SIMULASI *VIRTUAL PRIVATE NETWORK* (VPN) MENGGUNAKAN *SECURE SOCKET TUNNELING PROTOCOL* (SSTP) PADA JARINGAN KAMPUS UNIDAYAN BAUBAU

SIMULATION OF VIRTUAL PRIVATE NETWORK (VPN) USING SECURE SOCKET TUNNELING PROTOCOL (SSTP) ON UNIDAYAN BAUBAU CAMPUS NETWORK

Jabal Nur[1], La Raufun[2], Muhtita Afifa[3]
Program Studi Teknik Informatika
Universitas Dayanu Ikhsanuddin
Jl. Dayanu Ikhsanuddin No.124 Baubau, Sulawesi Tenggara
e-mail: [1]jabalnur@unidayan.ac.id, [2]el.raufun@gmail.com,[*3]afifa.muhtita97@gmail.com

Abstrak

Pertukaran informasi menjadi salah satu kebutuhan yang sangat mendukung kegiatan dalam Universitas. Tugas akhir ini bertujuan untuk mengatur dan mensimulasikan VPN yang menggunakan SSTP pada mikrotik agar dapat menghubungkan kampus palagimata dan kampus istana ilmiah unidayan Baubau. Penelitian ini menggunakan metode ping test dengan menggunakan command prompt dan new terminal. Hasil penelitian menunjukan simulasi sistem telah berhasil dibuat dengan menggunakan VPN SSTP. Dapat disimpulkan bahwa simulasi VPN SSTP ini dapat menghubungkan kampus palagimata dan kampus istana ilmiah unidayan Baubau.
Kata kunci : *SSTP, Tunneling, VPN.*

Abstract

The exchange of information is one of the needs that really supports activities within the University. This final project aims to set up and simulate a VPN using SSTP on the proxy so that it can connect the Palagimata campus and the Baubau Unidayan scientific palace campus. This study uses the ping test method using the command prompt and new terminal. The results show that the system simulation has been successfully created using SSTP VPN. It can be concluded that this SSTP VPN simulation can connect the Palagimata campus and the Baubau Unidayan scientific palace campus.
Keywords*: SSTP, Tunneling, VPN.*

I. PENDAHULUAN

Pertukaran informasi menjadi salah satu kebutuhan yang sangat penting dalam mendukung kegiatan dalam Universitas. Pertukaran informasi akan lebih mudah dan cepat jika memanfaatkan jaringan komputer. Internet merupakan salah satu teknologi pertukaran informasi secara luas yang menjadi popular saat ini. Internet adalah salah satu alat penghubung yang paling banyak digunakan antara komputer atau perangkat *end device* lainnya untuk bertukar data dan *file* karena pertimbangan efesiensi, kecepatan dan biaya. Oleh karena itu banyak perguruan tinggi besar yang menggunakan teknologi dan fasilitas internet untuk bertukar data antar cabang.

Seiring berjalannya waktu, jaringan internet juga mengalami perkembangan yang pesat, dimulai dari cakupan wilayah, kecepatan layanan data, media yang digunakan hingga tingkat keamanannya. Namun dengan seluruh kelebihannya internet juga memiliki beberapa kekurangan, salah satunya bersifat publik sehingga dapat diakses oleh banyak pihak sehingga tidak aman untuk mengirimkan

data pribadi atau rahasia. Keamanan bagi jaringan internet universitas sangat penting. Oleh karena itu, sebuah ide muncul dengan membuat jaringan terkesan privat namun pada jaringan publik. Teknologi ini merupakan *virtual private network* (VPN), dengan menggunakan VPN maka informasi data akan menjadi lebih aman berada di jaringan publik karena tersembunyi, sehigga pengguna lain tidak dapat mengetahui informasi data kemudian kerahasiaan data informasi dapat tetap terjaga.

Penelitian sebelumnya tentang Perancangan dan Implementasi VPN *Server* Dengan Menggunakan *Protocol Secure Socket Tunneling Protocol* (SSTP) Studi Kasus Kampus Universitas Sam Ratulangi. Berdasarkan hasil pengujian, *packet loss* pada L2TP dan SSTP *packet loss* bergantung pada kecepatan koneksi internet dan jumlah data. Sedangkan berdasarkan *round trip time* tidak ada perbedaan yang sangat besar, karena waktu transmisi datanya anatar 100ms sampai dengan 300ms [1].

