

Virtual Private Network Analysis Point To Point Tunneling Protocol

Analisis Jaringan Virtual Private Network Point To Point Tunneling Protokol

Adiman¹⁾; Indra Kanedi²⁾; Reno Supardi³⁾

^{1,2,3)} Fakultas Ilmu Komputer, Universitas Dehasen Bengkulu

Email : ¹⁾ 1

How to Cite :

Adiman., Kanedi, I., Supardi, R. (2022). Virtual Private Network Analysis Point To Point Tunneling Protocol. Jurnal Media Computer Science, 1(2). DOI:

ARTICLE HISTORY

Received [xx Month xxxx]

Revised [xx Month xxxx]

Accepted [xx Month xxxx]

KEYWORDS

VPN Remot, Mikrotik, winbox

This is an open access article under the
[CC-BY-SA](#) license



ABSTRAK

Penelitian ini bertujuan untuk melakukan Analisis Jaringan Virtual Private Network Point To Point Tunneling Protokol Pada UPTD Balai Diklat Koperasi Dan UKM Provinsi Bengkulu. untuk melakukan aktifitas yang terjadi pada jaringan wifi di UPTD Balai Diklat Koperasi Dan UKM Provinsi Bengkulu Dan juga sebagai salah satu syarat untuk memperoleh gelar sarjana strata 1 pada jurusan informatika universitas Dehasen Bengkulu. Metode penelitian yang dilakukan adalah menggunakan metode Network Development life Cycle (NDLC) yang bertujuan pada proses Pembuatan dan perancangan perancangan Virtual Private Network Point To Point Tunneling Protokol menggunakan mikrotik RB951Ui-2HnD. Proses pembuatan dan perancangan yaitu bagaimana mengkoneksikan mikrotik dengan komputer kemudian dengan membuat remot akses jarak jauh dari lokasi mikrotik dengan menggunakan aplikasi winbox. Mikrotik dapat melakukan konfigurasi pada suatu jaringan yang dibutuhkan pada jaringan UPTD Balai Diklat Koperasi Dan UKM Provinsi Bengkulu dengan menerapkan remot akses jarak jauh, hasil remot dan keamanannya saat melakukan login koneksi mikrotik dapat dengan menerapkan tampilan login dan password jaringan sehingga mengamankan saat melakukan koneksi ke mikrotik dan dapat memudahkan kita dalam mengoperasikan jaringan mikrotik dari jauh dan aman.

ABSTRACT

This research aims to conduct a network analysis of the Virtual Private Network Point To Point Tunneling Protocol at the UPTD of the Bengkulu Province Cooperatives and SMEs Training Center. to carry out activities that occur on the wifi network at the UPTD Cooperatives and UKM Training Center Bengkulu Province and also as one of the requirements for obtaining a bachelor's degree in the Department of Informatics, Dehasen Bengkulu University. The research method used is the Network Development Life Cycle (NDLC) method which aims at the process of making and designing a Virtual Private Network Point To Point Tunneling Protocol using a mikrotik RB951Ui-2HnD. The process of making and designing is how to connect the proxy with a computer then by making a remote access remote from the mikrotik location using the Winbox application. Mikrotik can configure a network that is needed on the UPTD network of the Bengkulu Province Cooperatives and SMEs Education and Training Center by applying remote access remotely, the remote results and security when logging in to the Mikrotik connection can be done by applying the network login and password display so that it is secure when connecting to the mikrotik. and can make it easier for us to operate the mikrotik network remotely and safely.

PENDAHULUAN

Keamanan jaringan merupakan hal yang sangat penting untuk diperhatikan, terutama di era teknologi sekarang ini. Banyak instansi atau organisasi yang tidak memperdulikan masalah keamanan. Namun ketika seseorang menggunakan jaringan sebagai media informasi, komunikasi ataupun pertukaran data. Penggunaan itu sendiri banyak memberikan dampak positif, tetapi tidak dapat dipungkiri lagi bahwa dampak negatif yang ditimbulkan dari segi kejahatan seperti pencurian informasi atau data.

Oleh sebab itu, Untuk mengatasi masalah remote Mikrotik dan keamanannya maka dibutuhkan *Virtual Private Network (VPN)* dengan metode PPTP (*Point To Point Tunneling Protocol*). Secara garis besar VPN adalah suatu jaringan lokal yang terhubung melalui media jaringan publik. Dan PPTP adalah suatu protokol jaringan yang memungkinkan pengiriman data secara aman dari remote client kepada perusahaan swasta dengan membuat suatu virtual private network (VPN) melalui jaringan data berbasis TCP/IP (Nugroho Et Al, 2015).

Sedangkan definisi dari VPN secara umum adalah sekumpulan komputer atau jaringan tersendiri yang dihubungkan bersama-sama melalui jaringan publik seperti internet. Banyak orang yang menggunakan jaringan VPN dengan kebutuhan seperti bisnis maupun kebutuhan pribadi (Frenkel, 2017).

