah sebagai berikut Tambahkan *interface* baru PPTP *client*, lakukan *dial* ke IP Public *router* kantor pusat (PPTP *server*) dan masukkan *username* dan *password* sesuai pengaturan *secret* PPTP *server*.



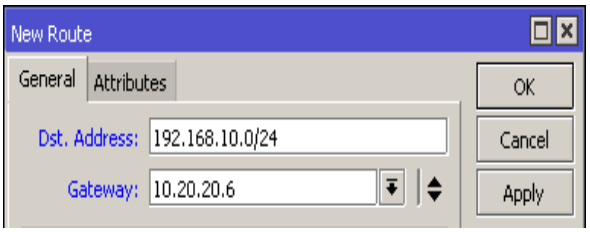
Gambar 5. Konfigurasi VPN *Client*

Catatan IP 10.10.10.100 adalah ip *public* dari *router server* kantor pusat. Setelah koneksi PPTP terbentuk, akan muncul IP *Address* baru di kedua *router* dengan *flag* D yang menempel di *interface* pptp sesuai dengan pengaturan *secret* pada PPTP *server*. Sampai disini koneksi VPN antar *router* sudah terbentuk, akan tetapi antar jaringan lokal belum bisa saling berkomunikasi.

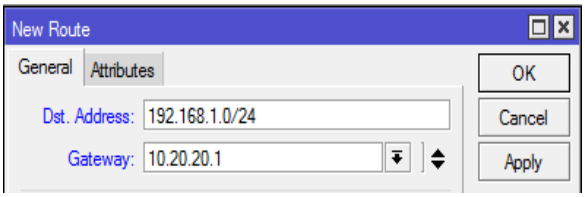
c. Konfigurasi *Routing Static*

Agar antar jaringan lokal bisa saling berkomunikasi, kita perlu menambahkan *routing static*. Berikut ini adalah konfigurasi *routing static*.

a. Dst-*Address* : jaringan lokal *router* kantor cabang
b. *Gateway* : IP PPTP *tunnel* pada kedua *router*.

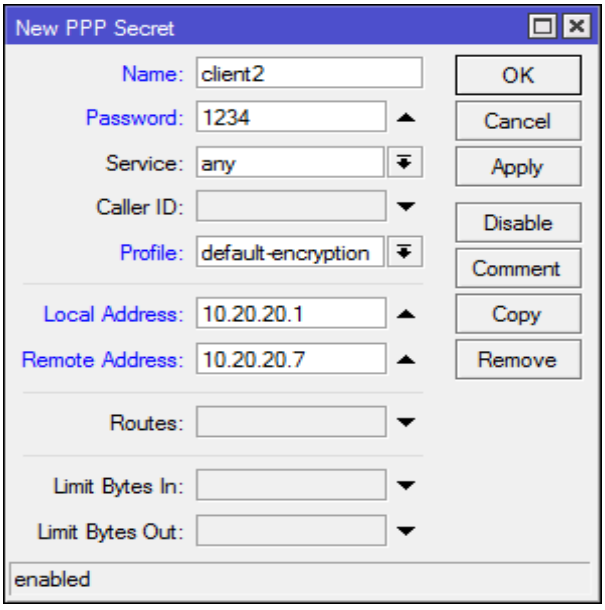


Gambar 6. Konfigurasi *Static Route* Kantor Pusat



Gambar 7. Konfigurasi *Static Route* Kantor Cabang

Client PPTP tidak harus menggunakan *router*. Seperti pada *topologi* jaringan di atas, ada sebuah *Remote Client* (Laptop) yang akan melakukan koneksi VPN ke *router* kantor pusat, maka kita perlu membuat *secret* baru pada PPTP *server* untuk melakukan *autentikasi remote client* tersebut. *Username* = *client2* *Password* = 1234, *Local Address* = 192.168.2.2, *Remote Address* = 192.168.2.72 .

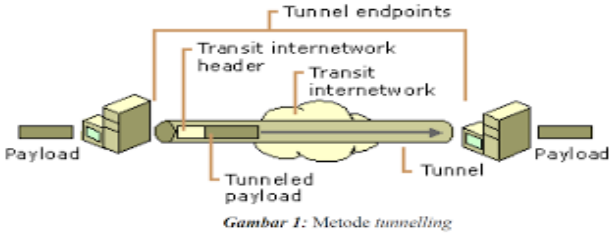


Gambar 8. Konfigurasi *Secret Remote Client*

Kemudian kita perlu melakukan konfigurasi PPTP c*lient* pada Laptop. langkah-langkahnya akan berbeda pada tiap OS (*system operasi*).

