Keamanan Jaringan Menggunakan VPN (Virtual Private Network) Dengan Metode PPTP (Point To Point Tunneling Protocol) Pada Kantor Desa Kertaraharja Ciamis

Sari Dewi [1] , Fajar Riyadi [2], Tika Suwastitaratu [3], Noer Hikmah [4]

[1] Sistem Informasi, Universitas Bina Sarana Informatika PSDKU Kota Pontianak
[2, 3] Teknologi Komputer, Universitas Bina Sarana Informatika
[4] Sistem Informasi, Universitas Bina Sarana Informatika
Corresponding Author.E-mail:sari.sre@bsi.ac.id ,fajarriyadi@gmail.com, tikasuwastitaratu@gmail.com, noer.nhh@bsi.ac.id

Abstract

Sistem Keamanan Jaringan semakin berkembang seiring dengan perkembangan teknologi. Instansi - instansi sudah melakukan komputerisasi, dimana setiap bagian di dalam instansi tersebut sudah menggunakan komputer dalam operasionalnya, hal ini membuat instansi pemerintahan meningkatkan kualitas dan kuantitas sistem teknologi informasi. Dengan adanya komputerisasi di pemerintahan perlu adakannya Sistem Keamanan Jaringan yang baik, agar pertukaran data dari kantor kabupaten ke kantor desa dapat dilakukan secara aman dan terkendali. Berbagai software sudah bisa mengatasi permasalahaan tersebut, akan tetapi dari segi keamanan data itu sendiri yang masih sangat dikhawatirkan kebocoran datanya, oleh karena itu dengan menggunakan teknologi *VPN* dengan metode *PPTP* sangat cocok digunakan untuk mengamankan pertukaran data, karena proses kerja *VPN* yaitu dengan membuat jaringan sendiri yang sifatnya rahasia dengan menggunakan IP Publik, membuat keamanan data lebih terjaga kerahasiaannya dan mencegah kebocoran data oleh pihak-pihak yang tidak bertanggung jawab.

Keywords: *VPN*, *PPTP*, Keamanan Jaringan, mikrotik, Data.

Abstract

Network Security Systems are increasingly developing along with technological developments. Agencies have done computerization, where every part in the agency has used computers in its operations, this has made government agencies improve the quality and quantity of information technology systems. With computerization in government it is necessary to have a good Network Security System, so that data exchange from district offices to village offices can be done safely and in a controlled manner. Various software can overcome these problems, but in terms of data security itself that is still very much concerned about data leakage, therefore using VPN technology with PPTP method is very suitable to be used to secure data exchange, because the VPN work process is to create its own network which is confidential by using Public IP, makes data security more confidential and prevents data leakage by irresponsible parties.

***Keywords: VPN, PPTP, Network Security, proxy, Data**.*

1. 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.Desa Ketaraharja merupakan salah satu Instansi Pemerintah Daerah Jawa Barat yang berada di Kabupaten Ciamis Jawa Barat yang memiliki luas wilayah 107,95 HA. Secara administratif Desa Kertaraharja terdiri dari dari 3 Dusun, 8 Rukun Warga dan 27 Rukun Tetanggga, adapun permasalahan yang terjadi dalam menjalankan roda Pemerintahan sistem informasi jaringan Desa Kertaraharja tersebut belum terintegrasi atau belum efisien seperti pengiriman sejumlah data yang mau di kirim ke Kecamatan dalam jaringan secara bersamaan ke server yang mengakibatkan troubleshooting, traffic dan gagal dalam pengiriman data tersebut. Kepala Desa menginginkan jaminan keamanan file data penting Desa agar tepat sampai ke tempat tujuan atau di Kecamatan yang di tuju yang mana pengiriman data penting itu menggunakan internet atau terhubung ke internet.Internet merupakan jaringan public yang merupakan jaringan dengan ketidaktersediaannya garansi keamanan di dalam koneksinya. Internet merupakan jaringan komputer yang terhubung menggunakan standar sistem global Transmission Control Protocol/Internet Protocol (TCP/IP) sebagai protokol(Supriyanto, 2019).