Saat ini, VPN telah dikenal oleh seluruh kalangan dari kalangan pelajar, perusahaan kecil maupun perkantoran, hingga lembaga-lembaga penting pemerintahan. Pemasangan VPN sendiri harus melihat skala kebutuhan pada suatu tempat yang akan dipasang VPN.

Kantor UPTD Balai Diklat Koperasi Dan UKM Provinsi Bengkulu, yang dalam kesehariannya melaksanakan kegiatan seperti biasa dalam proses kegiatan menggunakan internet, mengirim email, mengirim data, pencarian informasi dan lainnya, pihak kantor sudah berlangganan akses internet melalui internet *service provider (ISP)* yang sudah ada di kota Bengkulu.

Namun permasalahan yang sering terjadi pada saat admin dibutuhkan ketika terjadi gangguan ataupun gangguan pada jaringan namun admin yang berada diluar kantor ingin mengakses mikrotik, Namun jarak yang sangat jauh membutuhkan waktu yang lama dan tidak efisien maka dari itu, Untuk membantu pekerjaan admin yang berada diluar kantor dapat mengakses mikrotik jarak jauh agar mempermudah mengerjakan suatu pekerjaan dari jarak jauh maka diterapkannya remote access mikrotik jarak jauh. Agar tidak sembarang orang dapat mengakses ataupun mengendalikan Mikrotik jarak jauh, dari tindakan kejahatan seperti pencurian informasi atau data. Maka dibutuhkan juga keamanannya.

LANDASAN TEORI

Jaringan Komputer

Jaringan komputer adalah sebuah kumpulan komputer, printer dan peralatan lainnya yang terhubung dalam satu kesatuan. Informasi dan data bergerak melalui kabel-kabel atau tanpa kabel sehingga memungkinkan pengguna jaringan komputer dapat saling bertukar dokumen dan data, mencetak pada printer yang sama dan bersama-sama menggunakan hardware/software yang terhubung dengan jaringan

Virtual Private Network (VPN)

Menurut Elly Mufida Dkk.,(2017:10) VPN adalah sebuah teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk bergabung dengan jaringan lokal. Dengan cara tersebut maka akan didapatkan hak dan pengaturan yang sama seperti halnya berada didalam kantor atau network itu sendiri, walaupun sebenarnya menggunakan jaringan milik publik.VPN adalah sebuah proses dimana jaringan umum (public network atau internet) diamankan kemudian difungsikan menjadi sebuah jaringan privat (private network). Sebuah VPN tidak didefinisikan oleh rangkaian khusus atau router, tetapi didefinisikan oleh mekanisme keamanan dan prosedur-prosedur yang hanya mengijinkan penggunaanya yang ditunjuk akses ke VPN dan informasi yang mengalir melaluinya.

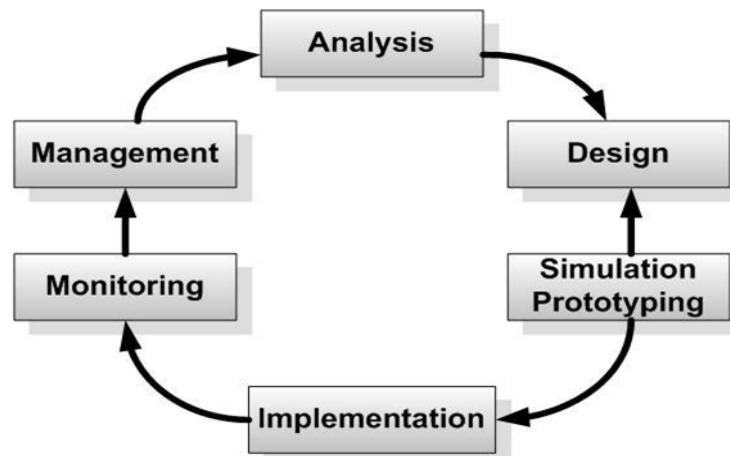
Point To Point Tunneling Protocol (PPTP)

Menurut Nugroho et al., dalam Sari Dewi Dkk., (2020:132) PPTP merupakan protocol jaringan yang memungkinkan pengamanan transfer data dari remote client ke server pribadi perusahaan dengan membuat sebuah VPN melalui TCP/IP. Teknologi jaringan PPTP merupakan pengembangan dari remote access Point-toPoint protocol yang dikeluarkan oleh Internet Engineering Task Force (IETF). PPTP merupakan protocol jaringan yang merubah paket PPTP menjadi IP datagram agar dapat ditransmisikan melalui internet. PPTP juga dapat digunakan pada jaringan private LAN-to LAN

METODE PENELITIAN

Metode Analisis

Metode penelitian yang digunakan adalah *Network Development Life Cycle* (NDLC). *Network Development Life Cycle* (NDLC) merupakan suatu metode yang digunakan dalam mengembangkan atau merancang jaringan infrastruktur yang memungkinkan terjadinya pemantauan jaringan untuk mengetahui statistik dan kinerja jaringan. Hasil analisis kinerja tersebut dijadikan sebagai pertimbangan dalam perancangan desain jaringan, baik desain jaringan yang bersifat fisik atau jaringan logis. NDLC terdiri dari enam tahapan, yaitu *analysis*, *design*, *simulation prototyping*, *implementation*, *monitoring* dan *management*.



