E-ISSN : 2623-1700
P-ISSN : 1693-3672

Implementasi VPN Server Menggunakan Protokol L2TP dan IPSEC Pada PT. Multi Terminal Indonesia

Hermawan FIkri, Mugi Raharjo

Program Studi Informatika, Fakultas Teknologi Informasi
Universitas Nusa Mandiri
Hermawanfikri8@gmail.com, Mugi.mou@nusamandiri.ac.id

Abstrak

Penelitian ini dilakukan bertujuan untuk membantu dalam pengaktifan dan keamanan perangkat hardware maupun software dengan menggunakan jaringan vpn l2tp/ipsec server dan client. yaitu menkonfigurasi network router mikrotik berbasis vpn l2tp/ipsec server dan client, dengan cara menghubungkan dua jaringan public dijadikan satu jaringan local. dan adapun perangkat hardware atau software yang dimaksud yaitu system keuangan SAP, Perangkat telpon avaya, dan monitorin cctv. Dengan dibuatnya jalur vpn l2tp server dan client ini bisa membantu dan memudahkan karyawan dalam bekerja, baik di area cabang maupun di area luar kantor PT. Multi Terminal Indonesia. Untuk metode analisis yang digunakan dalam penelitian/riset ini yaitu metode grounded, dimana metode grounded sendiri dilaksanakan dengan mengadakan data yang ada di lapangan, baik dalam perumusan masalah,membangun hipotesis, maupun penarikan simpulan penelitian. Oleh, karena itu penelitian ini sangat bergantung pada pengalaman dan kredibilitas peneliti.

Kata Kunci : Jaringan, VPN, L2TP, IPSec

Abtract

This research was conducted with the aim of assisting in the activation and security of hardware and software devices using a VPN L2TP/IPSec server and client network. namely configuring a Mikrotik router network based on VPN L2TP/IPSec server and client, by connecting two public networks into one local network. and the hardware or software devices in question are the SAP financial system, Avaya telephone devices, and CCTV monitoring. By creating a VPN L2TP server and client path, it can help and facilitate employees in working, both in branch areas and in areas outside the PT office. Multi Terminal Indonesia. The analysis method used in this research is the grounded method, where the grounded method itself is carried out by holding data in the field, both in formulating problems, building hypotheses, and drawing research conclusions. Therefore, this research is very dependent on the experience and credibility of the researcher.

Keywords: Network, VPN, L2TP, IPSec

PENDAHULUAN

VPN adalah sebuah Teknologi komunikasi antar jaringan yang berbeda yang berarti menciptakan jaringan *private* dengan cara *virtual* di atas jaringan *public* (umum) dengan menggabungkan dua atau lebih *provider* menjadi satu jaringan *local*.

Jaringan komputer yakni jenis sistem telekomunikasi yang memfasilitasi pertukaran data dan komunikasi antar komputer. Perangkat keras dan perangkat lunak digabungkan untuk membangun jaringan. Disebut sebagai *client* dan *server*, komponen jaringan tertentu berfungsi sebagai penerima atau penyedia layanan ketika dua atau lebih komputer dihubungkan untuk bertukar data. *Design* sistem ini sering dinamakan *Client-Server*.[1]

Kumpulan perangkat yang terhubung dengan kemampuan untuk berkomunikasi satu sama lain disebut jaringan. Di sisi lain, dibandingkan dengan *Wide Area Network* (WAN). internet mengacu pada jaringan yang terhubung yang mencakup wilayah yang lebih luas. Dengan penggunaan *Virtual Private Network* (VPN) menjadi sebuah cara untuk menjaga dan mengamankan transfer data melalui internet. Istilah "*Virtual Private Network*" atau VPN itu sendiri mengacu pada koneksi *virtual private* yang menghubungkan komputer ke jaringan publik tanpa memerlukan hadirnya jaringan fisik.[2]

Salah satu komponen penting yang mempengaruhi banyak aspek kehidupan, termasuk pendidikan, adalah jaringan komputer. Peran ini menjadi semakin penting seiring dengan kemajuan teknologi komputer, khususnya di bidang jaringan.[3] Koneksi yang sifatnya *virtual* dan *private* disebut sebagai VPN. Adapun alasan mengapa dinamakan *virtual* adalah karena jaringan ini tidak ada dalam bentuk fisik. Bersifat pribadi atau *private* karena tidak semua orang memiliki akses ke jaringan ini dan dibatasi. Jaringan VPN menghubungkan komputer pribadi ke internet atau jaringan *public*, tetapi tidak semua orang dapat terhubung atau menggunakannya. Demikianlah, keamanan data menjadi sangat penting.[4] Pembuatan *VPN* adalah salah satu cara dalam meningkatkan keamanan data dalam jaringan komputer (*Virtual Private Network*) *VPN* dapat mengirim data pengguna melalui layanan jaringan publik yang murah, khususnya melalui internet. Perihal tersebut tidak terlepas dari penggunaan jaringan internet yang dapat saling terhubung satu sama lain.[5]