Penelitian sebelumnya tentang VPN diantaranya dari penelitian yang berjudul Analisa *Virtual Private Network* Menggunakan *OpenVpn* Dan *Point To Point Tunnelinng Protocol*. Dalam laporan penelitiannya implementasi VPN menggunakan PPTP dan OpenVPN, bertujuan untuk dapat mengetahui efisiensi yang digunakan. Vpn yang menggunakan OpenVPN dan PPTP dapat digunakan pada jaringan server yang membuat pengguna atau *clien* dapat mengakses dimanapun melalui jaringan internet [2].

Penelitian selanjutnya yang berjudul Implementasi *Remote Site* Pada *Virtual Private Network* Berbasis Mikrotik. Berdasarkan hasil pengujian, dapat dibuktikan bahwa walaupun memiliki *packet loss* jaringan VPN yang digunakan memiliki *round trip* yang dapat mendownload data lebih cepat. Dengan ini menunjukan bahwa menggunakan jaringan VPN terbukti lebih aman [3].

Penelitian selanjutnya dengan judul Penerapan Sistem Keamanan Jaringan Menggunakan VPN Dengan Metode PPTP pada PT. Asri Pancawarna. Dalam penelitian penggunaan VPN PPTP dapat memudahkan pekerjaan dalam mengontrol dan mengatasi permasalahan jaringan perusahaan dari jarak jauh tanpa harus datang langsung ketempatnya dan dapat menjaga kerahasiaan serta kebocoran data oleh pihak-pihak yang tidak bertanggung jawab [4].

Penelitian selanjutnya yang berjudul VPN SSTP Menggunakan Raspberry Pi. Pada penelitiannya telah dilakukan pengujian kemanan yang menunjukan VPN SSTP aman terhadap serangan *sniffing*, hal itu ditunjukan pada hasil yang diperoleh bahwa *username* dan *password* yang digunakan untuk *login* tidak dapat diketahui oleh *attacker* [5].

Penelitian sebelumnya berjudul Implementasi VPN Menggunakan *Point to Point Tunneling Protocol* (PPTP) Mikrotik *Router* pada BPRS Bumi Artha Sampang. Untuk kegiatan berbagi *file* BPRS Bumi Artha Sampang menggunakan aplikasi hamachi. VPN merupakan jaringan komputer yang melalui jalur publik namun mempunyai *tunnel*. Aplikasi hamachi dapat digunakan secara gratis namun jika untuk digunakan dalam skala besar maka akan dikenai biaya. Agar proses komunikasi antar kantor berjalan lancar maka perlu dibuat jaringan *Virtual Private Network* (VPN), jaringan yang diusulkan menggunakan metode PPTP (*Point to Point Tunneling Protocol*). Setelah menerapkan metode ini kantor pusat dan kantor cabang dapat terhubung dan dapat saling berkomunikasi [6].

Penelitian Sebelumnya berjudul Implementasi *Virtual Private Network* (VPN) dengan Otentikasi Radius Server pada PT. Anugerah Tunggal Mandiri Jakarta. VPN merupakan solusi aman dalam hal pertukaran data yang menggunakan jalur publik, hasil *sniffing* menunjukan bahwa data yang ditransmisikan melalui jalur VPN tidak dapat terdeteksi, sehingga seolaholah tidak ada aktifitas pada jaringan tersebut. Dengan di implementasikannya VPN, akan memberikan kemudahan dalam transfer data karena tidak terbatas seberapa besar data yang akan di transmisikan. Berbeda dengan transfer data melalui email yang mempunyai keterbatasan. RADIUS server memberikan kemudahan dalam mengatur otentikasi pada user¸ sehingga hanya user yang terdaftar saja yang bisa terhubung ke jaringan VPN [7].

Penelitian sebelumnya berjudul Implementasi Jaringan VPN (*Virtual Private Network*) *Site to Site Mikrotik Router*. Dalam kasus ini Universitas Bina Darma mencoba membangun sebuah teknologi jaringan yang dapat menghubungkan kampus satu dan kampus lainnya yang berada di Kabupaten Kota yang letasknya kurang lebih berjarak 200-500 KM. Maka dengan VPN *Site to Site* inilah menjadi pilihan tepat mengingat VPN *Site to Site* secara umum bisa diartikan sebagai jaringan *private* yang menghubungkan beberapa lokasi yang berbeda secara lokal [8].

