

Metode *Point to Point Tunneling Protocol* Untuk Keamanan Jaringan Studi Kasus Kantor Walikota Administrasi Jakarta Barat

Fajar Akbar¹, Susafa'ati², Musriatun Napiah³

^{1,2,3} Program Studi Teknik Informatika

fajar.fkb@nusamandiri.ac.id, susafa'ati.suf@nusamandiri.ac.id, musnaf2015@gmail.com

Diterima	Direvisi	Disetujui
13-12-2019	15-12-2019	17-12-2019

Abstrak-Kemajuan dan perkembangan Ilmu Pengetahuan dan Teknologi saat ini sangatlah pesat, tentunya Sistem Keamanan Jaringan pun semakin berkembang seiring dengan kedua hal tersebut. Perusahaan – perusahaan sudah melakukan komputerisasi, sehingga setiap bagiannya menggunakan komputer dalam setiap operasionalnya, semakin maju dan berkembang perusahaan tersebut akan membuka cabang baru dalam operasionalnya baik di luar kota, negeri, ataupun benua untuk meningkatkan kualitas dan kuantitas produksi perusahaan. Dalam bidang administrasi pemerintah penting dalam manajemen pembagian jaringan, dan pertukaran data agar cepat, mudah, dan tepat dalam pengerjaannya, dan tidak mudah diakses pihak luar suku dinas pemerintahan. Sistem keamanan jaringan yang baik, sangat diperlukan dalam pertukaran data dari kantor pusat ke kantor cabang sehingga dapat dilakukan secara aman dan terjamin dari pihak luar. Ada berbagai macam software aplikasi yang bisa digunakan dalam hal keamanan pada suatu jaringan, akan tetapi tidak semua software terjaga keamanan datanya dalam proses pertukaran data. Oleh karena itu dengan metode *point to point tunneling protocol* pada VPN sangatlah cocok jika digunakan dalam pertukaran data antar perusahaan karena metode ini menggunakan jalur *private* dengan ip *public* dalam pertukaran datanya, sehingga keamanan dalam hal kebocoran data sangat terjamin dari pihak luar yang tidak bertanggung jawab.

Kata Kunci: *Point to Point Tunneling Protocol*, VPN, Sistem Keamanan Jaringan dan Kantor Administrasi Walikota Jakarta Barat

PENDAHULUAN

Pada era globalisasi zaman sekarang, kemajuan dan perkembangan dunia teknologi dan internet sangatlah pesat sehingga berdampak di setiap aktivitas perusahaan, instansi atau lainnya, sebagai kebutuhan pokok dalam media komunikasi antar cabang perusahaan kantor pusat atau sebagai media dalam pertukaran data (*sharing*) antar cabang yang dapat diakses melalui jaringan komputer. Aktivitas – aktivitas tersebut tentulah sangat beresiko apabila informasi yang penting dan berharga dapat diakses oleh pihak yang tidak berkepentingan. Keamanan suatu jaringan pada suatu perusahaan sangatlah penting dalam pertukaran data antar *server* dan *client*, misalkan dari kantor pusat *server* dengan kantor cabang *client*. Suatu perusahaan yang memiliki kantor cabang di berbagai daerah, kota, atau bahkan antar Negara diperlukan teknologi yang aman dan terpusat dalam pertukaran data perusahaan, begitupun halnya pada Kantor Walikota Administrasi Jakarta Barat mempunyai dua gedung yakni gedung *Server* dan gedung *Client* sehingga memerlukan teknologi keamanan pada pertukaran informasi. Data akan tersimpan di *server* terpusat dan akan diakses oleh *client* antar cabang perusahaan tersebut.

Sistem Jaringan yang aman pada Kantor Walikota Administrasi Jakarta Barat untuk mengatasi hal ini

adalah dengan Menerapkan VPN (*Virtual Private Network*) dimana bisa menghubungkan dua perusahaan yang berbeda gedung sehingga dapat saling terkoneksi, begitupun kurangnya SDM (Sumber Daya Manusia) pada bagian Sudin Kominfo di Kantor Walikota Administrasi Jakarta Barat dalam menangani permasalahan yang terjadi dalam jaringan. Keamanan data dan *enkripsi* data dalam teknologi VPN adalah sebagai standar utama dalam penerapannya dengan menyertakan fitur utama yaitu *enkripsi* dan *tunneling*.

