Implementasi Remote Site Pada Virtual Private Network Berbasis Mikrotik

Hendra Supendar [1,*]

[1] Program Studi Teknik Komputer; AMIK BSI Jakarta; Jl. RS Fatmawati No. 24, Pondok Labu - Jakarta Selatan, (021)39843000/ (021)39843007; email : hendrasupendar@gmail.com

* Korespondensi: email : hendrasupendar@gmail.com

Diterima: 5 Meil 2016; Review: 12 Mei 2016; Disetujui: 19 Mei 2016

Cara sitasi: Supendar H. 2016. Implementasi Remote Site Pada Virtual Private Network Berbasis Mikrotik. Bina Insani ICT Journal. 3 (1): 85 – 98.

Abstrak : Penggunaan flashdisk dan email untuk pertukaran data memang sangat dibutuhkan untuk kegiatan bisnis, namun penggunaan email dan pertukaran flashdisk cenderung lemah dalam mengantisipasi tingkat keamanan jaringan tersebut. Teknologi *Virtual Private Network* (VPN) merupakan teknik pengamanan jaringan yang bekerja dengan cara membuat suatu *tunnel* sehingga jaringan yang terpercaya dapat terhubung dengan jaringan yang ada di luar melalui internet. Teknologi ini menggunakan protokol *Point to Point Tunneling Protokol* (PPTP) dengan cara *remote site* merupakan solusi yang dapat di implementasikan pada kegiatan bisnis yang dapat menyediakan sarana transfer data dan jaringan yang lebih aman. Dari hasil pengujian ini dapat dibuktikan bahwa dengan dengan menggunakan jaringan VPN, walaupun mempunyai *packet loss* dari lebih banyak namun mempunyai *round trip* yang kecil dan dapat mendownload data lebih cepat kemudian secara keamanan menunjukkan bahwa mengunakan jaringan VPN terbukti lebih aman.

Kata kunci : *virtual private network*, *remote site*, *packet loss*, *round trip*

Abstract: *The use of flash and email to exchange data is greatly needed for business activities, but the use of email and flash exchanges are generally weak in anticipation of the level of network security. Virtual Private Network (VPN) is a network security technique that works by creating a tunnel to a trusted network can be connected to the existing network outside via the Internet. The technology uses a protocol Point to Point Tunneling Protocol (PPTP) by means of a remote site is a solution that can be implemented on the business activities that can provide a means of data transfer and more secure network. From the test results can be proved that by using a VPN network, despite having packet loss of more but has a small round trip and can download data faster then security shows that using a VPN network proved to be more secure.*

Keywords *: packet loss, remote sites , round trip, virtual private network*

1. Pendahuluan

Perkembangan jaringan komputer sangat pesat. Jaringan komputer sudah menjadi hal mendasar dalam sebuah kegiatan bisnis. Hal ini dapat di lihat dari mayoritas orang-orang di dunia yang sudah pernah mengaskses internet . Apakah akan aman dalam pertukaran data dari kemungkinan aksi Hacking dan data sniffing di dalam internet yang dapat di akses oleh orang-orang di dunia? Maka dari itu dibuat jaringan virtual yang hanya bisa digunakan oleh orang-orang yang mempunyai wewenang untuk mengakses data tersebut, yaitu jaringan pribadi atau di sebut juga Virtual Private Network (VPN). Private network ini dianggap lebih efisien karena kecepatan transfer data yang lebih besar dari pada kecepatan transfer data pada jaringan internet, selain itu keamanan pada jaringan private dianggap lebih bagus karena hanya bergerak dalam lingkup terbatas saja(Irnawan,2014).

Banyak perusahaan besar yang sudah mempunyai anak cabang di berbagai daerah atau

ISSN: 2355-3421 (Print) ISSN: 2527-9777 (Online); 85 – 98

perusahaan perusahaan yang mempunyai banyak rekanan di daerah daerah dan untuk menjalin koneksi dan menjaga keamanan data ketika melakukan suatu pengiriman data yang aman maka dibuatlah sebuah jaringan *Virtual Private Network* (VPN) sebagai solusi dalam pengiriman serta melindungi data penting perusahaan saat melakukan transmisi data. Demikian juga dengan PT. Anta Citra Arges (ACA) dan PT. Interdev (INT), dua perusahaan yang masih satu *owner* ini berjarak cukup jauh dan pertukaran data yang dialakukan olah ke dua perusahaan ini adalah menggunakan email, namun untuk data data yang bersifat penting dan besar cukup sulit bila menggunakan media email tersebut.

Penelitian ini disusun berdasarkan beberapa penelitian sebelumnya, diantaranya dari penelitian yang Berjudul Analisis Perbandingan Kinerja Jaringan Vpn Berbasis Mikrotik Menggunakan Protokol *Point to Point Tunneling Protokol* (Pptp) Dan *Layer 2 Tunneling Protocol* (L2tp) Sebagai Media Transfer Data. Dalam laporan penelitiannya VPN dibangun agar Penggunaan jaringan VPN dapat memberikan sebuah alternatif untuk melakukan akses pada sebuah situs web yang berdekatan dengan dengan jaringan VPN itu sendiri (Irnawan, 2014).

Kemudian penelitian tentang VPN-*PPTP* yang berjudul Perbandingan Performansi Jaringan *Virtual Private Network Metode Point To Point Tunneling Protocol* (Pptp). Tujuan penelitian ini untuk untuk membandingkan performasi tunneling jaringan *Virtual Private Network* metode *Point to Point Tunneling Protocol* (PPTP) dan metode *Internet Protocol Security* (IPsec) yang dapat membantu para pakar jaringan untuk menyesuaikan tunneling mana yang sesuai dengan kondisi lapangan karena dengan penelitian ini dapat terlihat perbadingan performansi dari sisi waktu transmisi, *delay*, *bandwidth*, *jitter* serta *troughput* saat proses transmisi data. Performansi dan arsitektur VPN yang seperti apa yang terbaik (Nugroho, 2015).

Penelitian ini juga di lakukan dengan menggunakan basis teori tentang :

Virtual Private Network *(VPN).*

Virtual Private Network (VPN) adalah sebuah teknologi komunikasi jaringan yang memungkinkan untuk dapat terkoneksi ke jaringan *public* dan menggunakannya untuk dapat bergabung dengan jaringan lokal. Dengan cara tersebut maka akan di dapatkan hak dan pengaturan yang sama seperti halnya berada didalam LAN itu sendiri, walaupaun sebenarnya menggunakan jaringan milik public (Nugroho, 2015).