Penelitian selanjutnya berjudul Analisis Jaringan VPN Menggunakan PPTP dan L2TP. Pada penelitian ini, dibandingkan penggunaan dua teknologi VPN yang berbeda, yaitu antara PPTP dan L2TP, dimana parameter QoS yang digunakan adalah *throughput, delay, jitter,* dan *packet loss*. Proses pengambilan data dilakukan dengan menambahkan beban trafik sebesar 512 kbps, 1024 kbps, dan 2048 kbps. Analisa terhadap paket data yang diperoleh menggunakan *Wireshark*. Dari hasil penelitian diperoleh data bahwa rata-rata nilai *delay* pada L2TP lebih besar hingga 41% dibanding saat menggunakan PPTP, rata-rata *throughput* PPTP naik hingga 34% dibandingkan L2TP, rata-rata jitter pada PPTP lebih besar hingga 44% dibandingkan L2TP, sedangkan *packet loss* yang terjadi pada masing-masing layanan adalah 0 [9].

Penelitian lain dengan judul Perancangan Dan Implementasi VPN Menggunakan Protokol SSTP Mikrotik Di Fakultas MIPA Universitas Tanjungpura. Dalam laporan penelitiannya keunggulan dari protokol SSTP adalah keamanan dari *socket tunneling* atau komunikasi jaringan. Dengan demikian manajemen jalur komunikasi yang dilakukan pengguna yang melewati jalur *private* akan diamankan oleh mikrotik dan komunikasi yang terjadi diamankan berdasarkan konfigurasi mikrotik dari admin jaringan [10].

SSTP merupakan salah satu tunnel VPN yang memiliki tingkat keamanan data yang lebih baik. SSTP ini dapat digunakan untuk menghubungkan jaringan tanpa menggunakan kabel sehingga lebih menghemat biaya. Kebutuhan Universitas Dayanu Ikhsanuddin akan data antara kampus istana ilmiah dan kampus palagimata yang lebih cepat dan aman maka di butuhkan jaringan yang menghubungkan Kampus Istana Ilmiah dan Kampus Palagimata. Berdasarkan latar belakang di atas, maka tujuan dari penelitian ini adalah untuk dapat mensimulasikan dan mengatur VPN menggunakan SSTP pada mikrotik agar dapat menghubungkan dan mengkomunikasikan kampus palagimata dan kampus istana ilmiah unidayan baubau.

.

II. METODE PENELITIAN

A. Teknik Pengumpulan Data

Teknik pengumpulan data yang dilakukan untuk mendapatkan keterangan yang akurat, diperlukan beberapa metode yaitu :

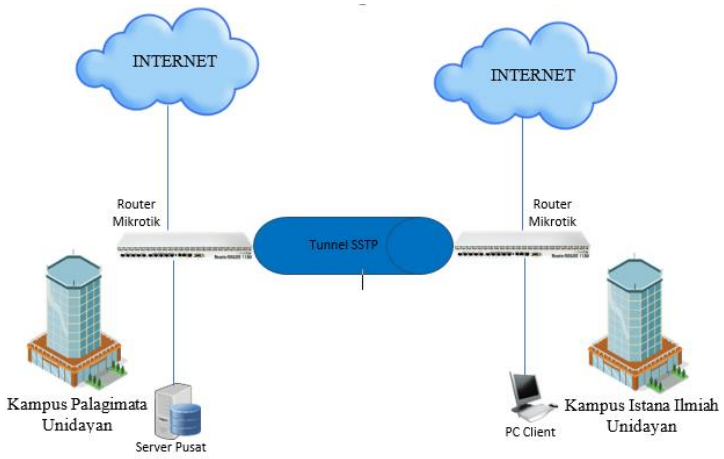
1) Metode pengamatan (observasi), Metode pengamatan (observasi), merupakan pengamatan dan pencatatan secara sistematis terhadap unsur-unsur yang nampak dalam suatu gejala pada objek penelitian.
2) Metode Pustaka, yaitu Metode Pustaka, yaitu teknik pengumpulan data dengan mengadakan studi penelaah terhadap buku-buku, literatur-literatur, catatan-catatan, dan laporan-laporan yang ada hubungannya dengan masalah yang dipecahkan.

B. Teknik Analisis Data

Teknik analisis data yang digunakan dalam penelitian ini yaitu dengan menggunakan metode *Network Development Life Cycle* (NDLC). NDLC merupakan metodelogi dalam pengembangan jaringan.

