

Virtual Private Network Menggunakan Point To Point Tunnel Protocol Berbasis Mikrotik

Berby Febriana Audrey*
Jurusan Sistem Komputer, Universitas Sriwijaya, Indonesia

*Korespondensi: 09011281823062@student.unsri.ac.id

ARTICLE INFO

Article History:

- Received 01 January 2022
- Received in revised form 25 January 2022
- Accepted 19 January 2022
- Available online 31 March 2022

ABSTRAK

Keamanan dalam sistem jaringan terus berkembang seiring dengan kemajuan teknologi yang pesat. Komputerisasi telah menjadi bagian integral dari setiap aspek operasional perusahaan dan kantor pemerintahan, menuntut perlunya sistem keamanan jaringan yang kuat. Dalam konteks pemerintahan, terutama, di mana setiap bagian telah mengadopsi teknologi komputer, pentingnya memiliki sistem keamanan jaringan yang solid menjadi semakin mendesak. Hal ini diperlukan agar setiap proses pengiriman dan penerimaan data antar komputer dapat dilakukan dengan aman dan terkendali. Meskipun banyak aplikasi perangkat lunak yang mendukung upaya menangani masalah keamanan, perspektif keamanan terkadang tidak sepenuhnya teratasi oleh software yang ada. Kekhawatiran terbesar adalah potensi kebocoran data yang dapat terjadi di berbagai tingkatan kantor maupun perusahaan. Sebagai respons terhadap tantangan ini, para ahli menciptakan solusi penangkal, yaitu teknologi VPN. Meskipun terdapat berbagai metode dalam implementasi VPN, kali ini akan fokus pada metode PPTP. VPN PPTP menjadi pilihan yang tepat untuk mengamankan pengiriman dan penerimaan data, membentuk jaringan yang bersifat rahasia dengan menggunakan IP Publik. Dengan demikian, teknologi VPN PPTP memberikan lapisan keamanan yang diperlukan untuk mencegah kebocoran data saat mentransfer informasi melalui jaringan, menjadikannya solusi yang efektif dan relevan dalam era keamanan jaringan yang terus berkembang.

Kata Kunci: VPN, Mikrotik, PPTP, Komputer, Network

ABSTRACT

Security in a network system is continually advancing, in line with the rapid progress and development of technology. Experts have embraced computerization, where every department in a company or government office utilizes computer technology in its operations. With the establishment of computerization in the government, there is a need for a robust Network Security System to ensure that the transmission and reception of data from one PC to another can be carried out securely and under control. While numerous software applications support addressing these issues, the security aspect may not necessarily be fully addressed by such software. There is a significant concern about potential data leaks in the offices of both governmental and private enterprises. Hence, experts have devised a countermeasure, namely VPN technology. There are various methods within VPN, but this time we will use the PPTP method. PPTP VPN is suitable for securing data from leaks during data transmission and reception. The process of VPN itself involves creating a network that is secretive and uses a Public IP. Therefore, PPTP VPN technology provides the necessary security layer to prevent data leaks when transferring information through the network, making it an effective and relevant solution in the continually evolving network security era.

Keywords: VPN, Mikrotik, PPTP, Komputer, Network

1. PENDAHULUAN

Waktu terus berlalu, dan seiring perkembangannya, teknologi di dunia IT semakin pesat, memicu peningkatan kompetisi antar individu. Seperti pada umumnya, terdapat aspek positif dan negatif dalam penggunaan teknologi. Beberapa orang memanfaatkannya untuk kepentingan pribadi, seperti terjadi pada insiden pembobolan data yang kini marak, mengancam keamanan informasi yang bisa disalahgunakan oleh pihak yang tidak bertanggung jawab.

Dalam rangka mencegah potensi tersebut, diperlukan sistem keamanan atau perisai untuk melindungi jaringan, dan salah satu contohnya adalah penggunaan Virtual Private Network (VPN) sebagai penghalang terhadap jaringan asing yang berusaha masuk ke dalam jaringan pribadi. Setiap perusahaan biasanya memiliki virtual private network untuk melindungi jaringan pada perkantoran maupun perusahaan tersebut, karena seperti disebutkan di atas, banyak data penting dan bersifat rahasia yang perlu diperketat penjagaannya agar tidak terjadi kebocoran.

