Perancangan Virtual Private Network Layer 2 Tunneling Protocol (L2TP) Berbasis Mikrotik

Mochammad Rafii Nanda Wicaksana*
Jurusan Sistem Komputer, Universitas Sriwijaya Palembang, Indonesia

*Korespondensi: 09011281823053@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

Seiring perkembangan zaman jaringan komputer semakin maju terutama dalam bidang keamanan jaringan yang pada saat ini sangat diperhatikan baik di perusahaan, pemerintahan, dan instansi Pendidikan. Dalam berkomunikasi ataupun melakukan pertukaran data, perusahaan ataupun instansi akan melakukannya melalui jaringan internet. Dalam hal ini pastinya instansi menginginkan data yang dikirim ke tujuan dapat sampai dengan aman tanpa masalah. Walaupun demikian, banyak orang-orang ketiga yang ingin menyusup ke dalam jaringan tersebut dan mencuri data untuk keuntungan pribadi yang tentu saja hal in dapat merugikan suatu instansi. Oleh karena itu untuk membuat suatu jaringan menjadi aman tanpa gangguan lain yaitu dengan menerapkan Virtual Private Network (VPN) Layer 2 Tunneling Protocol yang merupakan jaringan pribadi dalam internet. VPN L2TP akan membuat suatu jaringan yang hanya dapat diakses oleh pihak tertentu yang telah dirancang agar dapat melakukan pengiriman data. Dengan VPN L2TP, jaringan dalam suatu instansi dapat menjadi lebih aman dalam melakukan pengiriman data yang penting dan mencegah pihak ketiga yang ingin mencoba menganggu data tersebut.

Kata Kunci: VPN, L2TP, Keamanan, Jaringan, MikroTik.

ABSTRACT

Computer networks, especially in network security, are advancing as the era progresses, which is currently highly prioritized in companies, government agencies, and educational institutions. Companies or institutions typically utilize the Internet network in communication and data exchange. In doing so, they aim to ensure that the data sent to the destination arrives securely without any issues. Nevertheless, many third parties are attempting to infiltrate these networks and steal data for personal gain, which can be detrimental to an institution. Therefore, implementing the Virtual Private Network (VPN) Layer 2 Tunneling Protocol becomes crucial to secure a network without interference. This protocol establishes a private network within the internet. VPN L2TP creates a network that can only be accessed by specific authorized parties, designed to facilitate secure data transmission. By utilizing VPN L2TP, a network within an institution can become more secure when transmitting crucial data, preventing third parties from attempting to disrupt or intercept the data.

Keywords: VPN, L2TP, Security, Network, MikroTik.

1. PENDAHULUAN

Dalam dunia IT, Sebagian besar komunikasi dan pertukaran data dilakukan melalui jaringan internet. Perusahaan dan instansi yang memiliki beberapa kantor yang jaraknya cukup jauh harus menggunakan jaringan internet dalam melakukan komunikasi. Dalam suatu jaringan internet tentu saja banyak pengguna dari berbagai pihak. Dengan adanya

internet, data yang dikirimkan dapat sampai kemanapun dengan cepat. Walaupun demikian, tidak menjamin data tersebut akan aman. Keamanan suatu jaringan sangat diperlukan terutama bagi perusahaan dan instansi agar mereka dapat melakukan pertukaran data dengan aman. Seiring berjalannya waktu perkembangan keamanan jaringan semakin meningkat. Walaupun demikian dengan meningkatnya suatu keamanan jaringan, tetap saja semakin banyak orang-orang jahat yang ingin masuk tanpa izin ke suatu jaringan dan mencuri data tersebut untuk keuntungan pribadi yang disebut cybercrime atau penjahat siber.

Seringnya aksi cybercrime dalam mencuri data-data penting membuat perusahaan dan instansi khawatir apabila mereka ingin melakukan pertukaran data. Hal ini menjadi masalah serius dikarenakan banyak instansi-instansi yang mengalami kerugian yang cukup besar dikarenakan ulah cybercrime. Banyak cara yang dilakukan agar data mereka dapat terjamin sehingga mereka dapat beroperasi dengan baik. Untuk menjaga suatu jaringan agar data mereka aman dan tidak mudah untuk dicuri oleh orang lain yaitu dengan menerapkan Virtual Private Network (VPN).

