

PERANCANGAN JARINGAN VPN MENGGUNAKAN MIKROTIK DENGAN METODE L2TP/IPSec

Taufiqurrochman¹⁾, Satrio Broto²⁾, Armin³⁾

¹Prodi Sistem Informasi, Fakultas Teknologi, ITB Swadharma Jakarta

^{2,3}Prodi Teknik Informatika, Fakultas Teknologi, ITB Swadharma Jakarta

Correspondence author: Taufiqurrochman, taufiqurrohman@swadharma.ac.id, Jakarta, Indonesia

Abstract

Currently, computer networks are essential in supporting communication in the company. There are many advantages of using computer networks, for example, communication between clients becomes easier and faster, remote servers through computer networks and client-server applications within the company. Computer network security is very important for the efficiency and effectiveness of computer network performance. Reliable infrastructure in a computer network is very influential for its performance. PT. Megacom company in the field of computer spare part distributor. The problem faced is the absence of good and secure communication technology between the head office, branch offices, and distributors. The purpose of this study is to design a Wide Area Network network between the head office and branch offices of PT. Megacom. This study uses qualitative methods with observation and interview data collection techniques. The results of the study show that in the traceroute experiment during the network test from the head office to the branch, the packet path goes well through the tunnel with fast and secure data access through a VPN network with the designed L2TP/IPSec method.

Keywords: computer network, vpn, L2TP/IPSec, mikrotik

Abstrak

Saat ini jaringan komputer sangatlah penting dalam menunjang komunikasi di perusahaan. Banyak keuntungan dari penggunaan jaringan komputer, misalnya komunikasi antar klien menjadi lebih mudah dan cepat, remote server melalui jaringan komputer dan aplikasi klient-server di dalam perusahaan. Keamanan jaringan komputer sangat penting untuk efisiensi dan efektifitas kinerja jaringan komputer. Infrastruktur yang handal dalam jaringan komputer sangat berpengaruh untuk performanya. PT. Megacom perusahaan di bidang distributor spare part Komputer. Masalah yang dihadapi belum adanya teknologi komunikasi yang baik dan aman, antara kantor pusat, kantor cabang dan distributor. Tujuan dari penelitian ini merancang jaringan Wide Area Network antara kantor pusat dan kantor cabang PT. Megacom. Penelitian ini menggunakan metode kualitatif dengan Teknik pengumpulan data observasi dan wawancara. Hasil penelitian menunjukkan bahwa percobaan traceroute pada saat uji jaringan dari kantor pusat ke cabang, jalur paket berjalan dengan baik melewati tunnel dengan akses data

yang cepat dan aman melalui jaringan VPN dengan metode L2TP/IPSec yang dirancang.

Kata Kunci: jaringan komputer, vpn, L2TP/IPSec, mikrotik

A. PENDAHULUAN

VPN merupakan singkatan dari *Virtual Private Network* yang artinya membuat jaringan *private* secara virtual di atas jaringan publik seperti internet (Satryawati et al., 2022). Saat ini jaringan komputer sangatlah penting dalam menunjang komunikasi khususnya di perusahaan. Banyak keuntungan yang dapat diperoleh dari penggunaan jaringan komputer, misalnya komunikasi antar klien menjadi lebih mudah dan cepat, remote server melalui jaringan komputer atau juga untuk aplikasi klient-server di dalam perusahaan (Rahman et al., 2020). Banyak sekali manfaat dari hal di atas, tetapi ada satu hal yang tidak boleh dilupakan yaitu Keamanan. Keamanan jaringan komputer sangat penting untuk efisiensi dan efektifitas kinerja dari suatu jaringan komputer (Komariah, 2016; Suhanda et al., 2022).

Penggunaan infrastruktur yang handal dalam jaringan komputer sangat berpengaruh untuk mendukung kinerja atau performanya. Router adalah suatu perangkat jaringan yang digunakan untuk menjembatani antara dua atau lebih jaringan yang berbeda. Selain untuk menjembatani suatu jaringan, Router juga dapat digunakan untuk mengelola lalu lintas jaringan. Router yang digunakan untuk implementasi ini adalah Mikrotik yang mempunyai sistem operasi Mikrotik Router OS (Hasrul & Lawani, 2017). Mikrotik adalah sebuah merek dari sebuah perangkat jaringan, pada awalnya MikroTik hanyalah sebuah perangkat lunak atau software yang di-instal dalam komputer yang digunakan untuk mengontrol jaringan, tetapi dalam perkembangannya saat ini telah menjadi sebuah device atau perangkat jaringan yang andal dan harga yang terjangkau, serta

banyak digunakan pada level perusahaan penyedia jasa internet (ISP).

PT. Megacom merupakan perusahaan yang bergerak di bidang distributor spare part Komputer dan telah bekerja sama dengan beberapa distributor lain. Masalah yang dihadapi adalah belum adanya teknologi komunikasi yang baik dan aman yang terhubung antara kantor pusat, kantor cabang dan distributor yang bekerja sama dengan PT. Megacom dan juga menerapkan mobile user dimana setiap direktur atau manager bisa mengakses aplikasi dari luar dengan aman.

Perusahaan menggunakan internet sebagai media penyalur data dan pendukung kegiatan karyawan dalam berkomunikasi. Hal ini memungkinkan karyawan dapat mengakses data perusahaan dari jarak jauh yang tentunya juga harus didukung dengan infrastruktur jaringan komputer yang baik. Oleh karena itu, dibutuhkan jaringan *Local Area Network* komputer yang cepat, handal dan aman untuk mendukung kegiatan perusahaan.

Local Area Network (LAN) merupakan jaringan private untuk komputer dalam satu bangunan atau kampus sampai jarak beberapa kilometer (Wirastuti et al., 2016). Dua komputer yang terhubung juga sudah merupakan LAN. Jaringan LAN biasanya mencakup gedung, kampus, atau kantor. *Wide Area Network* (WAN) merupakan jaringan komputer yang dapat menjangkau area yang lebih luas dari jaringan LAN (Khasanah, 2014). WAN digunakan untuk menghubungkan jaringan lokal yang satu dengan jaringan lokal yang lain, sehingga pengguna atau komputer di lokasi yang satu dapat berkomunikasi dengan pengguna dan komputer di lokasi yang lain

Keamanan jaringan komunikasi data antar komputer akan menjadi suatu masalah kritis dalam suatu perusahaan. Kerahasiaan

data yang akan dikirim atau diterima dari pusat atau cabang tidak selalu terjamin keamanannya walaupun sudah terdapat sistem autentikasi yang diberikan oleh provider. Dengan alasan tersebut, sekarang ini ada teknologi dalam dunia jaringan komputer bernama *Virtual Private Network* (Sari et al., 2020).

