PENERAPAN JARINGAN *VIRTUAL PRIVATE NETWORK* UNTUK KEAMANAN KOMUNIKASI DATA BAGI PT. MEGA TIRTA ALAMI

Heru Supriyono [1] *, Jisnu Adi Widjaya* [2] *dan Agus Supardi* [1]

[1] Program Studi Teknik Elektro – Fakultas Teknik

[2] Program Studi Teknik Informatika - Fakultas Komunikasi dan Informatika

Universitas Muhammadiyah Surakarta

Email : Heru.Supriyono@ums.ac.id

ABSTRACT

PT. Mega Tirta Alami is a company engaged in the production and distribution of pured bottled drinking water with the brand "AXOGY". This is a fast growing company and now it has 42 branches in major cities spread throughout the island of Java, Sumatra and Bali. Currently, PT. Mega Tirta Alami using electronic mail (email) to transmit company's important data including financial data. By using email, the data are transmitted throughout public communication network and is vulnerable to various security threat. This problem could be solved by using a virtual private network (VPN) as data transmission channel. This paper discusses design and implementation of VPN for PT Mega Tirta alami which connect the head office to two the branch offices: Branch-1 (Bandung) and Branch-2 (Bekasi). The VPN was implemented using point to point tunneling protocol (PPTP) by using three Mikrotik routers. There is only few changes in the computer network configuration to minimize both implementation cost and time. Prior to make any data communication to the head office, user in Branch-1 or Branch-2 must provide username and password as part of verification and validation process. The newly developed VPN was tested on various technical aspects to ensure its reliability and operability. The test results showed that the VPN connected between from head office to Branch-1 and from head office to Branch-2. To maintain the security, the direct connection between Branch-1 and Branch-2 via developed VPN is strictly forbidden.

Kata kunci: *virtual private network, VPN, PPTP, mikrotik*.

PENDAHULUAN

PT. Mega Tirta Alami adalah perusahaan yang bergerak dalam bidang produksi dan distribusi air minum murni kemasan dengan merk "AXOGY" yang kantor pusatnya berada di daerah Tegalmulyo, Kelurahan Pabelan, Kecamatan Kartasura, Kabupaten Sukoharjo. Saat ini PT. Mega Tirta Alami sudah berkembang hingga mempunyai 42 kantor cabang yang tersebar di berbagai pulau di Indonesia meliputi Jawa, Sumatera dan Bali. Dalam kegiatan bisnis sehari-hari, semua kantor cabang selalu berkomunikasi dengan kantor pusat untuk mengirimkan data-data perusahaan seperti data-data penjualan, data-data stok barang

dan yang yang sangat penting adalah data laporan keuangan. Data-data perusahaan adalah termasuk informasi yang rahasia yang harus dijaga keamanannya. Keamanan data yang diperlukan meliputi perlindungan data dari hilang dicuri orang lain, perlindungan data dari diubah oleh orang lain yang tidak berhak, perlindungan data dari rusak (sebagai contoh tidak dapat dibuka/diakses) dan bahkan perlindungan data dari dibaca oleh orang lain yang tidak berhak. Kondisi saat ini, PT. Mega Tirta Alami menggunakan surat elektronik (*electronic mail*/email) untuk mengirimkan data-data perusahaan. Teknologi surel mempunyai kelebihan cepat, yaitu data dikirimkan secara real time, mudah dan sangat murah karena banyak website yang menyediakan layanan surel gratis seperti www.yahoo.com, www.google.com dan lainnya. Kelemahan surel adalah pada potensi ancaman keamanannya. Karena layanan surel melewati jalur internet publik, maka rentan terhadap kemungkinan ancaman pembajakan email dimana orang yang tidak berhak menguasai email perusahaan sehingga perusahaan kehilangan semua data-data perusahaan yang bersifat rahasia. Alternatif solusi yang bisa ditempuh oleh PT. Mega Tirta Alami adalah dengan menggunakan jaringan *virtual private network* (VPN) untuk komunikasi data perusahaan antara kantor cabang dan kantor pusat. VPN bisa dipandang seperti sebuah jaringan pribadi yang menghubungkan antara satu titik dengan titik yang lain (Astawa dkk, 2012). Sehingga, dengan menggunakan VPN, hanya data-data perusahaan PT. Mega Tirta Alami saja yang melewati jalur itu sehingga keamanan data-data perusahaan bisa dilindungi.

Berdasarkan analisis situasi dan studi pustaka untuk penyelesaian permasalahan pengiriman data-data perusahaan di PT. Mega Tirta Alami maka permasalahan yang akan diselesaikan adalah bagaimana merancang dan mengimplementasikan jaringan VPN untuk kantor PT.Mega Tirta Alami yang akan menghubungkan kantor pusat dan kantor cabang. Jaringan VPN akan diimplementasikan dengan menggunakan metode *point to point tunelling protocol* (PPTP).

