Jurnal Teknik Mesin, Industri, Elektro Dan Informatika (JTMEI)
Vol.1, No.3 SEPTEMBER 2022
e-ISSN: 2963-7805; p-ISSN: 2963-8208, Hal 69-88

IMPLEMENTASI JARINGAN TERPUSAT MENGGUNAKAN OSPF DAN VPN DENGAN FAILOVER LINK DI PT. ADVANTAGE SCM

Billy Doohan Oktavian
Universitas Nusa Mandiri
Email: billyd12180047@nusamandiri.ac.id
Irwan Agus Sobari
Universitas Nusa Mandiri
Email: rwan.igb@nusamandiri.ac.id

Korespondensi penulis: billyd12180047@nusamandiri.ac.id

Abstract*. The development of technology is increasingly advanced, everyone can easily access the internet network whenever and wherever they are. In this case, internet access in the office is mandatory to support the company's operations and development. The bigger a company is, the more security and good management it will be in exchanging data via the internet as well as monitoring branches of the company, attacks and data reconnaissance are scary things because they can threaten the company's sustainability from unwanted things. To overcome this problem, companies can implement network security using VPN (Virtual Private Network) technology with L2TP (Layer 2 Tunneling Protocol) and IPSec methods and use OSPF routing. This VPN technology is able to send data through the internet network by encrypting the data before it is sent so that it is safe from external threats.*

Keywords*: Virtual Private Network, L2TP, IPSec, OSPF*

Abstrak. Perkembangan mengenai teknologi sudah semakin maju, setiap orang bisa dapat dengan mudah mengakses jaringan internet kapanpun dan dimanapun berada. Dalam hal ini akses internet dalam perkantoran hal yang wajib untuk menunjang operasional dan perkembangan perusahaan. Semakin besar suatu perusahaan maka akan sangat membutuhkan keamanan dan manajemen yang baik dalam melakukan pertukaran data melalui internet serta monitoring cabang dari perusahaan tersebut, serangan dan pengintaian data menjadi hal yang menakutkan karena dapat mengancam keberlangsungan perusahaan dari hal yang tidak diinginkan. Untuk mengatasi masalah tersebut perusaahan dapat menerapkan keamanan jaringan dengan menggunakan teknologi VPN (Virtual Private Network) dengan metode L2TP (*Layer 2 Tunneling Protocol*) dan IPSec serta menggunakan *routing* OSPF. Teknologi VPN ini mampu mengirimkan data melalui jaringan internet dengan mengenkripsi data terlebih dahulu sebelum dikirimkan sehingga aman dari ancaman pihak luar

Kata kunci: *Virtual Private Network, L2TP, IPSec, OSPF*

Received Agustus 27, 2022; Revised September 2, 2022; September 28, 2022
** Billy Doohan Oktavian, billyd12180047@nusamandiri.ac.id*

LATAR BELAKANG

Perkembangan sebuah teknologi perusahaan dalam mengelola berbagai macam kegiatan yang berkaitan dengan operasional suatu perusahaan tersebut menuntut akan kehandalan infrastruktur dalam jaringan yang dapat dikembangkan untuk jangka panjang. Salah satunya dengan menerapkan algoritma *routing* dinamik OSPF. *Routing* dinamik ini memberikan kemampuan *router* untuk dapat membuat tabel *routing* secara otomatis, dimana dalam hal ini memudahkan *maintenance* dan monitoring jika dibandingkan dengan hanya menggunakan *routing* statik (Syarief & Rochmah, 2021). Dalam penelitian ini penulis membutuhkan sebuah VPN *Concentrator* untuk membuat sebuah jalur komunikasi yang baru secara *private* dan aman. VPN *Concentrator* ini menghubungkan antara *client* dengan *server* yang berada pada jaringan global (internet) dengan jaringan intranet (lokal) agar dapat saling berkomunikasi (Fathsyah et al., 2021).

Berkembangnya teknologi telekomunikasi ini lah yang dimanfaatkan berbagai perusahaan untuk menunjang kegiatan operasional. Salah satunya pada operasional di PT. Advantage SCM yang menerapkan akses jaringan melalui *Virtual Private Network* (VPN) menggunakan *Layer 2 Tunneling Protocol* (L2TP) untuk menghubungkan LAN pada semua cabang yang tersebar. Protokol *routing* yang akan digunakan dalam melakukan terjadinya proses pertukaran informasi berupa *routing table* antar cabang pada implementasi ini adalah *Open Shortest Path First* (OSPF) (Nusantara et al., 2017).

Dalam menerapkan implementasi ini jaringan harus selalu terhubung *internet* untuk dapat terkoneksi ke VPN dan bertukar informasi *routing*. Apabila jalur komunikasi ke *internet* terputus oleh factor tertentu, maka dalam hal ini akan terjadi *downtime* pada cabang tersebut yang mengakibatkan terganggunya operasional. Untuk mengatasi permasalahan tersebut, dibutuhkan sebuah koneksi internet cadangan(*Backup Link*) pada setiap cabang serta menerapkan *failover* pada *router* cabang.

e-ISSN: 2963-7805; p-ISSN: 2963-8208, Hal 69-88

Pada dasarnya teknologi *failover* ini merupakan teknik yang dapat mengalihkan jalur koneksi utama ke koneksi cadangan sehingga komunikasi pertukaran informasi *routing* dapat berjalan terus meski jalur koneksi utama terputus. Salah satu kasus pentingnya teknik *failover* ini adalah mengakses mesin *finger* cabang dari server terpusat. Teknik ini sangat baik untuk menghindarkan *downtime* yang menyebabkan data absensi tidak dapat diunduh ke server, sehingga dapat terus berinteraksi antara server dengan cabang.

KAJIAN TEORITIS

Konsep Dasar Jaringan

Teknologi jaringan VPN (*Virtual Private Network*) dimana menurut Numan Musyaffa VPN ini bertujuan untuk mengatasi masalah dalam menghubungkan pengguna dari jaringan lain yang jauh maupun terpisah secara geografis. VPN memungkinkan mengakses server yang hanya dapat dilakukan dari jaringan lokal dari segala resika yang ada di jaringan publik. Penggunaan yang aman ini tercipta dari adanya penggunaan koneksi yang terenkripsi, penggunaan private keys, certificates, usrname atau password dalam membangun koneksi. (Musyaffa & Ryansyah, 2020)

Teknologi jaringan VPN (*Virtual Private Network*) dengan tipe L2TP (*Layer 2 Tunneling Protocol*) sangat memungkinkan untuk mengamankan saat terjadinya pertukaran data dengan jarak yang jauh, karena proses kerja VPN ini membuat jaringan sendiri yang rahasia dengan menggunakan IP *Public*. (Putra et al., 2018)

L2TP

Layer 2 Tunneling Protocol (L2TP) merupakan perpaduan antara 2 buah protocol tunneling yaitu *Layer* 2 *Forwading* milik cisco dan PPTP yang dimiliki oleh Microsoft.