Gambar 1. Siklus NDLC

HASIL DAN PEMBAHASAN

Hasil

Agar mikrotik terhubung ke jaringan terlebih dahulu harus melakukan konfigurasi terhadap router mikrotik adapun konfigurasi yang perlu dilakukan sebagai berikut.

Konfigurasi *interface router*

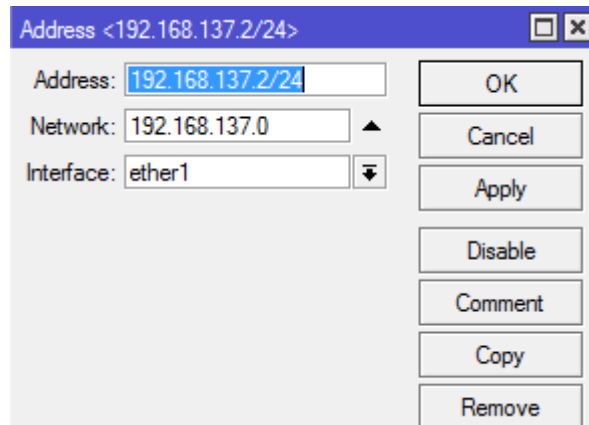
Konfigurasi *interface router* Mikrotik ini diperlukan untuk mengetahui di jalur *interface* mana jaringan akan terhubung. Dalam penelitian ini penulis menggunakan *interface* ether1 sebagai sumber koneksi internet dan *interface* ether2 sebagai penghubung jaringan WLAN ke *router* dan ether 3 sebagai jalur Ip Public VPN. Adapun hasil dari konfigurasi *interface* pada *router* mikrotik dapat dilihat seperti berikut.

Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet
R ether1	Ethernet	1500	1598	69.6 kbps	3.0 kbps	6	
R ether2	Ethernet	1500	1598	0 bps	0 bps	0	
R ether3	Ethernet	1500	1598	0 bps	0 bps	0	
R ether4	Ethernet	1500	1598	0 bps	0 bps	0	
R ether5	Ethernet	1500	1598	0 bps	0 bps	0	
R sstp-public	SSTP Client	1500		0 bps	0 bps	0	
WLAN wlan1	Wireless (Atheros AR9...	1500	1600	0 bps	0 bps	0	

Gambar 2. Hasil Konfigurasi interface Router Mikrotik

IP ADDRESS ETHER 1

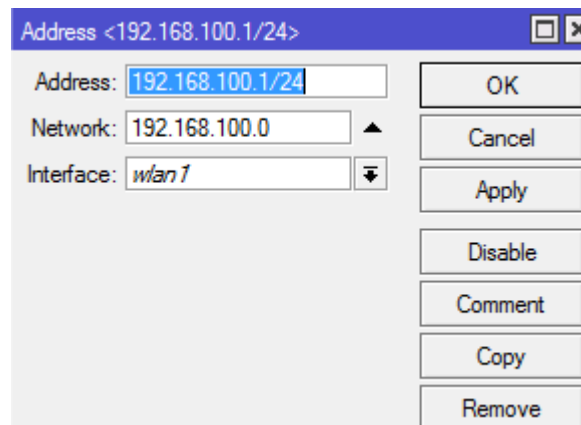
Pada "ip address add address" untuk menambah suatu ip address untuk menuju jaringan LAN pada setting address dengan ip "192.168.137.2/24" sesuai dengan ip yang telah ditentukan, pada jaringan ini ip yang digunakan untuk mendapatkan akses internet yaitu 192.168.137.2/24 pada ether1 seperti berikut.



Gambar 3. Ip Address Ether 1

IP ADDRESS ETHER 2

Konfigurasi ip address ether 2 sebagai jalur koneksi jaringan untuk Wlan dengan ip 192.168.100.1/24 sebagai berikut