VPN merupakan suatu bentuk *private internet* yang melalui *public network* (internet), dengan menekankan pada keamanan data dan akses global melalui internet. Hubungan ini dibangun melalui suatu *tunnel* virtual antara 2 node. VPN juga merupakan suatu jaringan private (biasanya untuk instansi atau kelompok tertentu) di dalam jaringan internet (publik), dimana jaringan private ini seolah-olah sedang mengakses jaringan lokalnya tapi menggunakan jaringan publik.

VPN ini merupakan suatu jaringan komunikasi lokal yang menumpang dalam jaringan publik. Dengan VPN, keamanan jaringan akan lebih mudah diatur dan dikontrol. VPN Layer 2 Tunnel Protocol L2TP merupakan pengembangan dari PPTP ditambah L2F (Basri et al., 2017; Maulana & Qomaruddin, 2022). *Network security Protocol* dan enkripsi yang digunakan untuk autentikasi sama dengan PPTP. L2TP merupakan protocol yang tinggi dengan standar dalam IETF RFC 3193 (Sari et al., 2020). L2TP biasanya digunakan dalam membuat *Virtual Private Dial Network* (VPDN) yang dapat bekerja membawa semua jenis protokol komunikasi didalamnya (Febrianto, 2022). L2TP memungkinkan penggunaannya untuk tetap dapat terkoneksi dengan jaringan lokal milik mereka dengan policy keamanan yang sama dan dari manapun mereka berada, melalui koneksi VPN atau VPDN (Rahino & Susila, 2022). Koneksi ini sering kali dianggap sebagai sarana memperpanjang jaringan lokal milik penggunaannya, namun melalui media publik.

Dengan melihat latar belakang yang sudah dipaparkan di atas, maka yang menjadi permasalahan dalam penelitian ini,

Bagaimana merancang Jaringan VPN L2TP Mikrotik pada Jaringan di PT. Megacom. Tujuan dari penelitian ini merancang dan mengusulkan jaringan usulan untuk memperbaiki jaringan *Wide Area Network* yang mampu menghubungkan kantor-kantor diseluruh nusantara bahkan dunia dalam sebuah jaringan yang handal.

B. METODE PENELITIAN

Metode penelitian merupakan suatu cara untuk dapat memahami suatu pembahasan, permasalahan, dan pemecahan masalah dalam sebuah sistem. Penelitian ini menggunakan metode kualitatif dengan Teknik pengumpulan data Observasi dan wawancara.

Metode pengumpulan data untuk memperoleh data yang dibutuhkan, dilakukan peninjauan langsung dan melakukan observasi dan mengamati khususnya pada bagian jaringan Local Area Network (LAN) dan Wide Area Network (WAN) di PT. Megacom. Selain observasi dilakukan juga pengumpulan data dan informasi dengan cara melakukan tanya jawab secara langsung dan sistematis, dan penulis melakukan wawancara secara langsung kepada kepala IT dan kepada karyawan yang memakai jaringan komputer di perusahaan.

Untuk menelaah masalah secara mendalam yang berkaitan dengan penelitian ini, maka penulis mencoba melakukan studi kepustakaan yaitu dengan mengumpulkan data-data teoritis dan mempelajari buku-buku atau literature dengan maksud untuk mendapatkan teori-teori dan bahan-bahan yang berkaitan dengan masalah tersebut diatas.

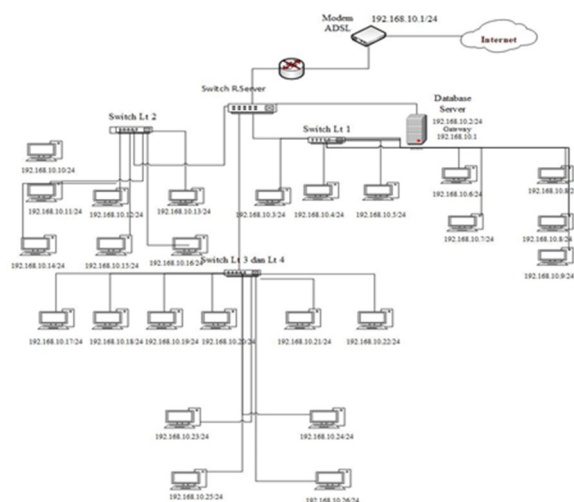
C. HASIL DAN PEMBAHASAN

Topologi yang sedang berjalan di PT. Megacom menggunakan topologi star dimana setiap komputer langsung terhubung ke *switch* dan saling terhubung ke komputer lain. Topologi jaringan disini hanya mencakup

satu area gedung dan belum mencakup mencakup kantor cabang. Arsitektur jaringan yang sedang berjalan menggunakan model OSI (*Open System Interconnection*). Untuk IP address disetting secara static menggunakan kelas C dengan network ID 192.168.0.0/24. Tujuan digunakannya IP *address static* pada jaringan ini adalah untuk mempermudah dalam hal monitoring dan *troubleshooting* apabila terjadi masalah jaringan pada PC klient. Alokasi *bandwidth* saat ini 20 Mbps, dan sudah dilakukan sistem manajemen *bandwidth* sehingga lalu lintas jaringan stabil.

Sistem keamanan jaringan, belum diterapkan secara maksimal, hanya mengandalkan sistem keamanan yang terdapat pada fitur sistem operasi Windows yaitu fitur *firewall* yang terdapat didalamnya dan *software* anti virus. Untuk keamanan pada router menerapkan fitur *firewall*.

Pada gambar 1 dapat dilihat skema jaringan komputer terdiri dari router, modem, switch, server, access point dan klient. Untuk router menggunakan Router OS Mikrotik, kemudian ada beberapa server yang digunakan untuk keperluan perusahaan. Yaitu File server digunakan untuk menyimpan data-data penting perusahaan dan backup email klient, Database server merupakan program komputer yang menyediakan layanan data lainnya ke komputer atau program komputer, dan web server.



Gambar 1. Topologi Jaringan PT. Megacom

ISP (*Internet Service Provider*) menggunakan indihome dengan alokasi *bandwidth* sekitar 20 Mbps, kemudian router mikrotik difungsikan untuk manajemen *bandwidth*, proxy dan gateway.

Spesifikasi Perangkat Yang Digunakan

Server digunakan untuk menjalankan aplikasi Network Monitoring System (NMS) Cacti, fungsinya adalah untuk melakukan monitoring terhadap semua perangkat.

Modem (*Modulator Demodulator*) merupakan sebuah perangkat keras yang berfungsi untuk komunikasi dua arah yang dapat mengubah sinyal digital menjadi sinyal analog atau sebaliknya. Bisa juga diartikan sebagai perantara untuk menghubungkan komputer ke jaringan internet. Modem yang digunakan di PT. Megacom merupakan modem tipe ONT (*Optical Network Terminal*), yaitu jenis modem yang dipakai pada jaringan yang menerapkan teknologi GPON (*Gigabit-Capable Passive Optical Network*).

Switch merupakan perangkat jaringan yang berada pada layer 2 di dalam susunan OSI Layer, fungsi *switch* yaitu sebagai *center point* untuk menghubungkan semua *host* yang ada pada jaringan.

