JUNIF
JURNAL NASIONAL INFORMATIKA

Vol. 1, No. 1, April 2020, pp. 57-65

IMPLEMENTASI *VIRTUAL PRIVATE NETWORK* (VPN) SEBAGAI SOLUSI *SECURITY* SELAMA *WORK FROM HOME*

Rino Subekti
Email: rino.subekti@ibi-k57.ac.id
Program Studi Informatika, Fakultas Ilmu Komputer
Institut Bisnis dan Informatika (IBI) Kosgoro 1957

ABSTRAK

Dalam penelitian ini penulis memberikan solusi keamanan dan solusi konektifitas untuk melakukan pekerjaan yang kaitannya dengan kegiatan harian kantor agar dapat dilakukan di rumah ditengah kondisi pandemic Covid 19. Virtual Private Network (VPN) memberikan solusi keamanan dan konektifitas untuk melakukan pekerjaan kantor, walaupu berada di luar kantor aplikasi dan datacenter yang berada dikantor dapat diakses dan data dapat diproses layaknya kita berada dilingkungan kantor.

Kata Kunci: ***Virtual Private Network, Networking, Mikrotik***

I. PENDAHULUAN

Pandemic Covid-19 memberikan dampak secara langsung hampir di seluruh sektor bidang pekerjaan, mengakibatkan banyak orang yang melakukan pekerjaan, kegiatan belajar mengajar, dan lainnya di rumah selama masa Pandemic berlangsung yang dikenal dengan istilah WFH *(Work From Home)* . Pekerjaan atau kegiatan selama masa pandemic dapat dilakukan di rumah karena perkembangan internet saat ini sudah mengalami peningkatan dibandingkan dengan beberapa tahun sebelumnya, kecepatan internet di rumah sudah sampai ada yang 1 Gbps menggunakan media kabel serat kaca atau dikenal dengan istilah FTTH *(fiber to the home),* dengan teknologi selular 4G ada kecepat internet bisa mencapai 512Mbps. Menjadi sebuah tantangan tersendiri ketika semua pekerjaan kantor dapat dilakukaan di rumah, hal ini tentunya dapat dilakukan apabila kantor tersebut sudah memiliki kesiapan internalnya untuk dapat melakukan pekerjaan secara online.

Keamanan, kemudahan dan kecepatan data merupakan faktor yang sangat penting disaat melakukan *"work from home"* sehingga diperlukan tools tambahan untuk menutupi kekurangan tersebut. Jaringan privat yang biasa dikenal dengan Virtual Private Network dan biasa disingkat dengan istilah VPN, merupakan proses dimana jaringan umum atau internet diamankan untuk memfungsikan sebagai jaringan pribadi *(private network)* sehingga perlu diimplementasikan untuk memaksimalkan kerja dan tugas selama masa Pandemi yang setiap harinya dilakukan di rumah.

II. METODE PENELITIAN

2.1. Mikrotik

Jílek & Žalud, (2012) Mikrotik adalah sebuah sistem operasi berbasis unix yang dikembangkan secara komersial dan dirancang khusus sebagai sistem operasi yang fokus kepada perangkat *network* sebagai perangkat komponen jaringan aktif seperti *router, access point, switch router* dan banyak lagi. Sistem operasi ini dikembangkan oleh perusahaan MikroTik yang berpusat di Latvia, diperlukan perangkat keras untuk menjalankan sistem operasi ini yang berupa perangkat komputer dengan cara melakukan instalasi pada komputer yang akan digunakan. Secara khusus sistem operasi ini dibuatkan perangkat kerasnya yang biasa dikenal dengan Mikrotik router board dan saat ini sudah diproduksi secara massal dengan berbagai varian dan serinya mulai dari yang sederhana untuk penggunaan personal sampai penggunaan *entrprise.* (Sofana, 2017) Walaupun Mikrotik ini di bangun dengan kernel linuk akan tetapi pendistribusian sistem operasi ini tidak menyertakan file *sorce code* kepada penggunanya. Karena dirancang khusus untuk mengelola jaringan komputer, perkembangan mikrotik sangat pesat sesuai dengan mottonya yaitu *routing the world* dengan maksud akan menghubungkan

antar dunia dengan mikrotik ini dikarenakan kemudahan dalam penggunaannya untuk membangun sebuah jaringan komputer baik sekala kecil ataupun sekala kompleks.