C. Rancangan Topologi Jaringan

Jaringan VPN SSTP akan diimplementasikan pada topologi *real* menggunakan jaringan internet. Rancangan topologi yang akan digunakan dalam penelitian ini adalah sebagai berikut.



Gambar 4.1 Rancangan Topologi Jaringan Secara Umum
Dengan Menggunakan Tunnel SSTP

Implementasi akan dilakukan pada 2 (dua) tempat yang berbeda yaitu Kampus Istana Ilmiah dan Kampus Palagimata Unidayan Baubau dengan 2 (dua) buah *router* dan 1 (satu) unit komputer *client* serta 1 (satu) unit server sesuai dengan topologi diatas.

Pembagian IP yang akan dikonfigurasi pada *interface router* dan komputer untuk penelitian sesuai dengan rancangan topologi yang telah dibuat adalah sebagai berikut.

Tabel 4.1. Pengalamatan IP Pada Kampus Palagimata Unidayan

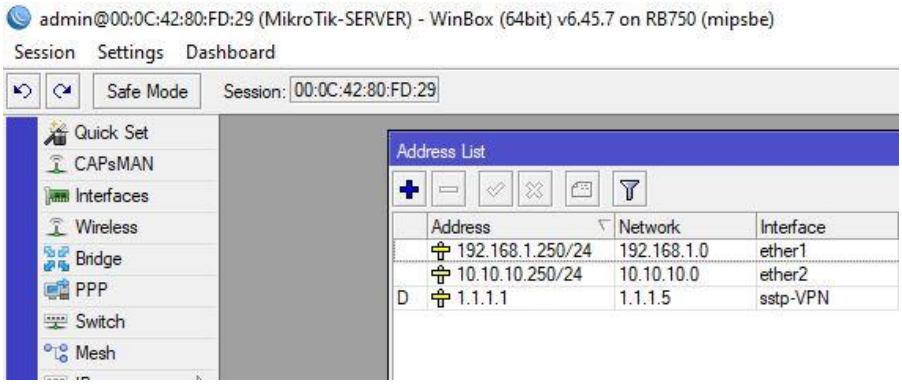
Keterangan	Alamat IP
IP Publik	125.162.212.90
IP SSTP *Tunneling*	1.1.1.1
IP PC Server	10.10.10.249

Tabel 4.2. Pengalamatan IP Pada Kampus Istan Ilmiah Unidayan

Keterangan	Alamat IP
IP SSTP *Tunneling*	1.1.1.2-1.1.1.5
IP PC *Client*	127.10.10.254

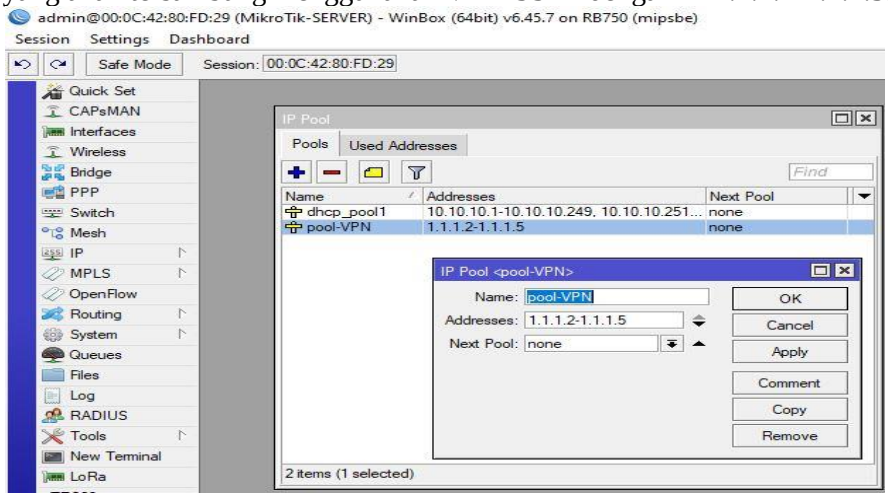
III. HASIL DAN PEMBAHASAN

Instalasi VPN-SSTP pada mikrotik server diawali dengan penyambungan mikrotik server pada modem internet agar mikrotik dapat mempunyai akses internet. Pada gambar dibawah ini merupakan IP-*address* dari mikrotik server yang tersambung pada modem internet yang ditandai dengan *interface ether* 1, IP-Address yang yang menyambungkan antara mikrotik server ke PC server yang ditandai dengan *interface ether* 2, dan IP-Address dari VPN-SSTP yang ditandai dengan *interface* sstp-VPN. Berikut merupakan gambar dari IP-*address* mikrotik server.