VPN sendiri menjadi security system terfavorit pada setiap teknisi jaringan karena sistem kerjanya yang mudah dipahami. Salah satu metodenya adalah PPTP atau Point to Point Tunneling Network, yang merupakan salah satu protokol VPN tertua dan masih digunakan hingga saat ini. Dikembangkan oleh platform Microsoft, protokol ini telah dipakai pada semua versi OS Windows[1].

Hampir semua perangkat elektronik seperti PC, desktop, dan smartphone saat ini didukung oleh PPTP[2]. Dengan menggunakan metode PPTP, terowongan atau tunneling pada VPN menjaga koneksi jaringan dan mengenkripsi data yang dikirim atau ditransfer melalui jaringan tersebut. Meskipun PPTP telah mengalami beberapa revolusi dalam melakukan enkripsi data, protokol ini tetap populer karena kemudahan penggunaannya dalam melakukan setup atau pengaturan.

2. TINJAUAN PUSTAKA

2.1. Virtual Private Network (VPN)

VPN merupakan singkatan dari Virtual Private Network, VPN sendiri berguna untuk mengkoneksikan jaringan antar PC satu dengan PC lainnya, ataupun antar gedung perkantoran, serta tempat umum sekalipun. Saat ini VPN telah digunakan oleh banyak user atau pengguna internet di seluruh penjuru dunia. Kenapa banyak yang memakai VPN. Karena untuk mendapatkan koneksi jaringan internet itu sendiri, seperti yang sudah dijelaskan sebelumnya. Tujuannya juga agar jaringan internet tersebut aman dari jaringan yang jahat atau yang ingin membobol data, dan juga menangkal dari kebocoran data serta dapat mengakses suatu jaringan secara remote[3].

VPN adalah jaringan yang bersifat privasi yang dibuat di atas jaringan publik atau internet pada umumnya, yang dimana memungkinkan user untuk berinteraksi atau saling transfer data secara aman dan terkunci atau terenkripsi. Ada banyak cara untuk membangun sebuah terowongan VPN tetapi semuanya sama saja fungsinya[4].

VPN ditemukan pada tahun 1996. Pada masa itu pekerja Microsoft yaitu Gurdeep Singh Pall menemukan sebuah cara membangun VPN yaitu PPTP yang dimana memungkinkan para user memperoleh koneksi internet yang aman [5]. VPN sendiri awalnya diciptakan bukan untuk perorangan, tapi untuk skala besar. Dahulu banyak data penting yang rentan terbobol atau

mengalami kebocoran. Maka dari itu VPN di buat atau di ciptakan, tetapi sekarang sudah menjadi hal yang lumrah VPN digunakan untuk para user secara perorangan bahkan sudah banyak VPN berlisensi yang gratis. Pada dasarnya setiap perusahaan sangat membutuhkan sebuah jaringan yang aman, untuk mengkoneksikan tiap PC atau Tiap kantor atau gedung sekalipun. Maka dari itu jawaban untuk semua permasalahan ini adalah jaringan yang bersifat privasi dan terenkripsi yang dimana dapat melindungi semua informasi rahasia ataupun data rahasia sebuah perusahaan. Jawab yang tepat ialah VPN, VPN sendiri jaringan lokal yang mudah di setting serta tidak menguras dompet alias murah.

Walaupun pada saat itu VPN diciptakan hanya untuk kepentingan perusahaan besar, tetapi penyedia layanan VPN menyadari sesuatu hal dimana mereka melihat bahwa VPN bisa menjadi keuntungan yang besar, dimana VPN bisa digunakan untuk para user perorangan. Terkhusus dikarenakan menyebarnya Wi-Fi, Hotspot maupun jaringan lainnya yang sudah menjadi salah satu kebutuhan kaum milenial saat ini. Jaringan tersebut sangat rentan dan tidak aman, apalagi jika menggunakan Wi-Fi umum. Maka dari itu VPN dibuat untuk perorangan pada akhirnya. Diperlukan enkripsi yang kokoh untuk menaungi data-data penting yang ditransfer melalui jaringan tanpa kabel, seperti saat menjalankan internet banking atau beberapa data yang bersifat keuangan, kartu kredit, belanja online dan sebagainya. Itu bersifat sangat krudensial

Pada kasus lain, mulai terjadinya pemblokiran pada situs-situs serta ada hal yang sangat mencengangkan yaitu dimana aksi penyadapan oleh lembaga dunia seperti NSA, yang dimana pada akhirnya menimbulkan spekulasi untuk membuat user internet mulai berpikir untuk menjaga privasi mereka[6].