pertukaran paket data untuk melayani pengguna di seluruh dunia. Dengan internet, maka lalu lintas data dari seluruh belahan dunia dapat saling berbagi informasi yang diperlukan. Internet Protocol (IP) merupakan inti dari TCP/IP dan merupakan protokol terpenting dalam Internet Layer, dimana IP menyediakan pelayanan pengiriman paket pada jaringan TCP/IP yang dibangun. Teknologi internet ini menggunakan fasilitas layanan yang biasa kita sebut dengan World Wide Web (www)

Menurut (Nugroho, Widada, & Kustanto, 2015) Dengan memanfaatkan internet, Selain mudah dan cepat, penggunaan internet dapat menekan biaya operasional perusahaan. Tetapi dengan segala kelebihannya, internet juga memiliki kelemahan. Internet yang dapat diakses oleh semua orang membuatnya menjadi tidak aman untuk mengirimkan informasi yang sifatnya rahasia. Apalagi sudah banyak bermunculan aplikasi-aplikasi yang bisa membobol pesan dengan sangat mudah, yang dilakukan oleh para hacker yang tidak beranggung jawab. Oleh karena itu,

penggunaan internet di dalam instansi juga harus disertai dengan penggunaan sistem keamanan yang terpercaya. Saat ini, Internet juga dapat digunakan untuk menghubungkan jaringan intranet kantor pusat, yaitu sebuah jaringan internal yang berada di dalam perusahaan, dengan 1 atau 2 jaringan intranet di kantor cabang. Teknologi jaringan yang dapat mendukung hal ini adalah teknologi VPN, yaitu teknik yang dapat menghubungkan beberapa jaringan local melalui jaringan publik (internet) dengan teknik VPN komunikasi seakan-akan kedua jaringan tersebut berada di dalam satu jaringan intranet yang besar. (Santoso, 2018). Teknologi private network (jaringan pribadi) adalah suatu komunikasi dalam jaringan sendiri yang terpisah dari jaringan umum.

Untuk mengatasi masalah keamanan dalam komunikasi data antara Kantor Kabupaten dan Kantor Desa maka dibutuhkan Virtual Privat Network (VPN) dengan metode PPTP (Point To Point Tunneling Protocol) . Secara garis besar VPN adalah suatu jaringan lokal yang terhubung melalui media jaringan publik. Dan PPTP adalah suatu protokol jaringan yang memungkinkan pengiriman data secara aman dari remote client kepada server perusahaan swasta dengan membuat suatu virtual private network (VPN) melalui jaringan data berbasis TCP/IP (Nugroho et al., 2015).

Menurut (Supendar, 2016)"Teknologi VPN (Virtual Private Network) memungkinkan setiap orang untuk dapat mengakses jaringan lokal dari luar dengan menggunakan internet. Melalui VPN, maka user dapat mengakses sumber daya yang berada dalam jaringan lokal, mendapatkan hak dan pengaturan yang sama seperti secara fisik berada di tempat dimana jaringan lokal itu berada. Keamanan data dan ketertutupan transmisi data dari akses yang tidak berhak dalam transmisinya pada internet menjadi standar utama dalam VPN, sehingga dalam VPN selalu disertakan akan fitur utama yaitu enkripsi dan tunneling.

2. Bahan Dan Metode

Virtual Private Network (VPN) adalah sebuah teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk dapat bergabung dengan jaringan local (Jordy Lasmana Putra 1, Luthfi Indriyani2, 2018). Dengan cara tersebut maka akan didapatkan hak dan pengaturan yang sama seperti halnya berada di dalam kantor atau LAN itu sendiri, walaupun sebenarnya menggunakan jaringan milik publik. Jaringan Virtual Private Network (VPN) sudah banyak meluas sehingga dapat melakukan penelitian Implementasi