1. Jaringan *virtual private network* (VPN)

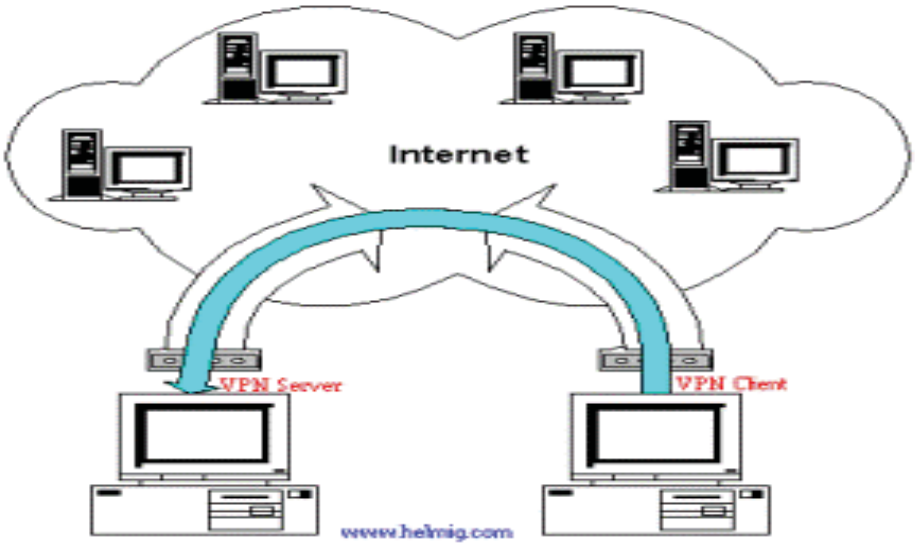
Dalam dunia internet, apabila titik A melakukan komunikasi dengan titik B maka data komunikasi akan dilewatkan jalur publik. Ilustrasinya adalah apabila seseorang dari kota A akan pergi ke kota B dengan mengendarai mobil atau motor maka dia akan melalui jalan umum yang digunakan oleh semua orang pengguna jalan raya. Karena menggunakan jalur publik dimana semua paket data dilewatkan, maka komunikasi pada jaringan komputer atau lewat internet rentan dengan ancaman keamanan yang dapat berupa hilangnya data baik sebagian atau seluruhnya dalam perjalanan, rusaknya data sehingga tidak dapat dibuka, data dibajak kemudian diubah oleh orang yang tidak berhak sehingga penerima akan menerima data yang salah maupun hanya sekedar disadap yaitu orang yang tidak berhak bisa mendengar atau membaca data yang dikirimkan.

VPN banyak digunakan untuk meningkatkan keamanan data-data komunikasi yang bersifat rahasia. Pada prinsipnya, VPN merupakan sebuah sambungan komunikasi yang bersifat pribadi dan dilakukan secara virtual. Secara sederhana VPN ini bisa dipandang sebagai pembuatan jalur komunikasi data untuk pribadi pada jaringan internet publik (Tanenbaum, 2003). VPN biasa disebut jaringan pribadi karena hanya data-data komunikasi pemilik yang berhak saja yang bisa lewat. Ilustrasi sebuah VPN adalah seperti dijalan raya yang kemudian dibuatlah jalur khusus untuk bus misalnya busway sehingga hanya bus saja yang boleh lewat

pada jalur itu. Secara teknis secara sederhana VPN bisa dilakukan dengan memanfaatkan enkripsi data pada jalur komunikasi sehingga hanya titik yang mempunyai *password* enkripsi yang berhak melakukan komunikasi (Ghozali, 2010; Stiawan & Palupi, 2009). Dengan cara ini komunikasi data akan lebih terjamin keamanannya.

2. Point to Point Tunneling Protocol (PPTP)

Pont to Point Tunneling Protocol (PPTP) adalah sebuah metode komunikasi data atau protokol yang memungkinkan terjadinya komunikasi anatara titik pada jaringan internet dengan membuat VPN. Pada metode PPTP, VPN membutuhkan sebuah server yang berfungsi sebagai penghubung antar komputer yang biasa disebut dengan client, baik komputer yang berada di kantor pusat maupun komputer yang berada di kantor cabang. Secara fisik server sebuah VPN dapat berupa komputer (biasanya berupa sebuah *personal computer* /PC) yang sudah di*install* dan diset dengan perangkat lunak VPN atau dapat berupa sebuah router. Secara teknis komunikasi antara komputer di kantor cabang dengan komputer di kantor pusat dilakukan melalui beberapa langkah yaitu pertama-tama komputer yang berada di kantor cabang akan mengontak server dan memasukkan username dan password. Selanjutnya server VPN akan melakukan verifikasi username dan password dari komputer client tersebut, apabila sesuai dengan data yang berada di server maka server akan memberikan sebuah alamat *internet protocol* (IP address) untuk komputer tersebut dan sebuah tunnel baru terbentuk sehingga kantor cabang bisa berkomunikasi dengan kantor pusat. Setelah jalur komunikasi VPN terbentuk maka komputer cabang dapat mengirimkan data ke kantor pusat atau melakukan pekerjaan lain seperti melakukan *remote desktop*. Gambaran umum arsitektur jaringan VPN dengan metode PPTP diilustrasikan pada Gambar 1.



Gambar 1. Ilustrasi arsitektur jaringan VPN dengan metode PPTP (diambil dari: http://teknodaninfokita.blogspot.com/2014/02/pengertian-vpn-dan-fungsinya.html)

3. Router

Pada prinsipnya secara teknis *router* adalah sebuah perangkat dalam jaringan komputer yang fungsinya adalah untuk menyalurkan data dari komputer asal ke komputer tujuan. Secara sederhana proses bekerjanya router adalah apabila ada paket data yang diterima oleh *router* dari komputer client maka router akan membaca alamat *internet protocol* (IP) asal paket data tersebut dan kemudian membaca alamat IP tujuan kemana paket data itu akan dikirimkan. Setelah router membaca alamat tujuan sebuah paket data maka kemudian *router* dapat memilih jalur mana yang harus dilalui oleh paket data tersebut agar sampai ke tempat tujuan dengan waktu yang paling optimal. Fungsi lain dari *router* adalah untuk mengelola sebuah jaringan termasuk mengatur berapa besar alokasi *bandwidth* untuk sebuah jaringan.