Gambar 4.2 IP-Address Mikrotik Server

Pada gambar 4.2 merupakan IP-POOL, dimana IP-POOL ini akan di jadikan IP-*address* pada *client* yang akan tersambung menggunakan VPN-SSTP dengan IP 1.1.1.2-1.1.1.5.



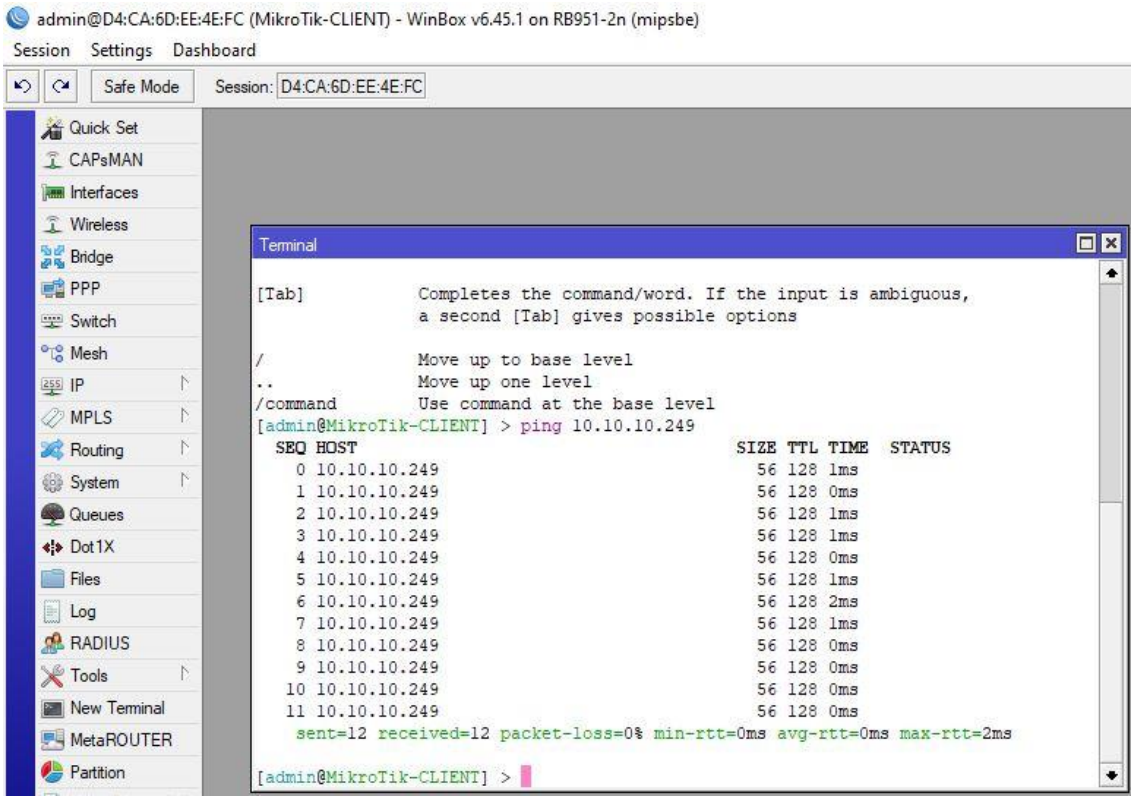
Gambar 4.3 IP-Pool Mikrotik Server.

Pada gambar 4.3 dibuat Profile dengan nama profile-VPN yang memiliki IP local addres yaitu 1.1.1.1 yang akan digunakan sebagai sebagai IP dari VPN mikrotik server.