Analisis Kebutuhan Jaringan

Berdasarkan hasil observasi dan analisis yang dilakukan pada PT. Megacom, disimpulkan kebutuhan jaringan sebagai berikut: Diperlukan sebuah perangkat switch yang memiliki 24 port Gigabit Ethernet agar dapat meng-handle traffic antar LAN yang sangat besar, ini dikarenakan user menggunakan file sharing untuk berbagi file dengan user lainnya, penggunaan switch dengan interface gigabit dipilih agar proses pertukaran data yang berukuran besar dapat dikirimkan dengan sangat cepat tanpa harus memakan waktu yang lama.

Diperlukan penggantian NIC (LAN Card) untuk masing-masing komputer klient yang masih menggunakan Fast Ethernet NIC dengan Gigabit Ethernet NIC.

Permasalahan Jaringan

Berdasarkan hasil analisa dan penelitian yang telah dilakukan pada sistem jaringan komputer PT. Megacom, terdapat permasalahan diantaranya adalah belum menerapkan sistem keamanan untuk saling tukar data antara kantor pusat dan kantor cabang. Belum menerapkan sistem remote access untuk memonitoring jaringan dan mengakses jaringan dari luar kantor. Kendala dalam pengiriman email baik berupa foto, file dan video antara kantor pusat dan cabang, jika terdapat data dengan ukuran besar. Beberapa komputer (PC) user belum dilengkapi dengan NIC Gigabit-Ethernet sehingga proses pertukaran data antar user belum maksimal.

Berikut analisis permasalahan menggunakan analisis SWOT (*Strength, Weakness, Opportunities, Threats*) untuk mengetahui permasalahan pada jaringan yang sedang berjalan di PT. Megacom

Strength (Kekuatan)

1. Memiliki alokasi bandwidth yang cukup besar.
2. Memiliki perangkat jaringan yang mendukung

Weakness (Kelemahan)

1. Belum menerapkan sistem keamanan untuk saling tukar data antara kantor pusat dan kantor cabang.
2. Belum menerapkan sistem remote access untuk memonitoring jaringan dan mengakses jaringan dari luar kantor.

Opportunities (Peluang)

1. Tersedia banyak pilihan perangkat yang dapat digunakan sebagai router.
2. Banyak metode yang dapat digunakan untuk metode remote access untuk saling tukar data antar cabang

Threats (Ancaman)

Adanya kesulitan untuk menghubungkan jaringan kantor pusat dan kantor cabang.

Strategi S-O

Menerapkan konfigurasi L2TP agar bisa bertukar data antara kantor pusat dan cabang.

Menerapkan Konfigurasi IPsec agar pertukaran data kantor pusat dan kantor cabang lebih aman.

Strategi W-O

Menggunakan perangkat mikrotik untuk digunakan sebagai konfigurasi L2TP dan IPsec untuk keamanan pada saat pengiriman data.

Menggunakan switch dengan port gigabit + NIC gigabit pada setiap PC user agar proses sharing file antar LAN dapat lebih maksimal.

Strategi S-T

Menggunakan perangkat Router mikrotik untuk membangun jaringan L2TP dan IPSec. Memiliki alokasi bandwidth yang cukup besar bisa lebih cepat pertukaran data.

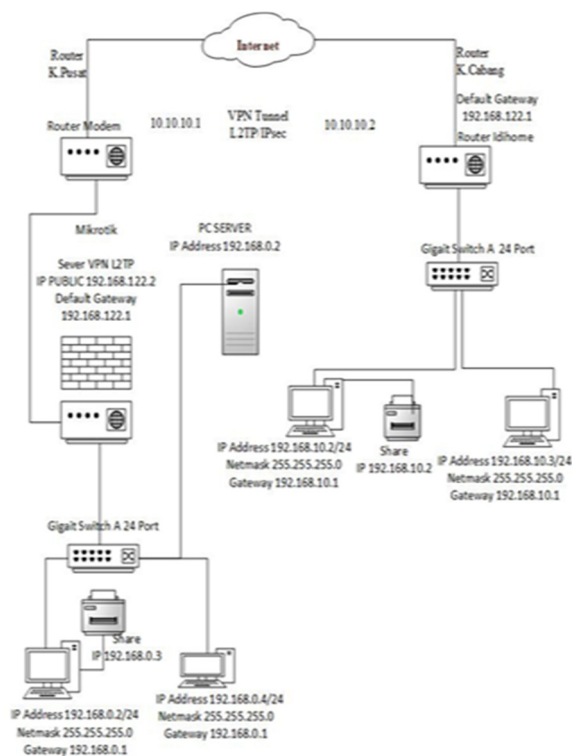
Strategi W-T

Menggunakan router mikrotik agar bisa diatur IPsec untuk keamanan jaringan sehingga paket data yang dikirim lebih aman. Menggunakan kabel fiber optic dan kabel belden untuk jaringan lebih stabil.

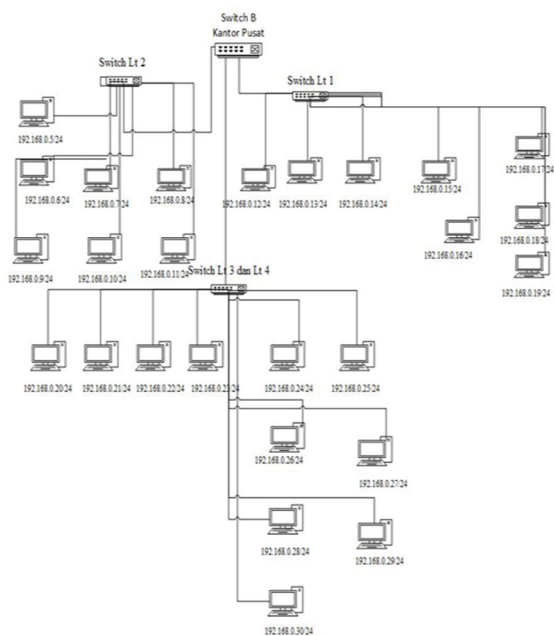
Topologi Jaringan Usulan

Topologi jaringan yang diusulkan menggunakan VPN (*Virtual Private Network*) dengan metode L2TP untuk menghubungkan kantor pusat dengan cabang. Menggunakan router Mikrotik yang sudah ada, kemudian dikonfigurasi untuk menerapkan sistem jaringan VPN. Untuk kantor pusat dikonfigurasi VPN server dengan metode L2TP, sedangkan kantor cabang L2TP Klient.

