

IMPLEMENTASI VIRTUAL PRIVATE NETWORK (VPN) BERBASIS MIKROTIK MENGGUNAKAN METODE PPTP PADA JARINGAN INTERNET DI FAKULTAS ILMU KOMPUTER UNUSIDA

Ilham Aji Laksono, Mochammad Machlul Alamin

Informatika, Universitas Nahdlatul Ulama Sidoarjo

Jl. Lingkar Timur KM 5,5 Rangkah Kidul, Kec. Sidoarjo, Kabupaten Sidoarjo, Jawa Timur 61234

Machlul410.tif@unusida.ac.id

ABSTRAK

Perkembangan teknologi informasi yang pesat menuntut institusi pendidikan untuk menyediakan akses jaringan yang aman dan handal, terutama dalam menghadapi tantangan keamanan data dan privasi. Fakultas Ilmu Komputer UNUSIDA sebagai salah satu institusi pendidikan yang mengandalkan jaringan internet untuk mendukung aktivitas akademik dan administratif, menghadapi permasalahan terkait kerentanan keamanan data saat mengakses sumber daya jaringan internal dari luar kampus. Hal ini menimbulkan risiko kebocoran data dan penyalahgunaan informasi yang sensitif. Oleh karena itu, diperlukan solusi untuk meningkatkan keamanan dan privasi data dengan memanfaatkan teknologi Virtual Private Network (VPN). Penelitian ini bertujuan untuk mengimplementasikan VPN berbasis MikroTik menggunakan metode Point-to-Point Tunneling Protocol (PPTP) pada jaringan internet di Fakultas Ilmu Komputer UNUSIDA. VPN digunakan untuk meningkatkan keamanan dan privasi data dengan membuat koneksi yang terenkripsi antara perangkat pengguna dan jaringan internal kampus. Metode PPTP dipilih karena kemudahan dalam konfigurasi dan kompatibilitasnya dengan berbagai perangkat. Implementasi dilakukan dengan mengkonfigurasi router MikroTik sebagai server VPN dan menguji koneksi dari beberapa perangkat client. Hasil pengujian menunjukkan bahwa penerapan VPN berbasis MikroTik dengan metode PPTP telah berhasil dilakukan di Fakultas Ilmu Komputer UNUSIDA. VPN tersebut mampu menyediakan akses yang aman ke sumber daya jaringan internal kampus dengan koneksi yang stabil dan terenkripsi.

Kata kunci : VPN, PPTP, Mikrotik, Jaringan Internet, UNUSIDA

1. PENDAHULUAN

Perkembangan teknologi informasi saat ini berkembang pesat, terutama dalam bidang komputer, mencakup perangkat keras dan aplikasi yang mendukung berbagai aktivitas manusia. Tidak dapat disangkal bahwa sistem komputerisasi memberikan kemudahan dalam menyelesaikan berbagai permasalahan. Internet juga memiliki peran besar dalam kehidupan manusia, terutama sebagai sarana cepat dan murah untuk memperoleh informasi. Seiring dengan kemajuan teknologi dan meningkatnya kebutuhan akses internet, aspek keamanan dan efisiensi dalam penggunaannya pun semakin perlu ditingkatkan [1].

Dalam era digital saat ini, keamanan jaringan merupakan aspek krusial yang perlu diperhatikan oleh setiap organisasi, termasuk institusi pendidikan. Fakultas Ilmu Komputer UNUSIDA, sebagai institusi pendidikan tinggi yang berfokus pada teknologi informasi, memerlukan tingkat keamanan dan privasi yang tinggi dalam akses jaringan internet. Beragam data sensitif, seperti data akademik, administrasi, dan penelitian, perlu perlindungan dari ancaman siber.

Virtual Private Network (VPN) telah menjadi solusi utama dalam menjaga keamanan komunikasi data di jaringan publik [2].

Teknologi ini memungkinkan transmisi data melalui jalur yang aman dengan enkripsi, sehingga dapat melindungi informasi sensitif dari ancaman

siber. Seiring meningkatnya kebutuhan akan privasi dan keamanan data, penggunaan VPN semakin meluas, terutama dalam lingkungan kerja yang mendukung akses jarak jauh. Sejak dikembangkan, VPN telah berevolusi menjadi alat krusial untuk mengamankan akses ke jaringan internal organisasi, khususnya saat bekerja dari rumah atau di lokasi dengan tingkat keamanan rendah [3].