VPN dapat dibentuk dengan menggunakan teknologi *tunneling* dan enkripsi. Koneksi VPN juga dapat terjadi pada semua layer pada protocol OSI (*Open System Interconnection*), sehingga komunikasi dengan VPN dapat digunakan untuk berbagai keperluan.

Mikrotik

Mikrotik adalah penamaan terhadap sebuah produsen router, yang telah berhasil membuat router yang handal. Ada dua jenis Mikrotik yaitu: perangkat keras, yang dikenal dengan Mikrotik Router Board, dan perangkat lunak yang dikenal dengan Mikrotik RouterOS dengan sistem operasi berbasis LINUX yang dapat diinstal pada komputer rumahan. [4] Mikrotik memiliki beberapa keunggulan, diantaranya dapat membuat PC menjadi router, pembaharuan versinya dilakukan secara berkala, memiliki user interface yang mudah dan konsisten, memiliki banyak cara dalam mengakses dan melakukan pengontrolan, proses instalasi cepat dan mudah serta memiliki banyak fitur(Afdal, 2010).

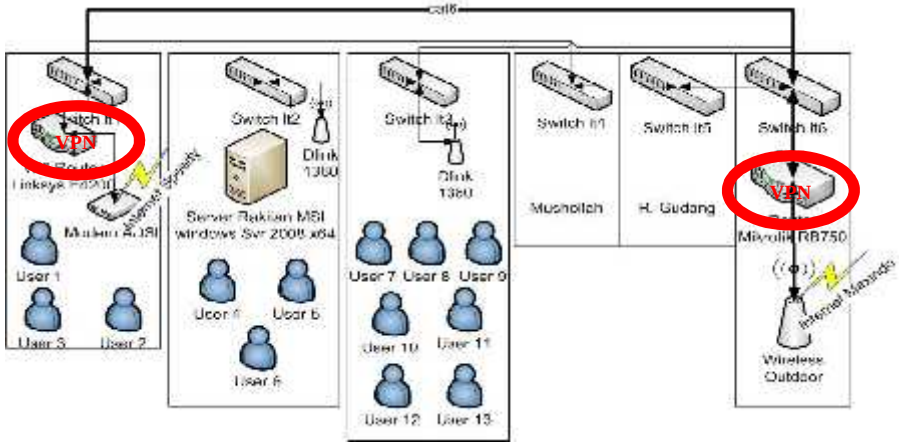
2. Metode Penelitian

Metodologi penelitian ini dilakukan menggunakan metode analisis terhadap kinerja suatu jaringan awal dimana permasalahan yang dihadapi saat ini adalah jaringan yang berada dalam satu area selain berhubungan dan berkomunikasi dengan menggunakan *flash disk* atau *sharing file*. Sementara untuk berhubungan antara kantor dengan kantor menggunakan internet dan email untuk mengirim data dan berkomunikasi. Hal ini menyebabkan keamanan data yang dikirim tidak bisa di jamin. Merancang dan mengimplementasikan *virtual private network* (VPN) menggunakan mikrotik secara remote site merupakan salah satu solusi alternatif dimana dapat membantu komunikasi atau transfer data antar-cabang secara aman melalui jalur koneksi internet seperti seolah-olah melalui jaringan lokal. Dengan merancang VPN ini diharapkan dapat memberi keamanan dan kemudahan proses transfer data dan komunikasi antar-cabang. Setelah di implementasikan maka jaringan VPN tersebut di teliti kembali untuk menguji kehandalannya. Metode ini lebih berkaitan dengan kinerja yang didasarkan oleh beberapa variabel dan parameter. MikroTik digunakan sebagai peralatan utama dalam proses penelitian tersebut.

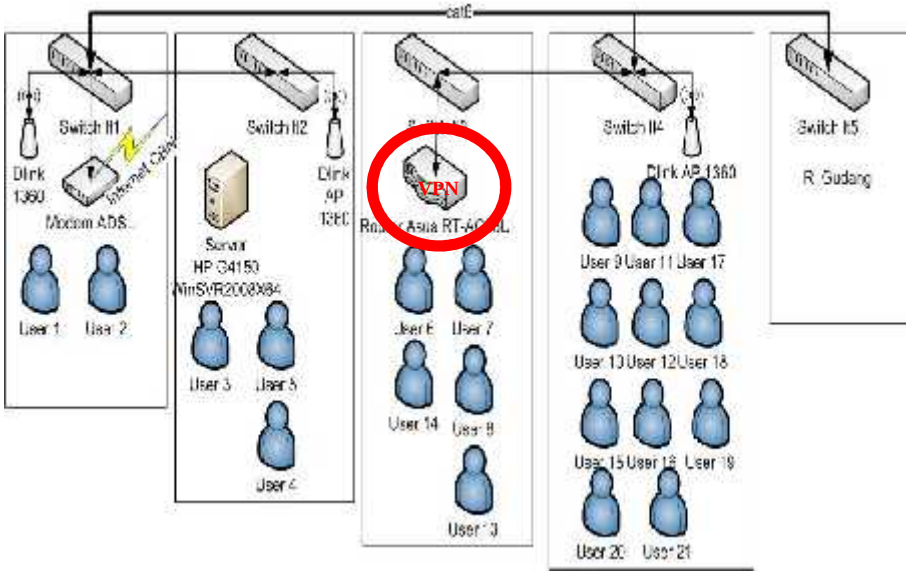
3. Hasil dan Analisis

Untuk melihat apakah *remote site* pada jaringan VPN dapat berjalan baik maka di buat sebuah topologi dan skema jaringan kedua buah perusahaan tersebut. Topologi yang digunakan masih sama yang sedang berjalan pada ACA dan INT. Karena rancangan implementasinya menggunakan router mikrotik yang telah ada pada ACA, router lainnya Linksys E4200 juga bisa diimplimentasikan. Untuk INT walaupun belum ada router mikrotik, router yang ada yaitu Asus RT-AC68U dapat juga diimplementasikan dengan VPN atau support dengan VPN yang akan dirancang.