Menurut (Putra, Luthfi, & Yeni, 2018)Metode PPTP merupakan protokol jaringan yang memungkinkan pengamanan transfer data dari remote client (client yang berada jauh dari server) ke server pribadi perusahaan dengan membuat sebuah VPN (*Virtual Private Network*) melalui jaringan data berbasis TCP/IP. Protokol ini dikembangkan oleh Microsoft dan Cisco. Teknologi jaringan PPTP merupakan pengembangan dari remote access Point-to-Point protocol yang dikeluarkan oleh Internet Engineering Task Force (IETF). Dari hasil penelitian di atas, penulis akan membahas pengamanan yang harus diterapkan pada Kantor Walikota Administrasi Jakarta Barat agar keamanan data dapat terjaga dalam pengaksesan, meminimalisir kurangnya SDM (Sumber Daya Manusia) dalam penanganan permasalahan yang terjadi agar cepat teratasi

METODE PENELITIAN

Teknik pengumpulan data yang digunakan oleh penulis dalam melakukan pengumpulan data dengan menggunakan metode sebagai berikut:

1. Metode Observasi

Observasi atau pengamatan merupakan salah satu teknik pengumpulan data atau fakta. Disini penulis melakukan observasi dengan mengamati secara langsung untuk mendapatkan data-data tentang analisa jaringan komputer dan konfigurasinya pada Kantor Walikota Administrasi Jakarta Barat.

2. Studi Pustaka

Dalam metode ini, pengumpulan data dilakukan dengan bersumber pada buku pegangan, Jurnal-jurnal ilmiah, catatan-catatan kuliah dan buku-buku lain yang ada kaitannya dengan pengumpulan data yang penulis butuhkan sebagai bahan perlengkapan analisa perbandingan penulis.

HASIL DAN PEMBAHASAN

1. Jaringan Komputer

Jaringan Komputer adalah hubungan antar dua komputer atau lebih dalam bentuk implementasi dan komunikasi data. Sebagaimana prinsipdasar dalam komunikasi data bahwa data yang dikirim harus diterima oleh komputer yang dituju dalam waktu yang secepatnya (Pratama;Marlinda, 2015)

2. Tunneling

Teknologi yang bertugas untuk menangani dan menyediakan koneksi *point-to-point* dari sumber tujuannya. Teknologi ini dibuat dalam pelaksanaannya dengan melintasi jalur umum namun tidak mempedulikan data milik orang lain yang sama-sama melintasi jalur tersebut, tetapi koneksi hanya melayani transportasi data dari pembuatnya (Mufida et al., 2018)

3. PPTP (Point to Point Tunneling Protokol)

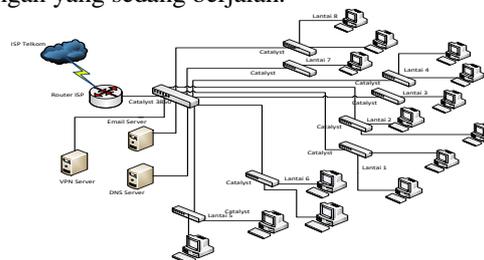
Protocol jaringan yang memungkinkan pengamanan transfer data dari *remote client* ke *server* pribadi perusahaan dengan membuat sebuah VPN melalui TCP/IP. Keunggulan utama dari PPTP adalah memberikan keamanan serta *enkripsi* komunikasi melalui PTSN (*Public Switched Telephone Network*) ataupun Internet (Mufida et al., 2018)

4. Topologi

Untuk topologi jaringan penulis mengusulkan agar tetap menggunakan topologi yang sudah ada karena sangat tepat diterapkan pada Kantor Walikota Administrasi Jakarta Barat baik pada gedung *server* maupun pada gedung *client*.