Tujuan utama dilakukannya kegiatan ini adalah untuk merancang dan mengimplementasikan jaringan VPN yang diharapkan bisa memberikan alternatif solusi pada keamanan komunikasi data antara kantor pusat dan kantor cabang pada PT. Mega Tirta Alami.

Manfaat yang diperoleh dari keberhasilan kegiatan ini adalah diperolehnya sebuah jaringan VPN yang diharapkan dapat menjadi alternatif solusi untuk meningkatkan keamanan komunikasi data antara kantor cabang dan kantor pusat pada PT Mega Tirta Alami.

METODE PELAKSANAAN

1. Waktu Dan Tempat

Semua tahapan kegiatan dilaksanakan sekitar 3 bulan yaitu bulan Juni sampai Agustus 2013. Tahap perancangan direncanakan dilakukan di Laboratorium Jaringan Komputer Program Studi Teknik Informatika Fakultas Komunikasi dan Informatika Universitas Muhammadiyah Surakarta sedang implementasi dan pengujiannya dilaksanakan di kantor PT.Mega Tirta Alami.

2. Peralatan Utama

Dalam kegiatan ini dibutuhkan beberapa piranti atau peralatan yang dapat berupa perangkat keras komputer maupun perangkat lunak komputer. Daftar peralatan yang digunakan dalam kegiatan ini dapat dilihat pada Tabel 1.

Tabel 1.
Daftar peralatan utama yang digunakan dalam kegiatan

No	Nama	Jumlah	Keterangan
1	Laptop	1	Untuk Konfigurasi
2	PC	1	Untuk *Server*
3	*Router* Mikrotik RB 450G	1	Untuk konfigurasi jaringan VPN *server*
4	*Router* Mikrotik RB 750	2	Untuk konfigurasi jaringan VPN *client*
5	Winbox	1	Untuk konfigurasi Mikrotik
6	MS.visio	1	Untuk pembuatan topologi

3. Tahapan Pelaksanaan Kegiatan

Kegiatan dilaksanakan dengan beberapa tahap sebagai berikut:

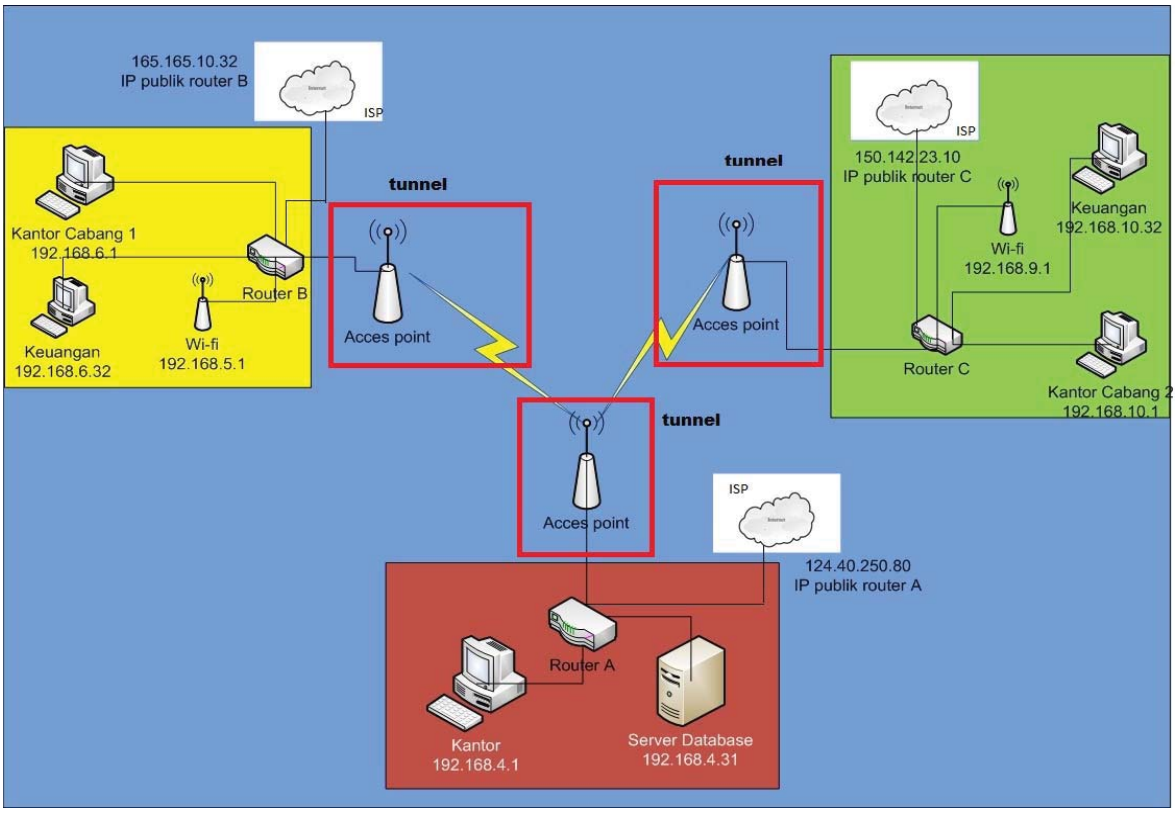
a. Tahap I: analisis kebutuhan.