Implementasi VPN berbasis Mikrotik pada jaringan Fakultas Ilmu Komputer UNUSIDA menghadapi beberapa permasalahan dan tantangan teknis. Keterbatasan pengetahuan dalam konfigurasi dan pemeliharaan VPN dapat menyebabkan kesalahan dalam pengaturan keamanan serta efisiensi jaringan. Selain itu, keterbatasan infrastruktur, seperti perangkat keras yang kurang mendukung serta bandwidth yang terbatas, turut memengaruhi performa VPN. Ketika jumlah pengguna yang mengakses jaringan meningkat secara bersamaan, keterbatasan ini dapat mengakibatkan penurunan kualitas koneksi dan menghambat akses data bagi mahasiswa maupun staf.

Di samping aspek teknis, tantangan lain dalam implementasi VPN adalah pemantauan dan pengelolaan lalu lintas jaringan yang belum optimal. VPN memerlukan sistem pemantauan yang komprehensif untuk menjaga stabilitas dan keamanan jaringan. Tanpa mekanisme pengawasan yang memadai, jaringan rentan terhadap ancaman keamanan seperti serangan brute-force atau

penyusupan yang dapat mengancam integritas data. Oleh karena itu, diperlukan strategi yang lebih efektif dalam manajemen dan pengamanan VPN agar dapat berfungsi secara optimal serta mendukung kebutuhan akademik yang terus berkembang.

Mengingat pentingnya keamanan jaringan serta kebutuhan akses yang aman bagi mahasiswa dan staf, penelitian ini akan menganalisis implementasi VPN pada jaringan internet di Fakultas Ilmu Komputer UNUSIDA. Diharapkan penerapan VPN ini dapat meningkatkan keamanan dan efisiensi akses jaringan.

2. TINJAUAN PUSTAKA

2.1. Penelitian Terkait

Sejumlah penelitian telah membahas efektivitas serta tantangan dalam implementasi VPN berbasis Mikrotik di berbagai lingkungan. Radju dkk [4] meneliti performa VPN Mikrotik dengan mengukur latency, throughput, dan packet loss dalam berbagai skenario jaringan. Hasil penelitian menunjukkan bahwa Mikrotik mampu menangani beban VPN yang tinggi dengan kinerja stabil, meskipun terjadi sedikit penurunan performa saat jumlah pengguna meningkat secara signifikan..

Sementara itu, penelitian oleh Elkana dan Widodo [5] mengimplementasikan VPN berbasis L2TP di untuk mengamankan akses ke sistem e-Rapor. Sebelum adanya VPN, jaringan sekolah menggunakan IP publik yang rentan terhadap peretasan. Dengan penerapan L2TP VPN, akses ke e-Rapor menjadi lebih aman, memungkinkan guru mengaksesnya dari mana saja dengan enkripsi yang melindungi data dari serangan siber. Penelitian ini menunjukkan bahwa VPN L2TP memberikan keamanan dan fleksibilitas akses, tetapi perlu pengelolaan bandwidth yang optimal agar tidak menghambat kinerja jaringan.

Penelitian yang dilakukan oleh Berliana S, dkk membahas penerapan VPN PPTP di PT Hinoka Sinergi Tanyo guna meningkatkan keamanan server komunikasi yang sebelumnya rentan terhadap akses tidak sah karena hanya dilindungi oleh Firewall NAT. Dengan mengimplementasikan VPN berbasis MikroTik, akses ke server menjadi lebih privat dan terbatas hanya untuk pengguna yang terotorisasi, terutama dalam koneksi jarak jauh. Hasil penelitian menunjukkan bahwa penggunaan VPN PPTP berhasil meningkatkan keamanan jaringan, mengurangi risiko kebocoran data, serta melindungi sistem dari potensi serangan siber [6].

2.2. Jaringan Internet

Internet merupakan jaringan global yang menghubungkan berbagai sistem komputer di seluruh dunia. Dengan menggunakan protokol standar seperti TCP/IP, internet memungkinkan komunikasi antarperangkat secara efisien serta mendukung transfer data secara luas. Internet tidak hanya berfungsi sebagai satu jaringan tunggal, melainkan sebagai ekosistem interkoneksi dari berbagai jaringan lokal yang beroperasi berdasarkan protokol yang sama [7].

Internet berperan penting dalam mendukung pertukaran informasi secara real-time, menjadikannya sebagai platform utama dalam ekosistem digital untuk berbagai layanan, seperti web browsing, email, dan streaming. Pemahaman mendalam mengenai protokol dan mekanisme jaringan menjadi aspek krusial dalam pengelolaan serta optimalisasi kinerja jaringan global.