Skema jaringanpun tidak ada yang berubah. Hanya saja sedikit berbeda pada manajemen jaringannya yaitu yang sebelumnya jaringan *internet* di *dial up* menggunakan *modem* namun pada konsep VPN yang men-*dial up* adalah *router.* Seperti terlihat pada skema jaringan sebagai berikut :



Gambar 1. Skema Jaringan ACA



Gambar 2. Skema Jaringan INT

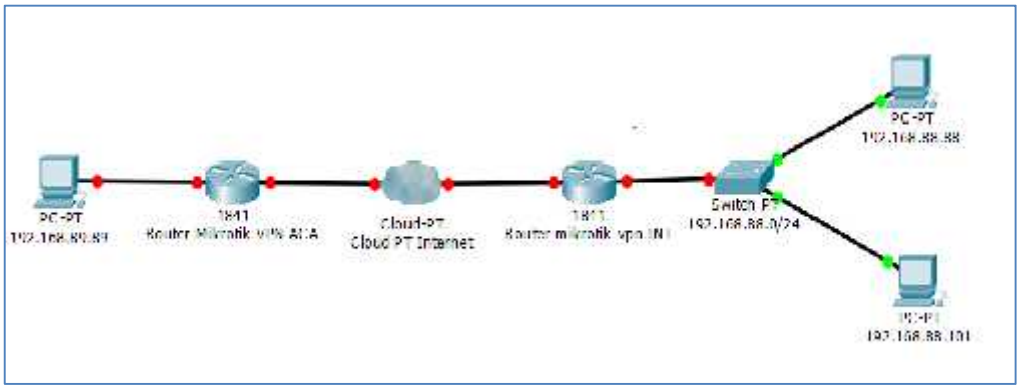
ISSN: 2355-3421 (Print) ISSN: 2527-9777 (Online); 85 – 98

Untuk implementasi yang sesungguhnya pada jaringan ACA hanya perlu mengkonfigurasi salah satu router-nya. Implementasi yang akan dijelaskan disini adalah membahas VPN *remote site* menggunakan mikrotik pada jaringan *public* speedy sebagai simulasi rancangan bahwa VPN ini dapat berjalan pada jaringan yang ada pada perusahaan.

Pengambilan data dilakukan dengan menggunakan jaringan sederhana pada setiap konfigurasi jaringan yang diujikan. Untuk melakukan uji coba terhadap dua Protokol VPN menggunakan topologi jaringan yang sama dengan objek penelitian, dalam perancangan sistem jaringan VPN ini penulis membuat sebuah simulasi yang akan diterapkan pada prakteknya nanti, untuk mempresentasikan topologi jaringan berjalan dengan baik atau tidak. Perancangan atau pembuatan simulasi bertujuan untuk (Seta, 2015):

a. Mengurangi resiko kegagalan saat proses perancangan dan implementasi sistem jaringan VPN dengan PPTP maupun OpenVPN yang sebenarnya.
b. Untuk menjamin bahwa kegagalan atau kesalahan yang terjadi pada waktu proses perancangan, pembangunan dan implementasi tidak mengganggu dan mempengaruhi lingkungan sistem yang sebenarnya.

Sebagai simulasi rancangan, penulis memiliki dua jaringan public speedy sendiri yang diibaratkan sebagai ACA dan jaringan satunya yang diibaratkan sebagai INT. Tentunya simulasi jaringan dengan topologi yang lebih sederhana. Topologinya sebagai berikut:

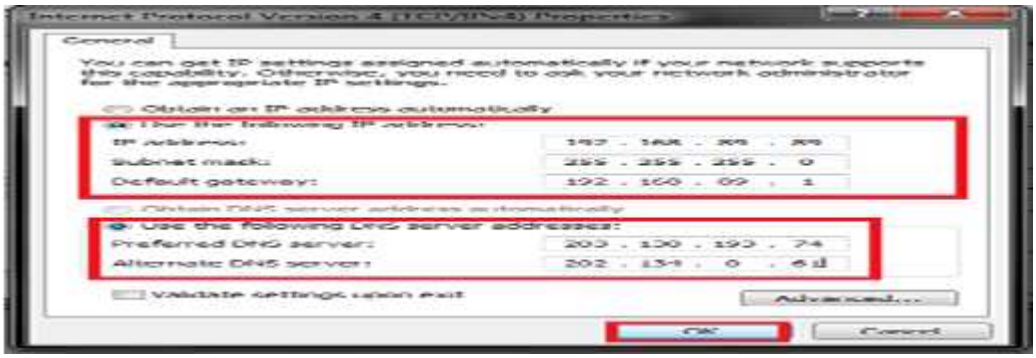


Gambar 3. Rancangan Topologi Simulasi

Konfigurasi Mikrotik Router

Langkah awal untuk membuat jaringan sesuai topologi adalah dengan mengatur IP pada semua perangkat yang akan digunakan. Agar lebih mudah disini akan menggunakan winbox. Konfigurasi yang akan dipraktekan adalah IP jaringan pada VPN ACA, karena konfigurasi pada VPN INT sama persis dengan VPN ACA, yang membedakan hanya IP address-nya saja.

Setting IP address pada PC (192.168.89.89).

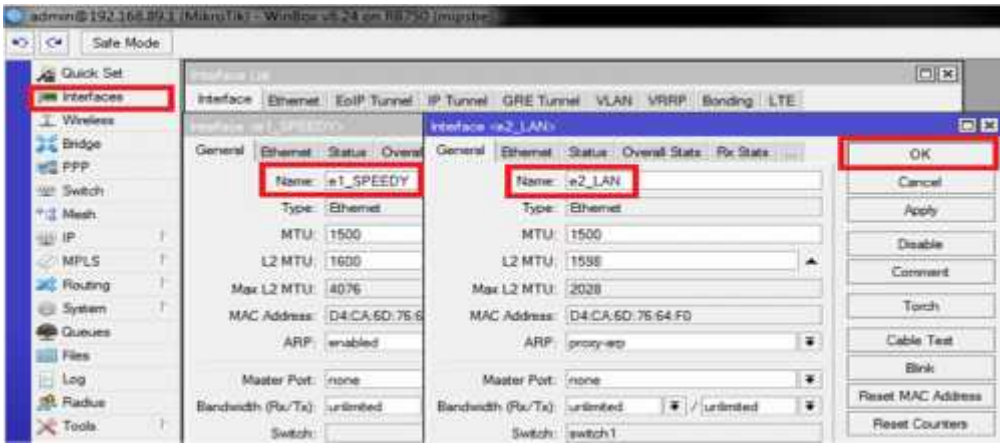


Gambar 4. *Setting IP Address* 192.168.89.89

Download winbox melalui browser dengan IP 192.168.89.1
Buka winbox yang telah di download, isi lalu klik connect