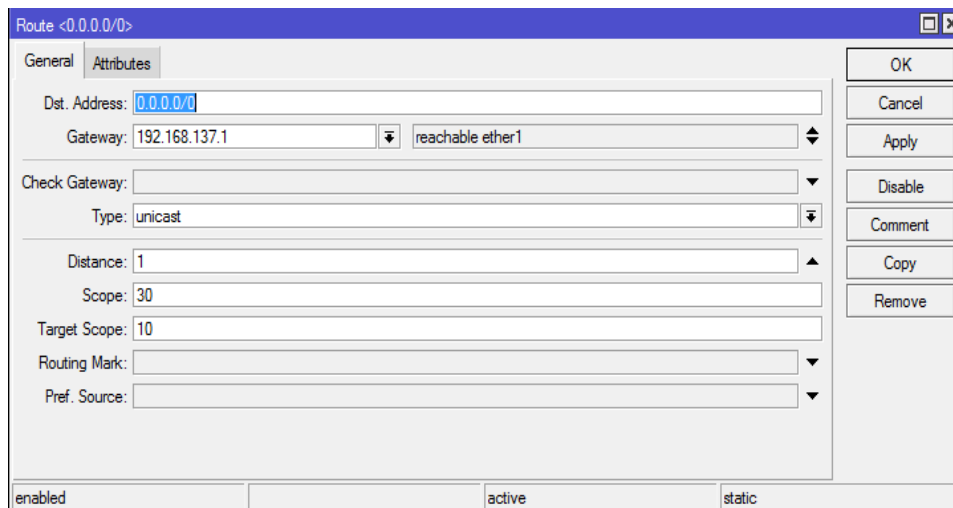
Gambar 4. Ip Address Ether 2

Konfigurasi DNS

DNS dalam penelitian ini akan mengikuti DNS yang digunakan oleh *router* yaitu "192.168.100.1" dan "8.8.8.8" sebagai berikut

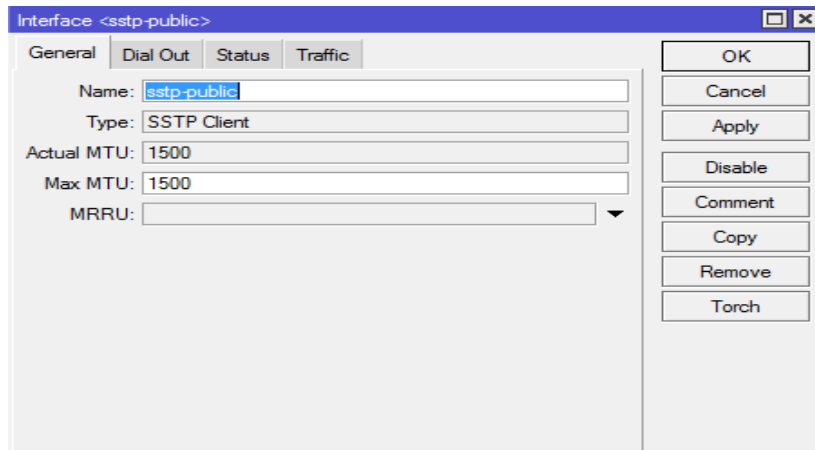
1. Konfigurasi static routing

Menambahkan pada tab ip>Routes tekan tambah, lalu pada dst address 0.0.0.0/0 dan gateway 192.168.137.1 yaitu dimana ip dari sumber internet kita yang pada kasus ini adalah laptop/pc



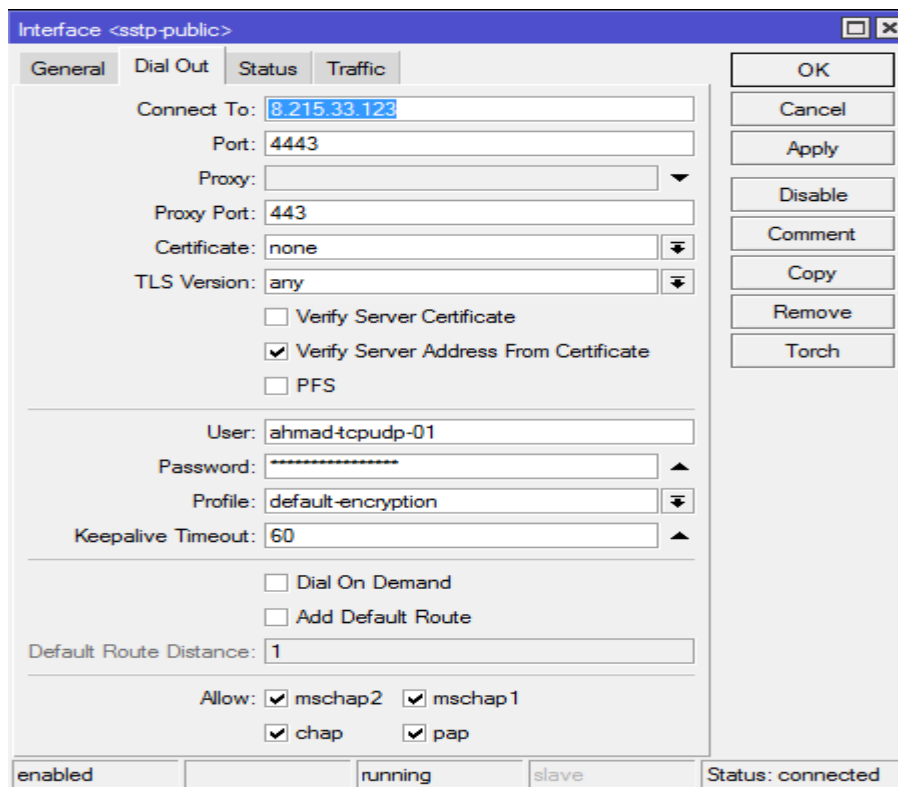
Gambar 5. Konfigurasi Static Routing

- Setting IP public yang sudah disewa. dengan detail sstp
Pada tab interface, tekan tambah "+" lalu tekan pada sstp client Masukan nama interface sstp-nya pada tab general misal "sstp-public" sebagai berikut.