2.2. PPTP (Point to Point Tunneling Protocol)

PPTP adalah salah satu dari sekian banyaknya metode dalam pengimplementasian jaringan virtual. PPTP merupakan sebuah protokol jaringan memungkinkan user untuk memiliki pengamanan dalam pengiriman data. Teknologi jaringan PPTP yang di keluarkan oleh IETF atau singkatan dari Internet Engineering Task Force. Fasilitas yang diberikan PPTP ialah dapat melakukan publik-switched telephone network yang biasa disingkat PSTN. PSTN sendiri merupakan pondasi dari VPN. PPTP mudah dikonfigurasi dan juga memiliki biaya yang tidak menguras dompet alias murah meriah, dapat digunakan untuk remote user dan mobile user karena memberikan keamanan dan enkripsi[4].

2.3. Cara Kerja PPTP

Cara kerja PPTP sendiri ialah dimulai dari sebuah remote dimana akses sebuah LAN perusahaan. Akses dilakukan dengan ISP Lokal. Client akan terhubung ke jaringan server NAS atau Network Access Server pada ISP. Maka NAS dapat berupa PFE atau Proser Front End, Server Dial In atau juga POP dimana singkatan dari point of presence. Setelah terhubung, Client dapat melakukan Transmisi data melalui Internet. NAS menggunakan Protokol TCP/IP untuk trafis yang melalui jalur nirkabel atau melalui internet. Client membuat sebuah koneksi PP ke ISP, panggilan dial up network yang kedua dibuat melewati server PPP yang telah ada sebelumnya. Selanjutnya data akan dikirimkan menggunakan koneksi. Kedua hal ini berbentuk IP Datagram yang berisikan paket PPP yang sudah enskapluasi, lalu selanjutnya panggilan kedua tersebut akan menciptakan koneksi antar VPN dan server PPTP pada LAN private. Koneksi inilah yang disebut Tunneling atau terowongan [7].

2.3.1. Kelebihan dan Kekurangan PPTP

Kelebihan dari PPTP adalah mudah di konfigurasi serta bisa melalui Remote Access dengan mudah mengakses komputer maupun jaringan kantor, dari mana saja selama terhubung dengan internet. Keamanan yang memadai dengan koneksi melalui VPN kita bisa Menggunakan Koneksi secara aman melalui akses internet publik seperti hotspot dan internet kantor dan sebagainya[7].

2.3.2. Kekurangan PPTP

Kekurangan PPTP sendiri adalah tidak mempunyai Control terhadap jaringan tersebut karena pada dasarnya, Cuma mencantumkan koneksi pada pihak lain. Kedua Faktor penggunaan jaringan Public di luar sana yang tidak bisa di prediksi akan bahayanya[8].