2.2. Virtual Private Network

Harmening, (2013) Jaringan personal buatan yang biasa dikenal dengan *virtual private network* dan biasanya disingkat dengan VPN adalah jaringan personal yang dibangun seolah olah berada dalam jaringan umum yang dapat digunakan sebagai media komunikasi data dan informasi yang aman. *Secure Sockets Layer* (SSL) *virtual private networks* (VPN) menyediakan akses jarak jauh yang aman ke sumber daya organisasi. Dalam hal keamana jaringan berlapis menyajikan pendekatan bertahap untuk perencanaan dan implementasi VPN yang dapat membantu dalam mencapai penyebaran VPN yang sukses. Ini juga membandingkan teknologi VPN dengan IPsec VPN dan solusi VPN lainnya. Informasi ini sangat berharga untuk membantu organisasi menentukan cara terbaik untuk menyebarkan VPN dalam lingkungan jaringan spesifik mereka. Karena VPN dapat digunakan melalui jaringan yang ada seperti Internet, VPN dapat memfasilitasi transfer data sensitif yang aman di seluruh jaringan publik. Bhiogade, (2002) *Secure Socket Layer* VPN terdiri dari satu atau beberapa perangkat VPN yang terhubung dengan pengguna menggunakan browser Web mereka. Lalu lintas antara browser Web dan perangkat VPN dienkripsi dengan protokol SSL atau penggantinya, protokol Transport Layer Security (TLS). Jenis VPN ini dapat disebut sebagai VPN SSL atau TLS VPN. Bab ini menggunakan istilah SSL VPN. *Secure Socket Layer* VPN memberikan pengguna jarak jauh dengan akses ke aplikasi Web dan aplikasi klien / server, dan konektivitas ke jaringan internal. Terlepas dari popularitas VPN *Secure Socket Layer* , mereka tidak dimaksudkan untuk menggantikan VPN Internet Protocol Security (IPsec). Kedua teknologi VPN tersebut saling melengkapi dan menangani arsitektur jaringan yang terpisah dan kebutuhan bisnis. VPN menawarkan fleksibilitas dan kemudahan penggunaan karena mereka menggunakan protokol *Secure Socket Layer*, yang disertakan dengan semua browser Web standar, sehingga klien biasanya tidak memerlukan konfigurasi oleh pengguna. VPN juga menawarkan kontrol bersamaan untuk pemakaian komputer secara bersamaan, mengakses *server* dari berbagai lokasi.

2.3. IPSec

IPsec adalah kumpulan protokol yang membantu melindungi komunikasi melalui jaringan IP. 14 IPsec protokol bekerja bersama dalam berbagai kombinasi untuk memberikan perlindungan bagi komunikasi. Authentication header (AH)

Bagian ini akan fokus pada tiga komponen utama Enkapsulasi Payload Keamanan (ESP), Otentikasi Protokol Header (AH), dan Internet Key Exchange (IKE) - yang menjelaskan tujuan dan fungsi masing-masing protokol, dan menunjukkan bagaimana mereka bekerja bersama untuk membuat koneksi IPsec. Juga, bagian ini akan membahas nilai menggunakan IP Payload Compression Protocol (IPComp) sebagai bagian dari implementasi IPsec.

2.4. EoIP

Kuswanto, (2017) *Ethernet over internet protokol tunnel atau biasa disingkat dengan (EoIP)* merupakan protokol yang ada pada Mikrotik RouterOs dan berfungsi membangun sebuah pipa penghubungan antar mikrotik Router di atas sebuah koneksi *TCP/IP*. Ada beberapa yang perlu diketahui mengenai EOIP diantaranya:

1) *Eoip* bisa berjalan di berbagai macam jenis koneksi yang mendukung IP
2) Maksimal jumlah *tunnel* yang dapat dibuat oleh *EoIP* adalah 65535 *tunnel.*
3) *Interface EoIP* dapat melakukan *Bridging* dengan *interface EoIP* yang lain.
4) Fungsi utama dari *EoIP* adalah secara transparan dapat melakukan *Bridge* ke *network remote*.
5) Kelemahan dari *EoIP* adalah tidak adanya enkripsi data.

2.5. Studi Literatur

Mempelajari literasi tentang tulisan yang berisi tentang teori dasar *networking* serta teori yang mendukung untuk penelitian ini termasuk mempelajari teori serta konfigurasi dari Routerboard Mikrotik, serta mempelajari pendukung lainnya.

2.6. Analisa dan perancangan sistem

Setelah mempelajari semua teori dan literasi pendukung lainnya, selanjutnya melakukan analisa dan perancangan untuk mendapatkan solusi keamanan dan konektifitas seleama bekerja di rumah. Analisa yang pertama dilakukan ada menentukan segmentasi IP yang akan digunakan, karena pengalamatan IP merupakan hal yang sangat *mandatory* yang akan menetukan berhasil atau tidaknya sebuah topologi *network* .