Gambar 1. Jaringan Internet

2.3. Virtual Private Network

VPN (*Virtual Private Network*) adalah teknologi yang memungkinkan koneksi aman melalui jaringan publik, seperti internet, dengan membentuk "terowongan" virtual antara perangkat pengguna dan jaringan yang diakses. VPN menggunakan tunneling untuk melindungi data selama transmisi, sehingga tidak dapat diakses oleh pihak yang tidak berwenang. Selain itu, VPN menerapkan enkripsi untuk memastikan bahwa data tetap aman meskipun ada upaya intersepsi [8].

Dengan kombinasi tunneling dan enkripsi, VPN memberikan keamanan dan privasi tambahan, terutama saat menggunakan jaringan publik yang rentan, seperti Wi-Fi umum [9].

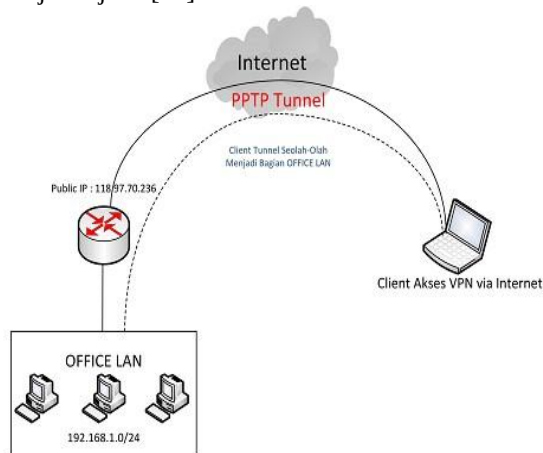
Teknologi ini menjadi solusi efektif dalam menjaga kerahasiaan dan integritas data, memungkinkan komunikasi yang lebih aman di lingkungan jaringan yang tidak terpercaya.

2.4. Point-to-Point Tunneling Protocol

Point-to-Point Tunneling Protocol (PPTP) adalah protokol jaringan yang digunakan untuk membangun koneksi VPN dengan memanfaatkan teknik tunneling untuk mentransmisikan data secara aman melalui jaringan publik. PPTP dikembangkan oleh Microsoft bersama konsorsium vendor pada tahun 1999 dan menjadi salah satu protokol VPN pertama yang diadopsi secara luas karena kemudahan implementasinya serta kompatibilitas dengan berbagai sistem operasi [10].

Protokol ini bekerja dengan mengenkapsulasi paket data menggunakan protokol GRE (*Generic Routing Encapsulation*), memungkinkan komunikasi yang efisien antara klien dan server. PPTP juga mendukung otentikasi pengguna menggunakan

protokol seperti PAP, CHAP, dan MS-CHAP, sehingga dapat digunakan dalam berbagai lingkungan jaringan yang membutuhkan koneksi terenkripsi dan akses jarak jauh [11].



Gambar 2. Topologi PPTP

2.5. Fakultas Ilmu Komputer Unusida

Fakultas Ilmu Komputer Universitas Nahdlatul Ulama Sidoarjo (UNUSIDA) adalah salah satu fakultas di bawah naungan Universitas Nahdlatul Ulama Sidoarjo, sebuah perguruan tinggi di Jawa Timur yang berafiliasi dengan organisasi Nahdlatul Ulama. Fakultas ini hadir sebagai bagian dari komitmen UNUSIDA dalam mengembangkan pendidikan tinggi yang berbasis nilai-nilai keislaman dan kemajuan teknologi.

Fakultas ini berfokus pada pemberian pendidikan berkualitas di bidang teknologi informasi dan ilmu komputer. Kurikulum yang diterapkan dirancang untuk memperkaya pengetahuan dan keterampilan mahasiswa, serta untuk mempersiapkan mereka menghadapi perkembangan pesat dalam teknologi informasi yang terus berubah.