Jaringan VPN Menggunakan Teknologi GRE Tunnel, serta dapat menghubungkan lebih dari satu router lainnya. Dengan menggunakan protokol GRE mampu menghantarkan paket (Umam & Roza, 2016)Penggunaan Virtual Private Network merupakan salah satu untuk membangun jalur komunikasi yang aman client dan remote server melalui jaringan public. Dengan adanya penelitian ini bertujuan untuk merancang serta mengimplementasikan VPN, serta menggunakan metode Point to Point Tunneling Protokol pada Kantor Desa Kertaraharja, Sedangkan VPN merupakan sebuah jaringan yang dibuat untuk melakukan transaksi data antara 2 atau lebih pengguna jaringan (Farly, Najoan, & Lumenta, 2017). Pada jaringan tersebut, masih menggunakan internet sehingga faktor sangat penting. Pada penelitian ini tentang rancang bangun sistem keamanan data di Kantor Desa Kertaraharja menggunakan VPN untuk mengamankan data yang akan dikirim, Pada mulanya sistem jaringan kelas menengah dan luas yaitu MAN dan WAN dikembangkan dengan menggunakan sistem sambungan langsung. Sistem ini menawarkan kecepatan transfer data yang tinggi namun membutuhkan investasi yang mahal. Sistem ini tidak efektif untuk perusahaan kelas menengah ke bawah serta perusahaan yang tersebar di berbagai wilayah yang berjauhan. Perkembangan internet yang sangat cepat menawarkan solusi untuk membangun sebuah intranet menggunakan jaringan publik (internet). Di lain pihak, kekuatan suatu industri juga berkembang dan menuntut terpenuhinya lima kebutuhan dalam intranet yaitu :

a) Kerahasiaan, dengan kemampuan mengacak atau enkripsi pesan sepanjang jaringan yang tidak aman.
b) Kendali akses, menentukan siapa yang diberikan akses ke suatu sistem atau jaringan, sebagaimana informasi apa dan seberapa banyak seseorang dapat menerima.c. Autentifikasi, yaitu menguji identitas dari dua ujung yang sedang melaksanakan transaksi.
c) Integritas, menjamin bahwa file atau pesan tidak berubah dalam perjalanan.
d) Non-repudiation, yaitu mencegah dua ujung saling menyangkal, bahwa mereka telah mengirim atau menerima sebuah file.

Kebutuhan ini sepenuhnya didukung oleh internet yang memang dirancang sebagai jaringan terbuka dimana pengguna mendapatkan kemudahan untuk transfer dan berbagi informasi. Solusi untuk tantangan ini adalah jaringan maya pribadi , lebih

dikenal sebagai VPN (Virtual Private Network) VPN memanfaatkan jaringan internet yang bekerja berdasar TCP/IP sebagai media intranet sehingga jangkauannya menjadi luas tanpa investasi yang besar. VPN menghadirkan teknologi yang mengamankan segala lalu lintas jaringan virtual sehingga memberikan rasa aman bagi semua pemakai jaringan(Satukan Halawa, 2016)**.**

Berikut adalah kriteria yang harus dipenuhi oleh *VPN* dalam menjawab tantangan industri tersebut:

a. *Autentikasi* pengguna

b. *Management* pengalamatan

c. *Enkripsi* data.

d. *Management* kunci

e. Dukungan untuk *multiprotocol*.

Protokol adalah bahasa atau standarisasi yang digunakan oleh dua buah media komputer atau lebih untuk agar dapat saling berkomunikasi. Beberapa *protokol* yang digunakan untuk pengembangan *VPN* adalah sebagai berikut:

a. *PPTP (Point to Point Tunelling Protocol)*

b. *L2TP (Layer Two Tunneling Protocol)*

c. *IPSec (Internet Protocol Security)*

d. *PPTP over L2TP*

e. *IP-in-IP*

Dua buah *protokol* yang paling sering digunakan adalah *PPTP* dan *IPSec*. Pemilihan *protokol* lebih banyak ditentukan oleh kondisi yang dihadapi pada saat *setting VPN* daripada oleh kebutuhan. Misalnya, jika pada saat *setting VPN server Windows NT* maka *protokol* yang digunakan adalah *PPTP* karena *protokol* ini adalah *default* dari *Windows NT*. Sedangkan setting *VPN* menggunakan *router* dengan tujuan pengguna akhir, maka *VPN* yang digunakan adalah *IPSec* karena *protokol* ini yang biasanya ter*install* secara *default* pada *router* tersebut (Oktivasari & Utomo, 2016)

2.1 Point to Point Tunneling Protokol (PPTP)

PPTP merupakan *protocol* jaringan yang memungkinkan pengamanan *transfer* data dari *remote client* ke *server* pribadi perusahaan dengan membuat sebuah *VPN* melalui *TCP/IP*. *Teknologi* jaringan *PPTP* merupakan pengembangan dari *remote access Point-toPoint protocol* yang dikeluarkan oleh *Internet Engineering Task Force* (*IETF*). *PPTP* merupakan *protocol* jaringan yang merubah paket *PPTP* menjadi *IP datagram* agar dapat ditransmisikan melalui *intenet*. *PPTP* juga dapat digunakan pada jaringan private *LAN-to LAN*. (Nugroho et al., 2015)