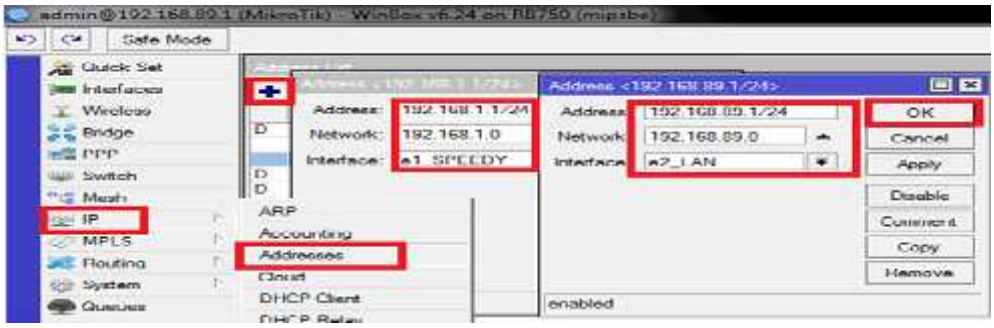
Gambar 5. *Connect WinBox*

Setelah masuk ke winbox, ubah nama ether1 = e1_SPEEDY dan ether2 = e2_LAN dengan cara:
Interface >> Klik 2X ether1 >> isi name dengan e1_SPEEDY.
Interface >> Klik 2X ether2 >> isi name dengan e2_LAN.



Gambar 6. *Setting Interface Name* pada *winbox*

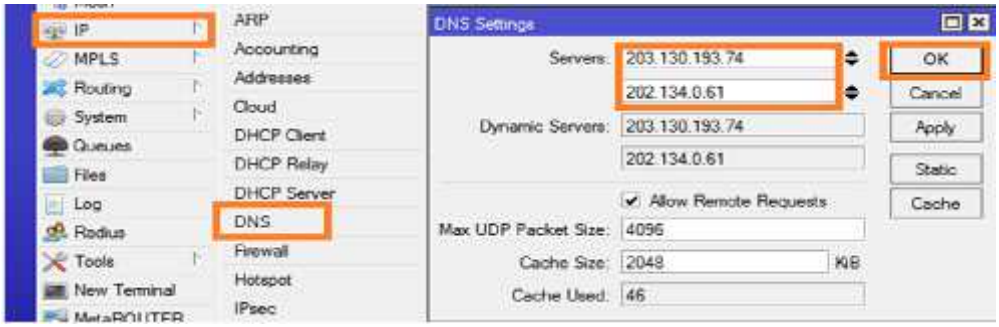
Berikan IP *address* pada e1_SPEEDY = 192.168.1.1/24 dan e2_LAN = 192.168.89.1/24



Gambar 7. *Setting IP Address Interface*

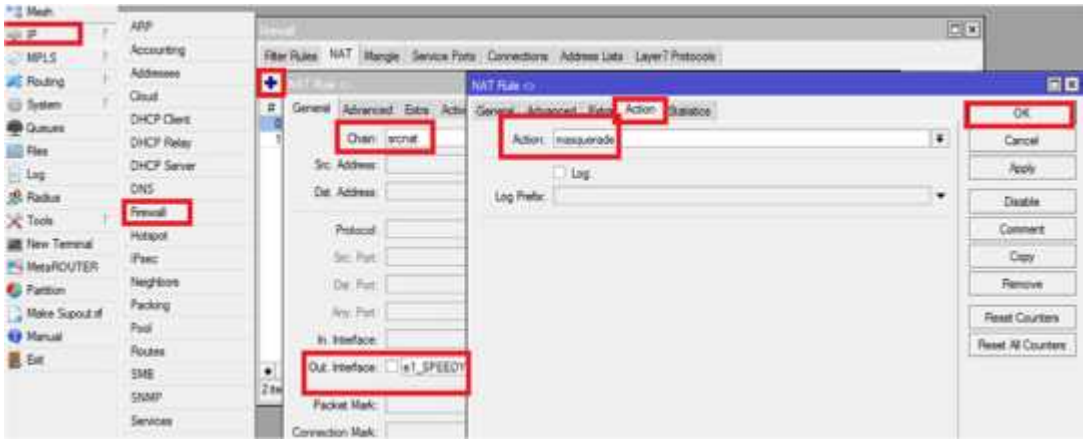
ISSN: 2355-3421 (Print) ISSN: 2527-9777 (Online); 85 – 98

Setting DNS dari Speedy. DNS1 = 203.130.193.74, DNS2 = 202.134.0.61



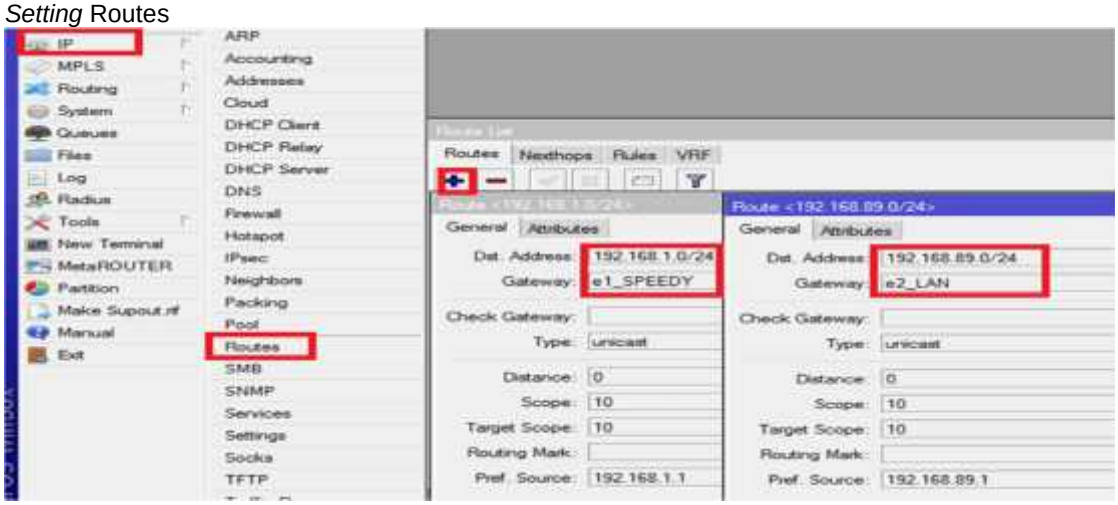
Gambar 8. *Setting* DNS dari Speedy

Setting NAT tujuannya untuk mengatur *interface* mikrotik sebagai *network address translator* sehingga IP *address* LAN dapat mengakses internet.