Penerapan beragam teknologi jaringan komputer dilaksanakan agar memperoleh performa jaringan yang optimal yang diperlukan oleh setiap perusahaan. Oleh karena itu pengamanan ketika mengirim atau menerima data sangat krusial dilaksanakan supaya data yang dikirim tidak jatuh pada pihak ketiga atau pihak yang tidak memiliki kepentingan, apalagi jika data tersebut bersifat mendesak atau rahasia.[6] Oleh karenanya dalam menyelesaikan permasalahan sebelumnya diperlukan pembuatan rancangan jaringan *Virtual Private Network (VPN)* dengan metode tunneling mode dapat *Layer2 Tunneling Protocol (L2TP)* yang dikolaborasikan dengan *IPSec* (*Internet Protocol Security*) serta mikrotik. Sejatinya *VPN* merupakan jaringan pribadi yang bersifat *private* (tidak dapat diakses untuk umum) tetapi senantiasa dapat akses jaringan internet dalam mengkoneksikan *remote* perangkat jaringan secara aman serta efisien. Adanya kolaborasi enkripsi serta tunneling selaku alternatif dalam menanggulangi permasalahan keamanan pada jaringan.[7]

L2TP merupakan tunneling protokol yang memadukan dua buah protokol yaitu Layer 2 Forwarding milik Cisco dan PPTP milik Microsoft. Umumnya digunakan untuk membuat Virtual Private Dial Network (VPDN) yang biasanya menggunakan port 1702 dengan protokol UDP.[8]

Perihal *protocol VPN (Virtual Private Network)* dipahami menjadi Solusi Alternatif dalam menyelesaikan permasalahan lalulintas jaringan yang terdapat pada cabang-cabang PT Multi Terminal Indonesia yang sudah beroperasi hingga saat ini. Kelebihan dari penggunaan sistem tersebut dalam aspek efisiensi biaya yaitu tidak mengeluarkan biaya sama sekali dikarenakan sudah ada perangkat pendukung sebelumnya yakni router OS Mikrotik dan berdasarkan aspek efisiensi waktu yakni tidak diperlukan datang kembali ke kantor cabang dalam waktu yang di tentukan, dikarenakan sudah menerapkan settingan *vpn L2TP Server* dan *Client* oleh karenanya bisa dilaksanakan *remote access* dalam jarak jauh sehingga pekerjaan akan lebih cepat selesai. Dengan dapat jaringan *public* tersebut maka user dapat mengakses berbagai fitur yang terdalam didalam jaringan lokal yang dimilikinya, memperoleh hak serta pengaturan yang sama seperti dengan cara fisik terdapat ditempat yang mana jaringan *local* tersebut hadir.

Pada proses perancangan, penulis dapat

perangkat Router mikrotik. Implementasi *VPN* dilaksanakan dengan dapat Tipe *Site to Site*. Protocol *VPN* yang dipakai yaitu *L2TP (layer 2 tunneling protocol)* dikarenakan kerap dipakai di sebagian besar *OS (Operting Sistem)* bisa menggerakkan *L2TP Server* maupun *Client* sekaligus mudah didalam pengembangan Implementasi.

Merujuk permasalahan sebelumnya, penulis mengambil judul "Implementasi VPN Server Dapat Protokol L2TP Dan IPSec Pada PT. Multi Terminal Indonesia" agar menjadi referensi bagi pihak perusahaan dalam menyelesaikan permasalahan yang hadir dalam perusahaan tersebut. Adapun maksud dan tujuan dari penulis dalam mengimplementasikan jurnal ini antara lain, Menganalisis berbagai masalah yang muncul dalam jaringan komunikasi pada PT. Multi Terminal Indonesia, Mengingkatkan efisiensi biaya dan efisiensi waktu serta memaksimalkan produktifitas kerja karyawan dengan adanya system jaringan *virtual private network (VPN),* Membantu Divisi IT dalam mengupdate topologi jaringan untuk kebutuhan dan kemudahan dalam *maintenance network*, Mempermudah dalam *Akses* dan *control* jaringan dengan dapat *remote access,* Implementasi jaringan *VPN (Virtual Private Network)* dengan metode *VPN L2TP.*

Adapun tujuan lain dari terbentuknya jurnal yang di buat oleh penulis yaitu untuk kebutuhan syarat kelulusan program strata satu(s1), dan untuk menambah ilmu khususnya untuk penulis maupun untuk orang lain, dan mudah-mudahan dapat bermanfaat untuk orang banyak.