d. Keamanan Jaringan

Karena media penghubung antar jaringannya adalah jaringan publik, diperlukan pengamanan dan pembatasan-pembatasan. Pengamanan diperlukan untuk menjaga agar tidak sembarang orang dari jaringan publik dapat masuk ke jaringan pribadi. Yang dikecualikan untuk dapat masuk ke jaringan pribadi hanyalah orang-orang yang terdaftar atau terautentifikasi terlebih dahulu, Pembatasan diperlukan untuk menjaga agar tidak semua orang atau *user* dari jaringan pribadi dapat mengakses jaringan publik (*internet*). Salah satu cara untuk membangun VPN adalah dengan metode *tunneling*. Sesuai dengan arti *tunnel* (lorong), cara membentuk suatu VPN dengan cara ini adalah dengan membuat suatu *tunnel* di dalam jaringan publik untuk menghubungkan antara jaringan yang satu dan jaringan lain dari suatu grup atau perusahaan yang ingin membangun VPN tersebut. Seluruh komunikasi data antar jaringan pribadi akan melalui *tunnel* ini, sehingga orang atau *user* dari jaringan publik yang tidak memiliki izin untuk masuk tidak akan mampu untuk menyadap, mengacak atau mencuri data yang melintasi *tunnel* ini. Di dalam *tunneling* terdapat proses *enkapsulasi*, transmisi dan *dekapsulasi* paket yang dikomunikasikan, Metode *tunneling* dapat digambarkan secara ringkas sebagai berikut.



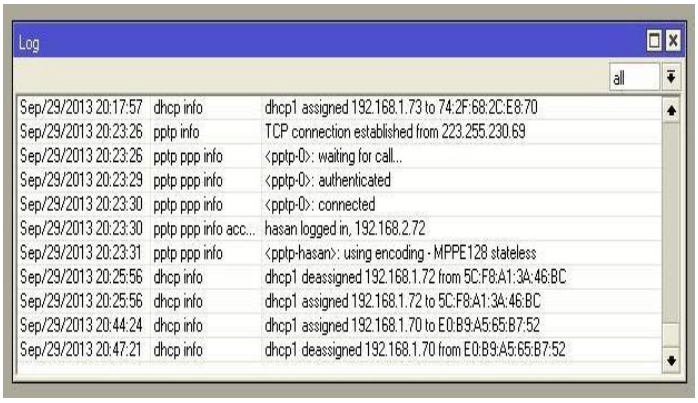
Gambar 1: Metode *tunnelling*

Gambar 9. *Proses Tunneling* Menggunakan PPTP

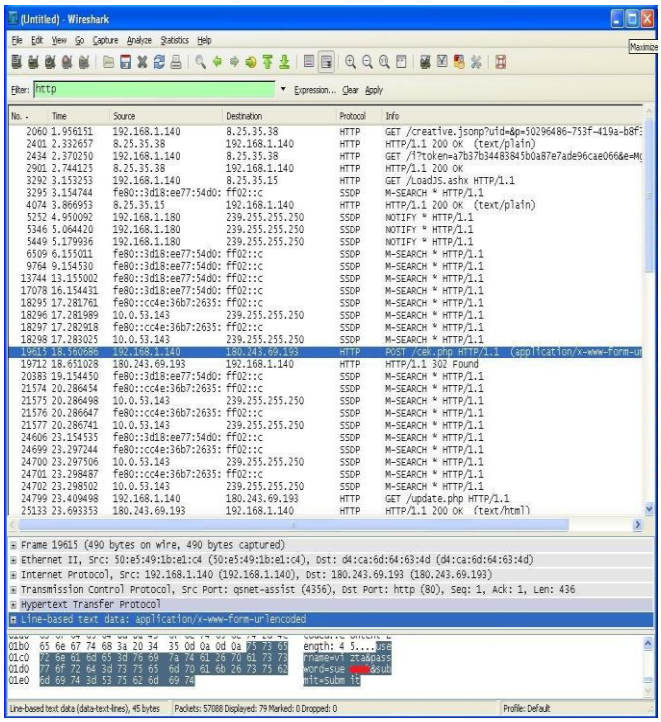
Teknologi *tunneling* dikelompokkan secara garis besar berdasarkan protokol *tunneling layer* 2 (*Data Link Layer*) dan layer 3 (*Network Layer*) model OSI *layer*. Yang termasuk ke dalam *tunneling layer* 2 adalah L2F, PPTP, dan L2TP.

Pengujian Jaringan

Pada sisi client, jaringan di hubungkan dengan mengisi ip public server VPN. Jika berhasil maka client akan di berikan *ip* oleh server berdasarkan *user client* yang dipakai. Jika sudah *connected*, maka vpn sudah dikatakan berhasil. Pada saat client menekan tombol *connected* maka jalur telah di *enkapsulasi* oleh *protocol pptp*. Dan proses selanjutnya ialah dengan mengetikan alamat url localhost yang ada dijaringan *local*.