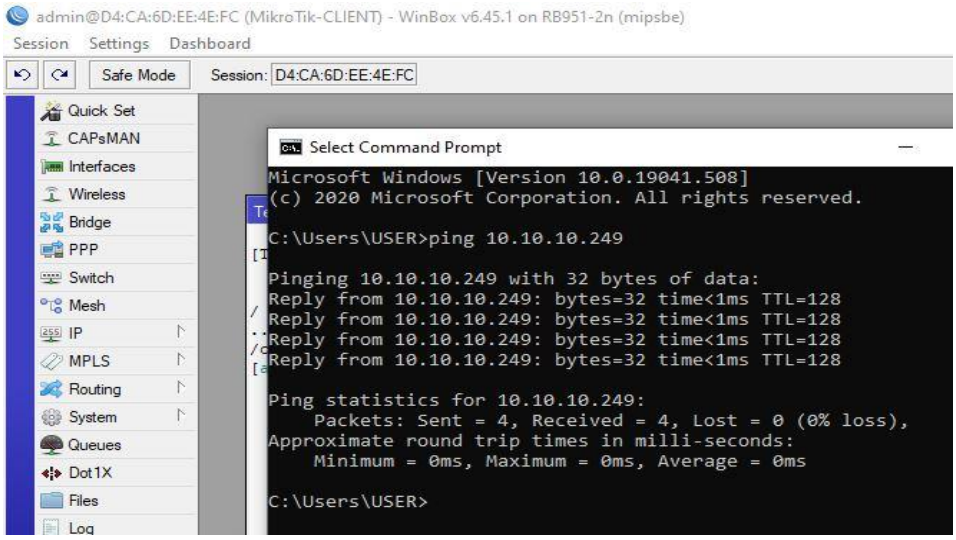
Metode pengujian yang dilakukan pada implementasi sistem ini adalah sebagai berikut:

1. *Ping test*, pada penerapan dilakukan pengujian menggunakan *command prompt* yang ada pada komputer dan *new terminal* yang ada pada aplikasi winbox untuk mengetahui kualitas koneksi VPN-SSTP dari *client* ke server.
2. Menggunakan aplikasi *wireshark*, dengan menggunakan aplikasi ini peneliti dapat melihat keamanan data pada *Tunneling* VPN-SSTP.

Pengujian ini bertujuan untuk melihat VPN-SSTP mikrotik server telah berhasil dikoneksikan dengan mikrotik *client*. Pengujian menggunakan *new terminal* yang berada pada aplikasi winbox dan *command prompt* di *client* dengan cara memping ip komputer server yang tersambung dari mikrotik ke komputer server yang telah berhasil dilakukan dengan adanya paket data yang terlihat pada gambar 4.4 dan 4.5