Tabel 1. Segmentasi IP

NO	AREA	SEGMEN IP
1	Server	192.168.10.x /24
2	User	192.168.1.x /24 – 192.168.5.x /24

2.7. Implementasi

Pada tahap implementasi sudah mulai kemudian dilakukan konfigurasi, pada tahapan ini dilakukan pengaturan konfigurasi *EoIP tunnel* pada router dimana semua aplikasi dan server berada sebagai jalur penghubung antar server aplikasi dengan analisis dan perancangan sistem. Pada tahap implementasi ini langkah-langkah yang dilakukan adalah sebagai berikut:

1) Konfigurasi *Eoip Tunnel*.
2) Konfigurasi *IP address interface EoIP*.
3) Konfigurasi *routing statik* pada Router.
4) Konfigurasi VPN akses untuk user

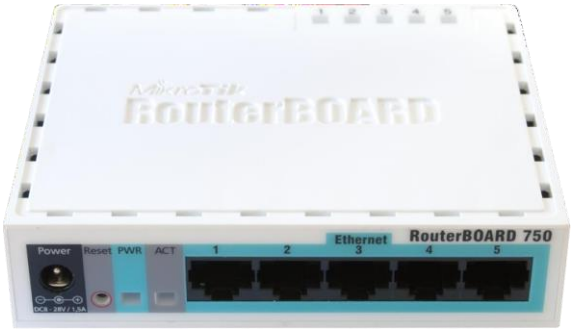
2.8. Pengujian

Syamsu, (2010) Setelah semua tahapan sudah dilakukan selanjutnya ada melakukan pengujian terhadap apa yang sudah di analisa dan implementasi, pada tahapan pengujian kita bisa ketahui apakah semua rancangan dan implementasi berjalan dengan baik atau berjalan dengan kendala atau bahkan mengalami kendala sehingga pada tahapan ini evaluasi selanjutnya dapat dilakukan agar tidak terjadi kesalah yang berulang, pengujian yang dilakukan diantaranya sebagai berikut:

1) Pengaturan konfigurasi *interface EoIP Tunnel* pada router
2) Melakukan tes *ping* dari PC router, router ke PC
3) Melakukan teng ping dari PC ke server aplikasi, server aplikasi ke PC
4) Melakukan remote desktop dari PC ke server

III. HASIL DAN PEMBAHASAN

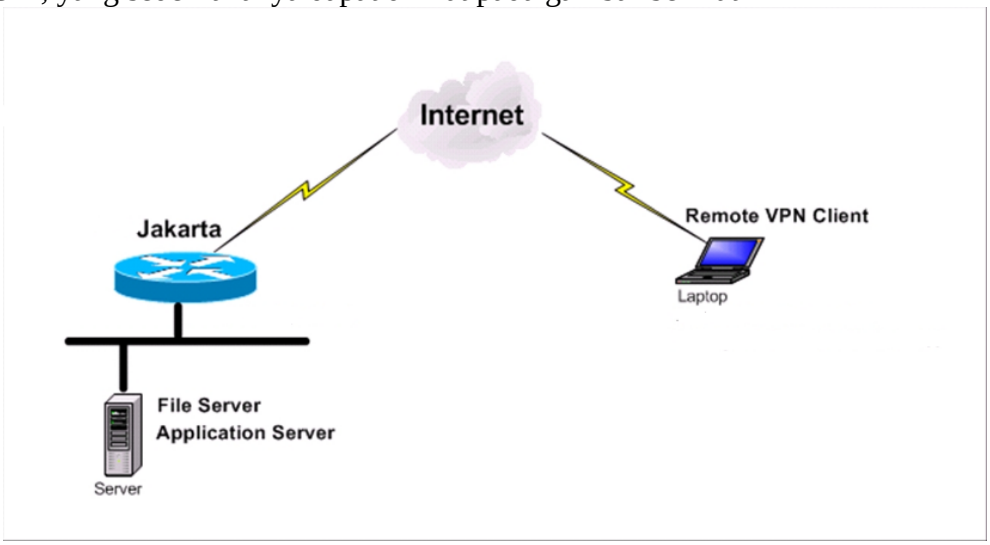
Sofana, (2017) Pada bab ini akan di jelaskan langkah-langkah implementasi VPN ke dalam jaringan komputer/laptop kantor, dan akan disertakan juga beberapa *screenshots* dari konfigurasi *remote access* VPN dengan aplikasi winbox. *Router* yang digunakan adalah *Router* seri RB951ui.