Umumnya L2TP ini menggunakan protocol UDP dengan port 1702 dalam membuat *Virtual Private Dial Network* (VPDN). Protokol L2TP disebut aman karena menggunakan IPSec untuk mengenkapsulasi data yang ada di dalamnya. (Zamalia et al., 2018)

IPSec

IPSec merupakan kumpulan protokol dan standar yang bertujuan untuk memberikan keamanan serta kerahasiaan saat pertukaran data. Dengan demikian meskipun data berhasil disadap oleh orang lain maka data tersebut tidak akan dapat diakses bagi siapapun karena data sudah terenkripsi dengan aman. IPSec akan memeriksa integritas data serta memeriksa keaslian sumber dari pengirim, yang lebih penting ialah kemudahan dalam penerapan dengan tidak membutuhkan syarat sistem yang tinggi dan mahal tentunya. Sehingga penguna komputer tidak perlu berpikir panjang untuk segera melakukan pengamanan data dengan menggunakan IPSec. (Sjafrina, 2019)

OSPF

OSPF (*Open Shortest path First*) merupakan sebuah *protocol routing dynamic* yang memiliki kemampuan fleksibilitas yang tinggi dan konvergensi cepat. Menggunakan penggunaan *bandwidth* sebagai *path metric* untuk mendapatkan jalur terbaik dalam pemilihan *routing*. Dikarenakan penggunaannya yang fleksibel, protokol ini dikembangkan secara terbuka oleh banyak vendor seperti yang digunakan pada *router* mikrotik dan cisco. (Budiman et al., 2019)

Jurnal Teknik Mesin, Industri, Elektro Dan Informatika (JTMEI)
Vol.1, No.3 SEPTEMBER 2022
e-ISSN: 2963-7805; p-ISSN: 2963-8208, Hal 69-88

Failover

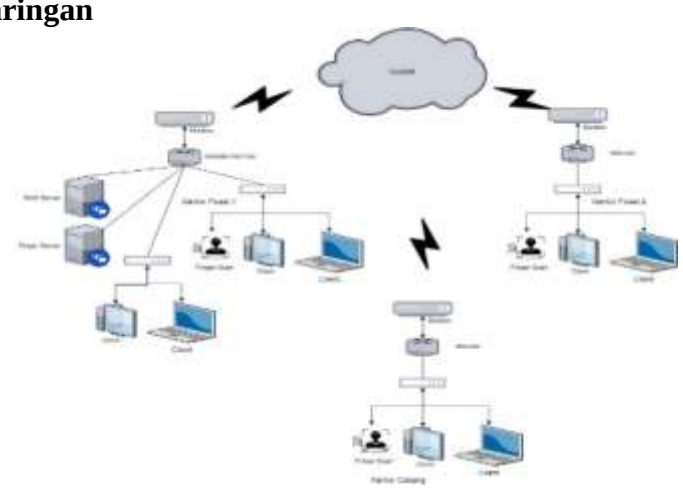
Failover ini berfungsi sebagai solusi untuk mengatasi permasalahan *downtime* yang terjadi saat masa perubahan dari jalur utama ke jalur *backup*. *Failover* ini akan bekerja secara otomatis untuk mempersingkat *downtime* dengan cara kerja mengirimkan ICMP *echo reply* secara berkelanjutan pada jalur utama. (Suryanto, Teguh Prasetyo, 2018)

METODE PENELITIAN

Penelitian yang akan dilakukan ini merupakan penelitian lapangan yakni dengan melakukan implementasi terhadap salah satu cabang dari PT. Advantage SCM yang belokasi di Jakarta Pusat. Berdasarkan latar belakang diatas, maka dari itu penulis membatasi permasalahan penelitian ini hanya berkaitan dengan penggunaan VPN L2TP terhadap interkoneksi, hasil interkoneksi antara cabang yang berhasil terhubung dengan OSPF dan hasil dari penerapan metode *FailOver Link*. Teknik pengumpulan data dengan menggunakan studi literatur, pengumpulan data (observasi) dan wawancara. Pengujian pada metode yang diterapkan dan dipilih berupa hasil dan manfaat sebagai solusi dalam masalah yang diangkat dalam penelitian.

HASIL DAN PEMBAHASAN

Skema Jaringan



Gambar 1. Skema Jaringan Perusahaan

Pada gambar 1 skema jaringan pada PT. Advantage SCM sudah terbilang cukup baik karena pertukaran data dari kantor pusat ke semua kantor cabang menggunakan server NAS yang ada di publik. Dari kantor pusat 2 biasanya meletakan file file dokumen yang diperlukan untuk kebutuhan kantor pusat 1 maupun kantor cabang. Namun file – file dokumen ini sangat lah beresiko jika harus bertransaksi pada jaringan yang publik. Dalam proses pertukaran datanya pun diperlukan ip publik dengan *bandwidth* yang besar pada kantor pusat 1 jika terdapat penarikan seluruh cabang. Hal ini menjadi kendala terhadap jaringan kantor pusat 1 dan server NAS itu sendiri.

Pada kantor pusat 1 juga mengakses ke server NAS untuk keperluan menampung semua software dan aplikasi yang dibutuhkan oleh perusahaan, menampung backupan dari server database kalau sudah penuh, menampung ribuan file dokumen seperti PDF ataupun excel dari divisi lain. Dengan masalah ini penulis ingin memberikan pengoptimalan perangkat jaringan yang sudah ada untuk dibangun sebuah teknologi VPN dengan metode L2TP. Selain keamanan yang lebih baik metode ini juga bisa memanfaatkan jaringan internet menjadi layaknya jaringan lokal, sehingga pertukaran data jauh lebih aman.

Rancangan Aplikasi

Dalam membuat skema jaringan penulis menggunakan software *packet tracer* namun dalam membuat rancangannya sendiri penulis menggunakan winbox untuk konfigurasi mikrotik dan menggunakan VPS berbayar untuk mensimulasikan penerapan jaringan secara *real* serta ada juga *routerboard* fisik yang akan digunakan sebagai kantor pusat dan kantor cabang untuk keperluan komunikasi data melalui jaringan internet.

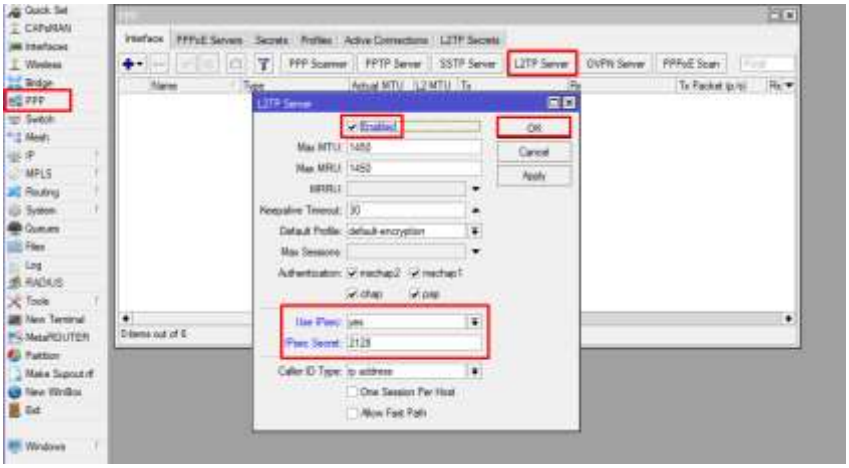
Langkah pertama adalah membeli dan membuat virtual mikrotik pada penyedia layanan VPS cloud.

e-ISSN: 2963-7805; p-ISSN: 2963-8208, Hal 69-88

Untuk selanjutnya mengkonfigurasikan mikrotik tersebut dengan bantuan aplikasi Winbox, dengan cara memasukan IP Publik yang didapatkan dari penyedia layanan server virtual. Setelah berhasil login ke mikrotik maka akan terlihat tampilan awal, pada tahap ini dilakukan konfigurasi mikrotik virtual sebagai tempat pengaturan VPN L2TP server.