Gambar 3. Gedung UNUSIDA

3. METODE PENELITIAN

3.1. Diagram Rancangan Penelitian

Diagram rancangan penelitian berfungsi untuk menggambarkan alur proses implementasi VPN secara sistematis. Tahapan diawali dengan identifikasi kebutuhan melalui studi kasus untuk menganalisis permasalahan dan menentukan solusi yang sesuai. Hal

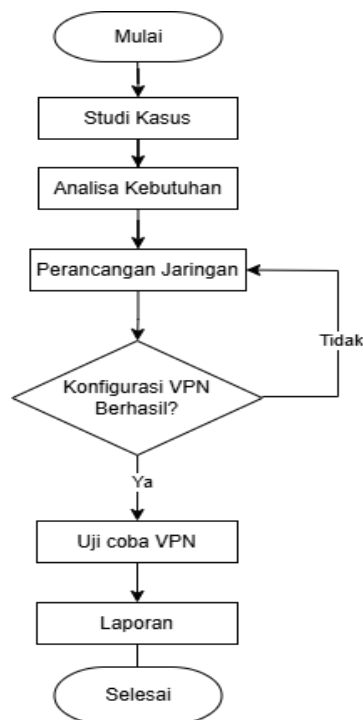
ini penting untuk memastikan bahwa solusi VPN yang dirancang dapat menjawab kebutuhan spesifik dari kasus yang dihadapi. Setelah kebutuhan teridentifikasi, langkah selanjutnya adalah merancang jaringan yang mencakup pemilihan topologi, konfigurasi perangkat, dan pengaturan protokol. Rancangan ini bertujuan untuk memastikan bahwa infrastruktur jaringan siap mendukung teknologi VPN yang akan diimplementasikan.

Setelah rancangan selesai, tahap implementasi dilakukan berdasarkan desain yang telah dibuat. Jika terjadi kegagalan selama proses implementasi, evaluasi dan penyesuaian dilakukan hingga VPN berfungsi sesuai dengan tujuan yang telah ditetapkan. Tahap ini memastikan bahwa setiap kendala yang muncul dapat diatasi dengan cepat dan efektif. Setelah VPN berhasil diimplementasikan, tahap pengujian dilakukan untuk memastikan bahwa seluruh fitur VPN berjalan optimal. Pengujian ini mencakup berbagai skenario untuk memverifikasi keandalan dan keamanan jaringan VPN.

Tahap uji coba ini melibatkan beberapa proses, dimulai dari konfigurasi server VPN pada router Mikrotik. Pada tahap ini, dilakukan pengaturan dasar seperti penentuan alamat IP untuk server VPN, konfigurasi protokol yang digunakan, serta pembuatan akun pengguna yang akan mengakses VPN. Proses autentikasi pengguna dikonfigurasi dengan menetapkan metode login yang aman, seperti penggunaan nama pengguna dan kata sandi yang terenkripsi. Selain itu, enkripsi data diaktifkan untuk memastikan bahwa informasi yang dikirimkan melalui VPN tetap terlindungi dari potensi ancaman keamanan. Parameter tambahan, seperti pengaturan firewall NAT dan akses kontrol, juga dikonfigurasi untuk membatasi akses hanya bagi pengguna yang berwenang. Dengan konfigurasi ini, diharapkan koneksi VPN dapat berjalan dengan aman dan stabil sebelum masuk ke tahap pengujian konektivitas.

Pengujian ini difokuskan pada pengujian konektivitas, yang mencakup uji ping untuk mengecek latensi serta verifikasi apakah perangkat klien dapat terhubung ke jaringan VPN dengan stabil. Selain itu, dilakukan pengecekan fungsionalitas dasar VPN, seperti keberhasilan proses autentikasi dan akses ke sumber daya jaringan internal. Hasil dari pengujian ini digunakan untuk mengevaluasi efektivitas implementasi VPN PPTP serta mengidentifikasi potensi perbaikan dalam aspek konfigurasi dan optimasi jaringan.

Hasil dari pengujian kemudian dicatat dalam laporan sebagai dokumentasi akhir sebelum proses dinyatakan selesai. Laporan ini berfungsi sebagai bukti bahwa VPN telah berhasil diimplementasikan dan memenuhi semua persyaratan yang telah ditetapkan. Setiap tahapan dalam proses ini dirancang untuk memastikan bahwa penerapan VPN berbasis MikroTik berlangsung secara efisien dan terstruktur, sehingga menghasilkan solusi yang handal dan sesuai dengan kebutuhan yang diidentifikasi pada awal proses.



Gambar 4. Diagram Rancangan Penelitian

3.2. Analisis Kebutuhan

Penerapan VPN berbasis MikroTik memerlukan dukungan perangkat keras dan perangkat lunak agar koneksi tetap aman dan stabil. Perangkat keras yang digunakan mencakup router MikroTik, switch, dan perangkat seperti laptop yang terhubung ke jaringan. Sementara itu, perangkat lunak mencakup pengaturan protokol VPN, sistem operasi pendukung, dan aplikasi untuk memantau serta mengelola koneksi jaringan.