Gambar 1. Gambar Topologi Jaringan

3.1. Rancangan Topologi

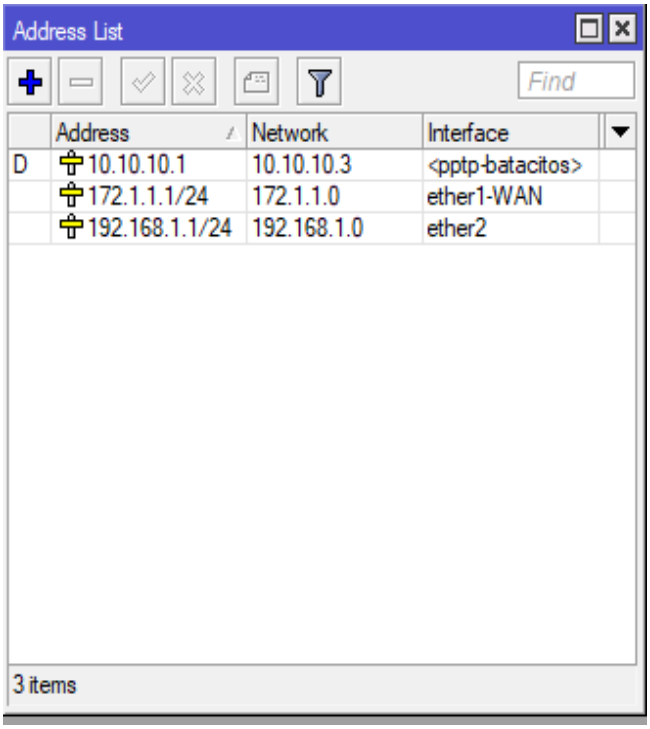
Topologi yang digunakan dalam implementasi ini jaringan VPN ini adalah menggunakan protokol EOIP, yang sederhananya dapat dilihat pada gambar berikut ini



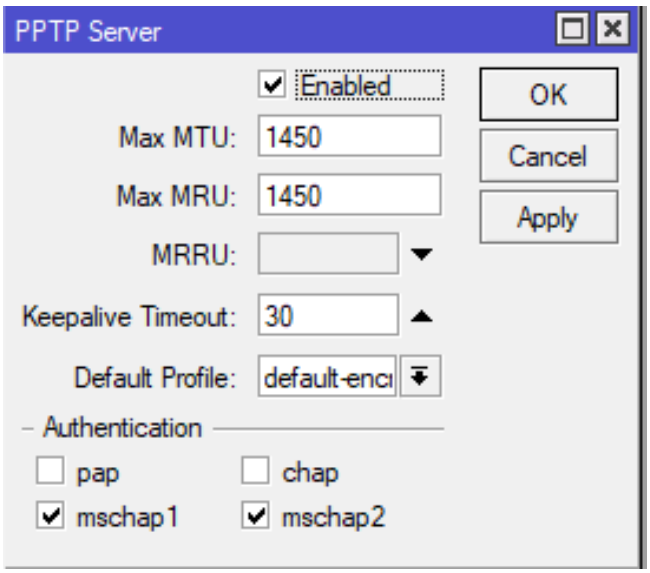
Gambar 2. Gambar Topologi Jaringan

Konfigurasi *Router R1*

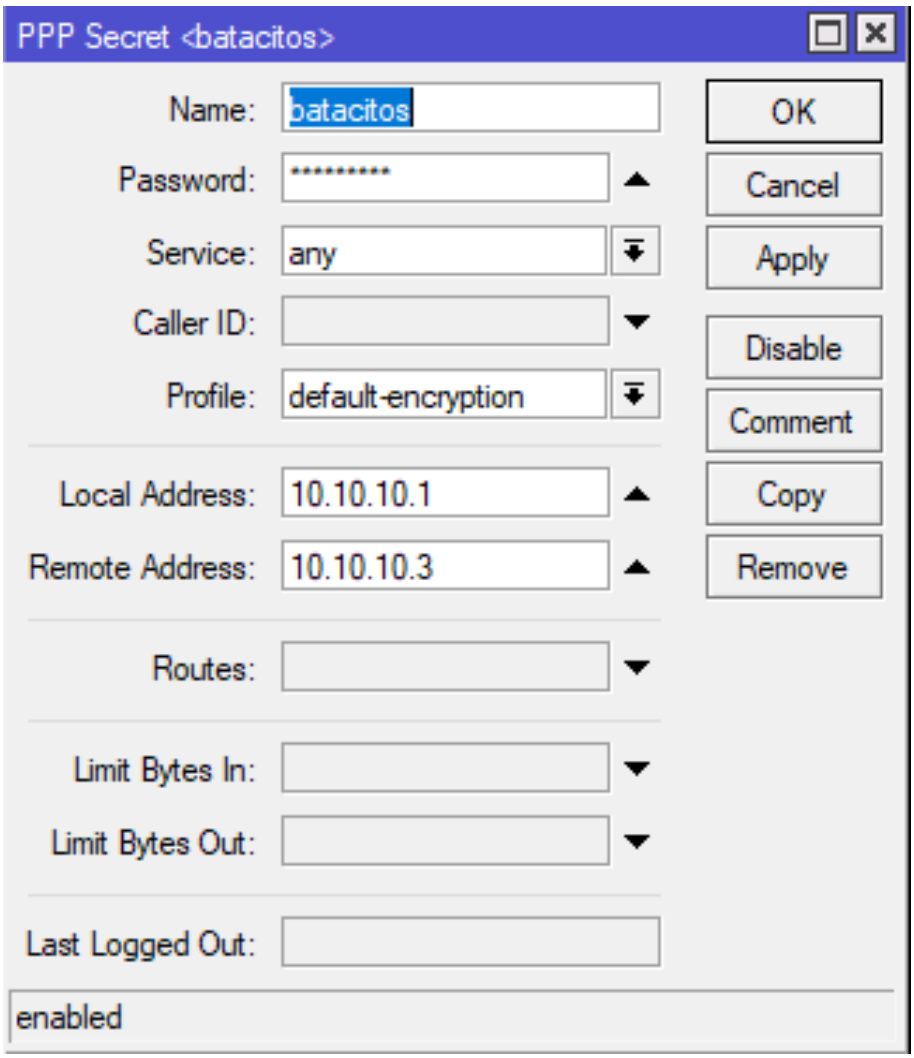
1) Konfigurasi *EoIP tunnel* /interface eoip> add name=eoip-to-router-R2 remote-address=119.252.164.166 tunnel-id=109
2) Konfigurasi *ip address interface EoIP* /ip address> add address=172.13.13.1/30 interface=eoip-torouter-R2
3) Konfigurasi *statik routing* /ip route> Add dst-address=10.10.10.0/26 gateway=172.13.13.2 check gateway=ping distance=1