Berikut adalah desain topologi jaringan usulan yang dapat diterapkan:



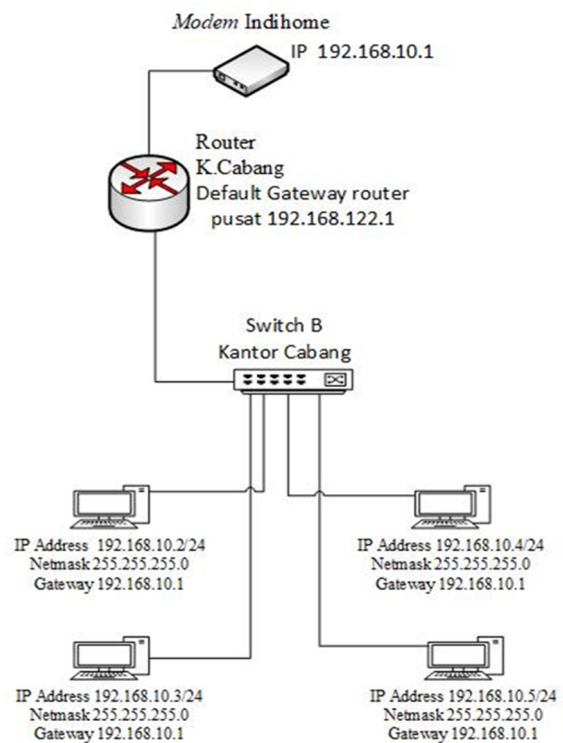
Gambar 2. Topologi Jaringan VPN Kantor Pusat dan Kantor Cabang yang dirancang.



Gambar 3. Topologi Jaringan Local (LAN) Kantor pusat

Dari rancangan desain topologi jaringan komputer pada gambar 2, menggunakan 2 buah router Mikrotik sebagai router kantor

pusat dan router kantor cabang, yang terhubung dengan jaringan Internet (ISP) dengan dua jalur berbeda antara kantor pusat dengan kantor cabang. Kedua router (kantor pusat dan kantor cabang) memiliki masing-masing IP address LAN lokal (private), dimana setiap IP Address lokal setiap kantor cabang berbeda network dengan IP address kantor pusat.



Gambar 4. Topologi Jaringan Local (LAN) Kantor Cabang

Perancangan Konfigurasi fitur VPN site-to-site.

Konfigurasi VPN site-to-site berbasis L2TP dan IPsec pada router kantor pusat dan kantor cabang adalah tahap dimana dilakukannya pengaturan-pengaturan parameter yang terdapat pada sebuah perangkat lunak

Adapun parameter-parameter yang akan kita setting pada komputer server, router dan klient adalah :

Konfigurasi router Kantor Pusat

1. Tahap konfigurasi router mikrotik Mulai Connect To = Ip address router kantor pusat, Login = admin, Password = Silahkan di kosongkan Kemudian Klik “Connect” setelah masuk ke gui nya mikrotik pertama-tama kita akan mulai dengan merubah nama interface pada router dengan nama interface kantor pusat, agar tidak menyulitkan pada saat konfigurasi.
2. Konfigurasi IP Address Selanjutnya memberi IP pada setiap Ethernet. Klik IP > address > “+” Address : 192.168.22.2/30 Network : (Di kosongkan) Interface : ether2 Kemudian klik “OK”
3. Konfigurasi DNS pada tahap ini DNS ini biasanya sudah diberikan juga bersamaan dengan IP Public, jika memiliki IP DNS, maka masukkan pada DNS tersebut. Jika tidak memiliki IP DNS maka kita akan menggunakan IP DNS Google disini menggunakan IP DNS Google yaitu: 8.8.8.8
4. Konfigurasi firewall NAT Membuat NAT=MASQUERADE yang digunakan agar IP LOCAL atau area local dapat terhubung internet. Dengan cara Klik IP > FIREWALL > NAT > + Tab general. Chain= srcnat, Out-interface= ether2, Tab action. Action=Masquerade kemudian klik OK
5. Konfigurasi L2TP Server konfigurasi untuk L2TP Server. Untuk mengaktifkan router sebagai L2TP server Pada menu PPP -> Pilih L2TP Server. Kemudian centang opsi 'Enabled'. Dengan otomatis L2TP Server aktif.
6. Konfigurasi Routing untuk menghubungkan segmen-segmen jaringan untuk bisa melakukan packet forwarding. Sedangkan packet forwarding adalah proses memancarkan atau menyiarkan jaringan ke segmen-segmen jaringan komputer.
ip address add address=192.168.122.2 /24 interface=ether1 Jaringan Public
ip address add address=192.168.0.0 /24 interface=ether2 Jaringan Local

```
iproute add dst-address=192.168.122.3/24 gateway=192.168.122.2
```

7. Konfigurasi IPsec Untuk menambah tingkat keamanan kita akan memadukan L2TP dengan IPsec. Pilih pada menu IP > IPsec. Kemudian kita akan melakukan setting terlebih dahulu pada tab 'IPsec Proposal'. Selanjutnya kita melakukan setting pada Tab 'IPsec Policy'. Setelah konfigurasi pada Tab 'IPsec Proposal' dan 'IPsec Policy' telah dilakukan, kita akan melanjutkan konfigurasinya pada Tab 'IPsec Peer'.
8. Tahap pengetesan ping antar perangkat router.

Konfigurasi router VPN klien kantor cabang

1. Tahap konfigurasi router mikrotik Mulai Connect To = Ip address router kantor cabang, Login = admin, Password = Silahkan di kosongkan Kemudian Klik “Connect” setelah masuk ke gui nya mikrotik pertama-tama kita akan mulai dengan merubah nama interface pada router dengan nama interface kantor cabang, agar tidak menyulitkan pada saat konfigurasi.
2. Konfigurasi IP Address Selanjutnya memberi IP pada setiap Ethernet. Klik IP > address > “+” Address : 192.168.22.3/30 Network : (Di kosongkan) Interface : ether2 Kemudian klik “OK”
3. Konfigurasi DNS pada tahap ini DNS ini biasanya sudah diberikan juga bersamaan dengan IP Public, jika memiliki IP DNS, maka masukkan pada DNS tersebut. Jika tidak memiliki IP DNS maka kita akan menggunakan IP DNS Google disini menggunakan IP DNS Google yaitu: 8.8.8.8
4. Konfigurasi Firewall NAT=MASQUERADE yang digunakan agar IP LOCAL atau area local dapat terhubung internet. Dengan cara Klik IP > FIREWALL > NAT > + Tab general. Chain= srcnat, Out-interface= ether2, Tab

action. Action=Masquerade kemudian klik OK

5. Konfigurasi L2TP Klient konfigurasi untuk L2TP Klient. Untuk mengaktifkan router sebagai L2TP Klient Pada menu PPP -> Pilih L2TP Klient. Kemudian centang opsi 'Enabled'. Dengan otomatis L2TP Klient aktif.

6. Konfigurasi Routing untuk menghubungkan segmen-segmen jaringan untuk bisa melakukan packet forwarding. Sedangkan packet forwarding adalah proses memancarkan atau menyiarkan jaringan ke segmen-segmen jaringan komputer.

```
IPAddress add address =192.168.122.3/24  
interface = ether1 Jaringan Public  
ip address add address=192.168.10.0 /24  
interface=ether2 Jaringan Local  
IProute add dst-address=192.168.122.2/24  
Gateway=192.168.122.1
```

7. Tahap pengetesan ping antar perangkat.

Perancangan dan Konfigurasi Router Kantor Pusat

Login ke dalam router Mikrotik dapat dilakukan menggunakan aplikasi winbox menggunakan alamat IP Address router Mikrotik kemudian buka aplikasi winbox. Pada winbox klik tombol **Connect** untuk login.