Berikut adalah perangkat lunak dan perangkat keras yang di gunakan dalam penelitian ini :

Tabel 1. Kebutuhan Perangkat Keras

No	Perangkat Keras	Tipe
1.	Kabel LAN	7814A Belden
2.	Router Mikrotik	RB 952
3.	Laptop	HP Intel(L)Celeron(R) N4020

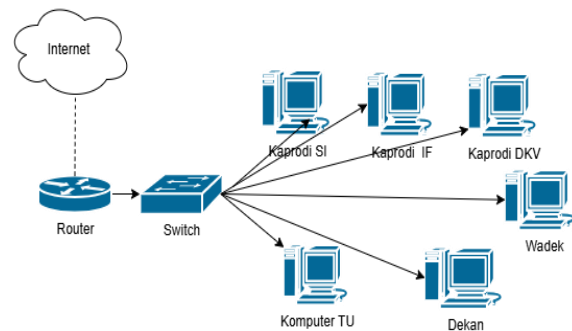
Tabel 2. Kebutuhan Perangkat Lunak

No	Perangkat Lunak	Tipe
1.	Winbox	Winbox 64bit
2.	RouterOS	Level 4
3.	Windows	Windows 11

3.3. Skema Jaringan

Jaringan komputer di Fakultas Ilmu Komputer UNUSIDA dirancang untuk mendukung kegiatan akademik, penelitian, dan administrasi melalui infrastruktur yang terintegrasi. Skema jaringan yang digunakan mencakup berbagai perangkat, seperti router, switch, dan server, serta koneksi internet yang dikelola secara terpusat guna memastikan keamanan dan efisiensi akses data.

Salah satu teknologi yang diterapkan adalah Virtual Private Network (VPN) berbasis MikroTik dengan metode Point-to-Point Tunneling Protocol (PPTP), yang memungkinkan akses jaringan secara aman bagi pengguna di luar kampus. Dengan implementasi ini, diharapkan fleksibilitas dalam pemanfaatan sumber daya akademik dan administratif dapat meningkat, serta mendukung efisiensi sistem jaringan di lingkungan FILKOM.



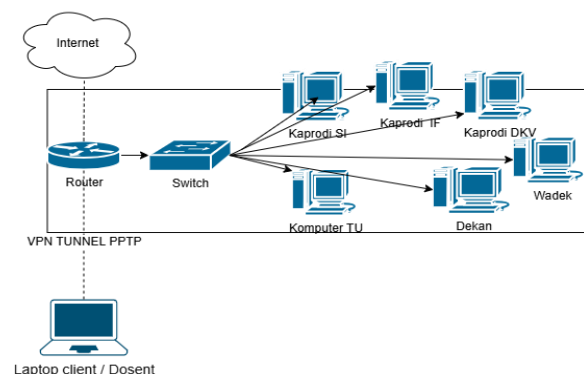
Gambar 5. Skema Jaringan Filkom UNUSIDA

3.4. Skema Topologi VPN

Perancangan topologi jaringan yang optimal merupakan aspek krusial dalam memastikan efisiensi, keamanan, dan skalabilitas sistem komunikasi data di suatu institusi. Dalam penelitian ini, diusulkan skema topologi jaringan yang sesuai dengan kebutuhan Fakultas Ilmu Komputer, guna meningkatkan kualitas layanan jaringan bagi pengguna, baik secara lokal maupun melalui akses jarak jauh.

Topologi yang diusulkan mempertimbangkan aspek kinerja, redundansi, serta keamanan, dengan penerapan Virtual Private Network (VPN) berbasis MikroTik menggunakan metode Point-to-Point Tunneling Protocol (PPTP) untuk mendukung akses yang aman dan fleksibel bagi mahasiswa, dosen, serta tenaga kependidikan.

Pada topologi usulan ini, akan dirancang agar laptop dosen atau karyawan bisa mengakses jaringan di Fakultas Ilmu Komputer baik secara lokal atau jarak jauh untuk mempermudah dan menghemat waktu.