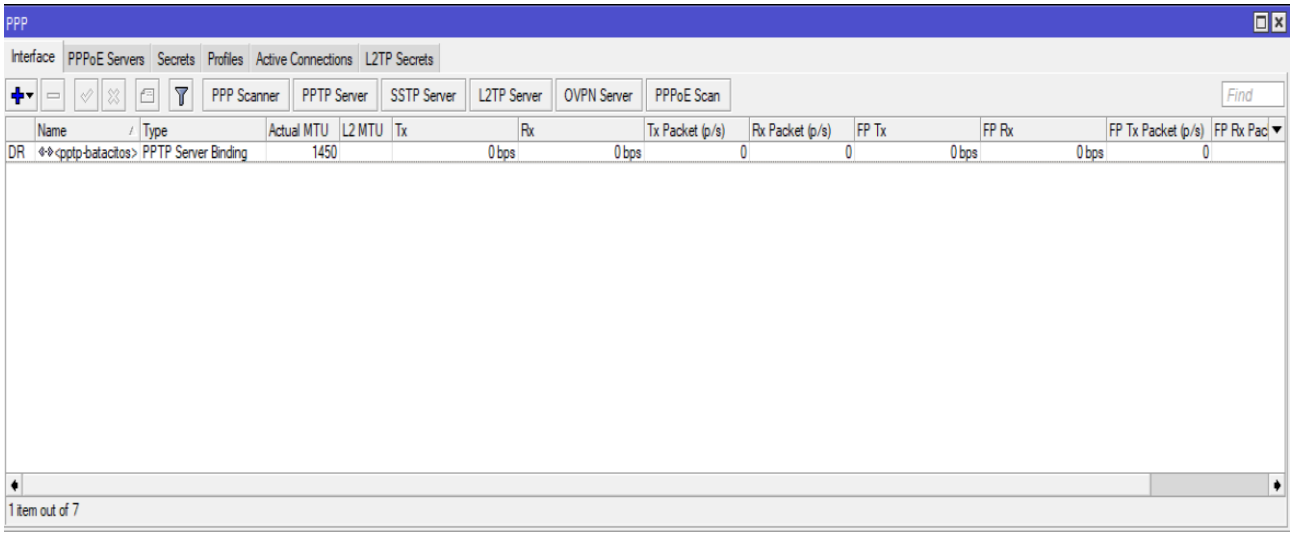
Gambar 3. Gambar Konfigurasi Router



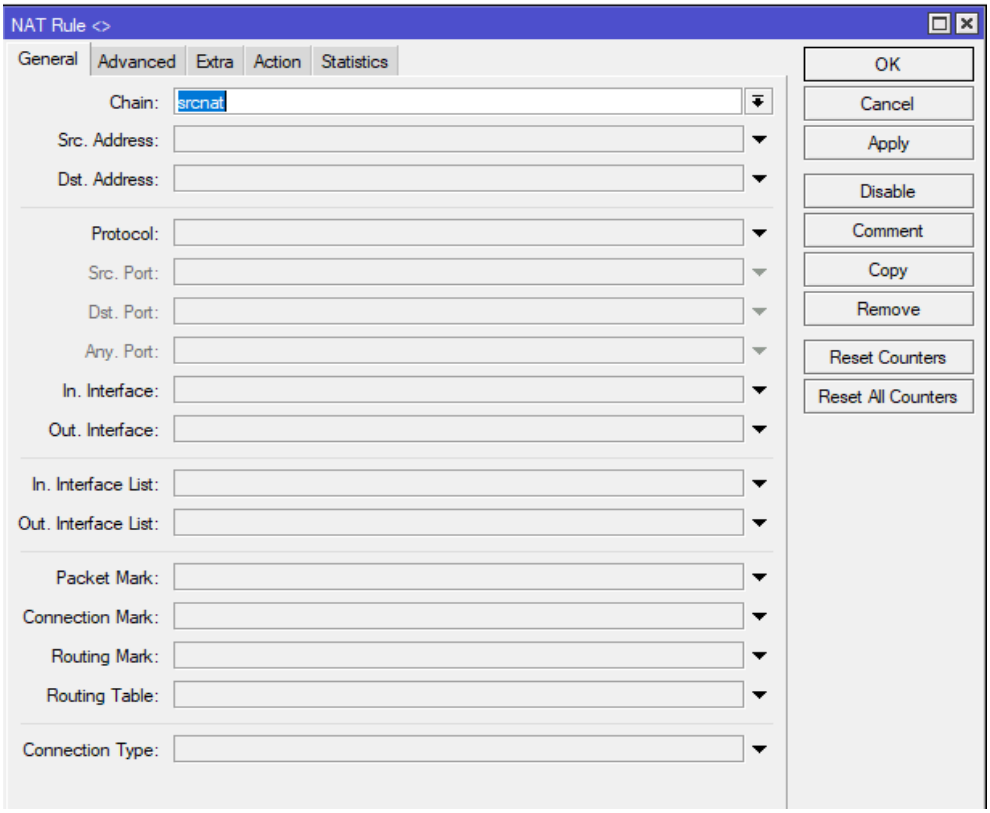
Gambar 4. Gambar Setting PPTP Server



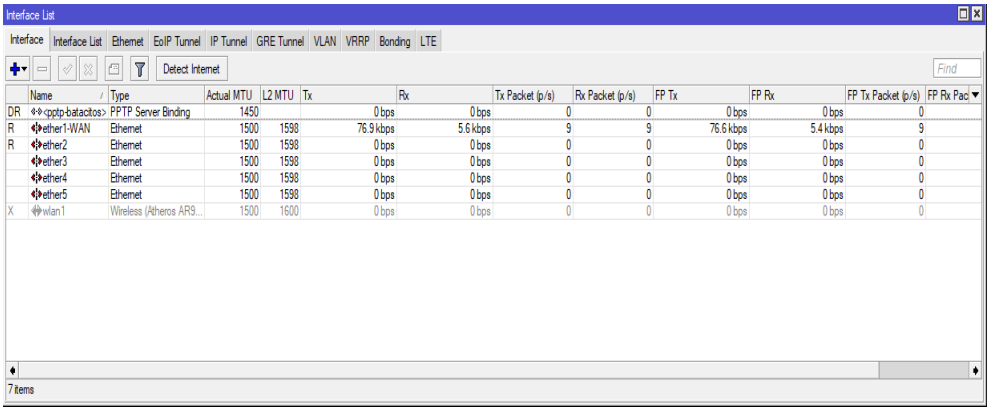
Gambar 5. Gambar PP Secret



Gambar 6. Gambar PP Interface