Salah satu *service* yang biasa digunakan untuk membangun sebuah jaringan VPN adalah *Point to Point Tunnel Protocol* (PPTP). Sebuah koneksi PPTP terdiri dari *Server* dan *Client*. Mikrotik Router OS bisa difungsikan baik sebagai *server* maupun *client* atau bahkan diaktifkan

keduanya bersama dalam satu mesin yang sama. *Feature* ini sudah termasuk dalam *package PPTP* sehingga perlu di cek di menu *system package* apakah paket tersebut sudah ada di *router* atau belum(Dahnial, 2019). Fungsi *PPTP Client* juga sudah ada di hampir semua OS, sehingga bisa menggunakan *Laptop/PC* sebagai *PPTP Client*.

PPTP ini digunakan untuk jaringan yang sudah melewati *multihop router* (*Routed Network*) (Umam & Roza, 2016). Jika ingin menggunakan *PPTP* pastikan di *Router* anda tidak ada *rule* yang melakukan *blocking* terhadap *protocol TCP 1723* dan IP *Protocol* 47/GRE karena *service PPTP* menggunakan *protocol* tersebut.

Adapun kesimpulan yang dapat penulis kutip dari bab-bab sebelumnya jaringan komputer adalah jaringan yang dapat melakukan komunikasi data dari komputer satu ke komputer lainnya agar dapat terkonesi dengan baik. Dengan Teknologi *Virtual Private Network* (*VPN*) dapat membentuk jaringan *private* antar dua tempat atau lebih yang cukup dengan memanfaatkan jaringan *public* (*internet*) dan dengan metode *Point To Point Tunneling Protocol* (*PPTP*) pengiriman data dapat di lakukan dengan secara aman dan *efisien* tanpa mengalami *traffic*, dan gagal pengiriman data(Umam & Roza, 2016) . Dimana dengan *Point To Point Tunneling Protocol* (PPTP) pun kita bisa melakukan *management Bandwidth* dimana yang pada awalnya kondisi *bandwidth* jaringan masih dalam keadaan normal, namun seiring berjalannya waktu, maka jumlah *client* semakin banyak dan ini berakibat pada meningkatnya pemakaian *bandwidth* yang ada pada jaringan computer (Saputra, 2016).

2.2 PPTP (Point to Point Tunnel Protocol)

PPTP merupakan salah satu type VPN yang paling sederhana dalam konfigurasi. Selain itu juga fleksibel. Mayoritas operating system sudah support sebagai PPTP Client, baik operating system pada PC ataupun gadget seperti android. Komunikasi PPTP menggunakan protokol TCP port 1723, dan menggunakan IP Protocol 47/GRE untuk enkapsulasi paket datanya(Riskiono, 2019). Pada setting PPTP, kita bisa menentukan network security protocol yang digunakan untuk proses autentikasi PPTP pada Mikrotik, seperti pap,chap,mschap dan mschap2. Kemudian setelah tunnel terbentuk, data yang ditransmisikan akan dienkripsi menggunakan Microsoft Point-to-Point Encryption (MPPE)(Kurniawan, 2018). Proses enskripsi biasanya akan membuat ukuran header paket yang ditransmisikan akan bertambah. Jika kita monitoring,

traffick yang melewati tunnel PPTP akan mengalami overhead(Mahardiyanto, 2016).

Dalam penelitian , Penulis akan melakukan beberapa metode dalam proses pengumpulan data, antara lain :

A. Analisa kebutuhan

Pada tahap ini dilakukan analisis kebutuhan mengenai spesifikasi jaringan internet yaitu dengan menetapkan kebutuhan penelitian yang menguraikan tentang strategi pengembangan jaringan, mengusulkan sebuah konsep arsitektur jaringan dengan topologi yang tepat dengan mengidentifikasikan pemanfaatan teknologi yang dapat memberikan dukungan rancangan hingga implementasi(Azhar & Romliyanto, n.d.).

B. Desain

Pada tahap ini dilakukan desain jaringan komputer yang ada pada Kantor Desa Kertaraharja dengan aplikasi *Microsot Visio 2016* yaitu desain jaringan komputer *VPN* pada Instansi tersebut yang selanjutnya dapat diimplementasikan pada pengembangan jaringan komputer.