Untuk memulai konfigurasi VPN Server dapat menambahkan ip *Loopback* pada *interface bridge1* untuk mengakses terhadap router itu sendiri tanpa terikat *hardware*.

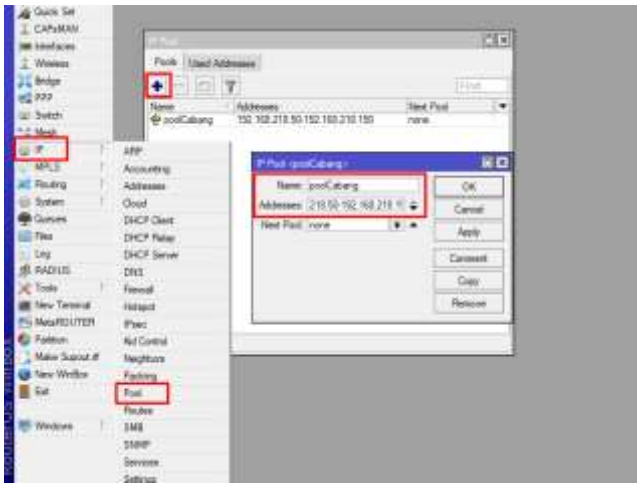
Selanjutnya mengaktifkan VPN L2TP Server melalui menu PPP, tekan L2TP Server. Centang *Enable* dan aktifkan fitur *Use IPsec* ubah *action* nya menjadi *Yes*, selanjutnya dibaris bagian bawah masukan angka *secret* yang akan digunakan sebagai keamanan pada saat mikrotik lain hendak melakukan koneksi VPN ke mikrotik server.



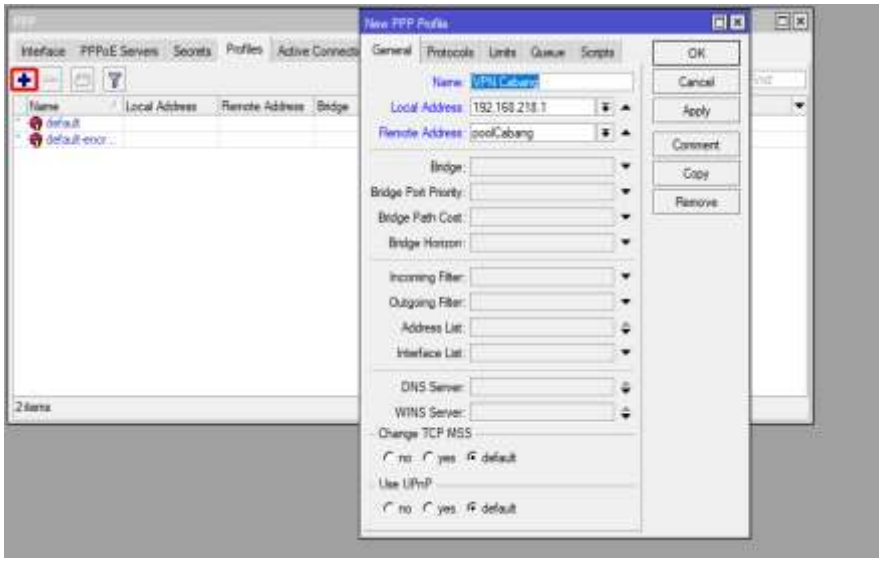
Gambar 2. Konfigurasi VPN L2TP Server

Selanjutnya masuk ke ip *pool* untuk menambahkan *virtual* ip secara *dynamic* agar VPN yang terkoneksi mendapatkan ip secara otomatis dari range yang sudah ditentukan. Disini penulis memberi *name* dengan poolCabang, dan dengan *addresses* 192.168.218.50-192.168.218.150, yang artinya addresses tersebut range yang akan didapat user VPN, lalu tekan *Apply*. Selanjutnya tekan tanda + lalu pada baris *name* isi

saja dengan VPN Cabang, pada *local address* diisi dengan ip 192.168.218.1 yang mana ip ini merupakan ip VPN server, kemudian *remote address* diisi dengan ip *pool* yang sudah di konfigurasi.