Virtual Private Network (VPN) merupakan salah satu cara untuk menerapkan keamanan pada jaringan internet yang mana teknologi ini membuat suatu jaringan privat atau bisa dibilang jaringan sendiri namun jaringan tersebut dapat beroperasi di internet sehingga komunikasi menjadi lebih aman. VPN merupakan teknik yang dapat menghubungkan beberapa jaringan lokal melalui jaringan publik atau internet dengan teknik VPN komunikasi seakan-akan kedua jaringan intranet yang besar[1]. Dengan demikian suatu perusahann atau instansi dapat melakukan komunikasi dan pertukaran data dengan jarak yang jauh tanpa khawatir.Salah satu protokol dalam VPN yaitu Layer 2 Tunneling Protocol (L2TP) Dengan menerapkan VPN L2TP, perusahaan atau instansi dapat mengatur siapa saja yang memiliki hak akses yang dapat terhubung ke jaringan instansi tersebut dan mencegah orang lain yang tidak memiliki hak akses terhadap jaringan sehingga keamanan dapat terjaga dan juga tidak membutuhkan biaya yang terlalu besar.

2. TINJAUAN PUSTAKA

2.1 Virtual Private Network (VPN)

VPN merupakan teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk dapat bergabung ke jaringan lokal[1]. Virtual Privat Network atau VPN merupakan terowongan virtual(Virtual Tunnel) dari jaringan ke jaringan lain yang terenkripsi[2]. VPN memungkinkan untuk setiap orang dapat mengakses jaringan privat melalui internet. Dengan VPN, seseorang yang memiliki hak akses dapat menggunakan data-data yang ada dalam jaringan tersebut. Fungsi VPN antara lain keamanan dalam berkomunikasi atau dalam pertukaran data, sehingga pihak lain tidak memiliki hak untuk masuk ke lalu lintas jaringan sembarangan. Konsep kerja dari VPN yaitu terdapat sebuah server yang akan dijadikan sebagai penghubung antar device. Semua komunikasi dan sambungan akan diatur oleh VPN Server sehingga suatu VPN Server harus memiliki kemampuan dan koneksi yang baik. VPN memiliki beberapa protokol untuk menjalankannya antara lain Point to Pint Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), Internet Protocol Security (IPSec), Secure Socket Layer (SSL) dan masih banyak lagi. VPN mempunyai tiga fungsi utama antara lain:

1. Confidentially

Fungsi VPN sebagai Confidentially atau kerahasiaan karena VPN menggunakan jaringan publik yang mana hal ini dapat menyebabkan pencurian data sering terjadi. Oleh sebab itu, VPN akan mengenkripsi data yang akan dikirim sehingga data akan sampai dengan aman meskipun data tersebut masih dapat dilihat tetapi data belum tentu dapat dibaca dengan mudah. Jadi, tujuan dari confidentially yaitu mengatur agar data dan informasi hanya bisa diakses oleh orang tertentu.

2. Data Integrity

   Fungsi VPN sebagai Data Integrity atau Keutuhan Data yaitu ketika suatu data dikirim dan akan melewati jaringan internet, maka ketika dalam perjalanan ke tujuan bisa saja data akan terganggu ataupun terdapat masalah seperti hilangnya isi data atau data telah berubah tidak sesuai dengan yang dikirim. Dengan VPN masalah tersebut dapat diatasi karena VPN dapat menjaga keutuhan data agar tetap aman sampai ke tujuan.

3. Origin Authentication

   VPN dapat melakukan autentikasi data atau melakukan pemeriksaan terhadap sumber data yang akan dikirim dan akan memperoleh informasi dari sumber pengirimnya. Dan pengirim data akan diperbolehkan untuk mengirim setelah diperiksa dan diautentikasi. VPN melakukan ini agar data yang akan dikirim dan diterima bersumber dari pihak yang dikenal dan bukan dari pihak yang bermaksud jahat sehingga data yang dikirim akan terjamin.

2.2 Layer 2 Tunneling Protocol (L2TP)

L2TP merupakan pengembangan dari PPTP ditambah dengan L2F. Network Protocol Security dan enkripsi yang digunakan sama dengan PPTP tetapi ketika melakukan komunikasi, L2TP menggunakan UDP port 1701[2]. Untuk keamanan yang lebih baik, biasanya protokol L2TP akan digabungkan dengan IPSec. Akan tetapi ketika menerapkan ini maka pengaturan yang akan di lakukan menjadi lebih susah kemudian dari sisi client juga harus sudah mendukung fitur IPSec. Untuk L2TP dikatakan lebih firewall friendly dari pada jenis protokol lainnya. L2TP membuat pengguna dapat terhubung ke jaringan lokal milik mereka dengan keamanan yang sama dimana pun posisi pengguna tersebut. Koneksi ini dianggap memperpanjang jaringan lokal pengguna. L2TP memiliki dua komponen utama yaitu LNS (L2TP Network Server) yang berfungsi untuk mengakhhiri dan mengotentikasi aliran PPP dan LAC (L2TP Access Concentrator) yang secara fisik akan mengakhiri panggilan[3]. Protokol ini tidak melakukan enkripsi sendiri melainkan melakukan enkripsi dengan protokol lain. L2TP biasanya digunakan untuk membuat Virtual Private Dial Network (VPDN) yang mampu membawa semua jenis protokol komunikasi di dalamnya.