C. Testing

Pada tahap ini desain jaringan komputer VPN yang telah dibuat akan diuji coba sehingga dapat diketahui bahwa desain jaringan tersebut berhasil di jalankan.

D. Implementasi

Tahapan implementasi menitik beratkan pada rancang bangun jaringan VPN yang sudah diuji sehingga dapat diimplementasikan pada Kantor Desa Kertaraharja.

Di dalam penelitian ini penulis melakukan implementasi *Virtual Private Network* dengan metode PPTP. Oleh sebab itu untuk mendukung penelitian ini penulis memerlukan beberapa perangkat keras dan perangkat lunak. Dibawah ini adalah analisa kebutuhan yang diperlukan dalam penerapannya :

a. Perangkat Keras (*Hardware*)
   1. Notebook/Laptop sebagai administrator untuk melakukan konfigurasi pada router mikrotik
   2. Modem untuk menghubungkan Kantor Kabupaten dan Kantor Desa

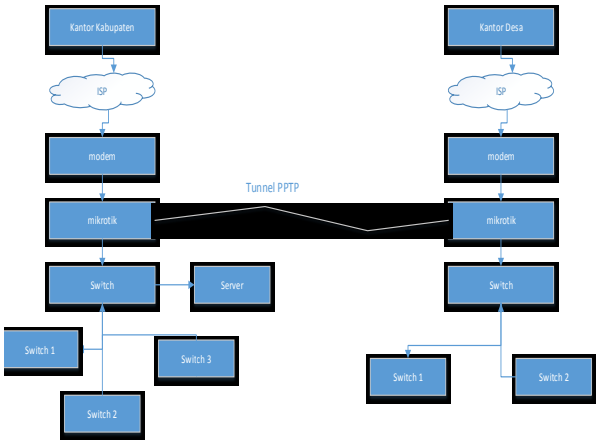
b. Perangkat Lunak (Software)
   1. OS (*Operating System*) Windows 10
   2. Aplikasi *Winbox tools*
   3. *Vmware*
   4. Mikrotik RouterOS

3. Hasil Dan Diskusi

Desain dan perencanaan yang dilakukan adalah membangun jaringan dengan menggunakan fitur *tunneling protocol* untuk membuat sebuah jalur *private* antara koneksi kantor kabupaten

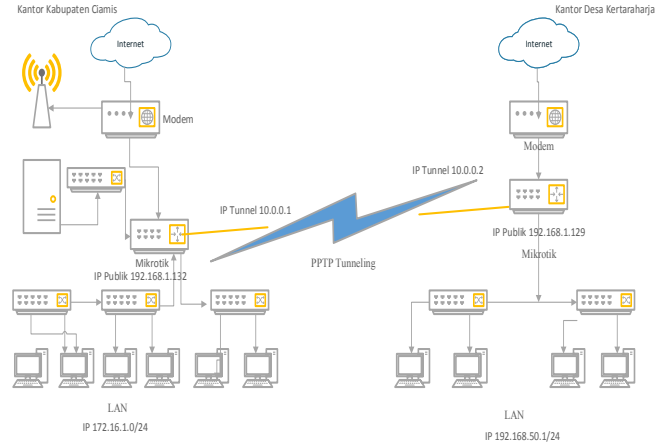
maupun kantor desa dengan aman. Begitu pun staff/karyawan dapat mengakses kantor instansi dengan aman meskipun dalam jarak jauh. Maka blok dan skema usulan yang diajukan dengan konfigurasi *Tunneling PPTP* yang dikonfigurasi dimikrotik pada masing-masing kantor

3.1. Blok Jaringan



Gambar 1. Blok Jaringan

3.2 Skema Jaringan



Gambar 2. Skema Jaringan

3.3 Keamanan Jaringan

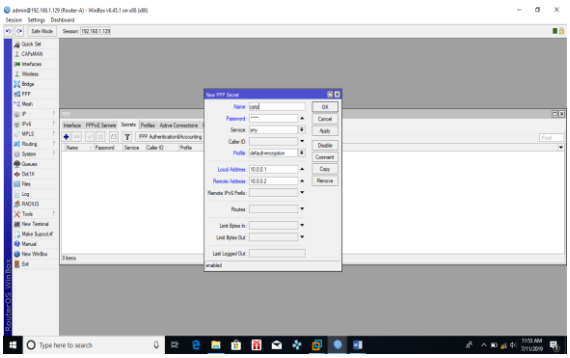
Sistem keamanan yang diterapkan baik pada kantor Kabupaten maupun kantor Desa, menerapkan *VPN* dengan metode *PPTP* untuk sistem keamanan jaringannya. Sehingga dapat mencegah kebocoran data ke luar karena *VPN* menggunakan jaringan yang *private*, sehingga keamanan data perusahaan lebih terjaga kerahasiaannya, baik di kantor Desa maupun di kantor Kabupaten.