METODE

Adapun metode penelitian adalah salah satu cara bagaimana penulis bisa memahami pembahasan, permasalahan, dan pemecahan masalah pada suatu sistem. Selanjutnya merupakan metode penelitian yang penulis pakai ada beberapa cara metode antara lain.

Metode Observasi, yaitu meninjau langsung serta melakukan pengamatan terhadap proses kerja secara khusus pada aspek jaringan *Local Area Network (LAN)* serta *Wide Area Network (WAN)* pada PT. Multi Terminal Indonesia.

Metode Wawancara, yaitu Mengumpulkan data serta informasi dengan cara melaksanakan tanya jawab dengan cara langsung serta sistematis, sekaligus penulis melakukan wawancara langsung kepada *Asisten Manager* yaitu pak asep supriyadi dan karyawan yang dapat jaringan komputer pada PT. Multi Terminal Indonesia.

Metode Studi Kepustakaan, yaitu Agar dapat mengkaji permasalahan dengan cara menyeluruh yang berhubungan dengan skripsi, maka penulis berupaya melakukan studi kepustakaan yakni dengan mengumpulkan berbagai data teoritis serta mempelajari berbagai buku ataupun literature yang bertujuan agar dapat memperoleh berbagai teori dan bahan yang berkaitan dengan permasalahan tersebut. Selain mengumpulkan data penulis juga juga melakukan analisa penelitian antara lain.

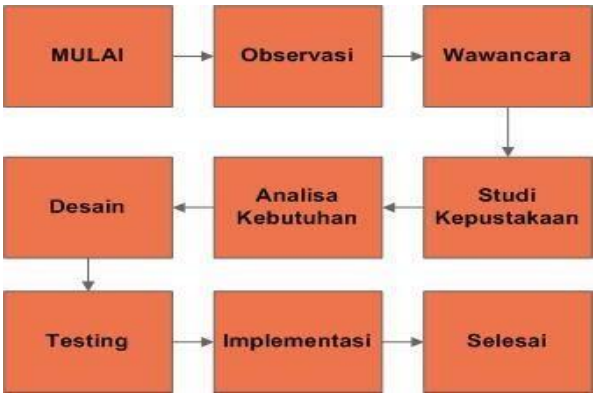
Analisa kebutuhan, Dalam tahapan ini dilaksanakan analisis kebutuhan apa saja yang dipakai dalam merancang jaringan *private* dalam *transfer* data yang semakin aman dengan *L2TP IPSec* misalnya router mikrotik serta winbox.

Desain, Berdasarkan berbagai data yang didapat sebelumnya, tahapan desain ini dapat menyusun gambar desain topologi jaringan *virtual private network (VPN)* dengan *L2TP IPSec* dapat *Microsoft Office Visio.*

Testing, Pada tahap ini penulis melakukan testing dengan cara mensetting 1 Unit PC yang ada dikantor pusat dengan sistem jaringan *VPN* dapat metode *L2TP IPSec* oleh karenanya bisa senantiasa terkoneksi serta terhubung.

Implementasi, Ditahap ini hendak diterapkan seluruh hal yang sudah direncanakan dan dirancang sebelumnya. Tahapan penerapan implementasi tersebut merupakan tahapan yang sangat menentukan keberhasilan atau gagalnya project yang hendak dibuat.

Gambar 1. Tahapan Penelitian dan Analisa



Analisa penelitian yang penulis lakukan yang terlihat pada gambar 1 adalah tahapan penelitian dan analisa, dimulai dari melakukan observasi dan di akhiri dengan implementasi, adapun penelitian

dan analisa ini penulis dapatkan dari hasil riset lapangan, dan merujuk pada analisa kebutuhan user yang ada pada PT. Multi Terminal Indonesia.

Pada metode dan analisa ini penulis membuat batasan sekadar pada perancangan dan penginstalan jaringan *VPN* dapat metode *L2TP server* dan *client* pada PT. Multi Terminal Indonesia kantor pusat dengan kantor cabang yang berlokasi di semarang. Serta *update topologi* yang dipakai saat ini yakni *topologi* dapat *topologi star*, dalam perancangan tersebut perangkat yang dipakai sekadar pada router yakni mikrotik router OS, dan ada pula perangkat lainnya yang berkaitan yakni perangkat pendukung. Tidak membahas metode keamanan *VPN* secara mendetail serta terperinci, serta fokusnya sekadar pada komunikasi *VPN* dalam kemudahan Akses dan kontrol jaringan.