2.3 Karakteristik L2TP

1. L2TP memiliki sifat media independent yang bisa berjalan pada media apapun.
2. Biasanya dikenal sebagai protocol dial-up, karena L2TP memperluas session PPP dial-up lewat jaringan publik.
3. Semua paket L2TP dikirim berbentuk UDP datagram
4. Biasanya akan digabungkan dengan protokol IPSec sebagai enkripsi disebut L2TP/IPSec
5. Dua titik Tunnel L2TP bernama LAC dan LNS

6. Saat tunnel telah dibuat, lalu lintas jaringan akan memulai koneksi LAC/LNS kemudian melakukan session saat koneksi berjalan.

2.4 Kelebihan dan Kekurangan L2TP

Kelebihan L2TP

1. Untuk meningkatkan keamanannya, bisa dikombinasikan dengan IPSec.
2. Kompatibel dengan berbagai sistem operasi seperti Windows, MacOS, dan Android
3. Konfigurasi yang simpel.

Kekurangan L2TP

1. L2TP tidak memiliki fitur enkripsi, oleh karena itu biasanya L2TP digabung dengan IPSec sebagai enkripsi.
2. L2TP/IPSec membutuhkan peralatan dan resource lebih dikarenakan terdapat fitur enkapsulasi ganda sehingga performa lebih lambat
3. Jika tidak diatur lebih lanjut, L2TP bisa diblokir oleh firewall NAT.

2.5 Tunneling

Tunneling merupakan dasar dari VPN untuk membuat suatu jaringan private melalui jaringan internet[4]. Tunneling merupakan enkapsulasi dari protokol ke paket protokol. Tunneling memakai suatu jaringan untuk mentransfer data lewat sambungan jaringan lain kemudian mengenkapsulasi protokol jaringan dalam data yang dibawa jaringan publik.

2.6 Routing

Routing merupakan proses untuk memilih jalur yang harus dilalui oleh paket[4]. Untuk menentukan jalur terbaik yang dipilih yaitu berdasarkan beban jaringan, Panjang datagram, dan pola lalu lintas. Intinya routing hanya memilih jalur yang terpendek.

2.7 MikroTik

Mikrotik adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer menjadi router network yang handal dan mencakup berbagai fitur[5]. Mikrotik didesain sedemikian rupa agar dapat digunakan dengan mudah dan sangat cocok untuk kebutuhan administrasi jaringan komputer seperti membangun dan merancang sistem jaringan yang mencangkup wilayah kecil hingga yang besar. Dahulunya Mikrotik adalah perusahaan kecil yang berkantor pusat di Latvia, bersebelahan dengan Rusia. Pendirinya yaitu John Trully dan Arnis Reikstins[6]. John meupakan orang Amerika yang pindah ke Latvia. Kemudian bertemu dengan sarjana fisika bernama Arnis tahun 1995. Lalu pada tahun 1996 mereka berdua mulai membangun mikrotik mulai dari sistem Linux dan MS-Dos. Jenis-jenis mikrotik antara lain:

1. Mikrotik RouterOS

   Mikrotik RouterOS merupakan sistem operasi yang digunakan untuk network router. Biasanya sistem operasi yang digunakan berbasis UNIX. Kelebihan yang dimiliki yaitu memiliki fitur seperti paket router, bridge, firewall, proxy server, hotspot dan masih banyak lagi. Untuk administrasi dan konfigurasinya bisa dilakukan lewat aplikasi windows yaitu WinBox. Kemudian untuk instalasi dari RouterOS dapat dilakukan pada PC standar.

2. RouterBoard

RouterBoard merupakan perangkat keras (hardware) yang dikembangakn perusahaan MikroTik yang berukuran sangat kecil dan praktis. Pada RouterBoard terdiri atas processor, flash memory, RAM, dan ROM. Sistem operasi yang digunakan yaitu RouterOS yang digunakan untuk router jaringan, proxy server, dhcp, bandwidth management, dns server dan juga dapat digunakan sebagai hotspot server.