3.4 Konfigurasi Sistem Jaringan

Berikut adalah konfigurasi Design dan Implementasi Jaringgan *Virtual Private Network (VPN)* dengan metode *Point To Point Tunneling Protocol (PPTP)* dengan Basis Mikrotik, dengan melakukan konfigurasi pada beberapa ethernet, seperti ethernet untuk *ip public, ip local, Dns, dll*. Kemudian *login* pada *winbox* dengan *ip public*. Lalu mulai mengkonfigurasi pada *winbox* mulai dari konfigurasi *ip address*, sampai pada konfigurasi *VPN*

1. Pada router A, *enable*-kan *PPTP Server*. Pilih *PPP* dan pilih *PPTP Server*.

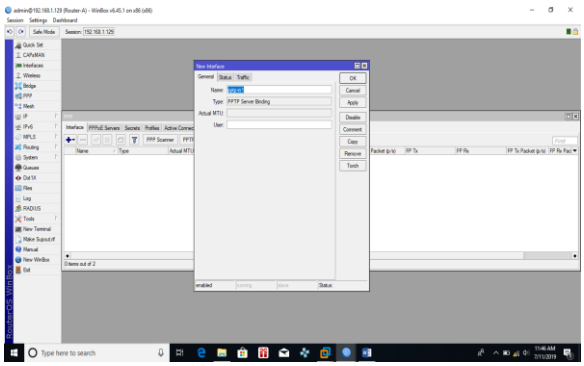
2. Buat secret untuk login pptp > klik menu secret > masukan nama dan pass > profil isi default encryption > isi local address untuk jalur akses pptp dan isi remote address untuk destinasi tujuan. Dapat dilihat pada gambar di bawah ini :



Gambar 3.Konfigurasi jaringan VPN

3. Buat pptp server > klik pptp server binding. Dapat dilihat pada gambar di bawah ini :

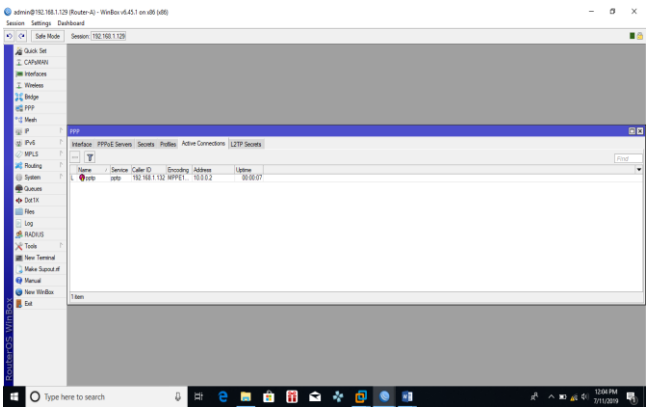
4. Membuat nama/*user* untuk *PPTP Server*. Dapat dilihat pada gambar di bawah ini :



Gambar 4. Konfigurasi jaringan untuk PPTP

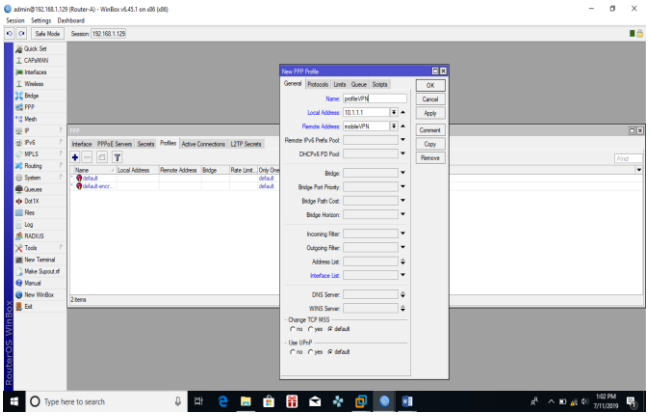
5. Pilih dial out > lalu isi beberapa *parameter* yang di perlukan supaya *router* B bisa terkoneksi ke *router* A