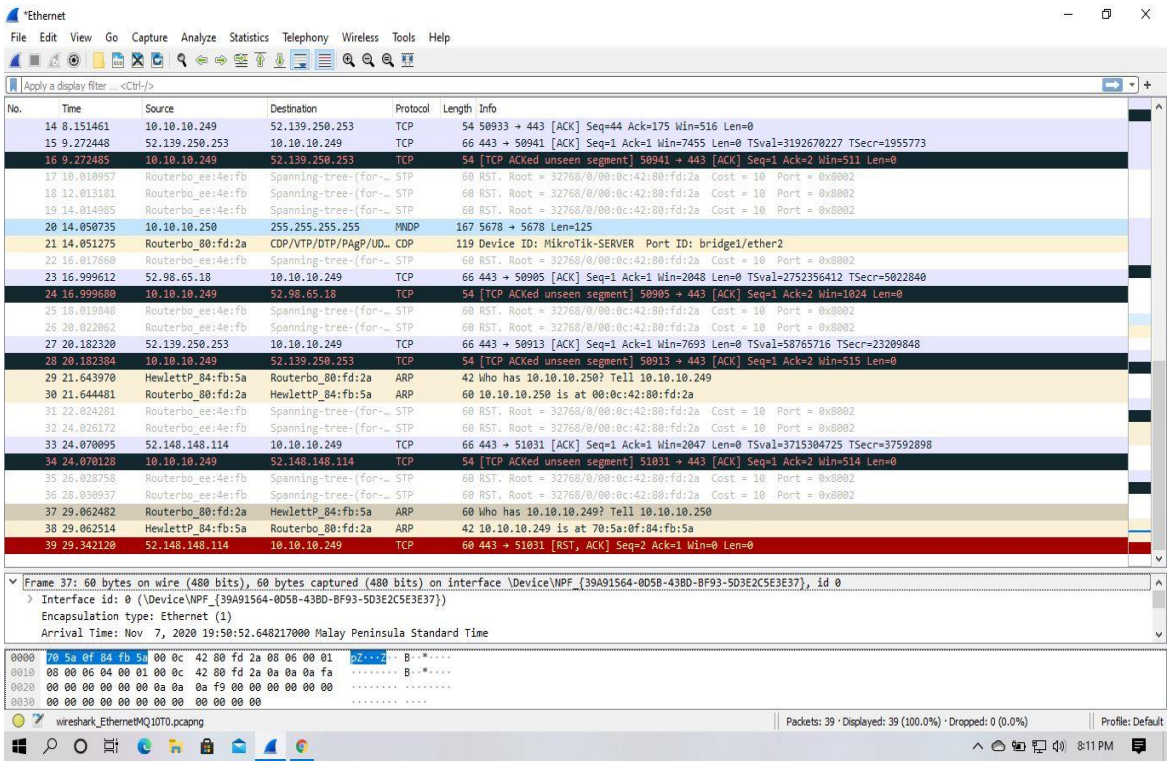


Gambar 4.4 *Ping Test* Menggunakan *New Terminal* Pada Winbox *Client* Dengan IP 10.10.10.249

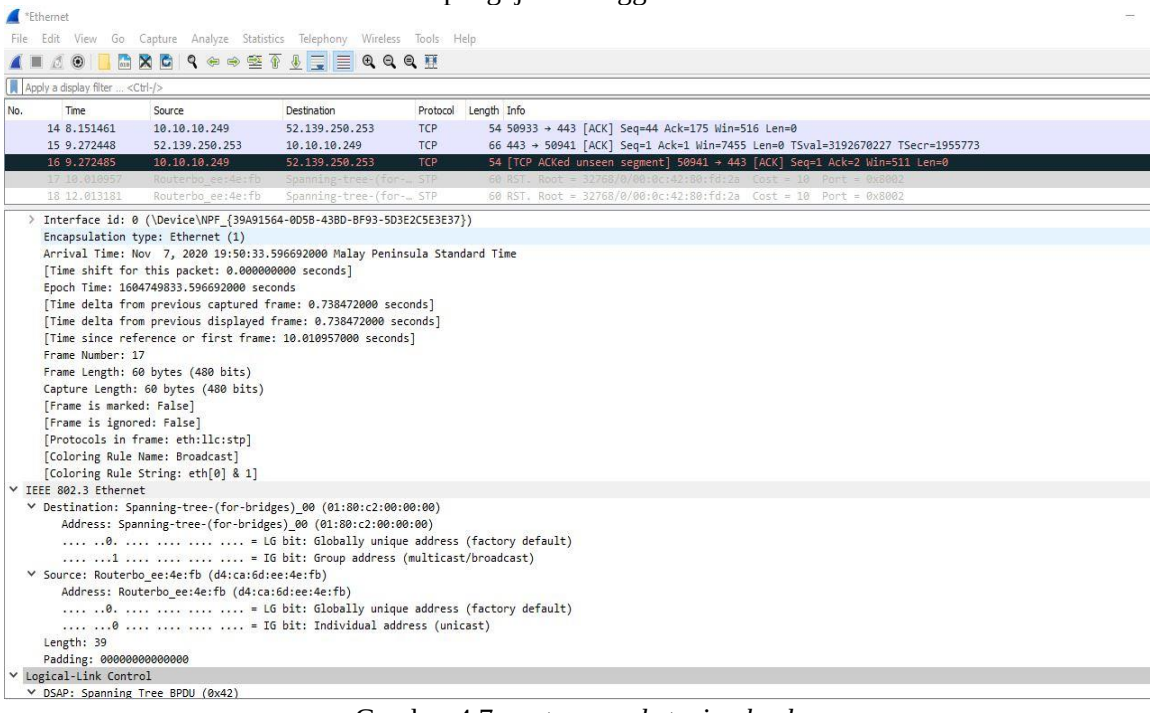


Gambar 4.5 *Ping Test* Menggunakan *Command Prompt* Pada Komputer *Client* Dengan IP 10.10.10.249.

Pengujian selanjutnya dilakukan dengan menggunakan aplikasi *wireshark* sebagai pihak ketiga untuk membantu melakukan pengecekan jaringan. Pada gambar 4.6 telah didapatkan *capture packet* secara *real time*. Pada gambar 4.7 terlihat bahwa data yang telah didapat telah terekripsi dengan baik mengunakan VPN-SSTP karena tidak dapat memperlihatkan alamat ip maupun alamat mac mikrotik dari *client* ataupun server.