Konfigurasi IP Address

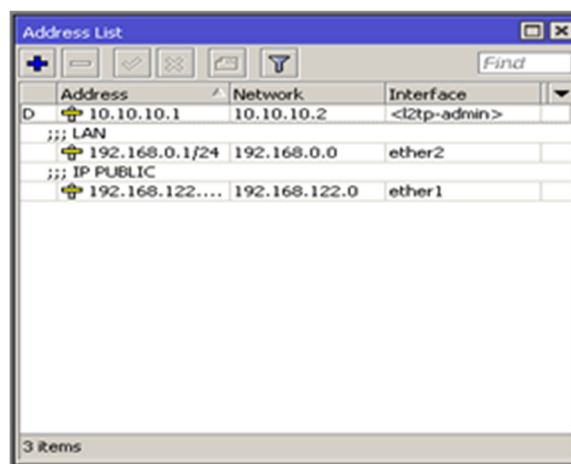
Setelah berhasil login ke dalam router, langkah berikutnya ialah menambahkan alamat IP pada masing-masing interface router, ada tiga interface yang harus dikonfigurasi, yaitu interface ether1 yang terhubung ke jaringan Public ether2 yang terhubung ke Switch (jaringan lokal), berikut detailnya :

Interface ether1 : IP Address : 192.168.122.2 /24 (Jaringan Public)

Interface ether2 : 192.168.0.1/24 (Switch / Jaringan Lokal)

Untuk menambahkan alamat IP pada

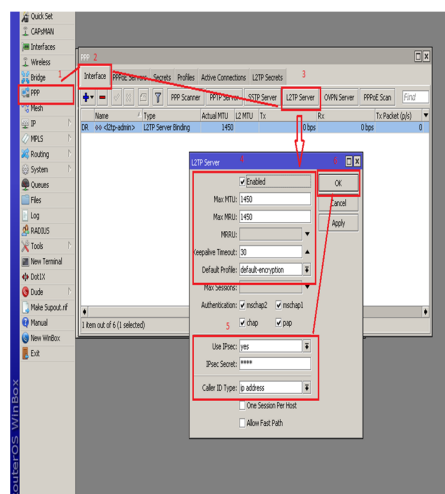
interface router, caranya klik menu **IP > Addresses**, lalu klik tombol **Add (+)** untuk menambahkan IP baru, berikut adalah tampilan konfigurasi untuk menambahkan alamat IP di interface ether1. Kemudian ulangi kembali langkah Konfigurasi IP Address di ether1 tadi sebanyak jumlah alamat IP yang akan ditambahkan pada router, hasil akhirnya akan terlihat seperti pada gambar di bawah.



Gambar 5. Hasil Akhir Konfigurasi Alamat IP di Semua Interface

Konfigurasi L2TP Server

Aktifkan L2TP Server, masuk ke menu PPP --> tab Interface --> pilih L2TP Server --> Centang Enabled --> Centang Use IPsec --> Masukkan IPsec Secret --> OK

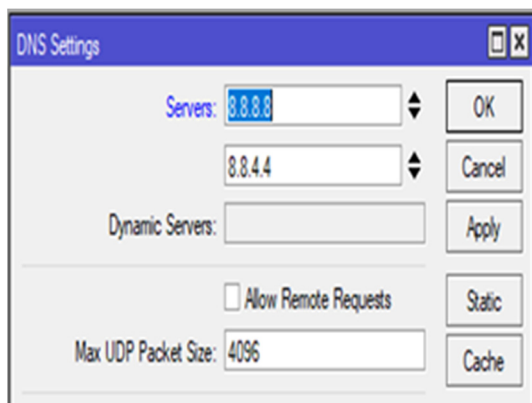


Gambar 6. Tampilan pengecekan interface router kantor pusat

Konfigurasi DNS Resolver

Agar *router* dapat mengenali nama domain dari situs-situs *web* yang ada di *internet*, maka *router* harus memiliki DNS *resolver*, tanpa konfigurasi DNS *resolver*, *router* hanya dapat mengenali alamat IP saja. Ada banyak sekali *Public DNS Server* di *internet* yang dapat digunakan sebagai DNS *resolver*, salah satunya ialah DNS *Google* (8.8.8.8 dan 8.8.4.4).

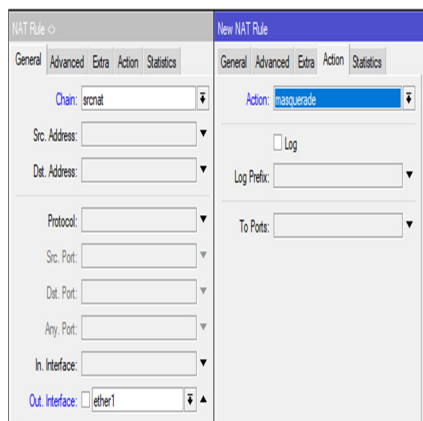
Untuk menambahkan DNS *resolver* pada *router*, caranya klik menu **IP > DNS**, kemudian masukkan alamat DNS *primary* dan *secondary* pada kolom **Server** seperti yang terlihat pada gambar di bawah ini.



Gambar 7. Tampilan Konfigurasi DNS Resolver

Konfigurasi NAT Masquerade

Agar semua *host* yang ada di jaringan lokal dapat terkoneksi ke jaringan *internet*, maka diperlukan NAT (*Network Address Translation*) *masquerade*.



Gambar 8. Tampilan Konfigurasi NAT Masquerade

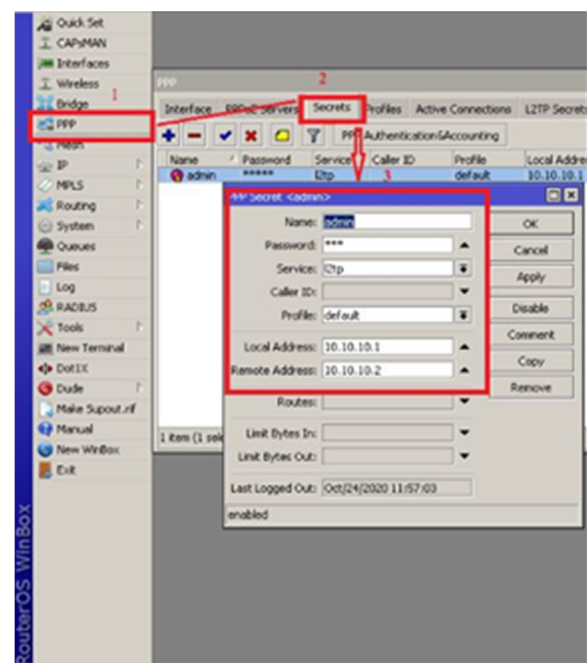
Fungsi dari NAT *masquerade* ini yaitu untuk mentranslasikan alamat IP *private* menjadi alamat IP *public* agar dapat dikenali oleh *host* lainnya yang ada di jaringan *public / internet*. Hal ini dikarenakan *user* yang menggunakan IP *private* tidak dapat berkomunikasi secara langsung dengan jaringan *public*.