2.8 Fitur-fitur Pada Router Mikrotik

Beberapa fitur yang dimiliki oleh router mikrotik antara lain:

- Firewall dan NAT
- Point to Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)
- Routing – Static routing
- Data Rate Management
- Simle Tunnel
- Hotspot
- Web proxy
- DHCP
- IPSec
- VRRP
- Universal Client
- UPnP
- SNMP
- NTP
- MNDP
- Monitoring/Accounting
- Tool

2.9 Kelebihan dan Kekurangan Mikrotik

Kelebihan Mikrotik

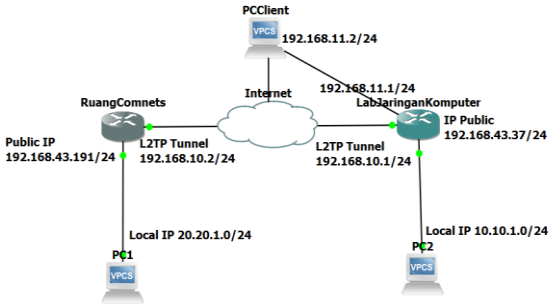
1. Sangat baik digunakan untuk kerja yang kecil hingga menengah
2. Mempunyai banyak fitur
3. Lebih hemat
4. Tegangan listrik yang digunakan rendah
5. Instalasi yang mudah
6. User friendly.

Kekurangan Mikrotik

1. Kurang mampu untuk digunakan dalam jaringan yang mencangkup area luas
2. Kurang cocok untuk Web Proxy Internal
3. Tidak bisa diperbaiki apabila perangkat mempunyai kerusakan yang besar.

3.METODE VLAN PADA MIKROTIK

3.1 Rancangan Topologi

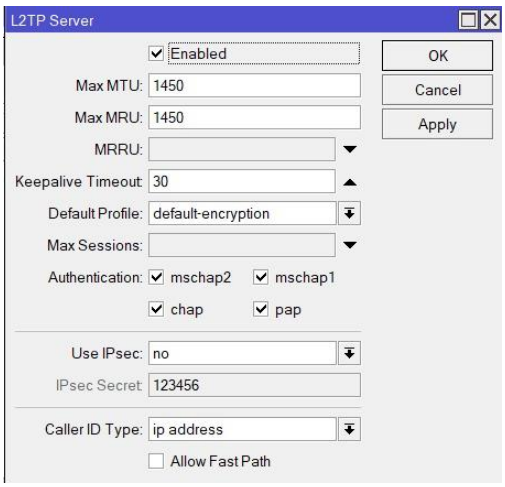


Gambar 1. Topologi Jaringan VPN

Untuk konfigurasi VPN L2TP dilakukan penghubungan jaringan pada topologi seperti pada gambar. Terdapat router Lab Jaringan Komputer dan router Ruang Comnets yang telah terhubung ke internet dan pada kedua router masing-masing memiliki jaringan lokal yang terhubung lewat port ether2. Selain itu pada topologi terdapat PC client yang juga sudah tersambung ke internet. Berikut ini beberapa langkah konfigurasi VPN menggunakan winbox.

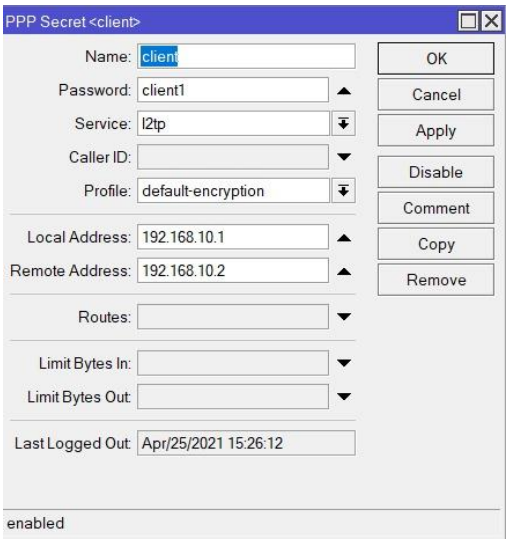
3.2 Konfigurasi L2TP Server

Pertama yang akan dilakukan konfigurasi yaitu L2TP Server dan router yang akan menjadi server yaitu pada Lab Jaringan Komputer. Aktifkan terlebih dahulu router sebagai L2TP Server dengan cara pada winbox masuk ke menu PPP > pilih L2TP Server kemudian ceklist opsi “Enabled” maka server akan secara otomatis aktif.