Gambar 6. Topologi VPN Filkom UNUSIDA

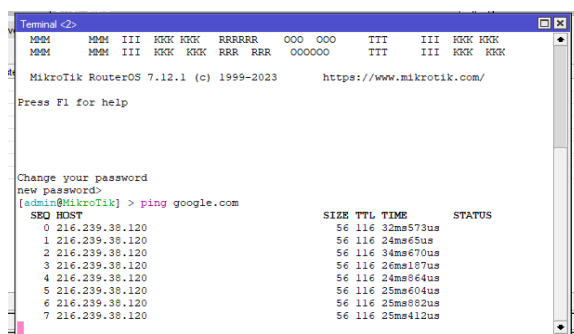
4. HASIL DAN PEMBAHASAN

Dalam perancangan Virtual Private Network (VPN) menggunakan protokol Point-to-Point Tunneling Protocol (PPTP), diperlukan serangkaian langkah yang harus diterapkan secara sistematis agar jaringan yang dibangun dapat beroperasi dengan baik, stabil, dan memiliki tingkat keamanan yang optimal.

4.1. Tahap Konfigurasi

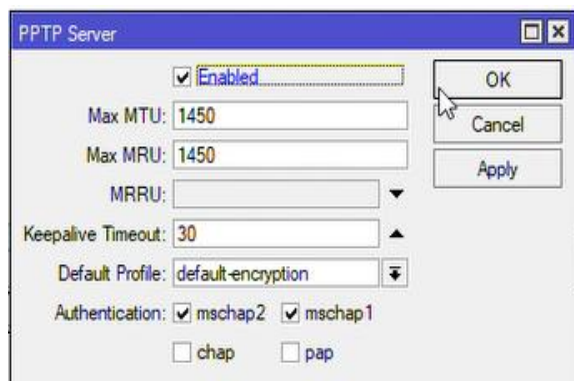
Setiap tahapan dalam proses ini harus dilakukan secara cermat, mulai dari persiapan perangkat keras dan perangkat lunak, konfigurasi server dan klien, hingga pengujian konektivitas untuk memastikan bahwa VPN dapat berfungsi sesuai dengan tujuan yang diharapkan. Berikut adalah langkah-langkah konfigurasi yang harus dilakukan:

- Dalam implementasi ini kita harus memiliki perangkat lunak yaitu Winbox untuk mengelola perangkat mikrotik. Sebelum melakukan konfigurasi pastikan mikrotik kita sudah terseting online atau sudah menerima jaringan seperti gambar di bawah ini.



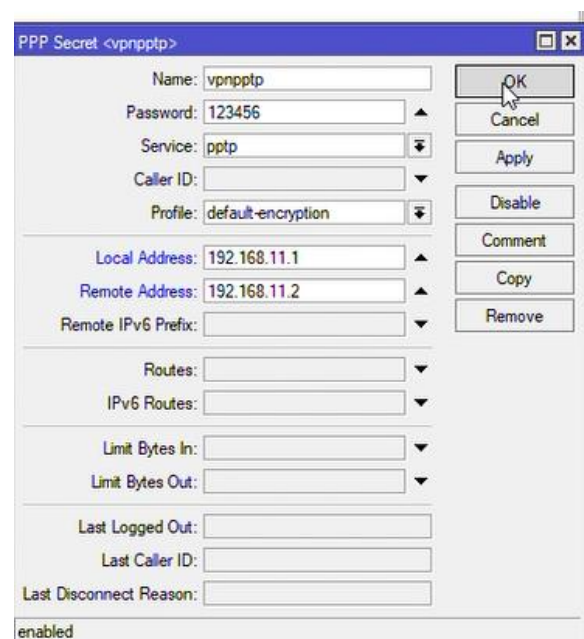
Gambar 7. Tes Ping Google

- Untuk mengaktifkan layanan PPTP, kita perlu mengaktifkan fitur PPTP Server di MikroTik. Dengan masuk ke menu PPP, kita dapat mengaktifkan PPTP Server dan mengatur profil default yang akan digunakan. Profil ini akan menentukan bagaimana klien VPN terhubung dan alamat IP yang akan mereka dapatkan. Dengan memilih profil default-encryption atau membuat profil baru, kita dapat memastikan komunikasi VPN lebih aman.