Gambar 4.6 pengujian menggunakan *wireshark*



Gambar 4.7 *capture packet wireshark*

IV. KESIMPULAN

Berdasarkan hasil penelitian dari Penerapan *Virtual Private Network* (VPN) Dengan Menggunakan *Secure Socket Tunneling Protocol* (SSTP) Untuk Membangun Jaringan Kampus Palagimata Dengan Kampus Istana Ilmiah Unidayan Baubau adalah sebagai berikut :

1. Sistem yang dibuat telah berhasil diimplementasikan secara langsung dengan menggunakan VPN-SSTP.

2. Dapat mengatur VPN yang menggunakan SSTP pada mikrotik sehingga dapat menghubungkan dan mengkomunikasikan Kampus Palagimata dan Kampus Istana Ilmiah Unidayan Baubau.
3. Penerapan VPN-SSTP atau VPN yang memakai *tunneling* berbeda harus menggunakan IP *Public static*, agar pemberiaan alamat pada *client* tidak diganti setiap saat.

V. SARAN

Adapun saran untuk pengembangan penelitian selanjutnya yang memiliki pokok permasalahan yang sama adalah sebagai beriku :

1. Sebelum mengimplementasi rancangan jaringan VPN-SSTP terlebih dahulu pastikan IP *public* modem atau IP yang berasal dari ISP harus *static*.
2. Sistem dapat dikembangakan lebih jauh lagi dengan menggunakan spesifikasi mikrotik yang lebih bagus agar dapat melayani banyak *client* dalam waktu bersamaan.

DAFTAR PUSTAKA

[1] K. A. Farly, X. B. N. Najoan, and A. S. M. Lumenta, "Perancangan Dan Implementasi Vpn Server Dengan Menggunakan Protokol Sstp (Secure Socket Tunneling Protocol) Studi Kasus Kampus Universitas Sam Ratulangi," *J. Tek. Inform.*, vol. 11, no. 1, 2017, doi: 10.35793/jti.11.1.2017.16745.

[2] P. Oktivasari and A. B. Utomo, "Analisa Virtual Private Network Menggunakan," pp. 185–202, 2016.

[3] H. Supendar, "Implementasi Remote Site Pada Virtual Private Network Berbasis Mikrotik," *Bina Insa. ICT J.*, vol. 3, no. 1, p. 234340, 2016.

[4] J. L. Putra, L. Indriyani, and Y. Angraini, "Penerapan Sistem Keamanan Jaringan Menggunakan VPN Dengan Metode PPTP Pada PT. Asri Pancawarna," *IJCIT (Indonesian J. Comput. Inf. Technol. p-ISSN 2527-449X, e-ISSN 2549-7421*, vol. 3, no. 2, pp. 260–267, 2018.

[5] Sugiyatno and P. D. Atika, "Virtual Private Network (VPN) Secure Socket Tunneling Protocol (SSTP) Menggunakan Raspberry Pi," *Inf. Syst. Educ. Prof.*, vol. 2, no. 2, pp. 155–166, 2018.

[6] S. Watmah, "Implementasi VPN Menggunakan Point-To-Point Tunneling Protocol (PPTP) Mikrotik Router Pada BPRS Bumi Artha Sampang," vol. 1, no. 1, pp. 6–12, 2020.

[7] Rosmana and F. Latifah, "Vol . XII No . 1 , Maret 2015 Jurnal Techno Nusa Mandiri DENGAN OTENTIKASI RADIUS SERVER PADA Abstrak," vol. XII, no. 1, pp. 23–34, 2015.

[8] Fatoni and D. Irawan, "Jaringan VPN site to site.pdf," *informatika*, vol. 3, no. 2301–5632, p. 98, 2015.

[9] S. Ikhwan and A. Amalina, "Analisis Jaringan VPN Menggunakan PPTP dan L2TP," *J. Infotel*, vol. 9, no. 3, 2017, doi: 10.20895/infotel.v9i3.274.

[10] I. Ruslianto and U. Ristian, "Perancangan dan Implementasi Virtual Private Network (VPN) menggunakan Protokol SSTP (Secure Socket Tunneling Protocol) Mikrotik di Fakultas MIPA Universitas Tanjungpura," *Comput. Eng. Sci. Syst. J.*, vol. 4, no. 1, p. 74, 2019, doi: 10.24114/cess.v4i1.11792.