Gambar 9. *Setting* NAT

Setting Routes



Gambar 10. *Setting Routes*

Lakukan test ping koneksi ke pc client = 192.168.89.89, modem speddy = 192.168.1.254

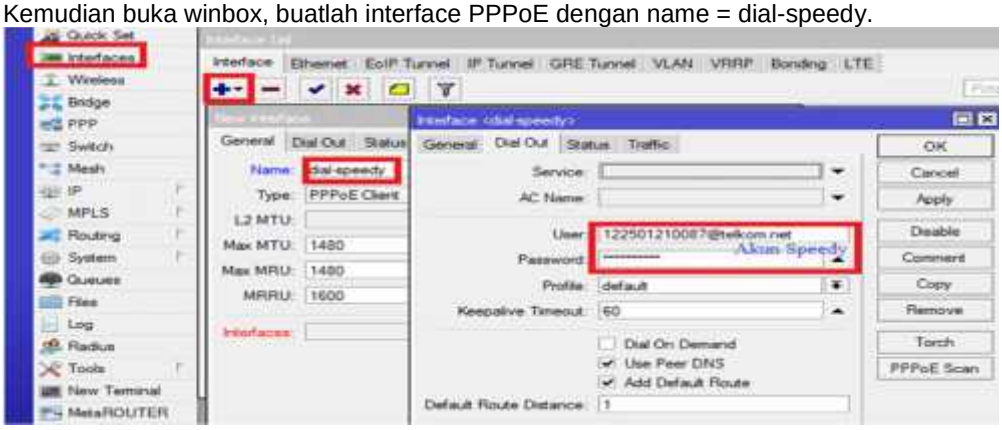
Gambar 11. Test Ping

Konfigurasi Modem ADSL untuk VPN Dial Up

Agar dapat melakukan konfigurasi mikrotik sebagai VPN Server maka Mikrotik tersebut harus di setting dengan IP Public. Sebagai simulasi mengunakan ISP Speedy, maka harus melakukan setting pada Modem ADSL menjadi Bridge Mode.

Gambar 12. Bridge Mode pada Modem Speddy

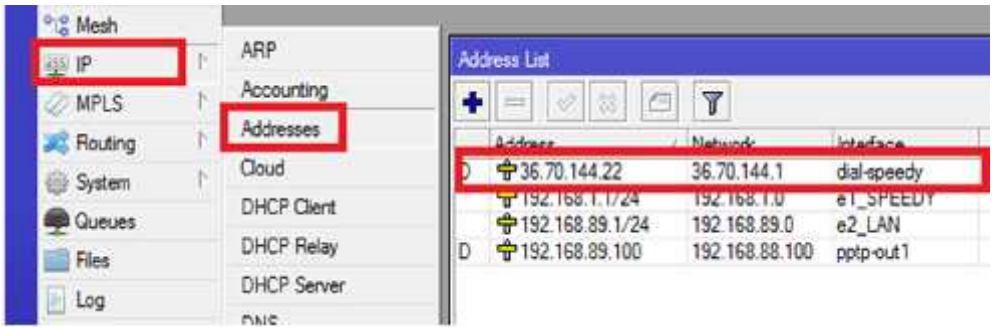
Kemudian buka winbox, buatlah interface PPPoE dengan name = dial-speedy.



Gambar 13. Membuat Interface PPPoE

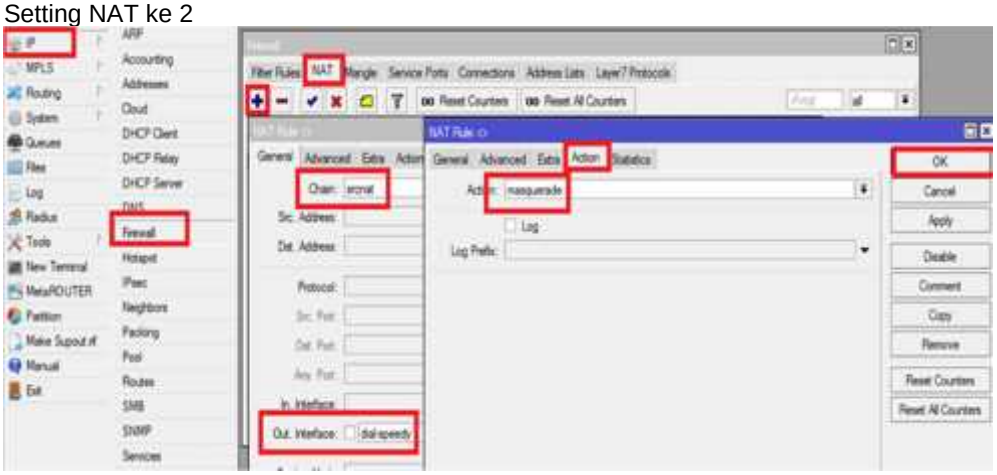
ISSN: 2355-3421 (Print) ISSN: 2527-9777 (Online); 85 – 98

Selesai melakukan setting PPPoE Client maka mikrotik langsung melakukan Dial Up ke modem speedy. Pada IP >> Addresses akan muncul sebuah IP address baru berupa IP public (125.161.64.xxx) dan pada IP >> Routes akan muncul tabel routing baru untuk IP public speedy. Hapus IP >> Routes yang menuju pada IP speedy (192.168.1.254).