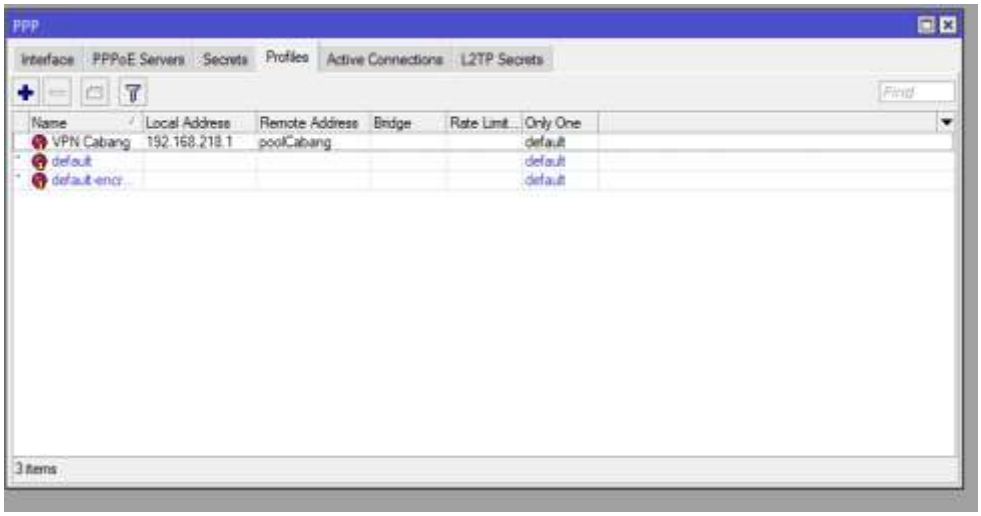
Gambar 3. Konfigurasi IP Pool



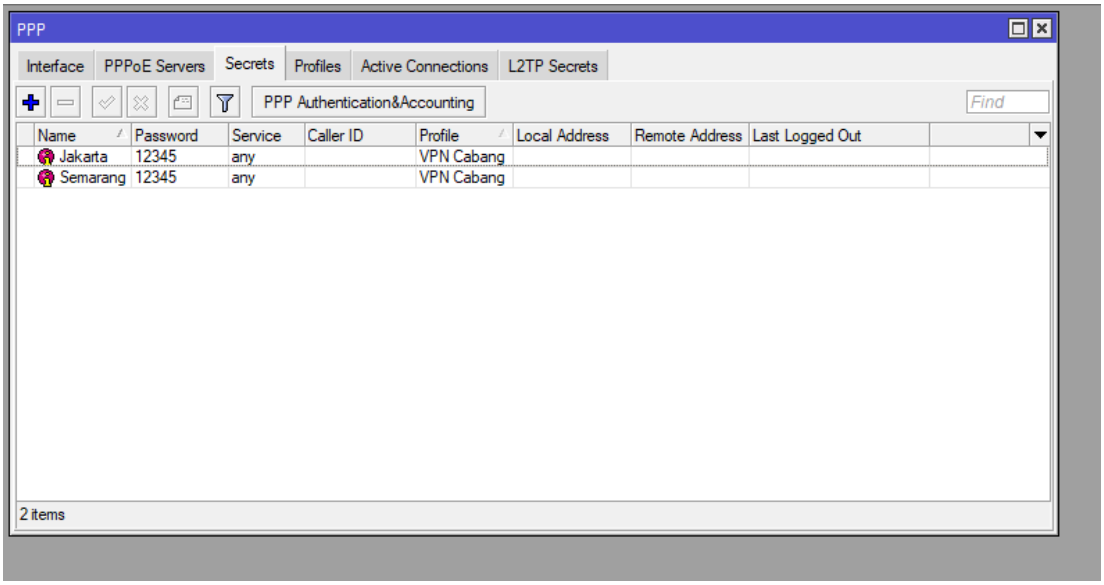
Gambar 4. Konfigurasi Profil untuk VPN Cabang

Langkah berikutnya adalah membuat *secret* untuk masing-masing kantor yang akan terhubung ke server VPN. Pada tampilan menu *secrets* lalu tekan tanda + selanjutnya isi bagian *name* , selanjutnya *password* bisa diisi dengan 12345 atau dapat menyesuaikan dengan kebutuhan masing-masing, pada *service* pilih *any* dan *profile* pilih profil VPN Cabang yang sebelumnya sudah pernah dibuat, lalu tekan Ok.

e-ISSN: 2963-7805; p-ISSN: 2963-8208, Hal 69-88



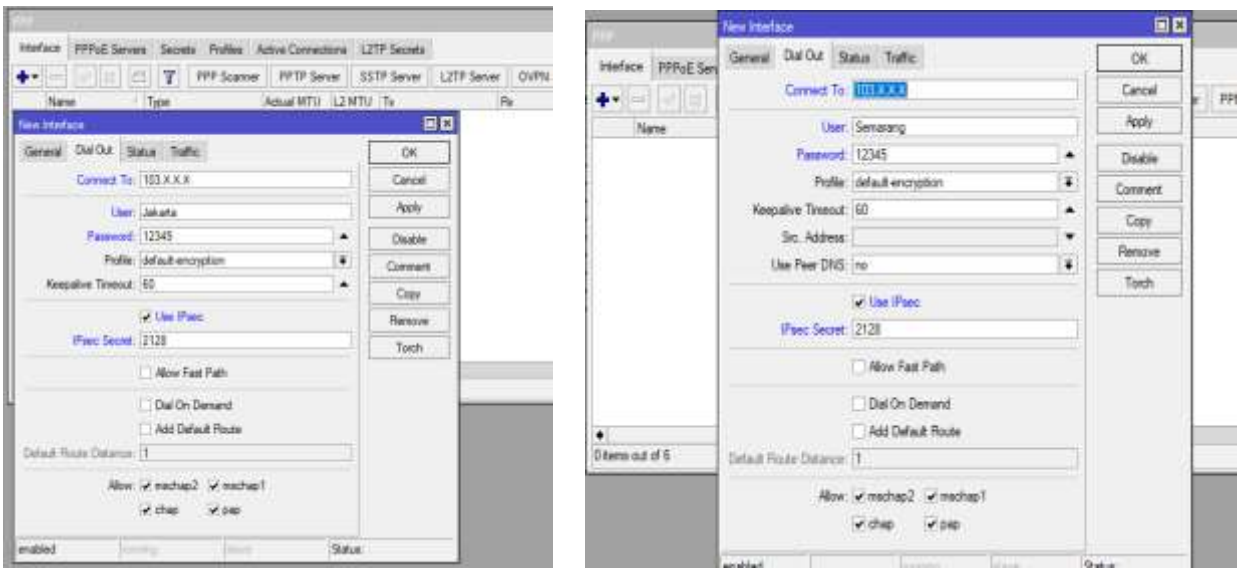
Gambar 5. Hasil Profile Yang Berhasil Dibuat



Gambar 6. Hasil *Secrets* Yang Berhasil Dibuat

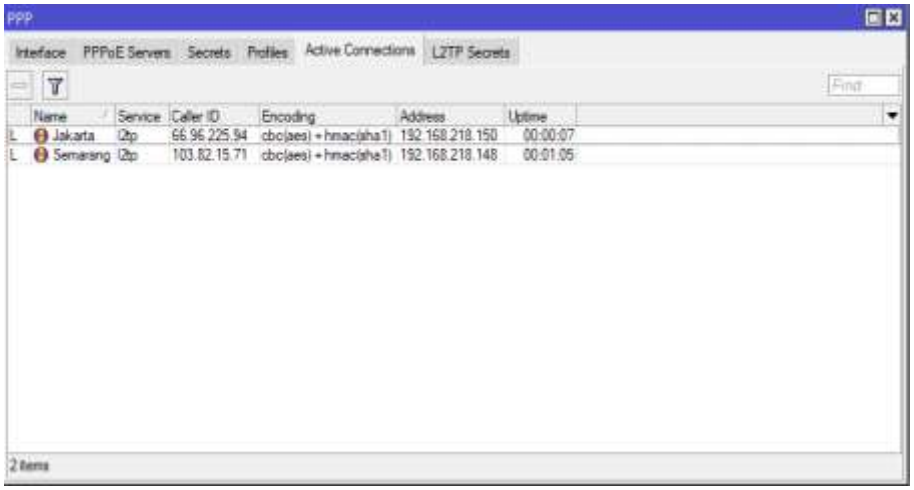
Selanjutnya konfigurasi vpn client mikrotik cabang Jakarta dan cabang semarang melalui winbox. Masuk ke menu PPP tekan tanda + lalu pilih vpn L2tp *Client*, pilih ke menu *dial out*, kemudian isi bagian *connect to* yang artinya alamat IP publik dari mikrotik virtual server disini penulis menggunakan ip publik 103.X.X.X (inisial) yang mana ip publik tersebut didapat saat memesan layanan untuk VPS publik, *user* diisi dengan nama

Jakarta, dengan *password* 12345, *profile* bisa dibiarkan saja dengan *default encryption*, pada *use ipsec* buat tanda centang, lalu *ipsec secrets* nya bisa diisikan 2128 sesuai dengan *password* yang telah dikonfigurasi pada pembuatan *secret*, lalu tekan Ok.



Gambar 7. Setting VPN Client pada Mikrotik Cabang

Saat ini mikrotik Jakarta dan Semarang sudah dapat terhubung ke VPN Server mikrotik.