Konfigurasi PPP Secrets

Buat user L2TP, masuk ke tab Secrets -->

Tambahkan user baru dengan parameter:

1. Name: masukkan username yang diinginkan
2. Password: masukkan password untuk username nya
3. Local Address: IP Address yang akan diberikan ke L2TP Server secara otomatis
4. Remote Address: IP Address yang akan diberikan ke L2TP Klient secara otomatis
5. Routes: Bisa diisi dengan network di Kantor cabang, nantinya akan muncul di tabel routing secara otomatis (dynamic route).

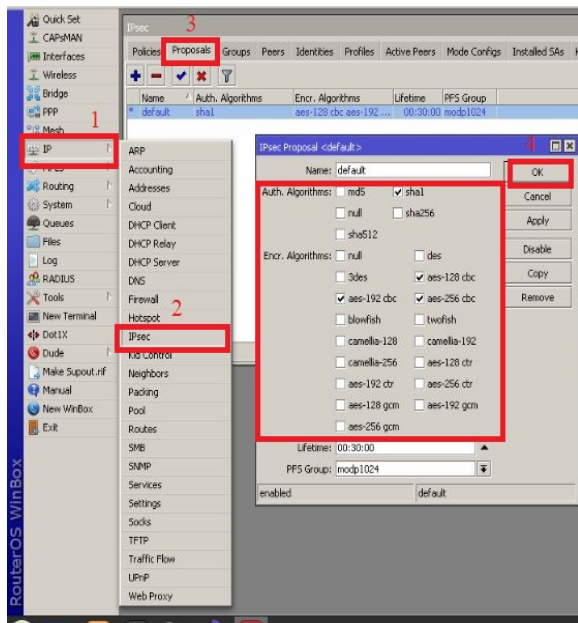


Gambar 9. Tampilan Konfigurasi PPP Secrets

Setting IPsec Proposals

Sekarang kita Setting IPsec nya. Masuk ke

menu IP --> IPsec --> tab Proposals --> buka default --> Silakan pilih Authentication Algorithms dan Encryption Algorithms nya --> OK



Gambar 10. Tampilan Konfigurasi IPsec Proposal

Perancangan dan Konfigurasi Router Kantor Cabang

Login ke dalam router Mikrotik dapat dilakukan menggunakan aplikasi winbox menggunakan alamat IP Address router Mikrotik kemudian buka aplikasi winbox. Pada winbox klik tombol **Connect** untuk login.

Konfigurasi IP Address

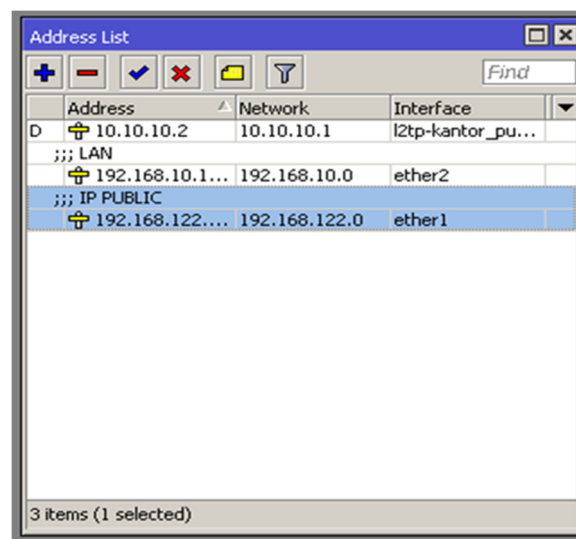
Setelah berhasil login ke dalam router, langkah berikutnya ialah menambahkan alamat IP pada masing-masing interface router, ada tiga interface yang harus dikonfigurasi, yaitu interface ether1 yang terhubung ke jaringan Public ether2 yang terhubung ke Switch (jaringan lokal), berikut detailnya:

Interface ether1: IP Address: 192.168.122.3 /24 (Jaringan Public) dan **Interface ether2 :** 192.168.10.0/24 (Switch / Jaringan Lokal)

Untuk menambahkan alamat IP pada interface router, caranya klik menu **IP >**

Addresses, lalu klik tombol **Add (+)** untuk menambahkan IP baru, berikut adalah tampilan konfigurasi untuk menambahkan alamat IP di interface ether1.

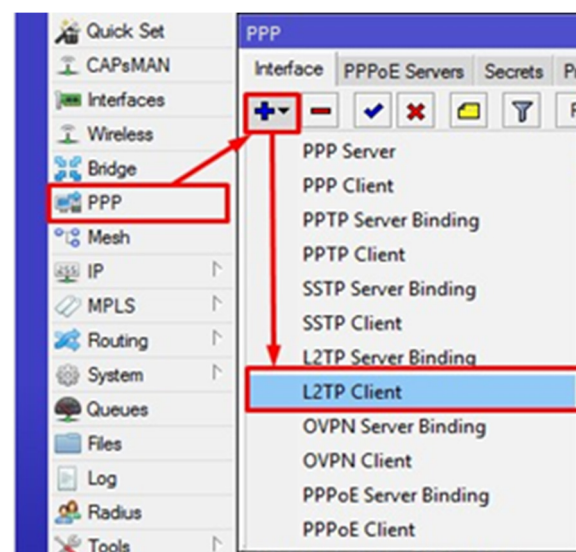
Kemudian ulangi kembali langkah menambahkan alamat IP di interface ether1. sebanyak jumlah alamat IP yang akan ditambahkan pada router, hasil akhirnya akan terlihat seperti pada gambar di bawah.