Gambar 7. Gambar NAT Rule



Gambar 8. Gambar Interface List

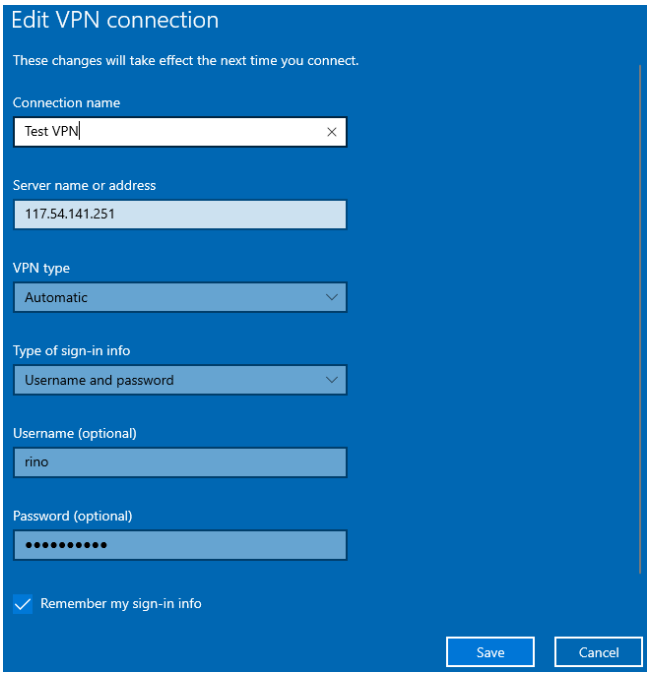
3.2. Hasil Pengujian

Setelah selesai melakukan konfigurasi disisi router kemudian dilakukan pengujian disisi router yang melakukan tes koneksi terlebih dahulu