Gambar 14. IP *Public* Muncul dari *Setting* PPPoE Client

Setting NAT ke 2



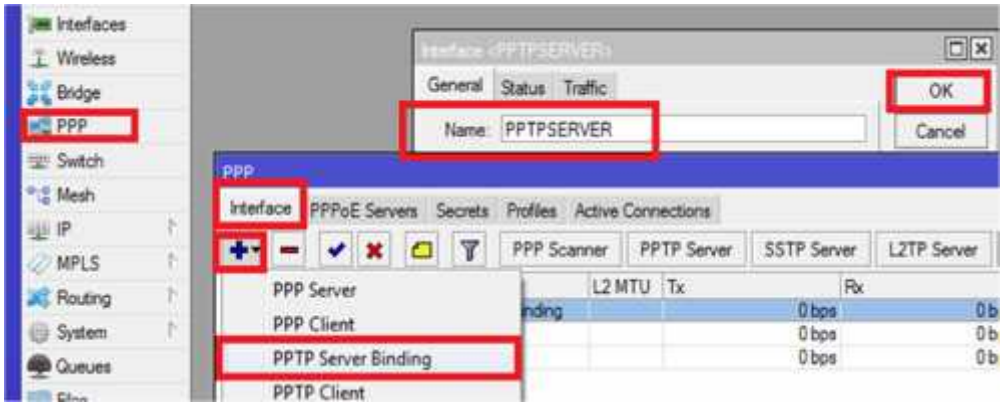
Gambar 15. *Setting* NAT ke 2

Konfigurasi Mikrotik VPN Server

Buatlah IP Pool : yang berfungsi memberikan IP address pada VPN client yang terhubung dengan VPN Server. IP Pool Address = 192.168.89.101 – 192.168.89.150 dengan cara IP >> Pool >>ok

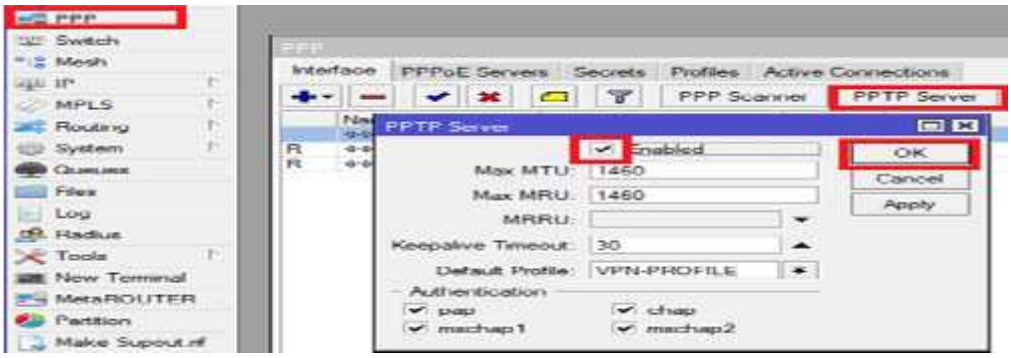
Gambar 16. VPN IP Pool

Buat PPTP Server : PPP >> Interface >> + >> PPTP Server Binding >> isi name dengan PPTPSERVER



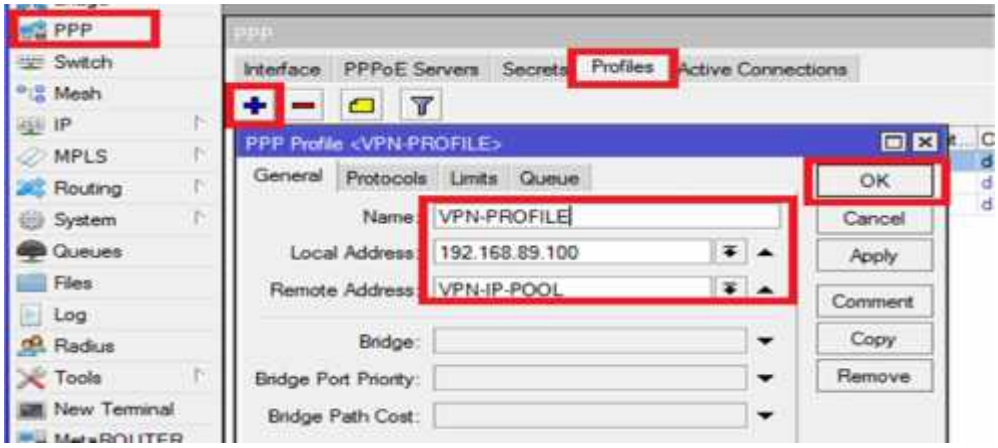
Gambar 17. PPTP server

Aktifkan fitur PPTP (Point to Point Tunneling Protocol) Server.



Gambar 18. *Fitur* PPTP

Buat VPN profile : yang berfungsi untuk me-remote IP pool.



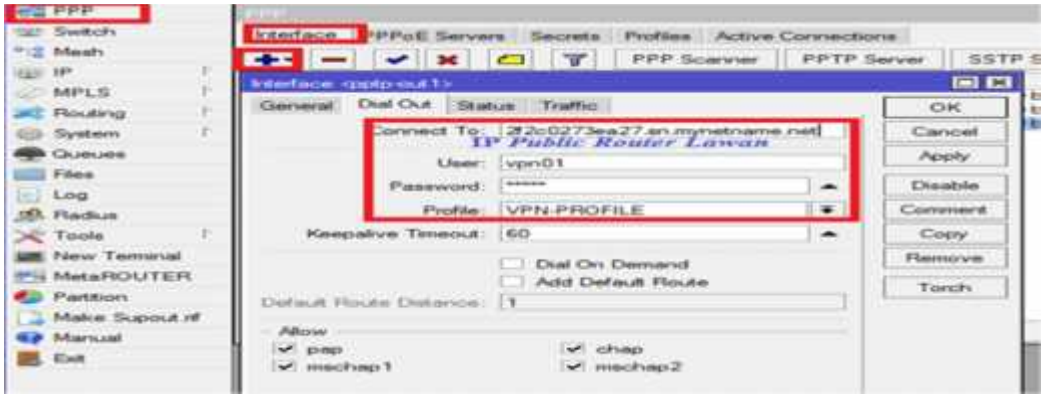
Gambar 19. VPN *Profile*

ISSN: 2355-3421 (Print) ISSN: 2527-9777 (Online); 85 – 98

Buat *account user* : Yang berfungsi sebagai authentikasi untuk koneksi ke VPN server.