Gambar 11. Hasil Akhir Konfigurasi Alamat IP di Semua Interface

Konfigurasi PPP L2TP Klient

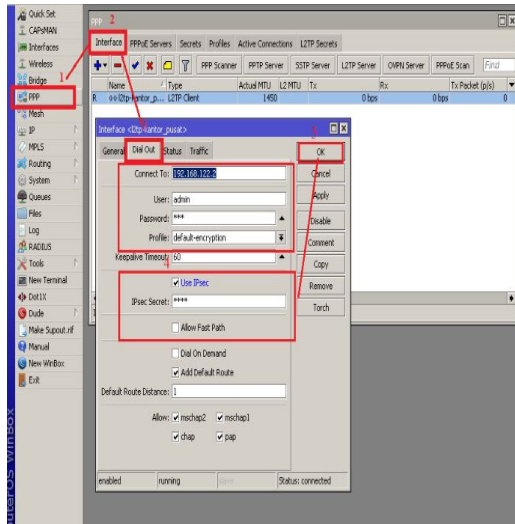
Masuk ke menu PPP --> tab Interface --> tambahkan Interface L2TP Klient



Gambar 12. Tampilan Konfigurasi PPP L2TP Klient

Konfigurasi Dial Out dari router cabang ke router pusat

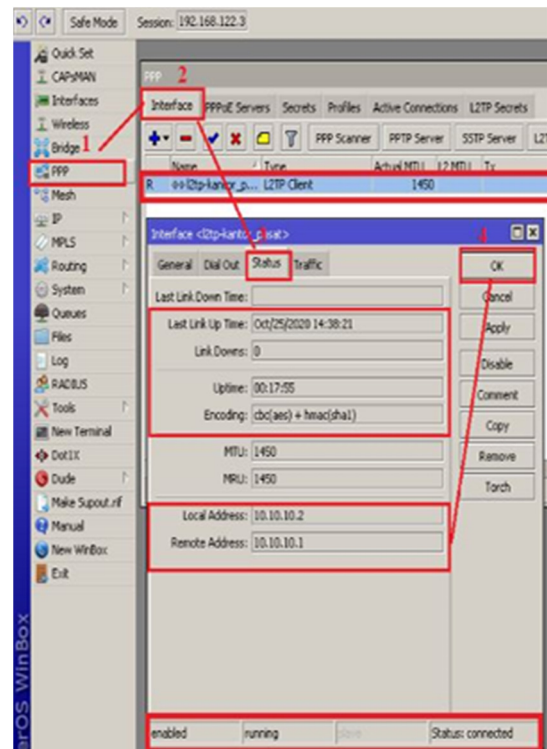
Pilih menu Dial Out > Isikan IP Public di :“Connect To > Masukkan user dan password > Klik OK



Gambar 13. Tampilan Dial Out ke router kantor pusat

Cek koneksi L2TP/IPsec

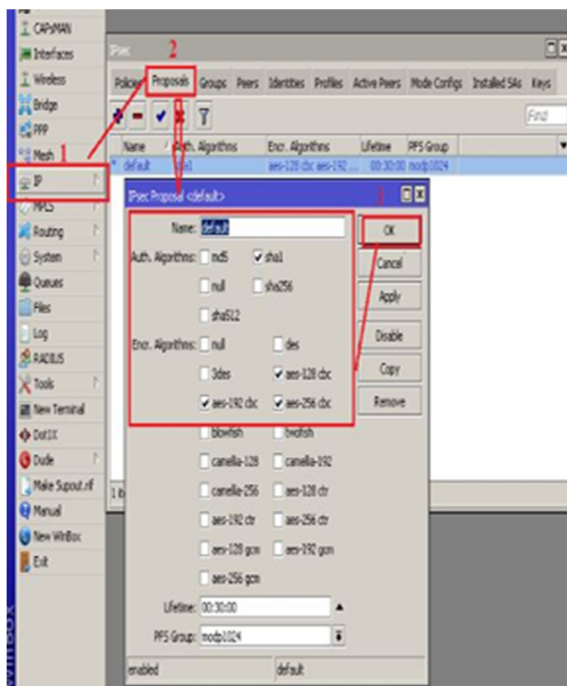
Cek koneksi L2TP nya apakah sudah konek. Masuk ke menu PPP --> Interface --> Pastikan interface nya sudah ada tanda R (Runing) dan pada Status interface nya sudah Connected.



Gambar 15. Tampilan koneksi L2TP Running

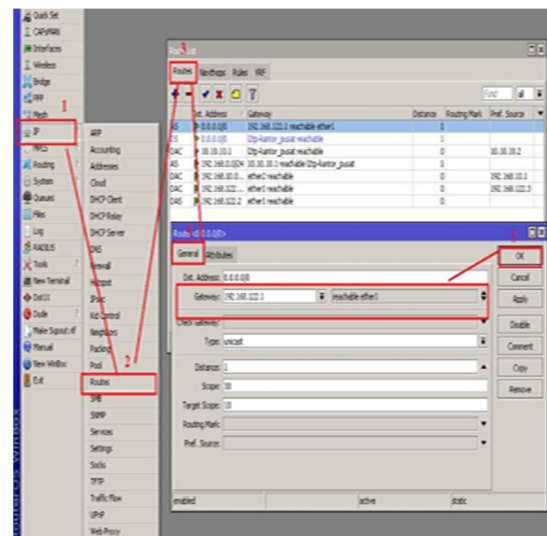
Konfigurasi IPsec

Setting IPsec di klient, IP --> IPsec --> tab Proposals --> default --> Samakan dengan isi proposal default di sisi Server.



Gambar 14. Tampilan IPsec

Konfigurasi ip route

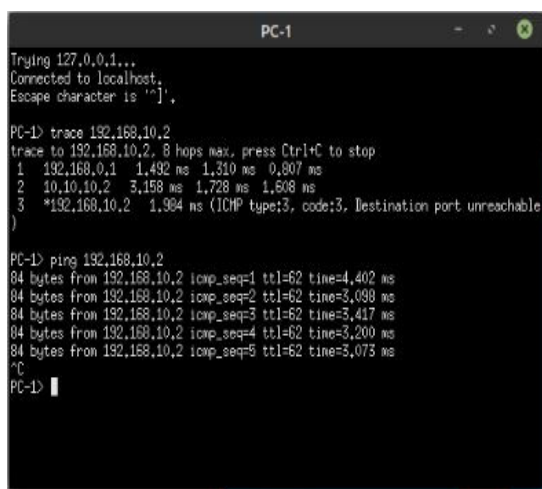


Gambar 16. Tampilan ip route gateway kantor pusat

Tambahkan static route di sisi Klient (kantor cabang) dengan memasukkan network pada sisi Server (kantor pusat) --> IP --> Route

Pengujian Sistem

Uji koneksi dari router Kantor pusat ke Klient pada kantor cabang. Melakukan *Trace Route* dari server ke Klient pada kantor cabang. Klient kantor pusat telah berhasil terhubung ke Klient kantor cabang.



```
PC-1
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

PC-1> trace 192.168.10.2
Trace to 192.168.10.2, 8 hops max, press Ctrl+C to stop
 1  192.168.0.1    1.492 ms  1.310 ms  0.807 ms
 2  10.10.10.2    3.158 ms  1.728 ms  1.608 ms
 3  *192.168.10.2  1.994 ms (ICMP type:3, code:3, Destination port unreachable)

PC-1> ping 192.168.10.2
84 bytes from 192.168.10.2: icmp_seq=1 ttl=62 time=4.402 ms
84 bytes from 192.168.10.2: icmp_seq=2 ttl=62 time=3.098 ms
84 bytes from 192.168.10.2: icmp_seq=3 ttl=62 time=3.417 ms
84 bytes from 192.168.10.2: icmp_seq=4 ttl=62 time=3.200 ms
84 bytes from 192.168.10.2: icmp_seq=5 ttl=62 time=3.073 ms
^C
PC-1>
```