Gambar 2. L2TP Server

Setelah itu masuk ke Tab Secret untuk melakukan konfigurasi username dan password. Hal ini bertujuan untuk proses autentikasi client agar dapat terhubung ke L2TP Server. Caranya pada Tab Secret > klik Add [+].

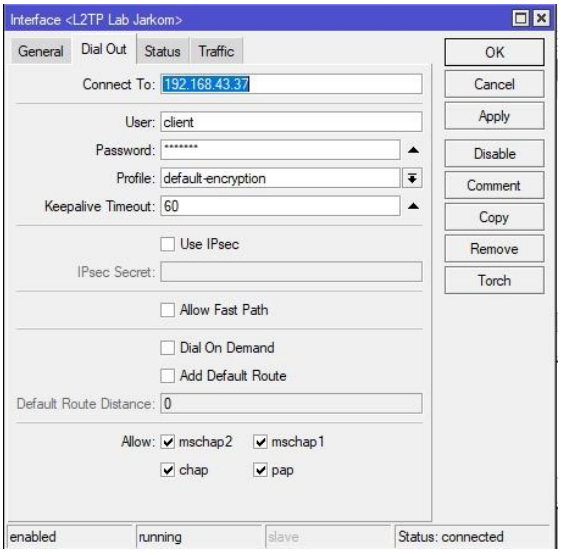


Gambar 3. User L2TP Server

Isi parameter yang tersedia seperti pada gambar. Name dan password diisi yang nantinya akan menjadi dial koneksi L2TP dari client. Pada services isi l2tp dan pada parameter local address dan remote address diisi dengan IP address yang mana local address merupakan alamat IP yang nantinya akan terpasang pada router yang menjadi server sedangkan pada remote address merupakan alamat IP yang akan diberikan kepada router client. Kedua IP ini nantinya akan diberikan secara otomatis setelat koneksi L2TP telah dibuat. Untuk konfigurasi pada server telah selesai dan selanjutnya yaitu melakukan konfigurasi pada L2TP client.

3.3 Konfigurasi L2TP Client

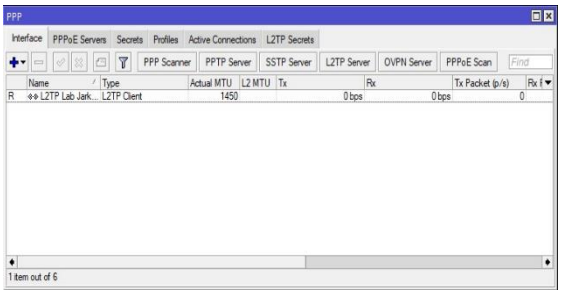
Setelah konfigurasi L2TP server, selanjutnya yaitu membuat L2TP client dan pada topologi yang menjadi client yaitu router Ruang Comnets. Setelah masuk ke konfigurasi winbox pada router client, pilih menu PPP > klik Add [+] lalu pilih L2TP Client.



Gambar 4. Interface L2TP

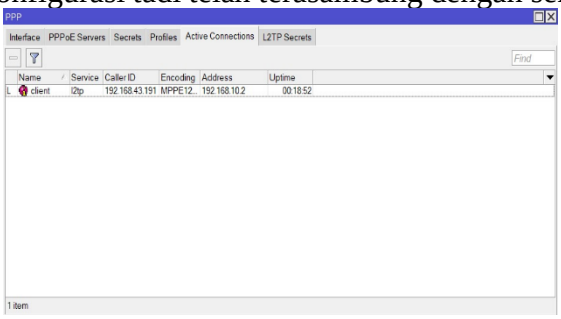
Isi parameter yang tertera pada gambar. Pada Connect To diisi dengan IP publik dari router server yang dalam kasus ini milik router Lab Jaringan Komputer. Kemudian parameter user dan password diisi dengan nama dan password yang telah diisikan pada secret yang telah dibuat di router server sebelumnya.

Setelah selesai melakukan pengisian klik OK kemudian akan tampil interface baru yang sudah dibuat dengan type L2TP Client. Cek apabila ada tanda flag R atau running maka client telah terhubung ke L2TP server.