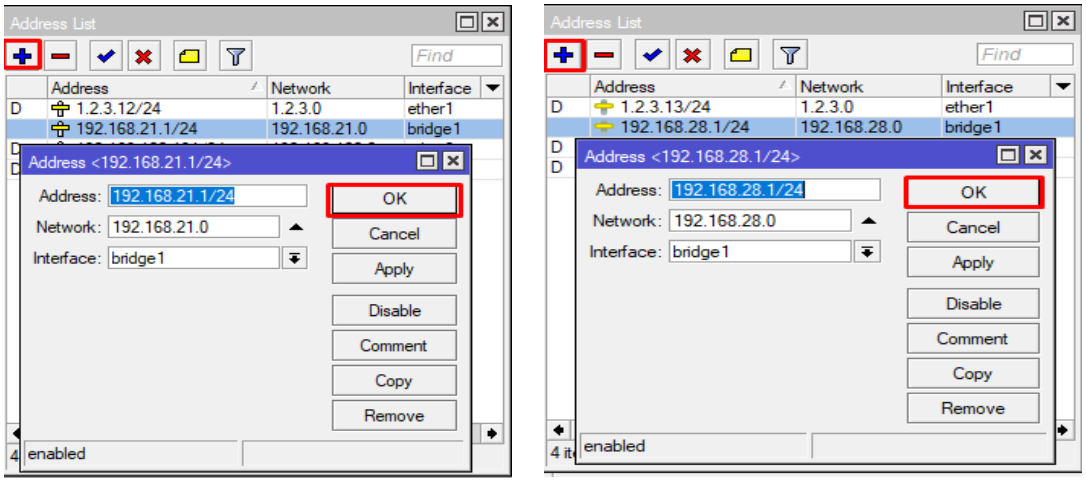
Gambar 8. Koneksi Status Aktif

Sampai pada tahap ini antar *side* belum bisa saling berkomunikasi sehingga perlu dibuatkan *route* secara statik terlebih dahulu. Namun penulis pada konfigurasi ini menerapkan *route* secara dinamis yaitu menggunakan OSPF. Yang pertama ip lokal di

e-ISSN: 2963-7805; p-ISSN: 2963-8208, Hal 69-88

Interface ethernet pada cabang Jakarta dan cabang Semarang harus aktif, atau dapat menggunakan *interface bridge* sebagai *loopback*. Pada fungsinya *bridge* pada mikrotik berfungsi untuk sebagai switch setiap port *ethernet* yang di tentukan. Pada winbox pada cabang, Pilih menu *bridge* untuk membuat port *bridge* tekan tanda +, lalu di ok saja biarkan secara *default*, kemudian pada *ports* masukan port *ethernet* yang akan dijadikan sebagai distribusi seperti switch, lakukan hal yang sama pada cabang Semarang untuk membuat port *bridge* atau *Loopback*.

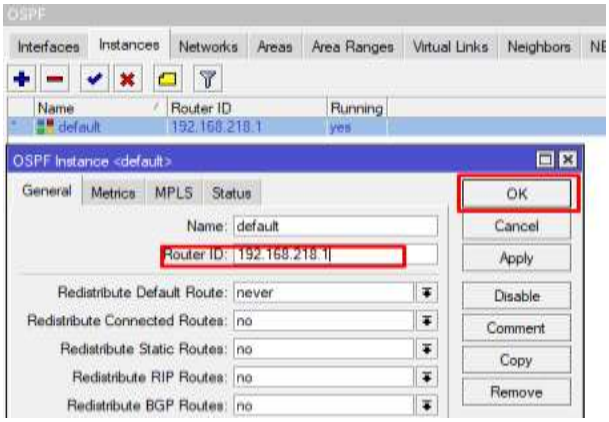
Selanjutnya masuk ke winbox pada masing masing mikrotik cabang untuk menambahkan *ip address* bisa diisi dengan sesuai kebutuhan cabang, penulis menerapkan ip 192.168.21.0/24 untuk cabang Jakarta dan 192.168.28.0/24 untuk cabang Semarang, lalu *interface* diarahkan ke *bridge1*, lalu tekan Ok.



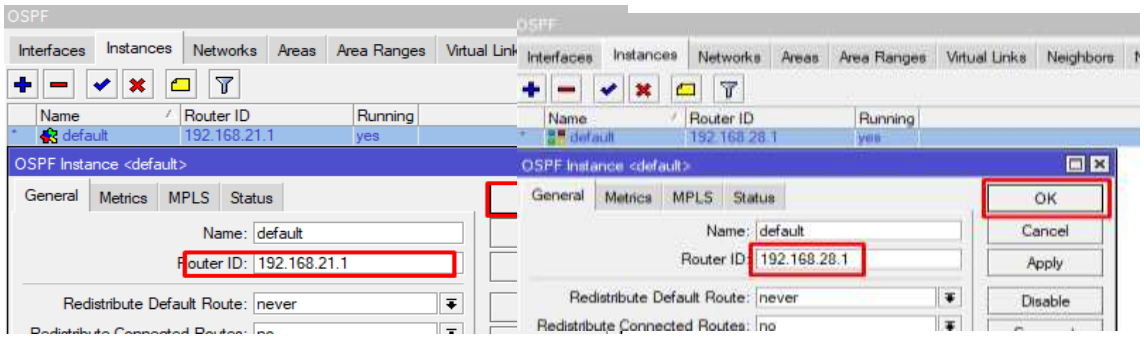
Gambar 9. Menambahkan IP Pada Mikrotik Cabang Jakarta dan Cabang Semarang

Berikutnya setelah IP pada setiap *interface* telah aktif, maka dilanjutkan untuk mengkonfigurasi *routing* dinamis OSPF pada setiap router yang saling terhubung. Yang pertama konfigurasi *route* OSPF pada mikrotik virtual server, kedua dilanjutkan

konfigurasi *route* OSPF pada mikrotik cabang Jakarta, dan ketiga konfigurasi *route* OSPF pada mikrotik cabang Semarang. Lalu dilanjutkan pada Gambar 4.19 yang telah masuk winbox mikrotik virtual server, tekan pilihan route, lalu pilih OSPF, pilih tab *instances.* Disini menggunakan profile default, lalu mengganti *Router* ID dengan ip lokal masing masing pada router. Fungsi *Router* ID sebagai identitas darimana berasalnya *routing table* yang dikirm secara *dynamic* berasal.