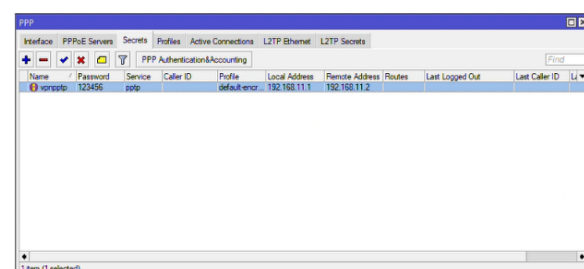
Gambar 8. Konfigurasi PPTP Server Menu PPP

- Tahap selanjutnya adalah konfigurasi pada tab secret MikroTik yang digunakan untuk mengatur akun pengguna VPN PPTP. Pada konfigurasi ini, Name diatur sebagai vpnppptp, yang merupakan nama akun VPN, dengan Password 123456. Service yang dipilih adalah pptp, yang menunjukkan bahwa akun ini digunakan untuk koneksi VPN dengan protokol PPTP. Profile yang digunakan adalah default-encryption, yang berarti enkripsi akan diterapkan sesuai dengan pengaturan default MikroTik. Local Address diatur ke 192.168.11.1, yang merupakan alamat IP MikroTik dalam jaringan VPN, sedangkan Remote Address diatur ke 192.168.11.2, yang merupakan alamat IP yang akan diberikan kepada klien VPN saat terhubung. Konfigurasi ini memungkinkan pengguna dengan kredensial yang sesuai untuk terhubung ke jaringan VPN dan mengakses sumber daya internal melalui MikroTik.



Gambar 9. Konfigurasi User Baru

- Setelah melakukan konfigurasi pada menu tab secret pastikan akun server VPN tersebut telah terbuat dan siap untuk di koneksikan seperti gambar di bawah ini.



Gambar 10. Interface PPTP Running

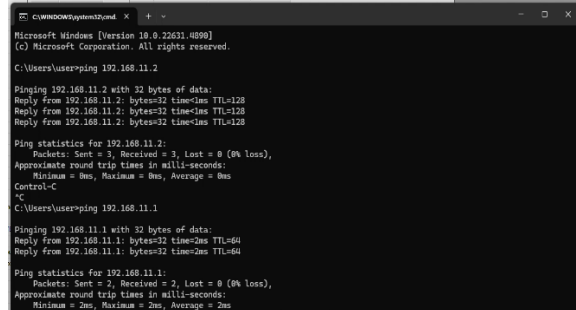
4.2. Tahap Pengujian

Selanjutnya lakukan koneksi VPN di sisi client tambahkan koneksi VPN baru melalui pengaturan jaringan pada sistem operasi yang digunakan, seperti Windows. Isikan informasi dari server seperti IP publik mikrotik, username, dan password. Setelah konfigurasi disimpan, koneksi dapat diaktifkan dengan menekan tombol "Connect", dan jika berhasil, status akan berubah menjadi "Connected".

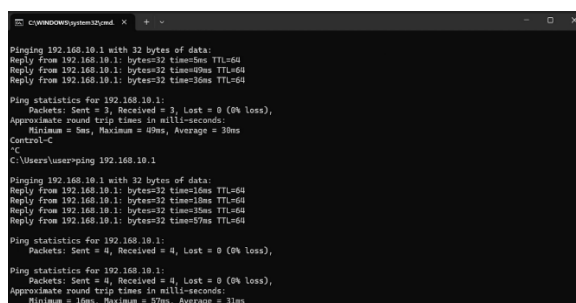


Gambar 11. VPN Connected

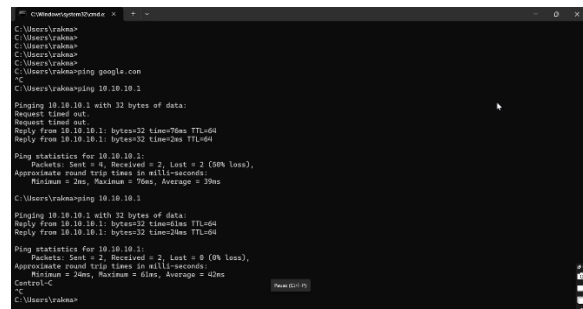
Untuk memastikan koneksi berjalan dengan baik, pengguna dapat melakukan uji konektivitas dengan perintah ping 192.168.11.1 melalui Command Prompt. Pada implementasi ini saya melakukan beberapa kali uji coba menggunakan IP yang berbeda beda seperti di gambar bawah ini.