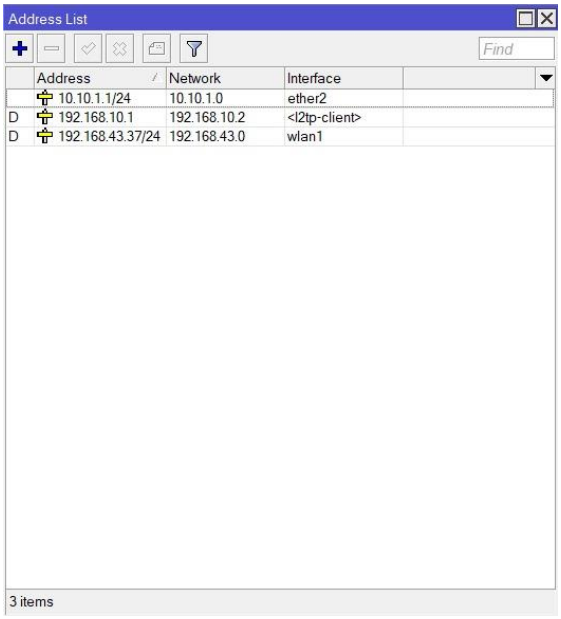
Gambar 5. VPN client

Apabila client telah running maka masuk kembali ke L2TP server lalu pilih tab Activation Connection. Cek apakah ada koneksi yang tersambung. Bisa dilihhat pada gambar bahwa client yang telah kita konfigurasi tadi telah terasambung dengan server.



Gambar 6. Koneksi L2TP

Kemudian cek IP address yang ada pada router server di menu IP > pilih Addresses dan bisa dilihat pada router server telah menerima IP address secara otomatis dan terhubung dinamik. IP address yang terisi secara otomatis tersebut merupakan IP yang diisi pada Secret sebelumnya yaitu pada local address. Interface nya berupa <l2tp-client> yang berarti terhubung ke client.

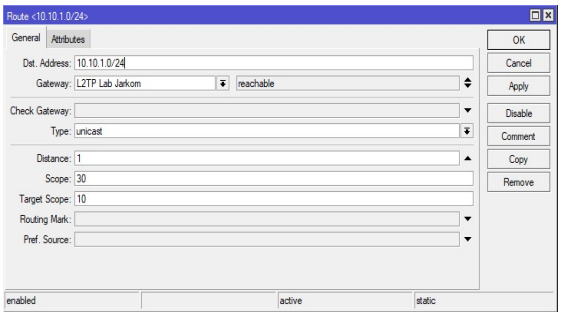


Gambar 7. Address List

Lakukan hal yang sama pada router client. Cek IP address pada router tersebut. Hal yang sama terjadi pada router client yaitu menerima alamat IP secara otomatis dan terhubung secara dinamik. IP tersebut juga diperoleh dari remote address yang telah diisi pada Tab Secret sebelumnya. Interface nya L2TP Lab Jarkom yang berarti telah terhubung ke router server.

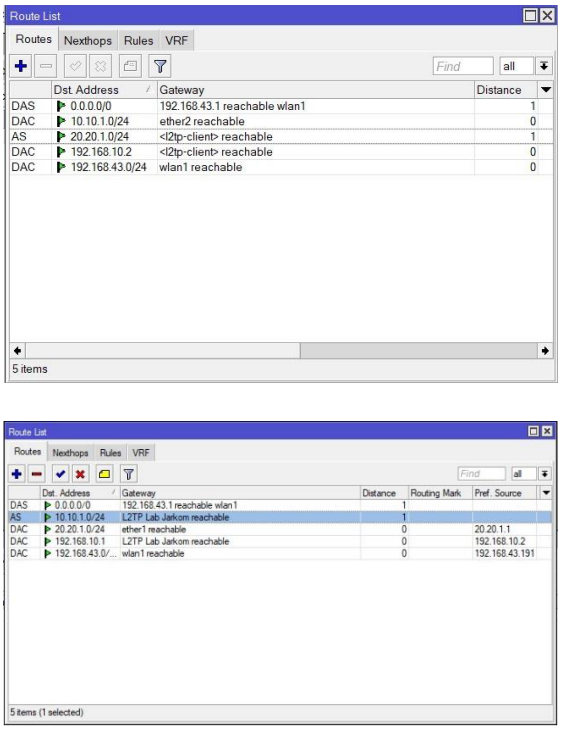
Setelah koneksi L2TP telah terbentuk, maka selanjutnya lakukan konfigurasi untuk sambungan antar jaringan lokal supaya tiap device dapat melakukan komunikasi. Berdasarkan topologi bahwa Lab Jaringan Komputer memiliki alamat network 10.10.1.0/24 dan di Ruang Comnets memiliki alamat network 20.20.1.0/24. Agar perangkat yang ada pada kedua jaringan tersebut dapat berkomunikasi maka lakukan konfigurasi rule routing baru.