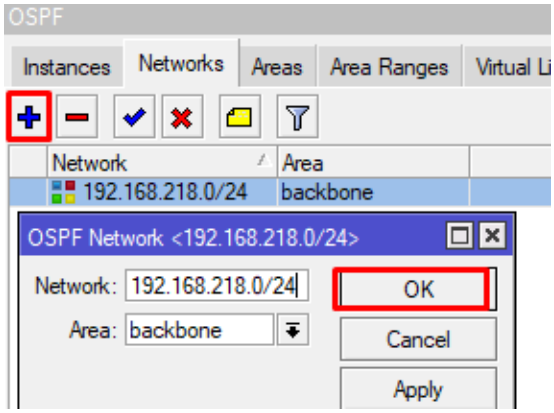
Gambar 10. Konfigurasi Instances Route OSPF pada mikrotik server



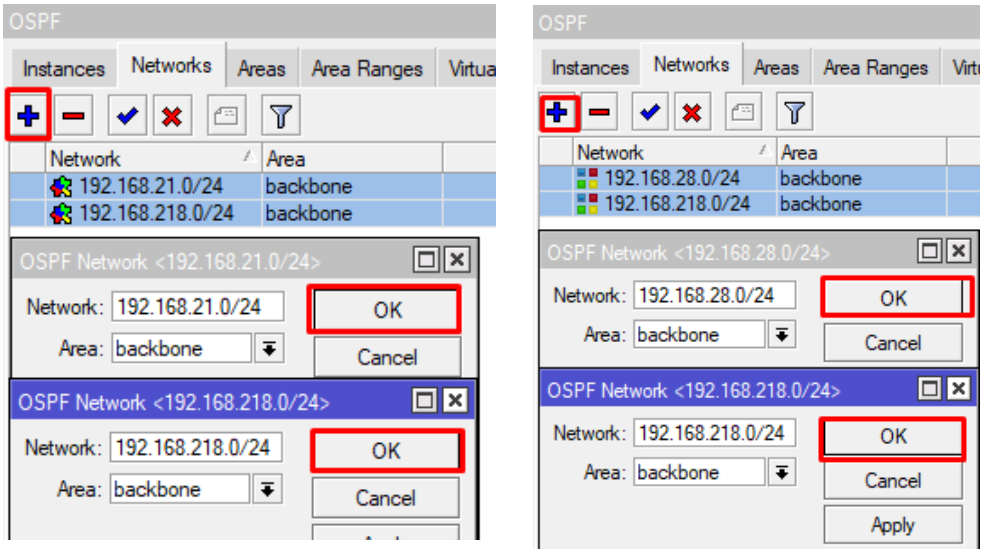
Gambar 11. Konfigurasi Instances Route OSPF pada mikrotik cabang Jakarta (Kiri) dan cabang Semarang (Kanan)

Jurnal Teknik Mesin, Industri, Elektro Dan Informatika (JTMEI)
Vol.1, No.3 SEPTEMBER 2022
e-ISSN: 2963-7805; p-ISSN: 2963-8208, Hal 69-88

Berikutnya setelah *Instances* pada setiap router sudah terkonfigurasi, selanjutnya mendaftarkan *network* yang akan selalu terhubung nantinya pada menu *Networks*. Untuk *network* yang didaftarkan pada mikrotik virtual server hanya *network* ip lokal yang digunakan untuk VPN saja dengan menekan tombol +, untuk cabang Jakarta dan cabang Semarang konfigurasi *networks* OSPF selain network ip lokal, network ip VPN yang terkoneksi harus ditambah juga pada masing masih router client. Pada konfigurasi area menggunakan default yaitu backbone, lalu pilih ok.



Gambar 12. Konfigurasi Networks OSPF pada Mikrotik virtual server

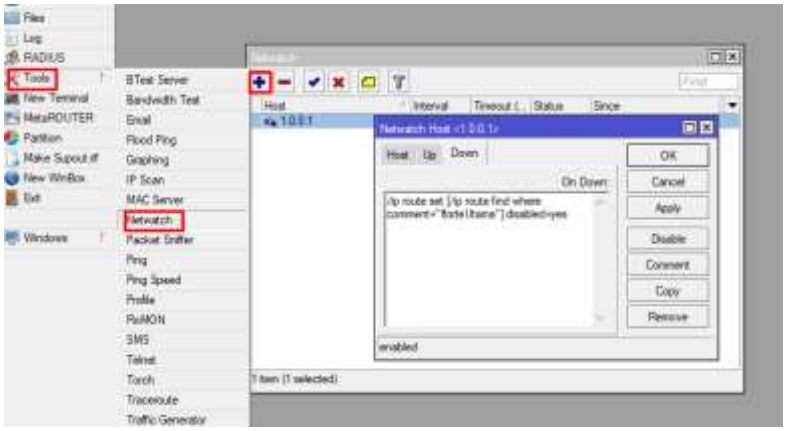


Gambar 13. Konfigurasi Networks OSPF pada Mikrotik cabang Semarang

Setelah konfigurasi pada tab *Networks* selesai maka semua jaringan yang telah ditambahkan sudah masuk dalam *routing table* OSPF.

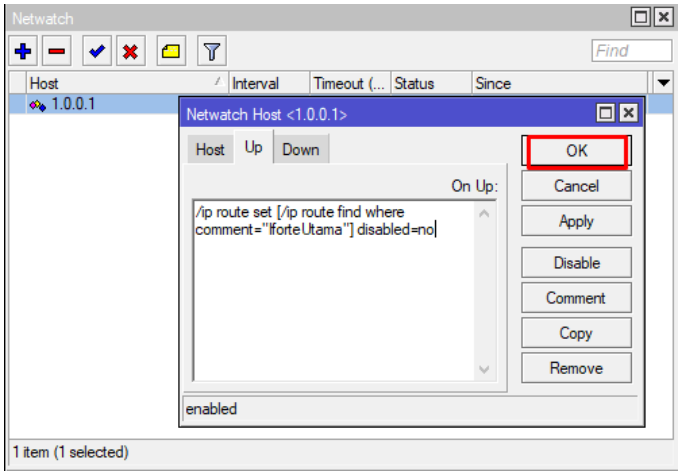
Selanjutnya melakukan konfigurasi untuk menerapkan teknologi *Failover* yang sederhana untuk mengurangi saat terjadinya gangguan pada layanan internet utama terjadinya *downtime* yang cukup lama dengan mengubah otomatis ke layanan internet cadangan yang tersedia. Untuk konfigurasi ini dilakukan hanya pada router router cabang saja, seperti pada kasus penulis ini untuk cabang Jakarta dan cabang Semarang. Untuk *failover* menggunakan fitur dari Mikrotik yaitu *Netwatch*. Hal pertama untuk konfigurasi ini adalah menentukan *gateway* utama dan cadangan. Setelah menentukan *gateway*, menentukan alamat IP yang akan dipantau oleh internet utama status nya, untuk kasus ini penulis menggunakan alamat IP 1.0.0.1 yang merupakan *alternative* DNS milik perusahaan *CloudFlare*. Seperti pada cabang Jakarta *gateway* iforte sebagai internet utama dan indihome sebagai cadangan.

Selanjutnya melakukan konfigurasi pada *netwtach* untuk merubah otomatis koneksi utama ketika sedang terkendala, cara kerja dari *netwatch* adalah ketika koneksi utama terdeteksi *down* atau terkendala maka akan menjalankan perintah untuk merubah *gateway* utama menjadi cadangan.