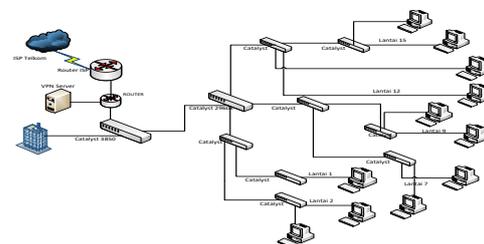
5. Skema Jaringan

Untuk skema jaringan tetap menggunakan skema yang sudah berjalan hanya saja penulis menambahkan satu buah *server* untuk VPN dengan menggunakan metode *point to point tunneling protocol* baik itu pada gedung *server* maupun pada gedung *client*, sehingga kedua jaringan tersebut dapat saling terhubung, karena disini menggunakan topologi star maka tidak akan mengganggu kinerja jaringan yang sedang berjalan.



Sumber : penelitian (2019)

Gambar 1. Skema Jaringan Usulan Gedung *Server*



Sumber : penelitian (2019)

Gambar 2. Skema Jaringan Usulan Gedung *Client*

6. Keamanan Jaringan

Keamanan yang diterapkan pada gedung *server* dan gedung *client* bertumpu pada PC Router, Sedangkan untuk *client* menggunakan antivirus pada masing-masing PC.

7. Antivirus

Berfungsi untuk mencegah penyebaran *virus* yang datang dari *client* pada jaringan tersebut. Antivirus ini akan memberikan perlindungan dan keamanan pada data dan system yang ada pada komputer.

8. VPN (Virtual Private Network)

Teknologi komunikasi pada sebuah jaringan yang memudahkan untuk berkomunikasi antara jaringan publik dengan jaringan lokal. VPN biasanya

digunakan untuk menghubungkan jaringan antar tempat yang berjauhan, seperti halnya antara kantor pusat dengan kantor cabang. Dengan cara tersebut maka setiap jaringan akan mendapatkan hak yang sama dan pengaturan yang sama seperti halnya berada dalam jaringan atau *network* itu sendiri (Mufida, Irawan, & Chrisnawati, 2018)

Sistem keamanan jaringan menggunakan VPN dengan metode *point to point tunneling protocol* dapat mencegah kehilangan data ke pihak luar yang tidak bertanggung jawab, karena *tunneling* menggunakan jaringan *private* sehingga kerahasiaan data dapat terjaga dari pihak luar baik di gedung *server* maupun di gedung *client*.

9. Rancangan Aplikasi

Untuk perancangan aplikasi penulis merapkan system keamanan dengan metode *point to point tunneling protocol* pada VPN dengan menggunakan mikrotik OS. Penulis melakukan konfigurasi pada beberapa *Ethernet*, seperti *Ethernet* untuk *ip public*, *ip local*, *DNS*, dll. Setelah melakukan konfigurasi penulis *login* pada *winbox* dengan menggunakan *ip public*. Dan berikutnya melakukan konfigurasi untuk *ip address* sampai dengan konfigurasi untuk VPN dengan metode *point to point tunneling protocol*. Hasil akhir dari konfigurasi dapat dilihat pada pengujian awal dan pengujian akhir.

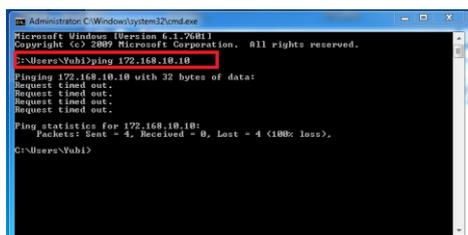
Pada bagian manajemen jaringan penulis membahas jaringan usulan untuk diterapkan pada Kantor Walikota Administrasi Jakarta Barat. Manajemen jaringan yang penulis usulkan yakni berhubungan dengan sistem keamanan jaringan menggunakan *point to point tunneling protocol*.

10. Pengujian Jaringan

Pada bagian pengujian jaringan, penulis akan membahas proses pengujian dari sebelum dilakukan konfigurasi VPN dengan metode *point to point tunneling protocol* sampai dengan telah dilakukan konfigurasi VPN.

a. Pengujian Jaringan Awal

Pengujian ini dilakukan sebelum adanya konfigurasi *point to point tunneling protocol* pada komputer *server* dan komputer *client*, bisa kita lakukan dengan tes koneksi PING.