6. Cek konektivitas user *PPTP client* pada router A. Dapat dilihat pada gambar di bawah ini



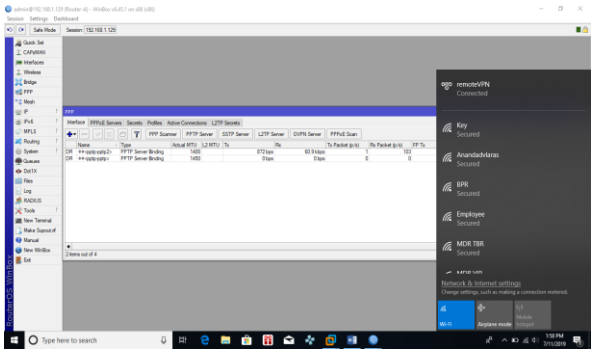
Gambar 5.Cek Konektivitas user

7. Pembuatan gateway untuk *PPTP*. Klik ip > route > dst addres isi dengan ip public Router-B / Router-A > gateway pilih user pptp yang sudah dibuat.
8. Membuat konfigurasi VPN. Dapat dilihat pada gambar di bawah ini :



Gambar 6.Konfigurasi jaringan VPN

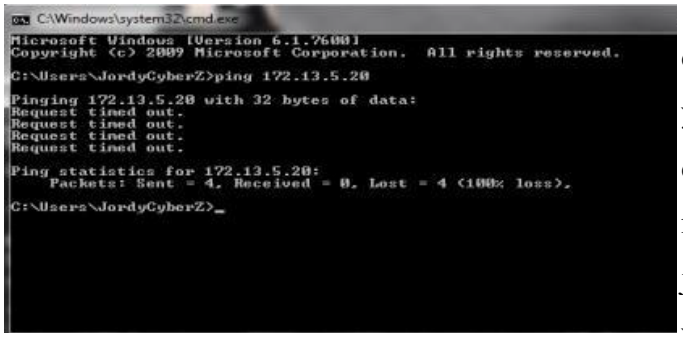
9. Hasil penyambungan ke VPN. Dapat dilihat pada gambar di bawah ini



Gambar 7. Hasil penyambungan VPN

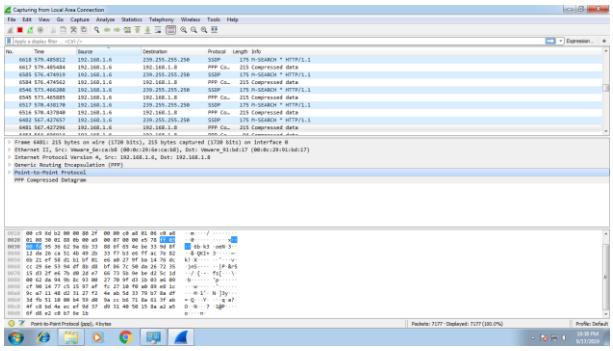
3.4 Evaluasi Konfigurasi Sistem Jaringan

Sebelum melakukan konfigurasi, pengujian awal yang di lakukan adalah melakukan test ping, yang mana Kantor Desa Kertaraharja dan Kantor Kabupaten Ciamis belum terhubung.



Gambar 8. Hasil pengetesan jaringan melalui cmd

Setelah melakukan konfigurasi, karyawan/staff dapat mengakses kantor instansi menggunakan jaringan dengan aman, walaupun karyawan tersebut berada di luar kantor instansi. Waktu yang dibutuhkan untuk menghubungkan jaringan lokal ke tempat lain juga semakin cepat. Dan berikut tampilan setelah Kantor Desa dan Kantor Kabupaten terhubung melalui VPN dengan metode PPTP.



Gambar 9. Hasil tes jaringan vpn pptp

Tampilan terhubung dengan VPN dengan metode PPTP

3.5 Evaluasi Keamanan Jaringan

Evaluasi keamanan jaringan yang di terapkan menunjukan hasil bahwa aktivitas di jaringan VPN lebih baik karena aktivitas yang di lakukan didalam tunnel *VPN* tidak di ketahui oleh orang lain. Selain itu dengan menerapkan *PPTP* sebagai keamanan jaringan meskipun bukan termasuk *VPN* yang aman dan *PPTP* pun bagus untuk digunakan sebagai keamanan cadangan.