Pada tahap ini dilakukan analisis secara teknis permasalahan apa yang dihadapi oleh PT. Mega Tirta Alami. Analisis dilakukan dengan metode wawancara dengan pimpinan perusahaan dan staf teknis bagian teknologi informasi. Selain itu analisis dilakukan dengan cara menginventarisir kondisi teknologi informasi yang ada dikantor pada saat ini untuk memastikan bahwa solusi yang akan ditawarkan tidak akan banyak mengubah kondisi jaringan komputer yang sudah ada di PT Mega Tirta Alami baik arsitektur/konfigurasi jaringannya maupun peralatannya karena semakin banyak pengubahan yang dilakukan maka akan semakin banyak biaya yang harus dikeluarkan oleh perusahaan.

b. Tahap II: merancang topologi jaringan VPN.

Walaupun pada saat ini PT. Mega Tirta Alami memiliki 42 kantor cabang yang tersebar di berbagai kota di beberapa pulau, namun pada kegiatan ini untuk sementara hanya dua kantor cabang saja, yaitu kantor cabang I yang berada di

Bandung dan Kantor Cabang II yang berada di Bekasi, yang akan dihubungkan dengan kantor pusat menggunakan jaringan VPN. Alasan pemilihan dua buah kantor cabang ini adalah karena untuk semestara dua kantor cabang ini yang mempunyai transaksi paling besar sehingga yang paling membutuhkan terhubung jaringan VPN dibandingkan dengan kantor cabang yang lain. Rancangan arsitektur/topologi jaringan yang diusulkan untuk PT. Mega Tirta Alami dapat dilihat pada Gambar 2



Gambar 2. Rancangan topologi VPN untuk PT.Mega Tirta Alami

Pada prinsipnya, PT. Mega Tirta Alami tetap berlangganan internet dari sebuah penyedia internet atau yang dikenal dengan internet service provider (ISP). Kemudian, VPN dibuat dengan membuat "terowongan" (*tunnel*) dari kantor cabang ke kantor pusat sehingga semua data dari kantor cang ke kantor pusat akan melewati "terowongan" yang sudah dibuat. Untuk keperluan pembuatan VPN maka di kantor pusat dan di kantor cabang diberi router pada titik masuk jaringan internet. Pada Gambar 2. *router-router* yang digunakan diberi notasi *Router* A adalah router yang dipasang pada kantor pusat, *Router* B adalah router yang dipasang di kantor cabang I yang berada di Bandung Jawa Barat, dan *Router* C adalah router yang dipasang pada kantor cabang II yang berada di Bekasi Jawa Barat. *Router* yang digunakan adalah Mikrotik 450G untuk kantor pusat dan Mikrotik RB 750 untuk masing-masing kantor cabang. Sebenarnya dipasaran terdapat banyak *router* yang tersedia seperti seri Cisco atau vendor ternama lainnya, namun dalam pelaksanaan kegiatan ini *router* Mikrotik dipilih karena unjuk kerjanya yang baik dan harganya yang relatif murah.

c. Tahap III: implementasi jaringan VPN

Setelah rancangan arsitektur/ topologi jaringan disetujui oleh PT. Mega Tirta Alami maka implementasi dimulai. Pada tahapan implementasi diusahakan jaringan komputer yang sudah ada hanya mengalami perubahan sedikit saja, hal ini dilakukan dengan tujuan untuk meminimalkan biaya yang dibutuhkan. Bagian yang paling banyak berubah adalah pada setting atau konfigurasi router yang dipasang pada kantor pusat maupun kantor cabang. Konfigurasi yang akan dilakukan meliputi kofigurasi IP *address* (pada konfigurasi ini akan menentukan IP *address* untuk semua *client* pada *headoffice, Branch-1* maupun *Branch-2*), konfigurasi *gateway*, konfigurasi DNS, konfigurasi NAT, konfigurasi *Mangle*, konfigurasi *Queue*, konfigurasi *Routing*, dan konfigursi PPTP

d. Tahap IV: pengujian jaringan VPN

Pada tahap ini dilakukan pengujian terhadap jaringan VPN yang sudah dibuat. Beberapa percobaan dilakukan untuk menguji apakah semua fungsionalitas jaringan VPN berfungsi dengan baik tanpa ada yang cacat. Beberapa percobaan teknis yang dilakukan pada tahap ini meliputi pengujian konektifitas antar *router* yang dipasang, pengujian fungsionalitas *router* yang difungsikan sebagai *server* (*router* A), pengujian IP *route*, pengujian *trace route*, pengujian ping dan pengujian *download*.

HASIL DAN PEMBAHASAN

1. Hasil Konektivitas *router*

Pengujian yang pertama kali dilakukan adalah pengujian konektifitas antar router. Apabila Router A berhasil disambungkan dengan Router B dan Router C maka Router a akan memunculkan alamat IP dynamic secara otomatis yaitu alamat IP 9.1.1.10 adalah alamat IP yang digunakan untuk membuat jalur VPN sedangkan *network* 9.1.1.1 dan *network* 9.1.1.2 adalah remote address yang menghubungkan antara *router – router* dalam pembuatan VPN.