Sumber : Penelitian (2019)

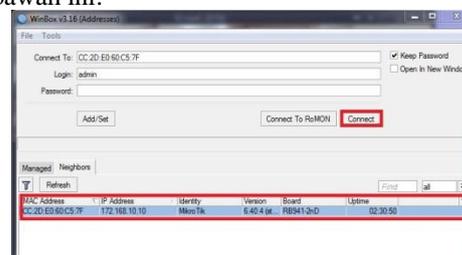
Gambar 3. Tes ping komputer *server* ke komputer *client*

dimana pengujian ini adalah sebelum adanya konfigurasi PPTP antar gedung *server* dengan gedung *client*, masih dalam kondisi RTO (*Request Time Out*) yang artinya masing-masing *server* yang ada di kedua gedung belum saling terkoneksi dalam jaringan VPN.

b. Pengujian Jaringan Akhir

Untuk tahap pengujian akhir disini penulis akan menjeleaskan mulai dari installasi mikrotik OS, pemberian *IP Address*, *IP Route Gateway*, *IP DNS*, dan PPTP *Client*, sampai berhasil atau tidaknya konfigurasi tersebut.

Pada bagian jendela *winbox*, lakukan login dengan menggunakan *IP Public*, dapat dilihat pada gambar di bawah ini:

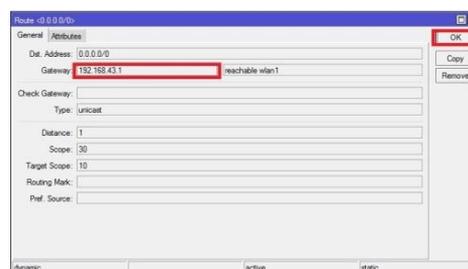


Sumber : Penelitian (2019)

Gambar 5. Login Winbox

Selanjutnya klik pada bagian *IP Address* kemudian pilih “connect” untuk masuk ke bagian konfigurasi dengan menggunakan *winbox*. Lakukan konfigurasi *IP Gateway*. Disini gateway merupakan penghubung pada sebuah jaringan komputer lainnya sehingga memudahkan dalam akses informasi.

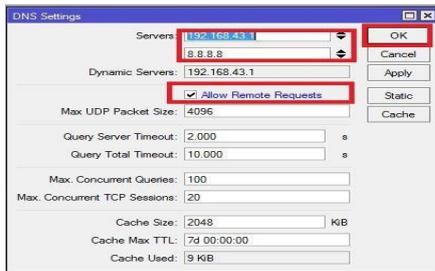
Masuk ke menu *IP > Route > Gateway > 192.168.43.1 > apply > ok*



Sumber : Penelitian (2019)

Gambar 6. Konfigurasi IP Gateway

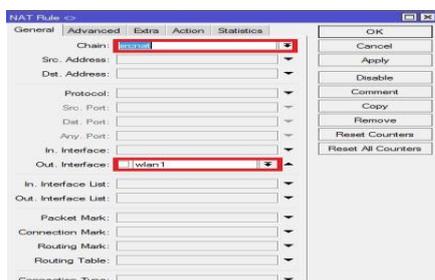
Lakukan konfigurasi *IP DNS* Klik menu *IP > DNS > Servers = 192.168.137.1, 8.8.8.8 > centang (☑) pada bagian allow-remote-request > apply > lalu pilih ok*



Sumber : Penelitian, 2019

Gambar 7. Konfigurasi IP DNS

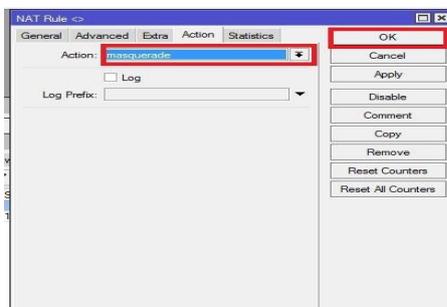
Lakukan konfigurasi *firewall* untuk bagian NAT, Pilih menu IP > Firewall > NAT > + > chain > pilih *srcnat* > out-interface > ether1



Sumber : Penelitian (2019)

Gambar 8. Konfigurasi IP Firewall

Kemudian pada bagian tab “action” kita pilih *masquerade*



Sumber : Penelitian (2019)