4. Kesimpulan

Berdasarkan pembahasan yang sudah dibahas pada bab sebelumnya maka dapat disimpulkan bahwa metode tunneling *protocol PPTP (Point-To-Point Tunneling Protocol)* yang di terapkan pada Kantor Desa Kertaraharja berdampak sangat positif karena dengan adanya penerapan metode

tunneling tersebut jaringan komputer antara kantor dapat saling berkomunikasi, dengan itu pekerjaan dan pertukaran informasi akan menjadi semakin fleksibel dan semakin cepat, dan juga administrator jaringan tidak perlu repot-repot melakukan kunjungan untuk memonitoring jaringan yang sedang berjalan pada masing-masing kantor.

References

Azhar, R., & Romliyanto, E. (n.d.). *ANALISA PERBANDINGAN Protokol Pptp Dan L2tp Menggunakan Video Call Melalui Jaringan Virtual Private Network (Vpn) Comparative Analysis Pptp Protocol And L2tp Using Video Call Through Virtual Private Network (Vpn)*. 13–21.

Dahnial. (2019). *Analisa Perbandingan Quality Of Service Antara Protokol PPTP dan L2TP Pada Virtual Private Network Berbasis Router Mikrotik*. *10*(02), 107–113.

Farly, K. A., Najoan, X. B. N., & Lumenta, A. S. M. (2017). *Perancangan dan Implementasi VPN Server dengan menggunakan Protokol SSTP (Secure Socket Tunneling Protocol) Studi Kasus Kampus Universitas Sam Ratulangi*. *11*(1).

Jordy Lasmana Putra 1, Luthfi Indriyani2, Y. A. (2018). *Penerapan Sistem Keamanan Jaringan Menggunakan*. *3*(2), 260–267.

Kurniawan, A. (2018). No Title. *Jom Fteknik*, *5*(Analisa Performansi Trafik Multimedia Pada Pemodelan Jaringan Vpn Menggunakan Metode Clsa), 1–8.

Mahardiyanto, M. P. (2016). *Jurnal JARTEL*. (November), 32–38.

Nugroho, I., Widada, B., & Kustanto. (2015). Perbandingan Performansi Jaringan Virtual Private Network Metode Point To Point Tunneling Protocol (Pptp) Dengan Metode Internet Protocol Security. *Jurnal TIKomSiN*, *3*(2), 1–9. https://doi.org/http://dx.doi.org/10.30646/tikomsin.v3i2.197

Oktivasari, P., & Utomo, A. B. (2016). *Analisa Virtual Private Network Menggunakan Openvpn Dan Point To Point Tunneling Protocol Analysis Of Virtual Private Network Using Openvpn And Point To*. 185–202.

Riskiono, S. D. (2019). *Analisis Dan Desain Jalur Transmisi Jaringan Alternatif Menggunakan Virtual Private Network (Vpn)*. *13*(2), 100–106.

Santoso, B. (2018). *Metode Internet Protocol Security (IPSec) Dengan Virtual Private Network (VPN) Untuk Komunikasi Data*. *6*(September), 179–188.

Saputra, D. (2016). *Implementasi Virtual*

Private Network Pada Sistem InforMASI PENGELOLAAN KEUANGAN. *6*(2), 18–31.

Satukan Halawa. (2016). Perancangan Aplikasi Pembelajaran Topologi Jaringan Komputer Untuk Sekolah Menengah Kejuruan (Smk) Teknik Komputer Dan. *Jurnal Riset Komputer (Jurikom),* 66–71.

Supendar, H. (2016). *Implementasi Remote Site Pada Virtual Private Network Berbasis Mikrotik*. *3*(1), 85–98.

Supriyanto, B. (2019). Perancangan Jaringan VPN Menggunakan Metode Point To Point Tunneling Protocol. *Jurnal Teknik Komputer AMIK BSI*, *V*(2). https://doi.org/10.31294/jtk.v4i2

Umam, C., & Roza, E. (2016). *Perancangan Jaringan Keamanan Virtual Private Network (VPN) Siteto Site*. 23–30.