Gambar 6. Name General Interface

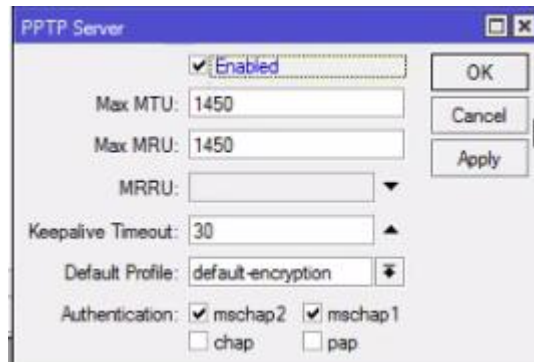
- DIAL OUT**
pada tab dial out, masukan connect to pada ip yang disediakan oleh penjual ip public misal "8.215.33.123" dan port 4443 lalu pada user dan password dimasukan sesuai yang diberikan oleh penyedia ip public disini ahmad-tcpudp-01 dan password ahmad-tcpudp01! serta pada profile di setting default-encryption. tekan ok. ip public berhasil di atur



Gambar 7. Konfigurasi Dial Out SSTP

Konfigurasi PPTP

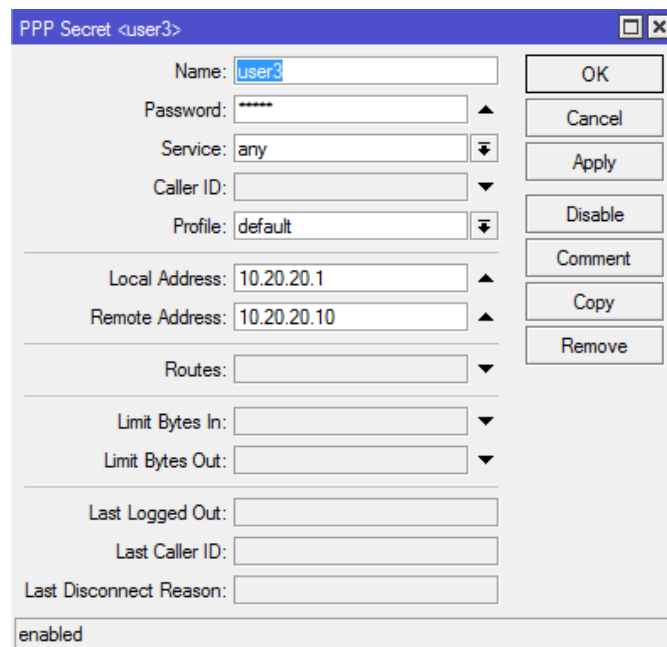
Untuk mengaktifkan encryption tekan pada tab PPP, lalu tekan tombol PPTP Server dan centang enabled, pada default profile diatur default-encryption dan tekan ok.



Gambar 8. Default Encryption PPTP

Konfigurasi PPP Secret

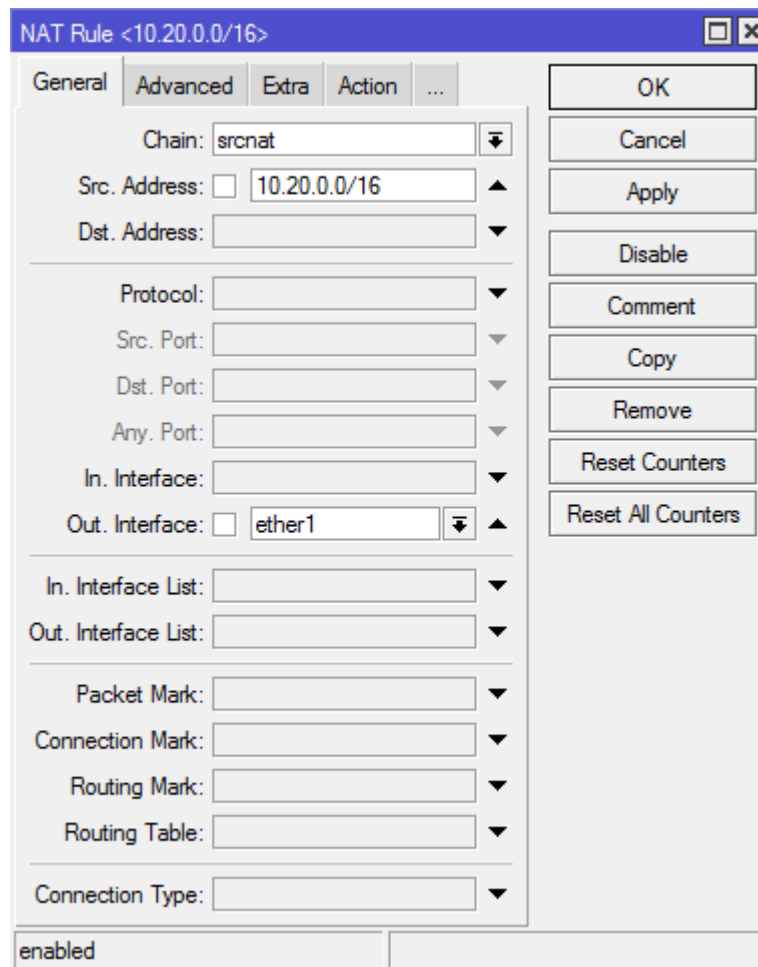
pada tab ppp secret tekan tanda tambah pada nama isi misal "user3" isi local address untuk gateway client pada topologi ini kita isi "10.20.20.1" pada remote address untuk ip client, misal "10.20.20.3" dan password yang akan di gunakan user untuk login ke pptp kita misal 12345