Rule routing dilakukan pada kedua jaringan baik pada Lab jaringan Komputer maupun Ruang Comnets dengan cara static routing. Isi parameter Dst. Address dengan alamat jaringan lokal tujuan dan Gateway dengan alamat IP L2TP Tunnel atau bisa diisi dengan interface.



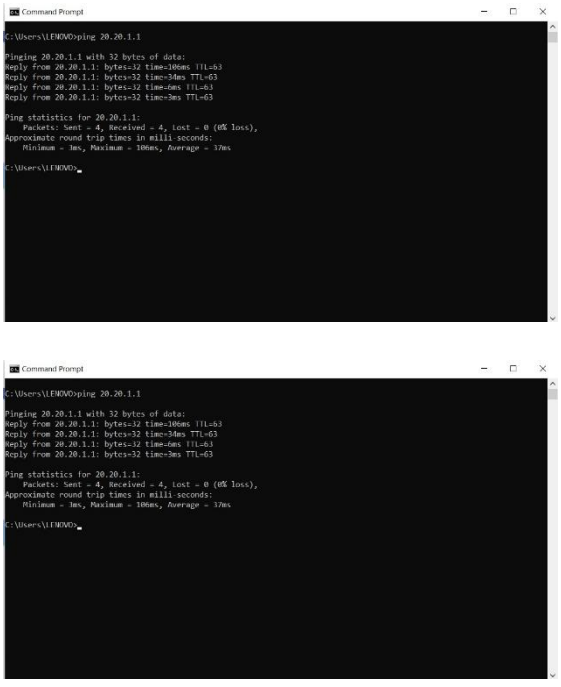
Gambar 8. Tabel Routing

Setelah selesai maka akan muncul list routing baru yang telah ditambahkan dengan Dst. Address dan Gateway sesuai dengan yang diisi.



Gambar 9. Update tabel routing

Untuk mengecek apakah kedua jaringan telah tehubung bisa dengan lakukan ping pada jaringan lokal pada Lab Jaringan Komputer dan pada jaringan lokal Ruang Comnets. Ketika ping telah berhasil maka perangkat yang ada pada kedua jaringan dapat saling berkomunikasi.

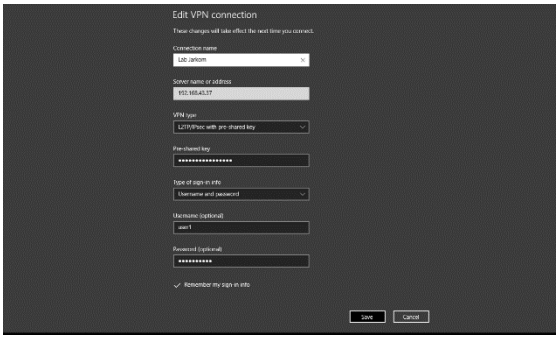


Gambar 10. Uji coba koneksi

3.4 Konfigurasi VPN PC Client

Setelah semua komnfigurasi L2TP telah selesai dan sambungan telah berhasil maka selanjutnya yaitu lakukan konfigurasi pada PC Client yang ingin masuk ke jaringan L2TP. Sesuai topologi bahwa PC Client akan melakukan koneksi dengan router Lab Jaringan Komputer lewat VPN. Untuk itu maka pada L2TP server tambahkan Secret baru yang akan digunakan untuk autentikasi pada PC Client agar dapat terhubung ke router server.

Setelah Secret telah ditambahkan selanjutnya lakukan konfigurasi VPN pada PC Client. Search VPN pada PC setelah itu klik [+] Add a VPN connection untuk menambahkan sambungan VPN baru.



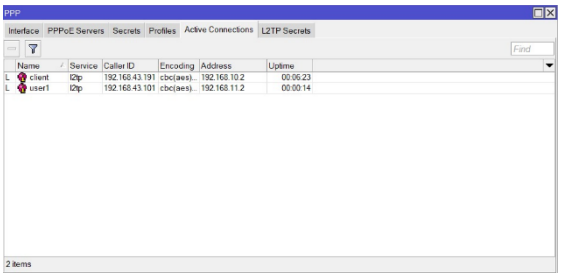
Gambar 11. VPN Client

Isi parameter yang tersedia seperti “Connection name” diisi sesuai keinginan. Untuk “Server name or address” diisi dengan IP Publik pada router Lab Jaringan Komputer. Lalu pada VPN type pilih L2TP/IPSec. Untuk Type of sign info pilih Username and password kemudian pada parameter “Username” dan “Password” isi sesuai dengan username dan password yang telah dibuat pada Secret di L2TP Server.