Gambar 14. Konfigurasi Script Down Netwatch

e-ISSN: 2963-7805; p-ISSN: 2963-8208, Hal 69-88



Gambar 15. Konfigurasi Script Up Netwatch

4.1.2 Manajemen Jaringan

Manajemen jaringan usulan yang yang digunakan oleh penulis yaitu membuat jaringan komputer yang bersifat pribadi dan terpusat dengan menggunakan teknologi VPN metode L2TP IPSec serta *routing dynamic* OSPF, dengan teknologi tersebut setiap user yang hendak terhubung dengan kantor harus melalui administrator jaringan terlebih dahulu untuk memastikan apakah benar yang meminta akses adalah seseorang yang bekerja di perusahaan tersebut, jika benar maka tinggal dibuatkan user akses VPN. Serta dengan teknologi *route* OSPF dapat memudahkan dalam hal *troubleshooting* ketika ada kendala pada suatu tempat yang jauh dan *monitoring* jaringan dalam skala yang besar.

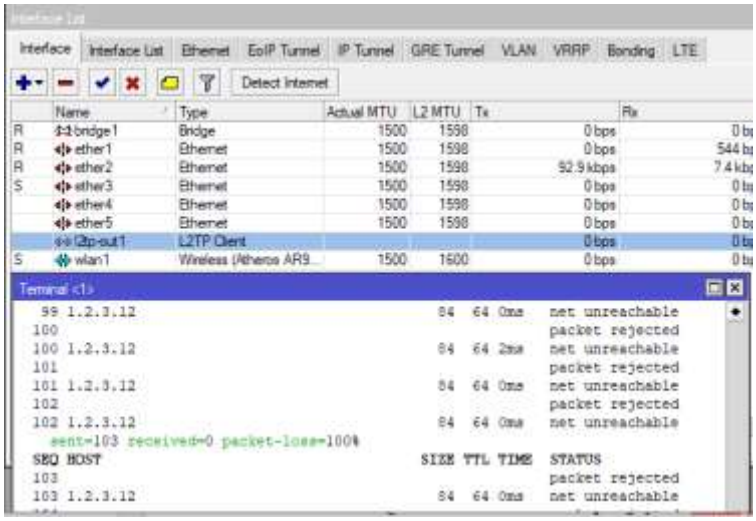
4.2 Pengujian Jaringan

Pengujian jaringan disini bisa menggunakan *test ping* dari terminal mikrotik atau *command prompt* untuk mengetahui koneksi jaringan usulan, apakah jaringan tersebut berjalan atau tidak.

4.2.1 Pengujian Jaringan Awal

Penulis melakukan *test ping* sebelum implementasi VPN L2TP IPSec beserta *routing dynamic* OSPF dari kantor cabang Jakarta dan cabang Semarang ke server mikrotik virtual dan hasilnya terjadi *timeout* artinya mikrotik cabang Jakarta dan cabang Semarang belum terhubung ke server VPN.

Selanjutnya pada Gambar 4.32 ketika terjadinya kendala pada layanan internet utama, maka koneksi ke VPN masih menggunakan *link* utama yang mengakibatkan terjadinya downtime karena tidak langsung berpinda otomatis ke *link* cadangan.

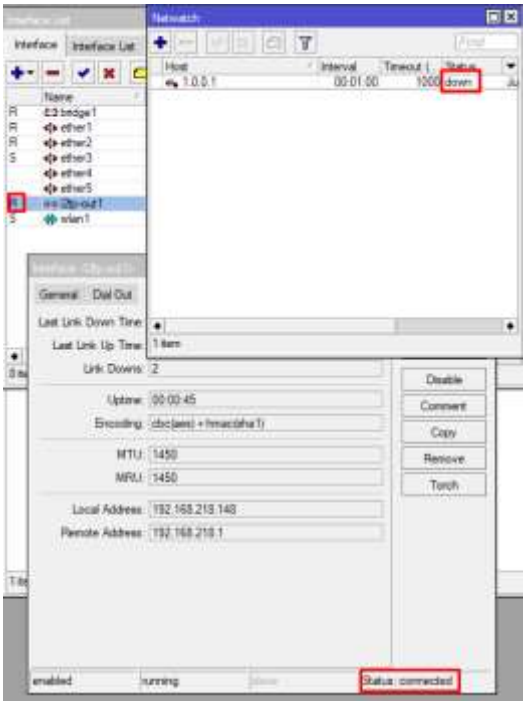


Gambar 16. VPN tidak terkoneksi

4.2.2 Pengujian Jaringan Akhir

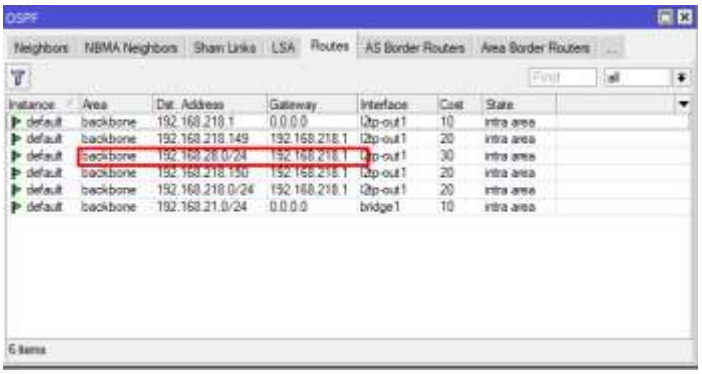
Pengujian terhadap link failover dilakukan untuk mengetahui script yang telah dikonfigurasi memantau layanan internet utama, pada pengujian ini penulis hanya lakukan pada cabang Jakarta karena hasilnya akan sama dengan yang lainnya. Dalam tahap pengujian ini parameter berjalannya atau tidak adalah ketika status di *netwatch* down maka VPN pada router tetap terkoneksi dengan koneksi cadangan.

Jurnal Teknik Mesin, Industri, Elektro Dan Informatika (JTMEI)
Vol.1, No.3 SEPTEMBER 2022
e-ISSN: 2963-7805; p-ISSN: 2963-8208, Hal 69-88

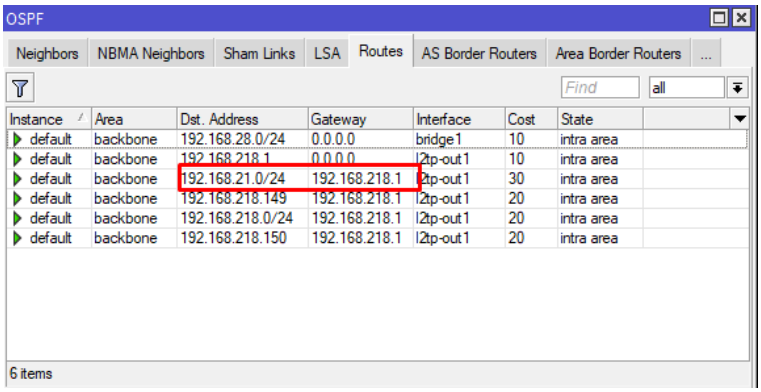


Gambar 17. Pengujian Netwatch

Setelah pengujian terhadap penerapan *FailOver* selesai, selanjutnya pengujian terhadap implementasi OSPF dengan VPN L2TP, untuk mengetahui hasil dari distribusi *routing* dinamik OSPF sudah berjalan dapat dilakukan pengecekan pada menu *routing*, lalu pilih OSPF, pilih tab *Routes*.