2. Hasil konfigurasi VPN menggunakan metode PPTP

Setelah memastikan *router* B dan *router* C telah terhubung semua dengan *router* A maka tahap selanjutnya memastikan konfigurasi VPN *site to site* yang sebelumnya

dibuat dengan menggunakan metode PPTP telah selesai dilakukan. Untuk melihat hasil dari konfigurasi dapat dilihat dengan mengetikan perintah seperti diperlihatkan pada Gambar 3.

```
[admin@HeadOffice] > ppp active print
Flags: R - radius
 #   NAME        SERVICE CALLER-ID       ADDRESS       UPTIME   ENCODING
 0   Branch-1    pptp    172.165.10.2    9.1.1.1       55s      MPPE128 s.
 1   Branch-2    pptp    172.165.10.3    9.1.1.2       55s      MPPE128 s.
```

Gambar 3. PPP aktif pada Router A

Pada gambar 3. Memperlihatkan bahwa *router* A sebagai PPTP *server* yang telah menghubungkan *router* B dan *router* C yang bertindak sebagai PPTP *client* .Apabila semua jalur telah terhubung dengan PPTP *server* yang ada pada *router* A maka akan muncul *Branch-1* dan *Branch-2* yang merupakan alamat VPN yang berada pada *router* B dan *ruoter* C .

3. Hasil pengujian IP *route*

a. Pengujian *IP route* pada *Router A*

Hasil pengujian IP *route* pada *router* A dapat dilihat pada gambar 4.

```
[admin@HeadOffice] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0   S  0.0.0.0/0                          124.40.250.79      1
 1 A S  0.0.0.0/0                          172.165.10.3       1
 2 ADC  9.1.1.1/32         9.1.1.10        <pptp-Branch-1>    0
 3 ADC  9.1.1.2/32         9.1.1.10        <pptp-Branch-2>    0
 4 ADC  124.40.250.80/30   124.40.250.80   ether1             0
 5 A S  165.165.10.32/30                   172.165.10.2       1
 6 ADC  172.165.10.0/29    172.165.10.1    ether2             0
 7 ADC  192.168.4.0/27     192.168.4.1     ether5             0
 8 ADC  192.168.4.32/29    192.168.4.32    ether3             0
 9 ADS  192.168.6.0/24                     9.1.1.1            1
10   S  192.168.6.0/27                     9.1.1.2            1
11 A S  192.168.7.32/30                    9.1.1.1            1
```

Gambar 4. Tampilan hasil pengujian IP Route pada *router* A

Gambar 4. menampilkan IP *address* dengan alamat 9.1.1.1/32 yang merupakan alamat dari PPTP *Branch-1* dan alamat 9.1.1.2 yang merupakan alamat dari PPTP *Branch-2* yang jalurnya dihubungkan oleh alamat dari VPN yaitu 9.1.1.10. Selain alamat IP tersebut terdapat pula alamat IP 192.168.7.32 yang merupakan alamat IP lokal untuk bagian keuangan kantor cabang 1 yang telah terhubung dengan jalur VPN yang memakai *gateway* 9.1.1.1 yaitu alamat dari *Branch-1* yang membuktikan sudah terhubung dengan *router* B yang berada pada kantor cabang 1.

b. Pengujian *IP route* pada *Router B*

Pada router B dilakukan juga pengujian IP *route* yang hasilnya dapat dilihat seperti pada Gambar 5. Pada

gambar tersebut dapat dilihat bahwa jalur VPN yang aktif pada *router* B adalah DST-ADDRESS 9.1.1.10/32 dengan *gateway* pptp-out1 yang berasal dari PREF-SRC 9.1.1.1. Gambar 5 juga memperlihatkan alamat IP 192.168.4.32/29 menggunakan jalur VPN dikarenakan melalui *gateway* 9.1.1.10

```
[admin@Ruter B] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 A S  0.0.0.0/0                          172.165.10.1              1
 1 ADC  9.1.1.10/32        9.1.1.1         pptp-out1                 0
 2 ADC  165.165.10.32/30   165.165.10.32   ether1                    0
 3 ADC  172.165.10.0/30    172.165.10.2    ether1                    0
 4 A S  192.168.4.32/29                    9.1.1.10                  1
 5   S  192.168.4.32/29                    9.1.1.10                  1
 6 ADC  192.168.5.0/24     192.168.5.1     ether5-local              0
 7 ADC  192.168.6.0/27     192.168.6.1     ether3-local              0
 8 ADC  192.168.7.32/30    192.168.7.33    ether4-local              0
```

Gambar 5. Tampilan hasil pengujian IP route pada Router B

c. Pengujian *IP route pada Router C*

Sama seperti router A dan *router* B, pengujian IP *route* juga dilakukan pada *router* C yang hasilnya dapat dilihat pada Gambar 6.

```
[admin@Router C] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 A S  0.0.0.0/0                          172.165.10.4              1
 1 ADC  9.1.1.10/32        9.1.1.2         pptp-out1                 0
 2 ADC  150.142.23.8/30    150.142.23.10   ether1                    0
 3 ADC  172.165.10.0/29    172.165.10.3    ether1                    0
 4 A S  192.168.4.32/32                    9.1.1.10                  1
 5 ADC  192.168.9.0/24     192.168.9.1     ether4-local              0
 6 ADC  192.168.10.0/29    192.168.10.1    ether2-local              0
 7 ADC  192.168.10.32/29   192.168.10.33   ether3-local              0
```