2.4 Mikrotik

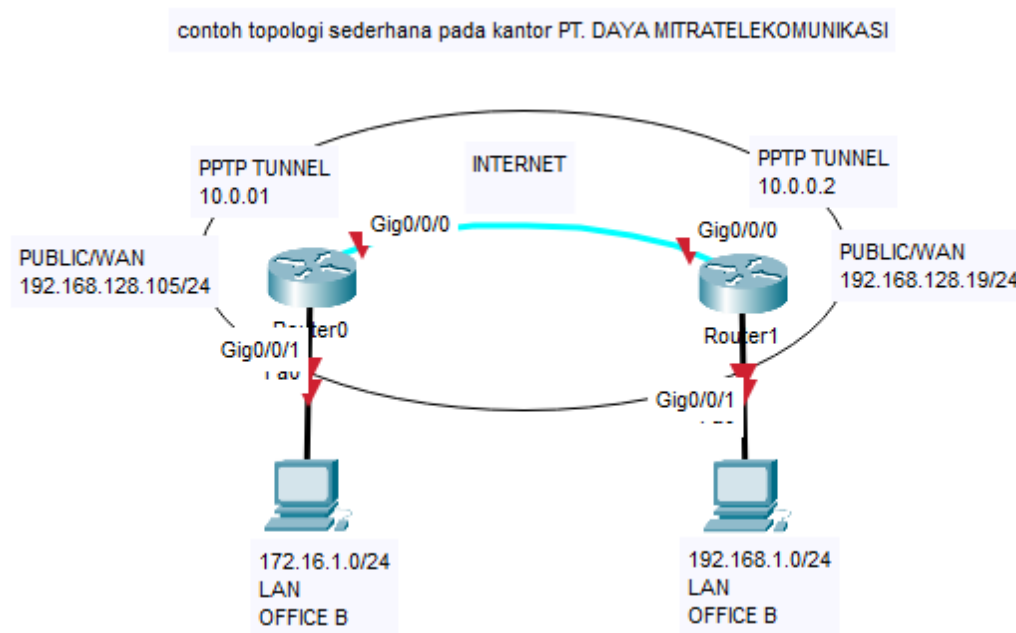
Mikrotik merupakan salah satu alternatif dalam dunia IT. Sudah banyak provider yang menggunakannya, seperti ISP, hotspot, warnet dan lainnya. Mikrotik sendiri menjadi pilihan umum dalam dunia IT karena mikrotik dijadikan sebagai Computer Route Network yang handal. serta dilengkapi dengan beberapa tools dan fitur yang baik, mikrotik sangat cocok untuk benda jaringan, jaringan kabel maupun jaringan wireless. Salah satu kenapa mikrotik menjadi router favorit di dunia IT karena sifatnya yang open source, sehingga semua bisa menggunakan dan menyetingnya dengan mudah.

Router sangat penting untuk jaringan internet karena fungsinya sendiri adalah mengatur koneksi antar dua atau lebih sebuah komputer. pengoperasiannya yang mudah, kebutuhan hardware yang rendah. MikroTik sendiri secara umum merupakan RouterOS. Untuk penginstalan Mikrotik diperlukan komponen tambahan. Mikrotik didesain secara khusus agar mudah digunakan untuk membangun sebuah jaringan, dalam skala kecil maupun skala besar.

Sistem operasi pada mikrotik sendiri adalah sistem operasi linux base yang dipakai sebagai sebagai network router. Dirancang agar memberikan kemudahan dan kebebasan bagi user. Setting pada administrasinya bisa dilakukan menggunakan Windows Application atau Winbox. Komputer atau PC yang nantinya akan digunakan sebagai router mikrotik pun tak memerlukan spek yang tinggi. Contohnya sebagai gateway. Kecuali mikrotik yang digunakan untuk keperluan beban yang besar maka memerlukan spek yang tinggi[9].

3. METODELOGI PENELITIAN

Metodologi dalam penelitian ini adalah menggunakan simulator jaringan komputer dengan topologi ditunjukkan pada gambar 1. Adapun topologi tersebut merupakan sebuah simulasi dari jaringan kantor PT. DAYAMITRA TELEKOMUNIKASI tempat peneliti melakukan percobaan. Topologi dan informasi yang tercantum pada topologi tersebut telah dilakukan sensor sehingga tidak mencantumkan informasi sensitif dan rahasia dari PT. DAYAMITRA TELEKOMUNIKASI.