Gambar 12. Test Ping Dari User Ke Server (192.168.11.2 – 192.168.11.1)

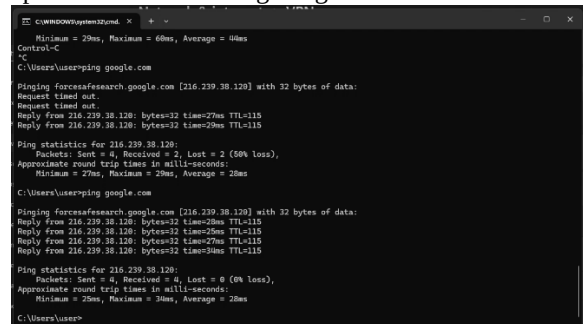


Gambar 12. Test Ping Dari User Ke Server (192.168.10.1 – 192.168.10.2)



Gambar 12. Test Ping Dari User Ke Server (192.168.2.1 – 10.10.10.2)

Lakukan juga test ping google.com untuk mengukur konektivitas jaringan antara perangkat apakah sudah terhubung dengan internet.



Gambar 14. Test Ping Google

5. KESIMPULAN DAN SARAN

Hasil yang diperoleh setelah proses perancangan dan implementasi menunjukkan bahwa penerapan Virtual Private Network (VPN) berbasis MikroTik dengan metode Point-to-Point Tunneling Protocol (PPTP) di Fakultas Ilmu Komputer UNUSIDA telah berhasil dilakukan. Dengan hasil pengujian latency adalah 16 ms. Hal ini menunjukkan bahwa semakin kecil latency, semakin cepat respon yang diberikan. Untuk memperluas referensi dan pemahaman lebih lanjut, penelitian ini sebaiknya dilanjutkan dengan membandingkan beberapa metode sekaligus guna menguji performa jaringan, khususnya dalam aspek keamanan, waktu transfer data, serta kenyamanan dalam komunikasi data saat menggunakan VPN.

DAFTAR PUSTAKA

- [1] Mesiono, M., Handoko, H., Siregar, A. H., & Hamdan, H. (2023). Peran Strategis Teknologi Informasi dan Komunikasi di STIT Al-Ittihadiyah Labuhan Batu Utara. *Journal On Education*, 5(3), 8362-8375.
- [2] Ekawati, I., & Irwan, D. (2021). Implementasi Virtual Private Network Menggunakan PPTP Berbasis Mikrotik. *JREC (Journal of Electrical and Electronics)*, 9(1), 41-48.
- [3] Audrey, B. F. (2022). Virtual Private Network Menggunakan Point To Point Tunnel Protocol Berbasis Mikrotik. *Journal Of Network And Computer Applications* (ISSN: 2964-6669), 1(1), 1-10.

- [4] Lingayat, A., Chandramohan, V. P., & Raju, V. R. K. (2020). Energy and exergy analysis on drying of banana using indirect type natural convection solar dryer. *Heat Transfer Engineering*, 41(6-7), 551-561.
- [5] Elkana, E., & Widodo, D. A. (2022). E Application of VPN based on L2TP untuk Mengakses e-Rapor di SMKN 5 Semarang. *Jurnal Fokus Elektroda: Energi Listrik, Telekomunikasi, Komputer, Elektronika dan Kendali*, 7(4), 212-218.
- [6] Fajrin, B. S., Priatno, P., & Effendi, M. R. (2024). PENERAPAN SISTEM KEAMANAN JARINGAN MENGGUNAKAN VPN DENGAN METODE PPTP PADA PT HINOKA SINERGI TANYO. *JSI (Jurnal sistem Informasi) Universitas Suryadarma*, 11(2), 185-196.
- [7] Ginting, S. H. N., Martin, A., Chyan, P., Imam, C., Mardiyanto, M., Nirawana, I. W. S., ... & Aghata, F. (2024). Pengantar Jaringan Komputer. Penerbit Mifandi Mandiri Digital, 1(01).
- [8] Gunawan, M. A., & Wardhana, S. (2023). Implementasi dan Perbandingan Keamanan PPTP dan L2TP/IPsec VPN (Virtual Private Network). *RESISTOR (Elektronika Kendali Telekomunikasi Tenaga Listrik Komputer)*, 6(1), 69-78.
- [9] Rijalul Akbar, R. (2025). *PENERAPAN KEAMANAN JARINGAN MENGGUNAKAN VIRTUAL PRIVATE NETWORK RASPBERRY Pi PADA SMA NEGERI 1 SUKAMAKMUR KABUPATEN ACEH BESAR* (Doctoral dissertation, UIN Ar-Raniry Banda Aceh).
- [10] Kurose, J., & Ross, K. (2021). Wireless and mobile networks. *Computer Networking: A Top-Down Approach*, 531-578.
- [11] Stallings, W. (2021). *5G Wireless: A Comprehensive Introduction*. Pearson.