Gambar 9. Konfigurasi PPTP Secret

Konfigurasi firewal pada Nat

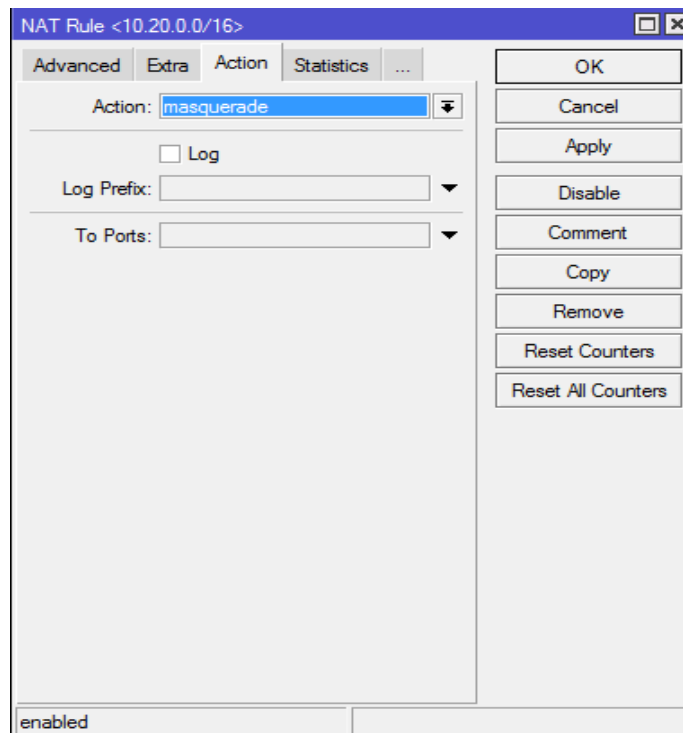
Setting NAT agar user pptp dapat mengakses internet ketika tersambung ke pptp kita dengan memberi nama pada general yaitu chain dengan srcnat dan Pada src address dengan network dari client pptp kita yaitu 10.20.0.0/16 pada Mikrotik yang di atur dan ini isi out interface dengan ether1, sebagai berikut



Gambar 10. Konfigurasi Nat Rule

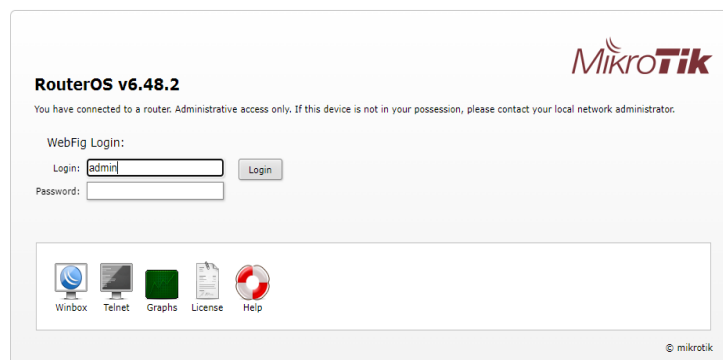
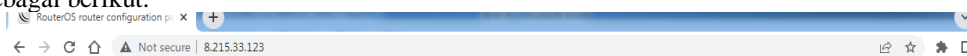
Konfigurasi Action Nat

pada tab action di atur pada masquerade berfungsi sebagai Ip address Private yang ada pada jaringan sebagai berikut