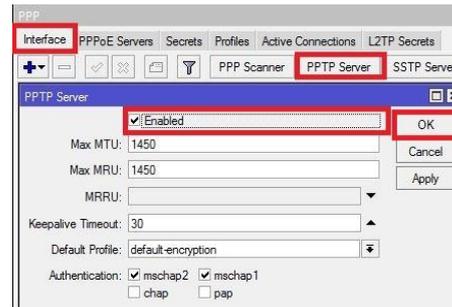
Gambar 9. Konfigurasi IP Firewall

Lakukan konfigurasi yang sama untuk *Router* dan gedung *server* pada gedung *client*.

c. Konfigurasi PPTP Server

Selanjutnya setelah kita melakukan konfigurasi dasar untuk masing-masing *Router*, kita akan melakukan konfigurasi untuk PPTP Server sesuai dengan skema jaringan usulan yang telah penulis gambarkan, maka kita akan melakukan konfigurasi PPTP Server pada gedung *server*.

Aktifkan PPTP Server, klik PPP > pilih PPTP Server > centang (☑) pada bagian *enabled* > apply > ok.

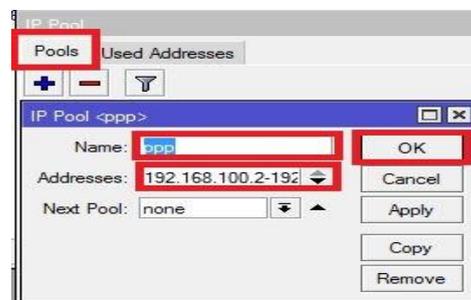


Sumber : Penelitian, 2019

Gambar 10. Konfigurasi PPTP Server

Disini kita akan menggunakan IP Pool untuk membuat PPTP.

Masuk ke menu IP > Pool > Klik + > isikan “name” dan “range” IP Address > pada kolom *address*.



Sumber : Penelitian (2019)

Gambar 11. Konfigurasi IP Pool

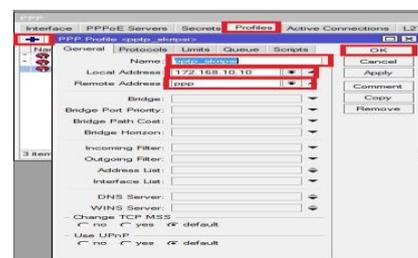
d. Konfigurasi untuk VPN Server

Masuk ke menu PPP > Klik tab *profiles* > tambahkan *profile* baru dengan mengklik “+” masukan data sebagai berikut:

Name: nama *profilenya*

Local Address: IP Address yang diberikan untuk VPN *Servernya*

Remote Address: pilih nama ip pool yang tadi dibuat jika sudah klik ok



Sumber : Penelitian (2019)

Gambar 12. Konfigurasi Profile VPN

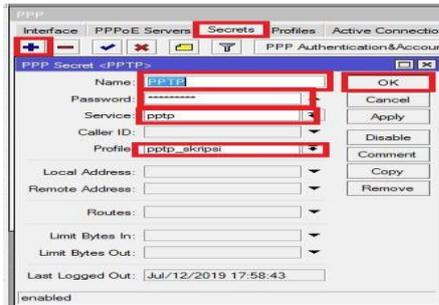
Pembuatan *user* baru pada PPTP, Klik pada menu PPP > pilih *Secrets* > + > lalu isikan:

Username & Password: untuk proses *otentikasi client* yang akan terkoneksi ke PPTP Server,

penggunaan huruf besar dan huruf kecil akan berpengaruh.

Local Address: alamat IP yang akan terpasang pada *router* itu sendiri (PPTP Server) setelah link PPTP terbentuk

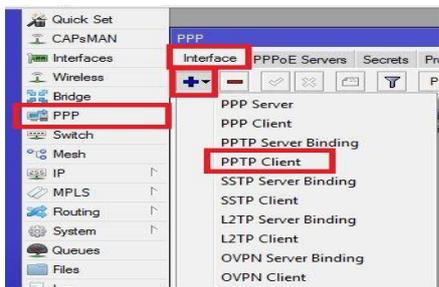
Remote Address: Alamat IP yang akan diberikan *Client* setelah link PPTP terbentuk untuk "Profile" pilih *profile* yang sebelumnya sudah dibuat kemudian *apply > ok*



Sumber : Penelitian (2019)
Gambar 13. Pembuatan user baru

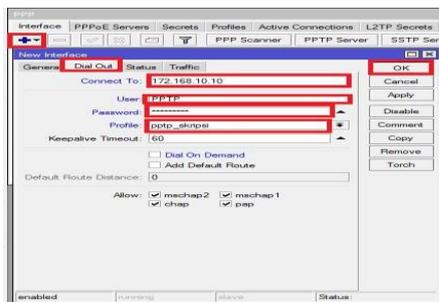
Sampai disini untuk konfigurasi *router* PPTP Server sudah selesai, selanjutnya kita lakukan konfigurasi untuk sisi *client*.