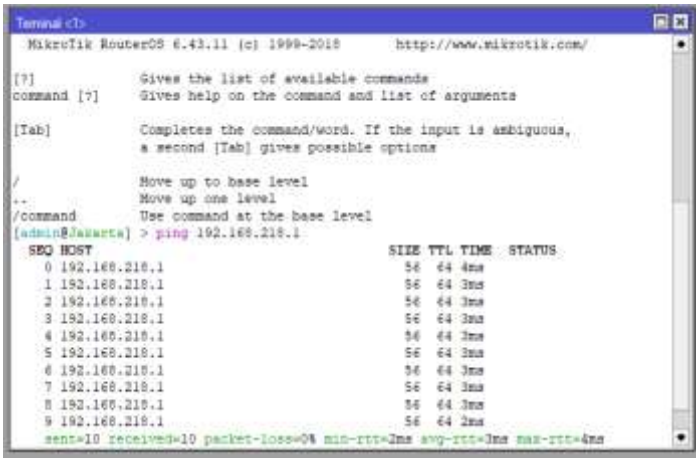


Gambar 18. Table Routing OSPF pada Mikrotik cabang Jakarta



Gambar 19. Table Routing OSPF pada Mikrotik cabang Semarang

Setelah semua cabang terkoneksi pada server VPN dan terkonfigurasi OSPF, maka dilakukan pengujian ping dari router. Untuk hasil berupa *Reply* tanpa *error* menandakan bahwa interkoneksi telah berhasil dilakukan.

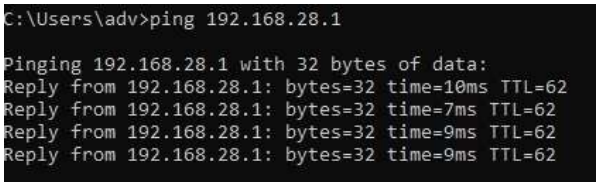


Gambar 20. Ping Dari Kantor Jakarta ke Server VPN

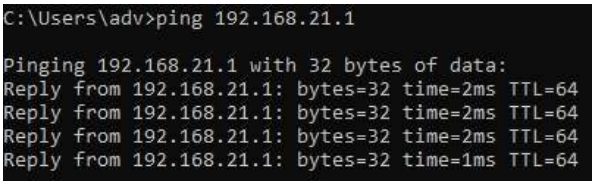
Gambar 21. Ping Dari Kantor cabang Semarang ke Server VPN

e-ISSN: 2963-7805; p-ISSN: 2963-8208, Hal 69-88

Setelah dilakukan pengujian pada router, maka selanjutnya pengujian dilanjutkan terhadap komputer user di kedua jaringan tersebut. Didapatkan hasil ping yang dilakukan di CMD dapat saling berkomunikasi pada kedua cabang tersebut.



Gambar 22. Ping Dari PC di Jakarta ke PC di Semarang



Gambar 23. Ping Dari PC di Semarang ke PC di Jakarta

KESIMPULAN DAN SARAN

Proses monitoring dan maintenance terhadap jaringan di kantor-kantor cabang yang jauh jadi lebih mudah dan cepat karena menerapkan teknologi VPN L2TP IPSec dengan OSPF. Dengan penerapan VPN L2TP IPSec meningkatkan keamanan dalam transfer data karena segala hal yang sensitif untuk di publikasi dapat dilakukan cukup dengan jaringan lokal saja. User atau karyawan saat ini dapat mengakses segala hal yang ada di lokal dimanapun mereka berada karena penerapan VPN ini. Tim IT lebih mudah dalam meremote ke kantor cabang saat sedang ada kendala, karena bisa langsung menggunakan aplikasi Winbox saat akses ke router cabang. Dengan menerapkan *Failover link* mengurangi terjadinya downtime yang lama ketika kantor-kantor cabang mengalami kendala pada jaringan utamanya. Untuk kedepannya, perlu dilakukan peningkatan terhadap perangkat perangkat yang sudah lawas dengan menggunakan antivirus tambahan selain antivirus bawaan windows seperti windows defender. Pada penggunaan

jaringan kantor baiknya menggunakan ISP yang non home atau bisnis, dengan tujuan meningkatkan kualitas jaringan itu sendiri.

DAFTAR REFERENSI

Budiman, A., Samsugi, S., & Indarto, H. (2019). Simulasi Perbandingan Dynamic Routing Protocol Ospf Pada Router Mikrotik Dan Router Cisco Menggunakan Gns3 Untuk Mengetahui Qos Terbaik. *Prosiding Seminar Nasional*, *4*, 16–20.

Fathsyah, M. M., Hadi, I., & Salamah, I. (2021). Implementasi Virtual Private Network Failover Menggunakan Mikrotik Pada Jaringan Lokal Politeknik Negeri Sriwijaya. *Jurnal Teknik Komputer*, *7*(2), 222–228.

Musyaffa, N., & Ryansyah, M. (2020). Implementation of VPN Using Router MikroTik at Al-Basyariah Education Foundation Bogor. *Jurnal Teknik Informatika CIT Medicom*, *12*(2), 49–55.

Nusantara, U., Guru, P., Indonesia, R., & Kediri, U. N. P. (2017). *ANALISIS DAN SIMULASI JARINGAN OSPF YANG BERACUAN PADA PT . SUPRA PRIMATAMA NUSANTARA Oleh : Dibimbing oleh : SURAT PERNYATAAN ARTIKEL SKRIPSI TAHUN 2017 Yang bertanda tangan di bawah ini : 01*(09).

Putra, J. L., Indriyani, L., & Angraini, Y. (2018). Penerapan Sistem Keamanan Jaringan Menggunakan VPN Dengan Metode PPTP Pada PT. Asri Pancawarna. *IJCIT (Indonesian Journal on Computer and Information Technology*, *3*(2), 260–267.

Sjafrina, F. (2019). Rancang Bangun Jaringan VPN Berbasis IPSEC Menggunakan Mikrotik Routerboard Pada PT. Zahir Internasional. *Proc. of the Seminar Nasional Teknologi Informasi Dan Komunikasi STI&K (SeNTIK 2019)*, *3*, 211–217.

Suryanto, Teguh Prasetyo, N. H. (2018). Implementasi Load Balancing Menggunakan Metode Per Connection Classifier (PCC) Dengan Failover Berbasis Mikrotik Router (Studi Kasus PT. Sumber Rejeki Power). *Seminar Nasional Inovasi Dan Tren (SNIT)*, *1*(1), A230–A238.

Syarief, A. F., & Rochmah, D. A. (2021). DISTRIBUSI JARINGAN PUBLIK MENGGUNAKAN ROUTING OSPF DENGAN METODE REDISTRIBUSI INFRASTRUKTUR TERPUSAT. *Jurnal Ilmiah Informatika Komputer*, *26*(3), 217–232. https://doi.org/10.35760/ik.2021.v26i3.5478

Zamalia, W. O., Aksara, L. M. F., & Yamin, M. (2018). Analisis Perbandingan Performa Qos, Pptp, L2Tp, Sstp Dan Ipsec Pada Jaringan Vpn Menggunakan Mikrotik. *SemanTIK*, *4*(2), 29–36.