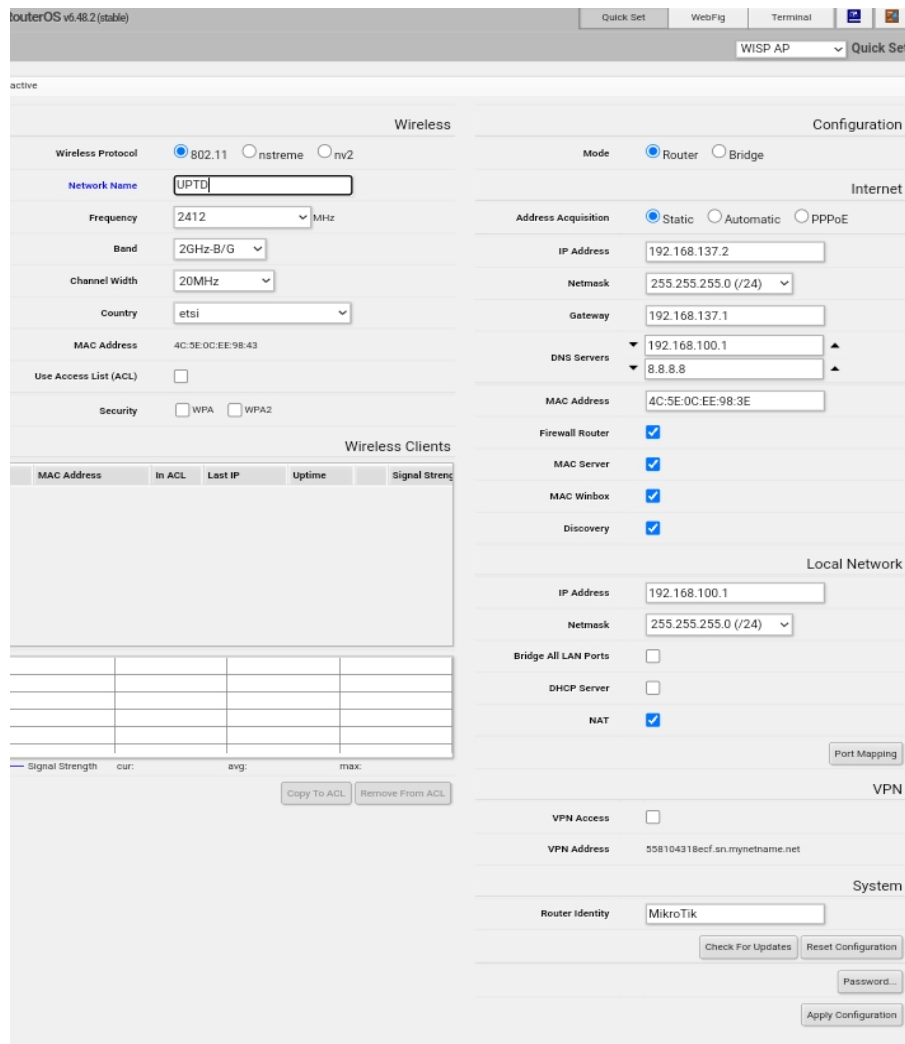
Gambar 11. Action Nat

Setelah semua konfigurasi di atas di terapkan pada Mikrotik RB951Ui-2HnD maka hasil dari konfigurasi yang telah dilakukan maka sudah dapat client untuk melakukan login Remote mikrotik menggunakan ip dinamis jarak jauh sebagai berikut.



Gambar 12. Login Mikrotik Webfig

Adapun hasil dari login router mikrotik dengan menggunakan *username* dan *password* yang benar dapat dilihat seperti berikut ini.



Gambar 13. Remote Router Mikrotik Jarak Jauh

Dari Gambar 13. Di atas dapat dilihat bahwa client terhubung router mikrotik webfig dengan ip dinamis dengan jarak jauh.

KESIMPULAN DAN SARAN

Kesimpulan

1. Pengoperasian mikrotik dengan winbox mempermudah IT administrator dalam melakukan konfigurasi jaringan
2. VPN merupakan solusi yang aman dalam hal pertukaran data yang menggunakan jaringan Public
3. Dengan menerapkan VPN PPTP Remote Mikrotik bisa diakses dimana saja selama terhubung internet
4. Agar tidak sembarang orang dapat melakukan Remote Mikrotik di terapkannya keamanan untuk setiap Login seperti username dan password.

Saran

1. Jalur VPN akan stabil dan lebih mudah dalam konfigurasi apabila disisi Mikrotik memiliki jalur internet dedicated dan memiliki IP Publik static.
2. PPTP terkadang susah untuk connect atau sering terputus, jika VPN sering digunakanya smartphone disarankan menggunakan L2TP VPN
3. Untuk perangkat client yang menggunakan OS Windows 7, hanya bisa terkoneksi apabila disisi Mikrotik mengaktifkan encryption