Setelah Selesai kemudian klik save maka VPN akan tersedia. Selanjutnya connect VPN tersebut dan tunggu beberapa saat hingga VPN berhasil terhubung ke L2TP Server.

Gambar 12. Koneksi VPN client dan server

Setelah VPN berhasil terhubung kemudian cek pada L2TP Server > pilih tab Active Connection. Bisa dilihat pada gambar bahwa ada koneksi baru yang aktif pada L2TP Server yaitu user1 yang merupakan koneksi VPN dari PC Client.



Gambar 13. Informasi L2TP Client

Setelah konfigurasi VPN selesai maka PC Client dapat akses dan berkomunikasi dengan router dan jaringan lokal pada Lab Jaringan Komputer.

4. ANALISIS PENELITIAN

Dari konfigurasi yang dilakukan, terlihat bahwa pembuatan suatu VPN L2TP dengan menggunakan Winbox dapat dilakukan dengan relatif mudah. Prosesnya tidak terlalu rumit, memungkinkan setiap orang untuk membuat jaringan privat mereka sendiri dengan menggunakan router MikroTik. Dengan kemudahan ini, siapa pun memiliki kesempatan untuk meningkatkan tingkat keamanan jaringan mereka. Router MikroTik menjadi alat yang dapat diandalkan untuk menciptakan jaringan privat yang lebih aman, menjadikan opsi VPN L2TP sebagai solusi yang dapat diimplementasikan secara luas untuk melindungi data dan informasi yang dikirim melalui jaringan tersebut. Pentingnya kesadaran akan cara membuat VPN L2TP dengan Winbox secara mandiri memberikan kontrol lebih kepada pengguna, memungkinkan mereka untuk mengelola dan mengamankan jaringan dengan lebih baik. Hal ini menggambarkan betapa pentingnya aksesibilitas dan kemudahan konfigurasi dalam mempromosikan penggunaan teknologi keamanan jaringan.

5. KESIMPULAN

Beberapa kesimpulan yang dapat diambil yaitu:

1. VPN merupakan teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk dapat bergabung ke jaringan lokal
2. L2TP merupakan pengembangan dari PPTP ditambah dengan L2F. L2TP membuat pengguna dapat terhubung ke jaringan lokal milik mereka dengan keamanan yang sama dimana pun posisi pengguna tersebut.
3. Mikrotik adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer menjadi router network yang handal dan mencakup berbagai fitur.
4. Salah satu keunggulan dari L2TP yaitu konfigurasi nya yang cukup mudah dan salah datu kelemahan dari L2TP yaitu membutuhkan resourch yang lebih untuk hasil yang baik.
5. Untuk membuat VPN L2TP tidaklah sulit karena konfigurasinya yang simpel sehingga dapat dibuat sendiri.

DAFTAR PUSTAKA

[1] S. Dewi, "Keamanan Jaringan Menggunakan VPN (Virtual Private Network) Dengan Metode PPTP (Point To Point Tunneling Protocol) Pada Kantor Desa Kertaraharja Ciamis," *EVOLUSI J. Sains dan Manaj.*, vol. 8, no. 1, pp. 128–139, 2020, doi: 10.31294/evolusi.v8i1.7658.

[2] 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.

[3] M. T. Roseno, "Analisis Perbandingan Protokol Virtual Private Network (VPN) – PPTP, L2TP, IPSEC – Sebagai Dasar Perancangan VPN pada Politeknik Negeri Sriwijaya Palembang," pp. 1–7, 2013.

[4] A. RACHMAWAN, "Perbandingan Protokol L2TP dan PPTP Untuk Membangun Jaringan Intranet di Atas VPN," *J. Manaj. Inform.*, vol. 8, no. 2, pp. 53–57, 2018.

[5] Rakhmat Dwi Jayanto, "Rancang Bangun Sistem Monitoring Jaringan Menggunakan Mikrotik Router OS," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 3, no. 4, pp. 391–395, 2019.

[6] A. Habibi and S. Arifin, "Membangun Jaringan Virtual Private Network (Vpn) Dengan Metode Tunneling Menggunakan Mikrotik Untuk Komunikasi Lokal Di Stmik Ppkia Pradnya Paramita Malang," *Jarkom*, vol. 6, no. 2, pp. 115–120, 2013.