Tambahkan *interface* baru PPTP Client
Klik pada menu PPP > > PPTP Client



Sumber : Penelitian (2019)
Gambar 14. Interface PPTP Client

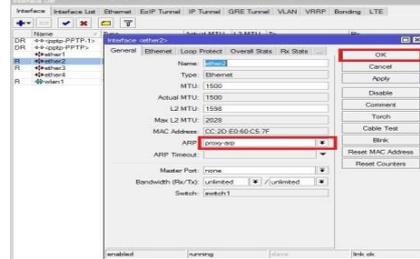
Lakukan *Dial Out* ke IP Public Router A (PPTP Server), masukan *username* dan *password* sesuai dengan pengaturan *secret* PPTP Server



Sumber : Penelitian (2019)
Gambar 15. Dial Out ke IP Public

Setelah koneksi PPTP terbentuk, akan muncul IP Address baru di kedua *Router*

Selanjutnya konfigurasi untuk ARP, klik menu *interface > pilih ether2 > klik tab general > ARP > proxy - arp > apply > ok*



Sumber : Penelitian (2019)
Gambar 16. Konfigurasi ARP

e. Membangun VPN

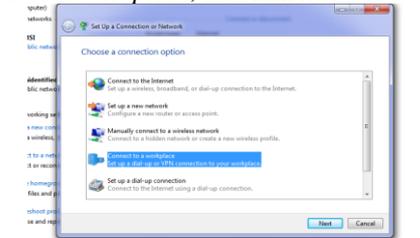
Lakukan penyettingan untuk VPN Server pada *winbox*, Pastikan laptop sudah terkoneksi dengan internet.

Buka *control panel* pada pc, kemudian pilih menu *open network and sharing center*, kemudian *create* koneksi baru dengan memilih *set up new connection or network*



Sumber : Penelitian (2019)
Gambar 17. Konfigurasi VPN Server

Pada tampilan *windows* selanjutnya, pilih *connect to a workplace*, lalu klik *next*



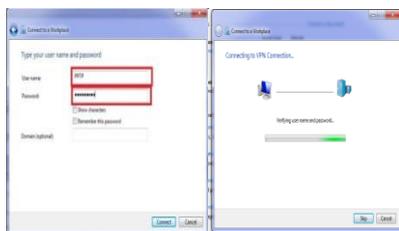
Sumber : Penelitian (2019)
Gambar 18. Konfigurasi VPN Server

Pada langkah berikutnya kita akan diminta untuk memasukkan IP Address yang akan melakukan koneksi yaitu IP Address *public router A*, *Destination name* adalah parameter untuk memberikan nama pada *interface* VPN yang sudah dibuat.



Sumber : Penelitian (2019)
Gambar 19. Konfigurasi VPN Server

Selanjutnya masukan *username* dan *password* yang sudah dibuat tadi di konfigurasi PPTP



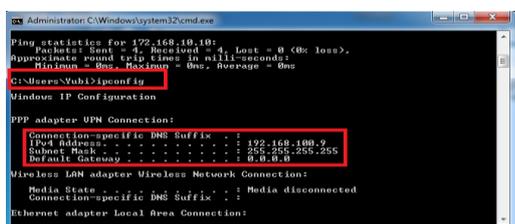
Sumber : Penelitian (2019)
Gambar 20. Koneksi VPN

Jika sudah selesai maka akan muncul *interface* baru sesuai dengan nama VPN *Connection*