DAFTAR PUSTAKA

- Apiyah, E., Dan Elpiani (2016) *Analisa Dan Perancangan Jaringan Komputer Menggunakan Teknologi Nirkabel Berbasis Wifi (Studi Kasus : PT Weha Indonesia)*. *Teknik Informatika Stmik Antar Bangsa*, 93 Vo 2 No.1 2016 92-101
- Ardianto, F., & Akbar, T. (2017). *Perancangan Sistem Monitoring Keamanan Jaringan Jarak Jauh Menggunakan Mikrotik Operational System Melalui Virtual Private Network*. *Surya Energy* , 135. Vol 2 No.1 2017 135-139
- Dewi, S., Riyadi, F., Suwastitaratu, T., & Hikmah, N. (2020). *Keamanan Jaringan Menggunakan Vpn (Virtual Private Network) Dengan Metode Pptp (Point To Point Tunneling Protocol) Pada Kantor Desa Kertaraharja Ciamis*. *Sains Dan Manajemen* , 130-132. Vol 8 No.1 2020 129-139
- Islamiati, T. S., Sofah, R., & Harlina. (2019). *Pengembangan Media Audio Visual Layanan Klasikal Bidang Karir Pada Materi Orientasi Masa Depan Di Sma Srijiaya Negara Palembang*. *Konseling Komprehensif: Kajian Teori dan Praktik Bimbingan dan Konseling* , 35. Vol 6 No.1 2019 30-39
- Khasanah, S. N., & Utami, L. A. (2018). *Implementasi Failover Pada Jaringan Wan Berbasis Vpn*. *Teknik Informatika Stmik Antar Bangsa Vol,4 No.1 Februari 2018*, 62-66.
- Kolyaan, Y. (2012). *Teknologi Internet Protocol Serta Perbandingan Teknologi Ipv4 Dan Ipv6*. *Ilmiah Mustek Anim Ha* , 129. Vol 2 No.3 2012 128-142
- Mufida, E., Irawan, D., & Chrisnawati, G. (2017). *Remote Site Mikrotik Vpn Dengan Point To Point Tunneling Protocol (Pptp) Studi Kasus Pada Yayasan Teratai Global Jakarta*. *Matrik* , Vol 16 No.2 9-19.
- Patih, D. F. (n.d.). Fitriawan, H., & Yuniati, Y. (2012). *Analisa Perancangan Server Voip (Voice Internet Protocol) Dengan Opensource Asterisk Dan Vpn (Virtual Private Network) Sebagai Pengaman Jaringan Antar Client*. *Informatika Dan Teknik Elektro Terapan* , Vol 1 No.1 Januari 2012 42-48.
- Sari, A. P., Sulistiyono, & Kemala, N. (2020). *Perancangan Jaringan Virtual Private Network Berbasis Ip Security Menggunakan Router Mikrotik*. *Prosisko* , 155. Vol 7 No.2 2020 150-164
- Septiani, Y., Arribe, E., & Diansyah, R. (2020). *Analisis Kualitas Layanan Sistem Informasi Akademik Universitas Abdurrab Terhadap Kepuasan Pengguna Menggunakan Metode Sevqual*. *Teknologi Dan Open Source* , 133. Vol 3 No.1 2020 131-143
- Susianto, D. (2016). *Implementasi Queue Tree Untuk Manajemen Bandwidth Menggunakan Router Board Mikrotik*. *Cendikia Vol 12 No.1 Bandar Lampung April 2016*, 1-7.
- Tutu, A. (2020). *Konfigurasi Mikrotik Menggunakan Metode Gui & Cli*. Yogyakarta: Budi Utama. 1-88.
- Umaroh, L., & Rifauddin, M. (2019). *Implementasi Virtual Private Network (Vpn) Di Perpustakaan Universitas Islam Malang* . *Dokumentasi dan Informasi* , 195. 2020 193-201
- Wagiu, R., Najoan, M., & Sengkey, R. (Juni 2016). *Evaluasi Dan Perancangan Peningkatan Unjuk Kerja Jaringan Wifi Di Kampus Unsrat* . *Teknik Elektro Dan Komputer* , Vol5 No.3 Juni 2016 41-48
- BIBLIOGRAPHY \1 1057* Wardoyo, S., Riyadi, T., & Fahrizal, R. (2014). *Analisis Performa File Transport Protocol Pada Perbandingan Metode Ipv4 Murni, Ipv6 Murni Dan Tunneling 6to4 Berbasis Router Mikrotik*. *Nasional Teknik Elektro* , Vol,3 No.2 September 2014, 106-117.
- Wahyuni, J., Paranthi, Y. W., & Wanto, A. (2018). *Analisis Jaringan Saraf Dalam Estimasi Tingkat Pengangguran Terbuka*. *Jurnal Infomedia* , 3, 18-24.
- Wongkar, S., Sinsuw2, A., & Najoan, X. (2015). *Analisa Implementasi Jaringan Internet Dengan Menggabungkan Jaringan Lan Dan Wlan Di Desa Kawangkoan Bawah Wilayah Amurang Ii*. *Teknik Elektro Dan Komputer* , 63. Vol 4 No.6 2015 62-68