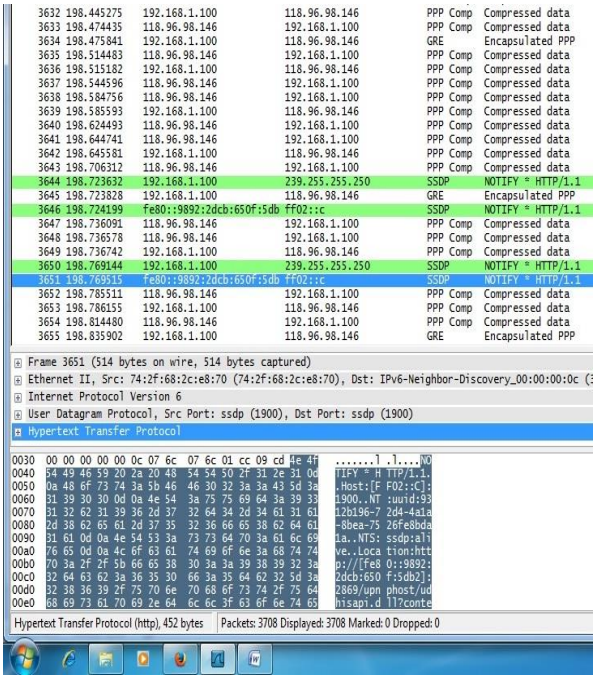


Gambar 10. Proses Autentikasi VPN pada mikrotik



Gambar 11. Hasil *capture* tanpa VPN dengan *wireshark*

Pada gambar terlihat jelas semua aktifitas yang dilakukan jaringan ini *tercapture* dengan *wireshark*. Oleh karena itu diperlukan adanya *enkapsulasi* data semua aktifitas dunia internet. Dengan menerapakan VPN maka elemen *autentikasi* dan *protocol* tersebut akan di *enkapsulasi* (dibungkus). Dalam proyek akhir ini digunakan VPN untuk mengenkapsulasi data. Berikut gambar hasil *monitoring* pada *tools wireshark* pada jaringan VPN yang terkoneksi dengan jaringan *local* di mana VPN *server* berada.



Gambar 12. Hasil *capture* setelah menggunakan VPN

Pada gambar terlihat jelas semua aktifitas yang dilakukan jaringan ini *tercapture* dengan *wireshark*. Sangat terlihat jelas perbedaannya pada hasil *capture* tersebut setelah menggunakan VPN semua aktifitas yang terjadi secara *otomatis* akan ter-enkapsulasi sehingga *username* dan *password* tidak terbaca karena sudah di-*enkapsulasi*. Sehingga membuat data yang melewati jaringan akan lebih aman

V. SIMPULAN

Kesimpulan yang dapat diambil setelah menjelaskan secara terperinci sejauh mana infrastruktur jaringan yang ada pada perusahaan ini, tentunya banyak hal yang bisa disimpulkan, di antarannya:

a. Pembangunan jaringan VPN di perusahaan mampu meningkatkan efisiensi waktu untuk mengakses jaringan LAN pada lokasi yang berbeda. Sehingga memberikan kemudahan kantor-kantor cabang untuk mendapatkan data ter-*update* dari kantor pusat dan sebaliknya.
b. Dengan menggunakan teknologi VPN, perusahaan tidak perlu mengeluarkan banyak biaya untuk menghubungkan jaringan LAN yang berbeda lokasinya. Karena tidak perlu menggunakan jasa dari provider yang biayanya sangat mahal untuk menghubungkan jaringan LAN tersebut, karena dengan menggunakan jaringan VPN cukup menggunakan koneksi internet untuk mengakses *server* VPN tersebut.
c. Pembangunan VPN diharapkan mampuh membuat jaringan perusahaan menjadi lebih fleksibel.

VPN merupakan solusi yang baik untuk implementasi pada perusahaan yang sedang berkembang, untuk menghubungkan beberapa kantor cabang supaya proses tukar data bisa lebih cepat dan aman.

DAFTAR PUSTAKA

[1] Sopandi D, 2007. Menggunakan MikroTik RouterOS™ , ANDI Publisher : Yogyakarta.
[2] Athailah. 2013. Panduan Singkat Menguasai Router. Jakarta. MediaKita.
[3] Herlambang, Moch. Linto dan Catur L, Azis. 2008. Panduan Lengkap Menguasai Router Masa Depan. Yogyakarta. C.V Andi Offset