Gambar 6. Tampilan hasil pengujian IP *route* pada router C

Pada Gambar 6 dapat dilihat jalur VPN yang aktif pada router C yaitu DST-ADDRESS 9.1.1.10/32 dengan *gateway* pptp-out1 yang berasal dari PREF-SRC 9.1.1.2. IP route router C juga memperlihatkan alamat IP 192.168.4.32/29 yang menggunakan jalur VPN dikarenakan melalui *gateway* 9.1.1.10. Daftar alamat IP aktif yang digunakan pada *router* A sebagai kantor pusat (*head office*), *router B* sebagai kantor cabang I *(Branch 1)* dan *router C* sebagai kantor cabang II (*Branch 2*) diperlihatkan pada Tabel 2 sedangkan daftar alamat IP sumber (*source)* aktif yang digunakan pada *Router* A sebagai kantor pusat (head office), *Router B* sebagai kantor cabang I *(Branch 1)* dan *Router C* sebagai kantor cabang II (*Branch 2*) diperlihatkan pada Tabel 3..

Tabel 2.
Daftar hasil *trace route* DST-*Address*

DST-Address		
Router A	**Router B**	**Router C**
9.1.1.1/32	9.1.1.10/32	9.1.1.10/32
9.1.1.2/32	165.165.10.32/30	150.142.23.8/30
124.40.250.80/30	172.165.10.0/30	172.165.10.0/29
165.165.10.32/30	192.168.4.32/29	192.168.4.32/32
172.165.10.0/29	192.168.4.32/29	192.168.9.0/24
192.168.4.0/27	192.168.5.0/24	192.168.10.0/29
192.168.4.32/29	192.168.6.0/27	192.168.10.32/29
192.168.6.0/24	192.168.7.32/30	
192.168.6.0/27		
192.168.7.32/30		

Tabel 3.
Daftar hasil *trace route* PREF-SRC

PREF-SRC		
Router A	**Router B**	**Router C**
9.1.1.10	9.1.1.1	9.1.12
9.1.1.10	165.165.10.32	150.142.23.10
124.40.250.80	172.165.10.2	172.165.10.3
172.165.10.1	192.168.5.1	192.168.9.1
192.168.4.1	192.168.6.1	192.168.10.1
192.168.4.32	192.168.7.33	192.168.10.33

Tabel 4. memperlihatkan daftar *gateway* aktif yang digunakan untuk jalur VPN pada *router* A sebagai *head office, router B* sebagai *Branch-1* dan *router C* sebagai *Branch-2.*

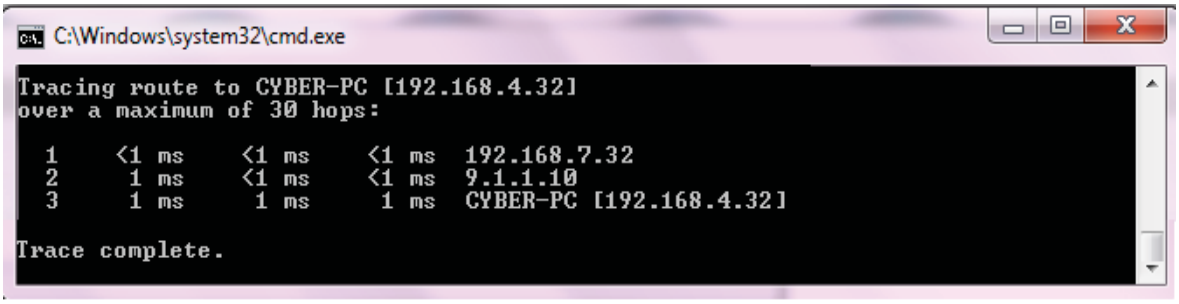
Tabel 4.
Daftar hasil *trace route gateway*

GATEWAY		
Router A	**Router B**	**Router C**
124.40.250.79	172.165.10.1	172.165.10.4
172.165.10.3	pptp-out1	pptp-out1
<pptp - Branch-1>	ether1	ether1
<pptp - Branch-2>	ether1	ether1
ether1	9.1.1.10	9.1.1.10
172.165.10.2	9.1.1.10	ether4-local
ether2	ether5-local	ether2-local
ether5	ether3-local	ether3-local
ether3	ether4-local	
9.1.1.1		
9.1.1.2		
9.1.1.1		