Gambar 17. Tampilan *Trace Route* dari server ke Klient

Uji koneksi dari router Kantor Cabang ke klient pada kantor Pusat. Melakukan *Trace Route* dari klient pada kantor cabang. Klient kantor pusat telah berhasil terhubung ke klient kantor pusat.



```
PC-2
Executing the startup file

Checking for duplicate address...
PC1 : 192.168.10.2 255.255.255.0 gateway 192.168.10.1

PC-2> trace 192.168.0.2
Trace to 192.168.0.2, 8 hops max, press Ctrl+C to stop
 1  192.168.10.1    1.210 ms  1.131 ms  0.873 ms
 2  10.10.10.1    2.915 ms  1.330 ms  1.144 ms
 3  *192.168.0.2    2.250 ms (ICMP type:3, code:3, Destination port unreachable)

PC-2> ping 192.168.0.2
84 bytes from 192.168.0.2: icmp_seq=1 ttl=62 time=3.697 ms
84 bytes from 192.168.0.2: icmp_seq=2 ttl=62 time=3.118 ms
84 bytes from 192.168.0.2: icmp_seq=3 ttl=62 time=1.982 ms
^C
PC-2> ping 192.168.0.3
84 bytes from 192.168.0.3: icmp_seq=1 ttl=62 time=6.347 ms
84 bytes from 192.168.0.3: icmp_seq=2 ttl=62 time=3.293 ms
84 bytes from 192.168.0.3: icmp_seq=3 ttl=62 time=3.325 ms
^C
PC-2>
```

Gambar 18. Tampilan *Trace Route* dari cabang ke pusat

Analisis Kelayakan Jaringan Usulan

Penggunaan Switch HP 1820-24G – J9980A dan Gigabit Ethernet NIC. (LAN Card) sudah cukup untuk keperluan VPN L2TP. Perlu dibuat dokumentasi secara lengkap mengenai perangkat apa saja yang digunakan oleh masing-masing user maupun perangkat yang digunakan pada infrastruktur jaringannya. Selain itu, monitoring setiap perangkat pendukung infrastruktur jaringan juga perlu dilakukan guna memastikan setiap perangkat berjalan dengan optimal dan tanpa kendala. Pemanfaatan perangkat dan juga teknologi yang diterapkan pada jaringan sudah sesuai dengan aturan yang berlaku.

D. PENUTUP

Untuk mengatasi masalah pertukaran data yang penting dengan ukuran besar dapat diterapkan sistem jaringan VPN site-to-site pada jaringan komputer. Dengan diterapkannya jaringan VPN, maka antara kantor pusat dan cabang akan saling terhubung, sehingga memberikan akses data yang baik, cepat dan aman. Jaringan VPN dengan metode L2TP/IPSec merupakan kombinasi protokol tunneling, dengan metode ini tingkat keamanan transfer data lebih baik dan dengan IP Security data juga akan terenkripsi. Hasil Traceroute (tracert) dari kantor pusat ke cabang bahwa jalur paket melewati tunnel sesuai yang telah dibuat dengan metode VPN L2TP/IPSec.

Dalam menjalankan simulasi GNS3 sebaiknya menggunakan spesifikasi PC atau Laptop yang lebih bagus, konfigurasi jaringan VPN sebaiknya dilakukan secara terstruktur dan penggunaan IPSec yang sesuai atau saling mendukung setiap perangkat router. Perlu dilakukan monitoring jaringan VPN pada setiap kantor.

E. DAFTAR PUSTAKA

Basri, H., Mulyani, A., & Budihartanti, C. (2017). Perancangan Jaringan Wide Area Network Pada PT . Vizta Pratama

- Cabang Jakarta Dengan Metode VPN. *Jurnal PROSISKO*, 4(2), 38–43.
- Febrianto, B. (2022). Perancangan dan Implementasi Jaringan VPN Dengan Metode L2TP / IPsec pada Kantor Cabang dan Kantor Pusat. *Oktal : Jurnal Ilmu Komputer Dan Sains*, 1(07), 879–885.
- Hasrul, H., & Lawani, A. M. (2017). Pengembangan Jaringan Wireless Menggunakan Mikrotik Router OS RB750 Pada PT . Amanah Finance Palu. *Jesik : Jurnal Elektronik Sistem Informasi Dan Komputer*, 3(1), 11–19.
- Khasanah, S. N. (2014). Perancangan dan Implementasi Wide Area Network (WAN) Dengan IP VPN Studi Kasus : PT . MDPU Finance. *Techno Nusa Mandiri*, 11(2), 105–111.
- Komaridah, D. (2016). *Security Management Control Pada Jaringan Komputer*. Fakultas Ilmu Komputer Universitas Sriwijaya.
- Maulana, F., & Qomaruddin, M. (2022). Perancangan VPN L2TP Menggunakan Mikrotik untuk Remote Access pada Kejaksaan Negeri Jakarta Barat. *Jurnal Keilmuan Teknologi Informasi Dan Ilmu Manajemen (Justifi)*, 2(1), 17–22.
- Rahino, B. G., & Susila, A. (2022). Implementasi Jaringan VPN (L2TP / Ipsec) Mikrotik Untuk Remote Access Sebagai Security Selama Work From Home. *Oktal : Jurnal Ilmu Komputer Dan Sains*, 1(11), 1911–1918.
- Rahman, T., Zaini, T. R., & Chrisnawati, G. (2020). Perancangan Jaringan Virtual Local Area Network (Vlan) & Dhcp Pada Pt.Navicom Indonesia Bekasi. *JIKA (Jurnal Informatika)*, 4(1), 36. <https://doi.org/10.31000/jika.v4i1.2366>
- Sari, A. P., Sulistiyono, & Kemala, N. (2020). Perancangan Jaringan Virtual Private Network Berbasis IP Security Menggunakan Router Mikrotik. *Jurnal PROSISKO*, 7(2), 150–164.
- Satryawati, E., Pangestu, D. A., & Budiman, A. S. (2022). Implementasi virtual private network menggunakan point-to-point tunneling protocol. *Jurnal Elektro Dan Informatika Swadharma(JEIS)*, 02(1).
- Suhanda, Y., Nurlaela, L., Dharmalau, A., & Widjojo, B. S. (2022). Perancangan Infrastruktur Jaringan Berbasis Aplikasi Packet Tracer Dengan Metode Hot Standby Router Protocol. *Teknologi Terpadu*, 8(1), 9–16.
- Wirastuti, N. M. A. E. D., Hartawan, I. G. A. K. D. D., & Suyadnya, I. M. A. (2016). Perancangan Dan Instalasi Jaringan Komputer Local Area Network (Lan) Di Sekolah Dasar Negeri 2 Kintamani Bangli. *Jurnal Udayana Mengabdikan*, 15(September), 37–42.