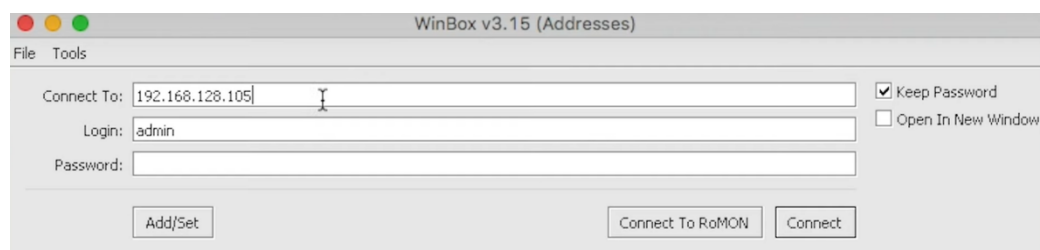
Gambar 1. Topologi Penelitian

Secara sederhana pada topologi tersebut ada 2 site yaitu :

1. Dimana Site pertama Office A akan difungsikan pada routernya sebagai PPTP Server sedangkan Site kedua Office B akan difungsikan pada routernya sebagai PPTP Client.
2. Kedua site akan di koneksi dengan satu jaringan menggunakan PPTP TUNNEL.

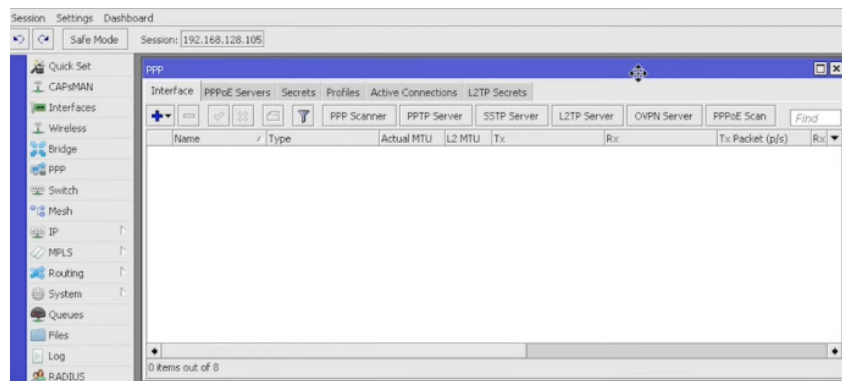
Untuk memulai pembentukan jaringan VPN dengan teknologi PPTP, maka akan dilakukan Langkah-langkah pembentukan server PPTP. Adapun konfigurasi yang harus dilakukan adalah sebagai berikut

1. Konfigurasi server VPN dimulai dari melakukan remote dengan aplikasi winbox seperti pada gambar 2. Untuk router Office A sendiri disimulasikan IP routernya 192.168.128.105.



Gambar 2. Remote router dengan menggunakan winbox

2. Selanjutnya konfigurasi PPTP. Untuk menunya sendiri ada pada Tab PPP sebelah kiri nomor enam dari atas. Seperti di tunjukan pada gambar berikut ini:



Gambar 3. Menu PPTP

3. Untuk mengaktifkan PPTP Server, Klik Tombol PPTP Server. Setting seperti gambar
4. Setelah tersetting maka sistem otomatis mengaktifkan PPTP Server.



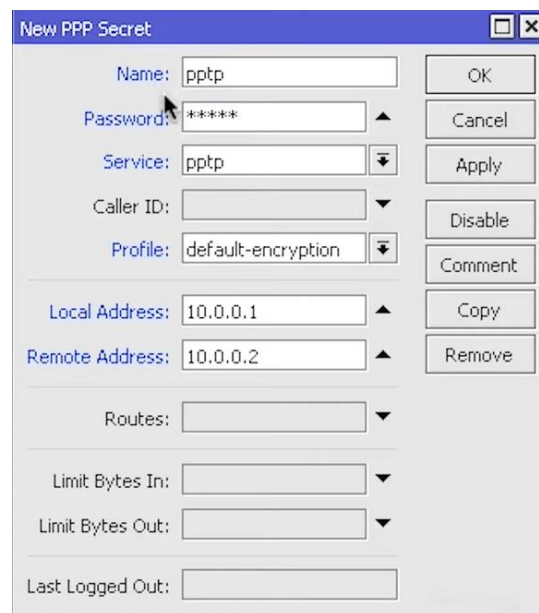
Gambar 4. Mengaktifkan PPTP Server

4. Selanjutnya membuat akun yang nantinya akan digunakan untuk login PPTP Client. Adapun proses yang harus dilakukan ditunjukkan pada gambar 5.