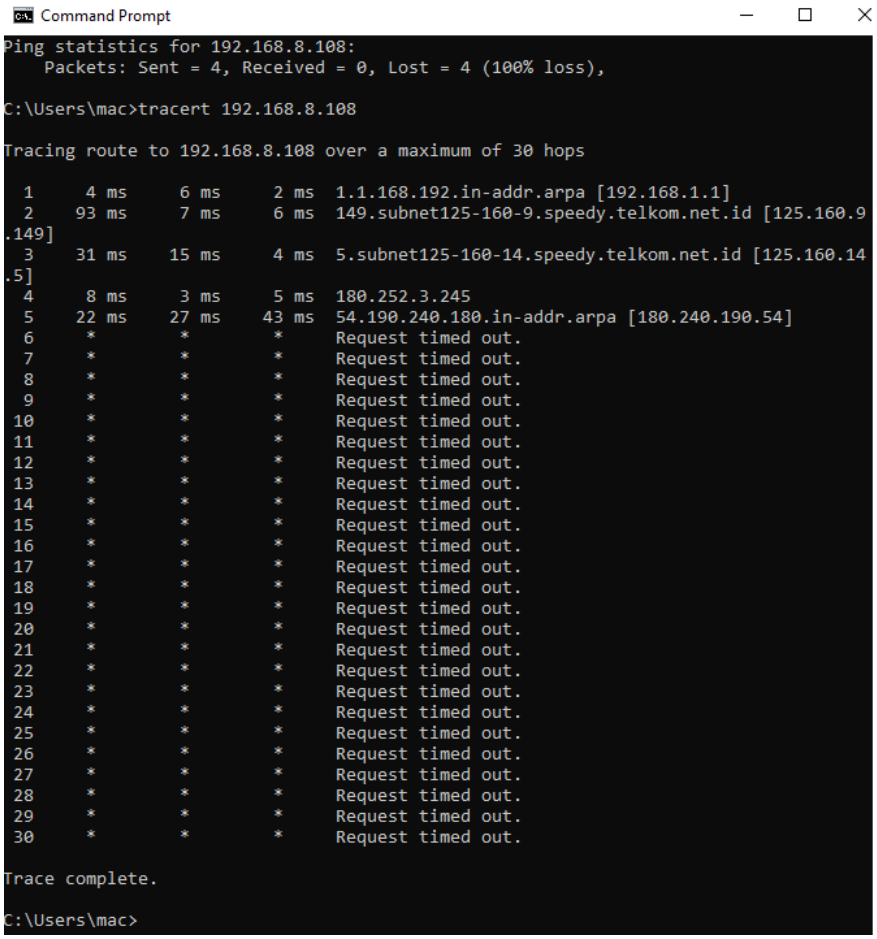
```
[admin@BataCitos] > ping 172.1.1.1
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 172.1.1.1                                  56  64 0ms
    1 172.1.1.1                                  56  64 0ms
    2 172.1.1.1                                  56  64 0ms
    sent=3 received=3 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms

[admin@BataCitos] > ping 192.168.1.1
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 192.168.1.1                                56  64 0ms
    1 192.168.1.1                                56  64 0ms
    2 192.168.1.1                                56  64 0ms
    3 192.168.1.1                                56  64 0ms
    4 192.168.1.1                                56  64 0ms
    5 192.168.1.1                                56  64 0ms
    6 192.168.1.1                                56  64 0ms
    sent=7 received=7 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms

[admin@BataCitos] > ping 192.168.1.2
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 192.168.1.2                                56  64 0ms
    1 192.168.1.2                                56  64 0ms
    2 192.168.1.2                                56  64 0ms
    sent=3 received=3 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms

[admin@BataCitos] >
```