Gambar 20. *Account User*

Konfigurasi Mikrotik VPN Client
interface baru PPTP Client :



Gambar 21. *Setting VPN Client*

Konfigurasi VPN Client pada PC

1. Masuk pada menu Control Panel >> *Network and Sharing* Internet, kemudian *create* koneksi baru dengan memilih *Setup a new connection or network*.
2. Pada tampilan window selanjutnya, pilih *connect to a workplace*, lalu klik *next.*
3. Pilih Use My Internet Connection (VPN)
4. masukkan IP publik speedy dan nama VPnnya.

Gambar 22. IP Publik dan nama VPN

5. Masukkan username dan password sesuai pengaturan pada secret.

Gambar 23. Username dan Password

6. Akan ada authentikasi, jika settingan benar maka akan terkoneksi dengan VPN server

Keamanan VPN

Dengan menerapkan VPN ini berarti sistem rancangan yang berjalan telah melakukan keamanan seperti:

1. Protokol VPN yang digunakan adalah PPTP, berarti sesuai konsep PPTP yaitu suatu protokol jaringan yang membungkus paket PPP ke dalam IP Datagram untuk transmisi yang dilakukan melalui jaringan public/internet berbasis TCP/IP.
2. Dengan menggunakan protokol PPTP transmisi data asli yang lewat melalui internet akan di enkripsi dengan MPPE (Microsoft Point to Point Encryption).
3. Untuk dapat terkoneksi dengan VPN ini, user perlu mempunyai username dan password,, pada saat dikoneksikan akan adanya proses authentikasi. Authentikasi ini adalah proses mengidentifikasi komputer/user untuk memulai koneksi VPN.
4. Dengan VPN integritas data akan terjamin, maksudnya paket data yang dilewatkan di jaringan public tidak terjadi perubahan data karena VPN menggunakan metode algoritma *hash message authentication code* (HMAC) versi *Message Digest* 5 (MD5) atau *hash message authentication secure hash algorithm* (HMA-SHA-1).

Pengujian Konektivitas VPN

Merujuk pada penelitian mekanisme pengujian konektifitas dilakukan dengan parameter berikut (Yana, 2012):

1. Packet Loss
2. Round Trip
3. FTP Transfer

Mekanisme pengujian konektivitas jaringan diatas akan penulis lakukan pada rancangan VPN ini. Sebagai data pembanding, penulis informasikan tentang bandwith jaringan masing-masing cabang sebagai berikut: ACA bandwith 2 Mbps, INT bandwith 5 Mbps dan USB modem 3G Sierra 312U 42 Mbps.

1. **Pengujian *Packet Loss***.

Pengujian ini untuk memantau rata-rata minimum dan maksimum *packet loss* yang melalui *tunnel* VPN. Di setiap lokasi pengujian berikut dilakukan ping masing-masing selama 5 menit menggunakan timer sebanyak 10 kali.

Tabel 1. Perbandingan *Packet Loss* pada Tunnel VPN

Jenis Koneksi	IP Sumber	IP Tujuan	*Min. Packet Loss*	*Max. Packet Loss*	*Average Packet Loss* (%)
ACA ke INT	192.168.89.89	192.168.88.88	2	17	10,6
INT ke ACA	192.168.88.88	192.168.89.89	7	20	12
USB *Modem* 3G ke ACA	-	192.168.89.89	0	8	0,13
USB *Modem* 3G ke INT	-	192.168.88.88	1	14	0,66

ISSN: 2355-3421 (Print) ISSN: 2527-9777 (Online); 85 – 98

Hasil : Pada pengujian ini yang terlihat pada Tabel. 1 menunjukkan koneksi VPN menggunakan USB modem 3G lebih baik dibanding dengan ISP Speedy pada ACA dan INT. USB modem 3G dengan VPN yang melakukan test ping ke server data INT dan ACA memiliki packet loss yang sedikit. Ini menunjukkan jaringan modem 3G lebih stabil dari jaringan ISP Speedy pada saat pengujian sebanyak 10 kali test ping.

2. Pengujian *Round Trip*

Pengujian ini untuk menghitung rata-rata dan maksimum waktu *round trip* pada test ping ke server data dengan VPN. Pengujian ini sama halnya pada pengujian *packet loss* dengan ping karena hasilnya satu kesatuan pada perintah ping yaitu untuk menghitung waktu statistik *round trip* dan *packet loss*. Round trip adalah perjalanan paket ping dari komputer yang digunakan untuk melakukan ping, kemudian ke host server data kembali lagi ke komputer client. Atau secara sederhana diartikan perjalanan pulang pergi (Yana, 2012).

Tabel 2. Round Trip pada Tunnel VPN

Jenis Koneksi	IP Sumber	IP Tujuan	*Min. Round Trip* (ms)	*Max. Round Trip* (ms)	*Average Round Trip* (ms)
ACA ke INT	192.168.89.89	192.168.88.88	49	589	86
INT ke ACA	192.168.88.88	192.168.89.89	49	733	94
USB *Modem* 3G ke ACA	-	192.168.89.89	56	2490	133
USB *Modem* 3G ke INT	-	192.168.88.88	68	2702	166

Hasil : Tabel. 2 menunjukkan hasil dari round trip yang telah dilakukan pada proses test ping sebanyak 10 kali ke server data. Test ini mengambil round trip terkecil dan terbesar dalam hitungan milisecond serta rata-ratanya. Tabel tersebut menjelaskan bahwa jaringan ISP Speedy lebih baik dibanding dengan USB modem 3G dari minimum, maximum dan average round trip.

3. Pengujian FTP Transfer

Pengujian ini untuk mengetahui waktu yang dibutuhkan dalam mengambil file (download) dari FTP server pada router mikrotik. Sebelumnya telah disiapkan data pada router mikrotik ACA dan INT dengan file yang sama. Data percobaan berupa dokumen dengan nama file “Cover.docx dan file musik dengan nama “Fatin – Grenade.mp3” ukuran pada Cover.docx sebesar 123 KB dan Fatin – Grenade.mp3 sebesar 2,48 MB.

Berikut adalah hasil pengujian *download file* pada FTP *server,* dengan memperhatikan waktu yang dibutuhkan untuk men-*download file,* alat hitung yang digunakan adalah *stopwatch* dan pengujian dilakukan hanya 1 kali *test download* pada masing-masing koneksi.