Gambar 5. Membuat user baru

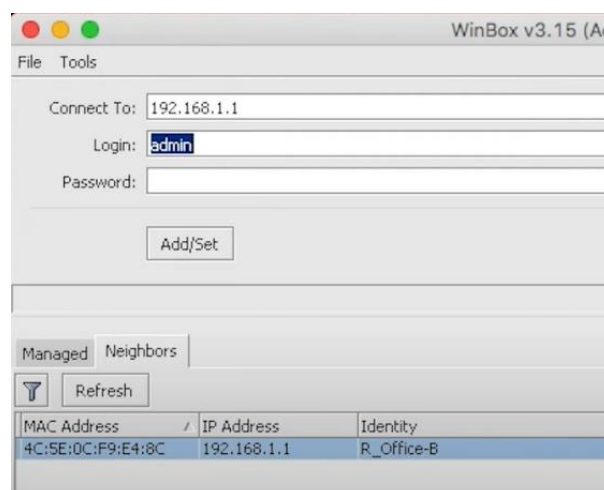
5. Kemudian klik tombol +, lalu akan muncul parameter seperti gambar 6. Setting semua seperti yang ada di gambar tersebut. Dengan password : 12345. Maka untuk konfigurasi PPTP Server pada Site Office A sudah selesai



Gambar 6. Parameter user baru

Kemudian jaringan VPN dengan teknologi PPTP yang telah dibuat sebelumnya, selanjutnya dapat digunakan oleh PPTP client. Adapun konfigurasi yang harus dilakukan oleh PPTP client adalah sebagai berikut:

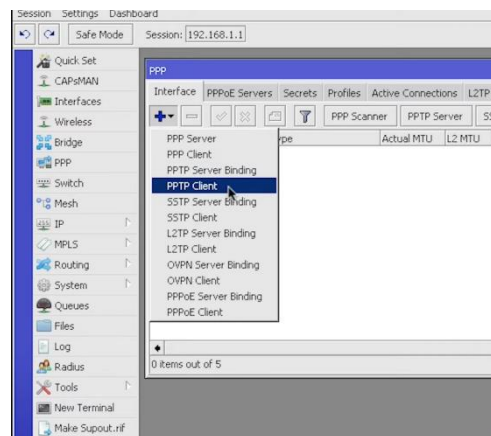
1. Konfigurasi client VPN dimulai dari melakukan remote dengan aplikasi winbox seperti pada gambar 7. Untuk router Office B sendiri disimulasikan IP routernya 192.168.128.19.



MAC Address	IP Address	Identity
4C:5E:0C:F9:E4:8C	192.168.1.1	R_Office-B

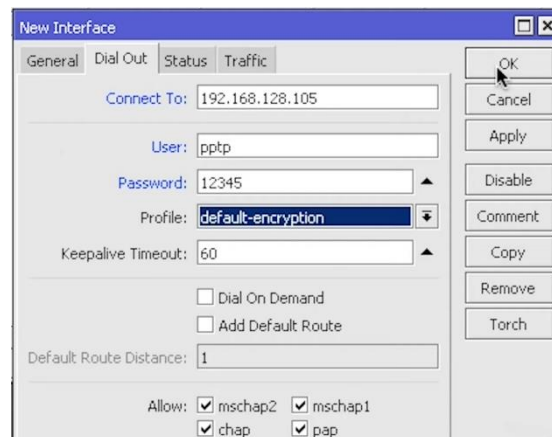
Gambar 7. Remote Router B

2. Selanjutnya masuk ke Menu PPP. Klik Tab Interface. Lalu klik tombol +, Kemudian pilih PPTP Client. Adapun Langkah tersebut ditunjukkan pada gambar 8 berikut ini.