Gambar 9. Gambar Test Uji Koneksi Di Server

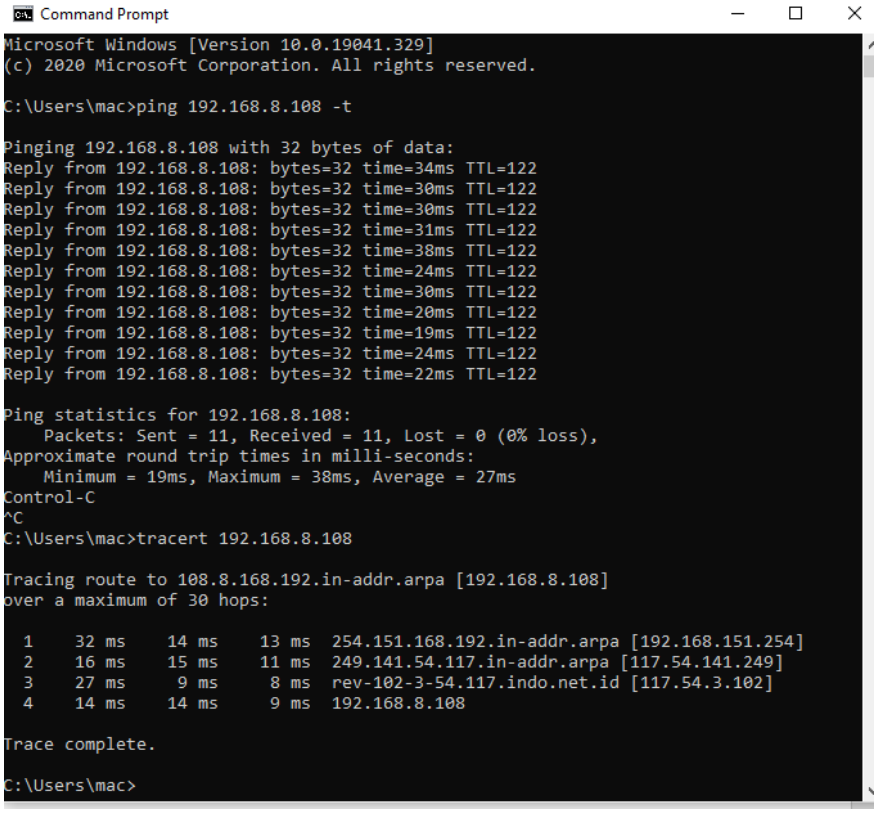
Setelah selesai disisi router kemudian konfigurasi dan pengujian juga dilakukan disisi Komputer yang akan melakukan akses ke servernya. Pada saat penelitian ini dilakukan menggunakan Windows 10 dengan tampilan sebagai berikut:



Gambar 10. Gambar konfigurasi VPN Windows 10



Gambar 11. Gambar Ping Test Sebelum VPN Diaktifkan



Gambar 12. Gambar Ping Test Dan Trace Route Setelah VPN Diaktifkan

Setlah dilakukan pengujian, walaupun kita berada di rumah kita dapat mengakses sumber daya server yang berada di kantor seolah-olah kita berada dilingkungan network kantor, aplikasi berbasis web yang diaksesnya menggunakan Private IP dapat dibuka dari luar lingkungan kantor, sehingga walaupun karyawan berada di luar lingkungan kantor karyawan dapat melakukan pekerjaan layaknya berada di kantor .

IV. KESIMPULAN

Dengan bermodalkan router mikrotik tidak terlalu mahal di pasaran, menggunakan protokol *EoIP Tunel*, perusahaan yang sudah mempunyai koneksi internet, selain mendapatkan *bandwidth* internet, dapat juga memanfaatkan jaringan publik atau internetnya sebagai penghubung jalur private atau biasa dikenal dengan intranet, sehingga seolah-olah antara kantor karyawan yang berada di rumah terhubung dalam satu segmen jaringan intranet, walaupun dalam aspek keamanan *EoIP* tidak memberlakukan enkripsi seperti *VPN-IP*, namun administrator dapat mengaktifkan fungsi *firewal* atau *filtering* dan *monitoring* pada *interface EoIP*nya. Penerapan Implementasi *Virtual Private Network* seperti ini sangat berguna bagi perusahaan yang ingin menerapkan *Work From Home* untuk karyawannya dengan biaya relatif lebih murah, dibandingkan dengan biaya sewa layanan *VPN-IP* dari ISP.

DAFTAR PUSTAKA

Bhiogade, M. (2002). Secure Socket Layer. *Proceedings of the 2002 InSITE Conference, June*. https://doi.org/10.28945/2441

Harmening, J. T. (2013). Virtual Private Networks. In *Computer and Information Security Handbook*. https://doi.org/10.1016/B978-0-12-394397-2.00048-9

Jílek, T., & Žalud, L. (2012). Security of remote management of embedded systems running MikroTik RouterOS operating system using proprietary protocols. *IFAC Proceedings Volumes (IFAC-PapersOnline)*, *11*(PART 1), 169–173. https://doi.org/10.3182/20120523-3-cz-3015.00034

Kuswanto, H. (2017). Implementasi Jaringan Virtual Private Network (VPN) Menggunakan Protokol EoIP. *Paradigma*.

Sofana, I. (2017). Jaringan Komputer Berbasis MikroTik. In *Jaringan Komputer*.

Syamsu, S. (2010). Konsep Routing. *Modul Jaringan Komputer - STMIK AKBA*.