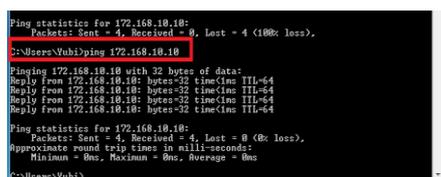
Sumber : Penelitian (2019)
Gambar 21. Koneksi VPN

Tampilan hasil koneksi VPN dari *server* ke *client* yakni antar gedung *server* dan gedung *client*



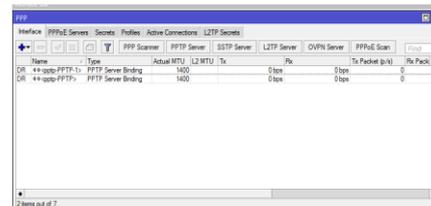
Sumber : Penelitian (2019)
Gambar 22. Hasil Koneksi VPN

Disini kita cek *ip address* yang di dapatkan si *client* setelah terkoneksi ke VPN, sesuai dengan IP Pool yang telah kita tentukan di konfigurasi PPTP *Server* di atas, yaitu 192.168.10.10, selanjutnya kita tes koneksi ping ke *server*:



Sumber : Penelitian (2019)
Gambar 23. Hasil Koneksi VPN

Berikut ini adalah tampilan pada PPTP *Server* ketika ada *client* yang terkoneksi pada VPN



Sumber : Penelitian (2019)
Gambar 24. Tampilan PPTP *Server*

KESIMPULAN

Dari pembahasan yang telah penulis jelaskan di atas mengenai peranan jaringan komputer dalam kehidupan sehari-hari, dengan ini penulis menarik kesimpulan bahwa dengan adanya penerapan keamanan jaringan komputer menggunakan metode PPTP (*Point to point tunneling protocol*) pada VPN memberikan suatu kemudahan bagi pihak pekerja IT dalam mengatasi permasalahan yang terjadi antar kantor yang berjauhan jaraknya, dan memberikan keamanan pada pengiriman data yang di *transmisikan* dengan metode *enkripsi* dalam jaringan *private*, sehingga sangat terjaga keamanannya dari pihak yang tidak bertanggung jawab.

REFERENSI

- Mufida, E., Irawan, D., & Chrisnawati, G. (2018). Remote Site Mikrotik VPN Dengan Point To Point Tunneling Protocol (PPTP) Studi Kasus pada Yayasan Teratai Global Jakarta. *Jurnal Matrik*, 16(2), 9. <https://doi.org/10.30812/matrik.v16i2.7>
- Pratama;Marlinda. (2015). Perancangan Jaringan Komputer Menggunakan Aplikasi Vhp Online Reporting System. *Teknik Komputer AMIK BSI*, 1(1), 106–113.
- Putra, J. L., Luthfi, I., & Yeni, A. (2018). Penerapan Sistem Keamanan Jaringan Menggunakan. 3(2), 260–267.
- Mufida, E., Irawan, D., & Chrisnawati, G. (2018). Remote Site Mikrotik VPN Dengan Point To Point Tunneling Protocol (PPTP) Studi Kasus pada Yayasan Teratai Global Jakarta. *Jurnal Matrik*, 16(2), 9. <https://doi.org/10.30812/matrik.v16i2.7>
- Pratama;Marlinda. (2015). Perancangan Jaringan Komputer Menggunakan Aplikasi Vhp Online Reporting System. *Teknik Komputer AMIK BSI*, 1(1), 106–113.
- Putra, J. L., Luthfi, I., & Yeni, A. (2018). Penerapan Sistem Keamanan Jaringan Menggunakan. 3(2), 260–267.
- Mufida, E., Irawan, D., & Chrisnawati, G. (2018). Remote Site Mikrotik VPN Dengan Point To Point Tunneling Protocol (PPTP) Studi Kasus pada Yayasan Teratai Global Jakarta. *Jurnal*

Matrik, 16(2), 9.
<https://doi.org/10.30812/matrik.v16i2.7>
Pratama;Marlinda. (2015). Perancangan Jaringan
Komputer Menggunakan Aplikasi Vhp Online
Reporting System. *Teknik Komputer AMIK*

BSI, 1(1), 106–113.
Putra, J. L., Luthfi, I., & Yeni, A. (2018). *Penerapan
Sistem Keamanan Jaringan Menggunakan.*
3(2), 260–267.