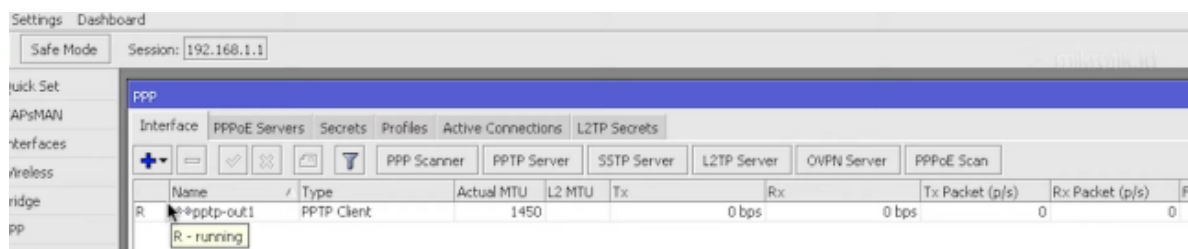
Gambar 8. PPTP Client

3. Selanjutnya masukan informasi ip, user dan password dari PPTP server yang ditunjukkan pada gambar 9 berikut ini



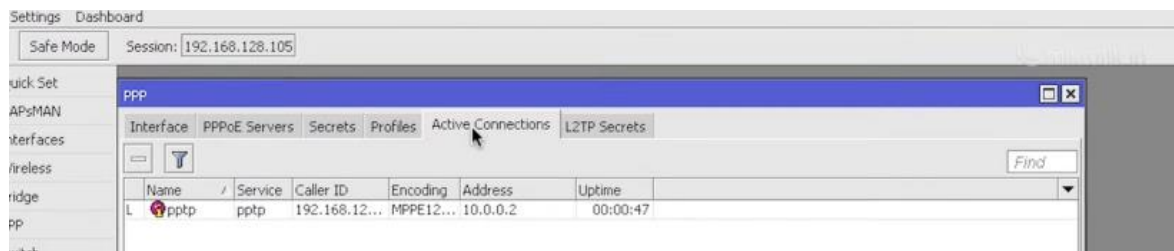
Gambar 9. Konfigurasi PPTP client

4. Maka selanjutnya otomatis akan dibuatkan sistem interface baru dengan nama pptp-out1. Seperti ditunjukkan pada gambar 10.



Gambar 10. Status interface PPTP

5. Bila muncul Huruf R maka dipastikan interface tersebut telah running yang artinya sudah terkoneksi. Untuk pengecekan berhasil atau tidaknya, bisa di cek melalui PPTP Server. Seperti ditunjukkan pada gambar 11.



Gambar 11. Interface PPTP running

4. HASIL PENELITIAN

Dari implementasi di atas, terbukti bahwa konfigurasi VPN dengan metode PPTP menggunakan Routerboard dan Winbox memberikan kemudahan dalam penggunaan. Routerboard dan Winbox menyediakan antarmuka yang sederhana dan intuitif, menjadikan proses konfigurasi VPN PPTP mudah diakses oleh pengguna. Kemudahan ini meningkatkan tingkat keterbacaan dalam pengelolaan jaringan, memungkinkan pengguna untuk dengan cepat memahami langkah-langkah yang diperlukan untuk mengatur VPN PPTP. Sebagai salah satu dasar pembuatan jaringan pribadi virtual, VPN PPTP berperan penting dalam menyediakan konektivitas yang aman dan terenkripsi. Metodenya yang teruji dan telah diterapkan secara luas membuat PPTP menjadi pilihan umum di berbagai lingkungan IT. Keandalan dan kemudahan penggunaan VPN PPTP menjadi poin utama dalam mendirikan sistem keamanan jaringan yang kokoh.

Melalui implementasi VPN PPTP, percobaan dilakukan untuk menguji kinerja dan keamanan sistem. Hasil-hasil ini memberikan wawasan yang berharga tentang efektivitas metode PPTP dalam mengamankan dan memfasilitasi lalu lintas data. Evaluasi teliti terhadap hasil percobaan membantu mendapatkan pemahaman yang lebih mendalam tentang keunggulan dan kelemahan dari penggunaan VPN PPTP. Kesimpulannya, konfigurasi VPN PPTP menggunakan Routerboard dan Winbox memberikan solusi yang efektif untuk menciptakan jaringan pribadi virtual. Kemudahan penggunaan, keandalan, dan kemampuannya untuk menyediakan konektivitas yang aman menjadikan VPN PPTP sebagai pilihan yang layak dalam pengelolaan keamanan jaringan. Hasil dari percobaan PPTP juga dapat digunakan sebagai dasar untuk peningkatan lebih lanjut pada sistem keamanan jaringan, memberikan landasan yang kuat untuk pengembangan teknologi keamanan informasi di masa mendatang.