4. Hasil pengujian traceroute

a. Hasil pengujian *traceroute* pada *Branch-1*

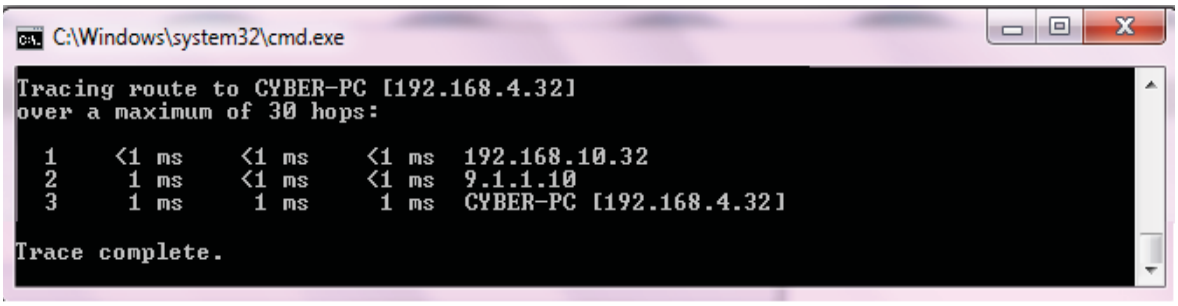
Hasil pengujian traceroute yang diperlihatkan pada Gambar 7 memperlihatkan hasil *traceroute Branch-1* bahwa alamat IP lokal untuk bagian keuangan 192.168.7.32 adalah melalui jalur VPN dengan *gateway* 9.1.1.10 untuk menuju ke *server database* dengan IP 192.168.4.32 sehingga dapat disimpulkan bahwa jalur VPN yang telah dipasang siap digunakan.



Gambar 7. Tampilan hasil pengujian *traceroute Branch-1*

b. Hasil pengujian *traceroute* pada *Branch-2*

Gambar 8 memperlihatkan hasil pengujian *traceroute* untuk *Branch-2*. Dari gambar tersebut dapat dilihat bahwa alamat IP lokal untuk bagian keuangan adalah 192.168.10.32 melalui jalur VPN dengan *gateway* 9.1.1.10 untuk menuju ke server database dengan alamat IP 192.168.4.32 sehingga dapat disimpulkan jalur VPN yang telah dipasang dapat digunakan.



Gambar 8. Tampilan hasil pengujian *traceroute Branch-2*

5. Hasil pengujian *PING*

a. Hasil pengujian ping koneksi dari *Branch-1 ke server*

Hasil pengujian PING pada jakur dari Branch-1 ke server seperti yang diperlihatkan pada Gambar 9 memperlihatkan bahwa bagian keuangan *Branch-1* dapat melakukan ping koneksi ke server basis data yang menunjukkan bahwa bagian keuangan *Branch-1* sudah terhubung dengan server melalui jalur VPN.

```
[admin@Router B] > ping 192.168.4.32
HOST                                     SIZE TTL TIME  STATUS
192.168.4.32                               56  64 1ms
192.168.4.32                               56  64 0ms
192.168.4.32                               56  64 0ms
192.168.4.32                               56  64 0ms
192.168.4.32                               56  64 0ms
192.168.4.32                               56  64 1ms
    sent=6 received=6 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=1ms
```

Gambar 9. Tampilan hasil pengujian ping koneksi *Branch-1* ke server

b. Hasil pengujian ping koneksi dari *Branch-2 ke server*

Hasil pengujian ping pada jalur Branch-2 ke server yang ditunjukkan pada Gambar 10 memperlihatkan bahwa bagian keuangan *Branch-2* dapat melakukan ping koneksi ke server database yang berarti bagian keuangan Branch-2 sudah terhubung dengan server melalui jalur VPN.

```
[admin@Router C] > ping 192.168.4.32
HOST                                     SIZE TTL TIME  STATUS
192.168.4.32                               56  64 1ms
192.168.4.32                               56  64 0ms
192.168.4.32                               56  64 0ms
192.168.4.32                               56  64 0ms
192.168.4.32                               56  64 0ms
192.168.4.32                               56  64 1ms
    sent=6 received=6 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=1ms
```

Gambar 10. Tampilan hasil pengujian ping koneksi *Branch-2* ke server

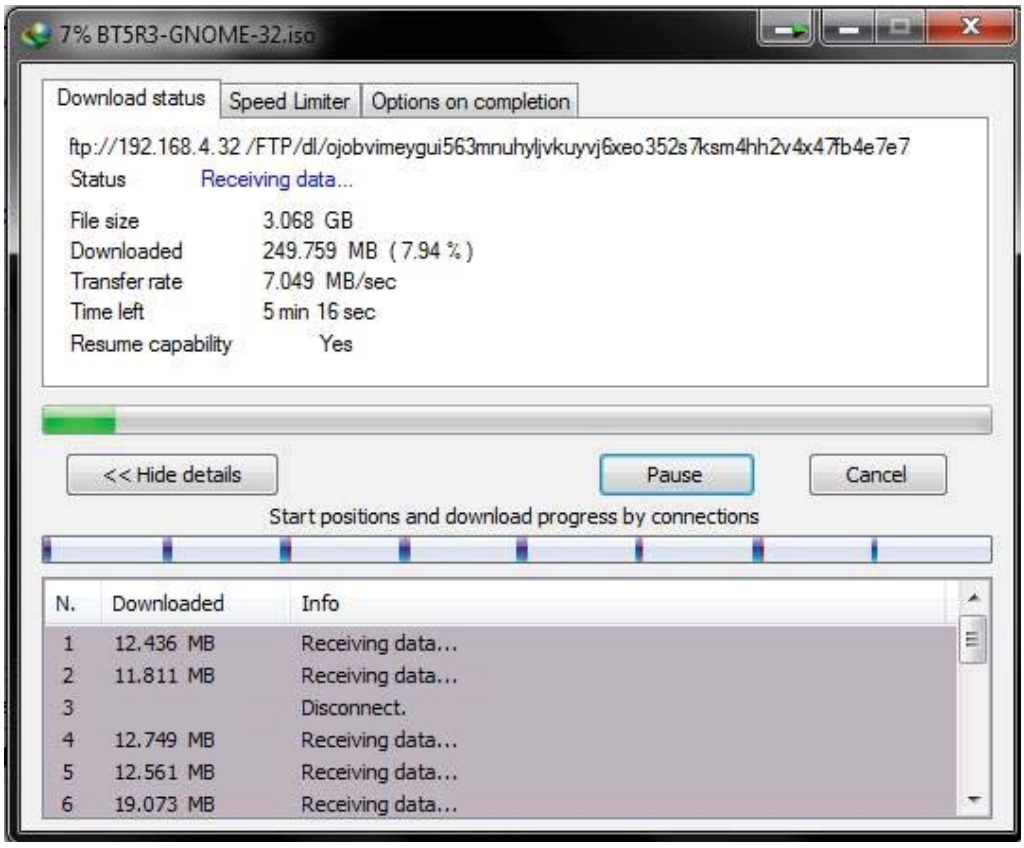
c *Hasil pengujian ping koneksi dari bagian keuangan Branch-1 ke bagian keuangan Branch-2*