Tabel 3. *Download via* FTP pada *Tunnel* VPN

Jenis Koneksi	Data	IP Sumber	IP Tujuan	Waktu
ACA ke INT	Cover.docx	192.168.89.89	192.168.88.88	< 1 detik
	Fatin – Grenade.mp3	192.168.89.89	192.168.88.88	5:13 detik
INT ke ACA	Cover.docx	192.168.88.88	192.168.89.89	< 1 detik
	Fatin – Grenade.mp3	192.168.88.88	192.168.89.89	6:12 detik
USB *Modem* 3G ke ACA	Cover.docx	-	192.168.89.89	2:67 detik
	Fatin – Grenade.mp3	-	192.168.89.89	36:88 detik
USB *Modem* 3G ke INT	Cover.docx	-	192.168.88.88	4:21 detik
	Fatin – Grenade.mp3	-	192.168.88.88	57:97 detik

Hasil : Bahwa waktu yang dibutuhkan untuk men-*download data* pada jaringan ISP Speedy lebih baik dibanding dengan USB *modem* 3G.

4. Pengujian Keamanan VPN

Pengujian keamanan VPN dengan melakukan attack pada komputer server menggunakan metode Denial of Service (DoS). Serangan ini bertujuan untuk menghentikan atau mematikan service pada komputer target dalam hal ini server VPN. DoS yang akan di coba menggunakan aplikasi cmd dengan perintah ping IP target yang akan diserang adalah IP public server vpn INT (36.70.153.4).

Langkah-langkah serangannya adalah sebagai berikut:

Buka command Prompt (start >> run >> cmd)

Tuliskan perintah

Ping 36.70.153.4 –n 10000

n adalah banyaknya paket yang dikrimkan

Efek dari serangan ini akan mengganggu koneksi antara VPN client dan VPN server. Proses ini akan terhenti setelah jumlah paket ping yang dikirimkan telah terpenuhi yaitu 10000 paket maka koneksi IP target normal kembali. DoS ini akan sangat berbahaya jika serangan dilakukan secara bersamaan, aplikasi yang lebih berbahaya adalah pingflood.exe karena dapat menentukan ukuran data yang dikirimkan tiap paketnya.

Untuk mengatasi hal ini, pada mikrotik blokir protokol ICMP (*Internet Control Message Protocol*) agar IP Public tidak dapat di ping.

Selanjutnya, untuk keamanan VPN dilakukan perbandingan antara jaringan tanpa VPN dan jaringan denganVPN. Menurut Nurmansyah (2014) Perbandingan ini untuk menunjukkan bahwa dengan VPN menggunakan protocol PPTP data akan di kompres, paket akan dibungkus (*encapsulation*) PPP dan data yang lewat melalui *internet* akan di enkripsi dengan MPPE (*Microsoft Point to Point Encryption*). Untuk evaluasi jaringan menggunakan *software wireshark*. W*ireshark* adalah *tool* yang ditujukan untuk penganalisisan paket data jaringan.

a. Evaluasi Keamanan Jaringan tanpa VPN

Pengujian ini mencoba melakukan *sniffing* pada jaringan tanpa VPN di CMS dan hasilnya adalah pada koneksi tanpa VPN tidak ada data yang dikompres, tidak ada paket enkapsulasi dan tidak ada paket yang dienkripsi.

b. Evaluasi Keamanan Jaringan dengan VPN

Pengujian ini mencoba melakukan *sniffing* pada jaringan VPN di CMS. dan hasilnya adalah pada koneksi dengan VPN terdapat kompres data pada IP Publik dan enkapsulasi pada IP lokal.

4. Kesimpulan

Dengan menggunakan VPN dapat mempermudah dan efeisiensi waktu dalam pertukaran data hanya dengan mengaktifkan VPN *client.* VPN dengan protokol PPTP terbukti memberikan keamanan pada data dan konektivitas jaringan. Hal ini ditunjukan pada saat VPN *client* melakukan *log in* ke VPN *server* akan terdapat authentikasi *username* dan *password,* terdapat juga enkapsulasi dan enkripsi data serta integritas data yang telah terbukti pada simulasinya.

VPN rentan terhadap serangan *Denial of Service* (DoS) atau serangan lainnya namun dapat ditangani dengan memblokir protokol ICMP sehingga IP public tidak dapat di *ping*. Dengan membandingkan jaringan yang berjalan dengan VPN dan dengan jaringan yang menggunakan modem 3G maka ternyata jaringan yang memgunakan VPN walaupun mempunyai packet *loss* yang lebih banyak namun mempunyai *round trip* yang lebih baik serta memiliki transfer data yang lebih cepat.

Pada evaluasi keamanan jaringan terbukti bahwa menggunakan VPN dengan protokol PPTP terdapat kompres data, enkapsulasi dan enkripsi.

Referensi

Irnawan FD, Triyono J, Rachmawati RY. 2014. Analisis Perbandingan Kinerja Jaringan Vpn Berbasis Mikrotik Menggunakan Protokol Pptp Dan L2tp Sebagai Media Transfer Data. Jurnal JARKOM. 2014 ISSN:2338-6313 Vol. 2 No. 1. hal 26 -35.

ISSN: 2355-3421 (Print) ISSN: 2527-9777 (Online); 85 – 98

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 Teknologi dan Informasi(TIKomSiN). ISSN : 2338-4018 Vol 3, No 2. hal 1-9.

Seta BS, Ridwan M, Wati T. 2015. Perbandingan Virtual Private Network Protokol Menggunakan Point to Point Tunnel Protocol dan OpenVPN. Konferensi Nasional Sistem & Informatika 2015 STMIK STIKOM Bali, 9 – 10 Oktober 2015. Hal 1-6.

Afdhal, Gani TA, Ardiansyah H. 2010. Pengaturan Pemakaian Bandwidth Menggunakan Mikrotik Bridge. Jurnal Rekayasa Elektrika. Oktober 2010. Vol. 9, No. 2. Hal 69-76.

Yana H. 2012. Evaluasi Implementasi Keamanan Jaringan Virtual Private Network (VPN) (Studi Kasus pada CV. Pangestu Jaya). Jurnal Teknologi. Desember 2012. Vol. 5, No 1. Hal 132-142.

Nurmasyah, Rachmat, Akbar M, Yadi IZ. 2014. Perancangan Sistem Keamanan Data Samba Server Berbasis VPN Menggunakan Protokol SSL dan IP Tunneling. Jurnal Ilmiah Teknik Informatika Ilmu Komputer. April 2014. Vol. xx, No.x. Hal 1-08.