5. KESIMPULAN

Secara keseluruhan, dalam studi kasus ini, penyelesaian untuk implementasi point-to-point atau peer-to-peer telah berhasil. Prosesnya dimulai dengan pembuatan server, yang kemudian diatur di sisi kantor B sebagai PPTP client pada koneksi dial-up. Setelah terjalannya koneksi antara PPTP server dan PPTP client, langkah selanjutnya adalah membuat pengaturan Static Routing untuk memungkinkan komunikasi antar Local Area Network (LAN) di setiap kantor. Setelah konfigurasi Static Routing selesai, langkah penting berikutnya adalah melakukan uji coba atau testing. Pengujian dilakukan dengan mengirimkan data atau sinyal komunikasi dari router satu ke router lainnya untuk memastikan bahwa koneksi antara keduanya berjalan dengan baik. Tes ini penting untuk memverifikasi apakah pengaturan dan konfigurasi yang telah diimplementasikan berfungsi sebagaimana mestinya. Jadi, pada tahap ini, keseluruhan proses telah mencakup langkah-langkah mulai dari konfigurasi awal hingga uji coba konektivitas antara router di kedua kantor. Hasil dari pengujian ini nantinya dapat

memberikan keyakinan bahwa implementasi point-to-point atau peer-to-peer telah berhasil dan dapat diandalkan untuk mendukung komunikasi antar dua kantor tersebut.

DAFTAR PUSTAKA

- [1] W. Erawati and S. Heristian, "Implementasi Virtual Private Network (Vpn) Menggunakan Protokol Pptp Mikrotikrouter," *J. Tek. Inform. STMIK Antar Bangsa*, vol. IV, no. 1, p. 28, 2018.
- [2] E. Mufida, D. Irawan, and G. Chrisnawati, "Remote Site Mikrotik VPN Dengan Point To Point Tunneling Protocol (PPTP) Studi Kasus pada Yayasan Teratai Global Jakarta," *J. Matrik*, vol. 16, no. 2, p. 9, 2017, doi: 10.30812/matrik.v16i2.7.
- [3] P. B. Gentry, "What is a VPN?," *Inf. Secur. Tech. Rep.*, vol. 6, no. 1, pp. 15–22, 2001, doi: 10.1016/s1363-4127(01)00103-0.
- [4] H. Supendar, "Implementasi Remote Site Pada Virtual Private Network Berbasis Mikrotik," *Bina Insa. ICT J.*, vol. 3, no. 1, p. 234340, 2016.
- [5] Y. Putra, Jordy Lesmana, Indriyani, Luthfi, Angraini, "Penerapan Sistem Keamanan Jaringan Menggunakan," *IJCIT (Indonesian J. Comput. Inf. Technol.)*, vol. 3, no. 2, pp. 260–267, 2018.
- [6] S. Jahan, M. S. Rahman, and S. Saha, "Application specific tunneling protocol selection for Virtual Private Networks," *Proc. 2017 Int. Conf. Networking, Syst. Secur. NSysS 2017*, no. January, pp. 39–44, 2017, doi: 10.1109/NSysS.2017.7885799.
- [7] S. Watmah, "Implementasi VPN Menggunakan Point-To-Point Tunneling Protocol (PPTP) Mikrotik Router Pada BPRS Bumi Artha Sampang," *Insa. – J. Inov. dan Sains Tek. Elektro ISSN 2722-574X*, vol. 1, no. 1, pp. 6–12, 2020.
- [8] E. Prasetyo, A. Hamzah, and E. Sutanta, "Analisa Quality of Service (QOS) Kinerja Point to Point Protocol Over Ethernet (PPPOE) dan Point to Point Tunneling Protocol (PPTP)," *J. Jarkom*, vol. 4, no. 1, pp. 29–37, 2016.
- [9] F. Ardianto, "Penggunaan mikrotik router sebagai jaringan server," *Pengguna. Router Mikrotik*, no. 1, pp. 26–31, 2020.