Hasil pengujian ping dari bagian keuangan Branch-1 ke bagian keuangan Branch-2 yang diperlihatkan pada Gambar 11 memperlihatkan bahwa settingan VPN tidak memperbolehkan koneksi antara bagian keuangan *Branch-1* dengan bagian keuangan *Branch-2* dikarenakan untuk menjaga keamanan. Koneksi VPN hanya dibatasi untuk *Branch-1* dengan *Headoffice* maupun *Branch-2* dengan *headoffice*. Sama seperti koneksi *Branch-1* dan *Branch-2* untuk koneksi *Branch-2* ke *Branch-1* diberikan juga batasan, oleh karena itu *Branch-2* hanya terhubung dengan *headoffice.*

```
[admin@Ruter B] > ping 192.168.10.32
HOST                                     SIZE TTL TIME  STATUS
192.168.10.32                                         timeout
192.168.10.32                                         timeout
172.165.10.2                              84  64 631ms host unreachable
192.168.10.32                                         timeout
192.168.10.32                                         timeout
192.168.10.32                                         timeout
192.168.10.32                                         timeout
192.168.10.32                                         timeout
192.168.10.32                                         timeout
    sent=9 received=0 packet-loss=100%
```

6. Hasil pengujian *download*

Percobaan download adalah mencoba melakukan proses pengunduhan (*download*) data yang tersimpan di kantor pusat pada kator cabang melalui jaringan VPN yang telah dibuat. Pada kegiatan ini, percobaan download dilakukan dengan memanfaatkan perangkat lunak download manager. Hasil percobaan menunjukkan semua proses download dapat dilakukan dengan baik yang menunjukkan jaringan VPN sudah berjalan dengan baik. Contoh tampilan proses *download* dari kantor pusat dapat dilihat pada Gambar 12.



Gambar 12. Tampilan proses download file dari *head office*

SIMPULAN DAN SARAN

1. Simpulan

Setelah menyelesaikan tahapan-tahapan pelaksanaan kegiatan dari analaisis kebutuhan sampai dengan pengujian dan pembahasan hasilnya, dapat ditarik kesimpulan sebagai berikut:

a. Setelah jaringan VPN dibangun pada PT.Mega Tirta Alami, terbentuk sebuah jaringan baru yang terdiri dari Headoffice, kantor Branch-1 dan kantor Branch-2 melalui jalur VPN dengan *gateway* 9.1.110.
b. Dengan menggunakan metode PPTP pembangunan VPN di PT.Mega Tirta Alami dapat memberikan keamanan dengan adanya enkripsi disetiap komunikasi data dan memberikan username dan password sebagai pengenal untuk setiap branch.

2. Saran

Untuk kegiatan selanjutnya harapannya jaringan VPN tidak hanya diterapkan pada dua kantor cabang namun juga pada seluruh kantor cabang yang ada.

PERSANTUNAN

Tim pengabdian mengucapkan terima kasih kepada semua pihak yang membantu atas terlaksananya kegiatan ini diantaranya yaitu Lembaga Penenelitian dan Pengabdian kepada Masyarakat Universitas Muhammadiyah Surakarta dan PT. Mega Tirta Alami.

DAFTAR PUSTAKA

Astawa, I Nyoman Gede Arya; Atmaja, I Made Ari Dwi Suta. 2012. "Implementasi Vpn Pada Jaringan Komputer Kampus Politeknik Negeri Bali", *Jurnal Matrix Vol.2, No.1*.

Ghozali, Afif, 2010. *Pembatasan Akses Jaringan Vpn Dengan Iptables*, Skripsi, Universitas Narotama, Surabaya

Stiawan, Deris; Palupi; Rini Dian. 2009. "Optimalisasi Interkoneksi VPN Dengan Menggunakan *Hardware Based* Dan *Iix* (Indonesia Internet *Exchange*) Sebagai Alternatif Jaringan Skala Luas (Wan)", *Jurnal Ilmiah Generic vol 4, No.1*.

Tanenbaum, Andrew S. 2003. *Computer Networks Fourth Edition*, Prentice Hall, ISBN: 0-13-066102-3

————————, Pengertian VPN dan Fungsinya, online: http://teknodaninfokita.blogspot.com/2014/02/pengertian-vpn-dan-fungsinya.html, online tanggal 1 Juni 2013 dan tanggal 18 April 2014