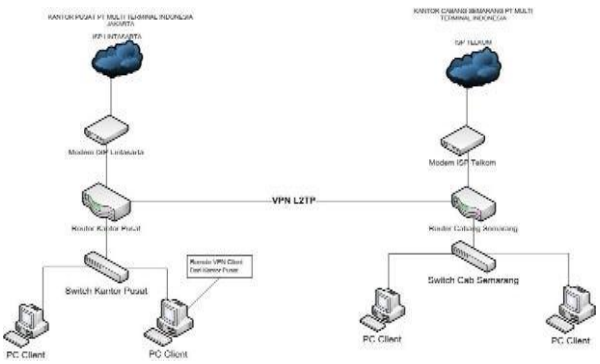
HASIL DAN PEMBAHASAN

Setelah penulis menjalani Proses analisa dan pengamatan pada sitem jaringan yang telah berjalan, penulis mempunyai konsep usulan dari permasalahan yang ditemukan setelah melakukan riset tidak jauh berbeda dalam penerapan jaringan maupun topologi yang sudah berjalan pada PT. MTI, yaitu pada penggunaan *VPN* dengan *protocol L2TP* dan *IPSec*. Dengan menghubungkan lalu lintas antar jaringan kantor pusat MTI dan kantor cabang MTI semarang dan cabang-cabang lain, sebagaimana PT. MTI sendiri mempunyai beberapa cabang di pulau jawa maupun diluar pulau Jawa. Dengan penerapan *VPN protocol L2TP* dan *IPSec* ini penulis mengharapkan dapat mempermudah karyawan dalam bekerja.

A. Skema Jaringan Usulan

Adapun dalam penerapan topologi pada PT. MTI sendiri yaitu Penggunaan *VPN* dengan *protocol L2TP* dan *IPSec*, dengan penerapan topologi ini dapat mempermudah team IT dalam maintenace jaringan dari jarak jauh dengan remote access mikrotik langsung, dan juga dapat menambah keamanan jaringan pada router mikrotik dengan penerapan IPSec.

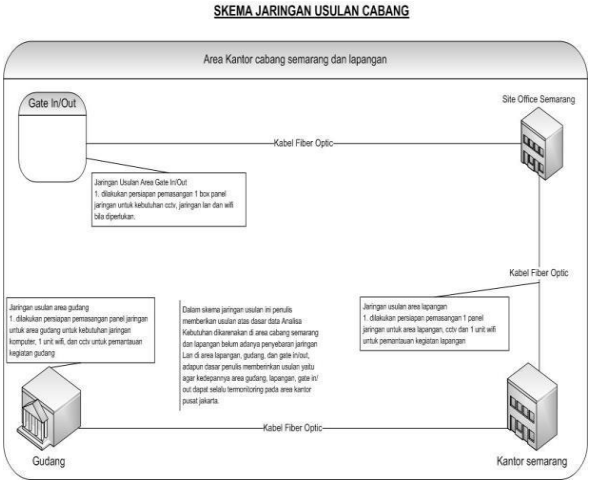
pada konsep jaringan yang penulis telah uraikan yaitu terdapat *VPN L2TP Server* utama pada kantor MTI pusat Jakarta dan *VPN L2TP Client* terdapat pada cabang-cabang kantor MTI, dengan penggunaan skema ini team IT bisa dengan mudah dalam memanagemen jaringan dari jarak jauh, dan adapun skema topologi terdapat pada gambar dibawah.



Gambar 2. Skema VPN Kantor Pusat dan Cabang

Pada gambar 2 di atas skema VPN kantor Pusat dan cabang, dapat di simpulkan bahwa harus di lakukan konfigurasi jaringan VPN Server dan Client dengan protokol L2TP dan IPSec, untuk menghubungkan kedua kantor menjadi satu jaringan local. Adapun skema vpn ini dibuat yaitu untuk kebutuhan perangkat hardware dan software yang harus berjalan pada cabang area semarang, perangkat tersebut meliputi telpon avaya, monitoring cctv untuk kebutuhan monitoring pada area jakarta pusat, dan aplikasi SAP Keuangan.

Adapun skema jaringan tambahan yang penulis usulkan adalah skema jaringan yang terdapat pada cab semarang dikarenakan setelah dilakukan wawancara dan riset langsung terdapat cabang semarang yang baru berpindah lokasi office, skema tersebut merujuk pada kebutuhan area lapangan, gudang, gate in/out.



Gambar 3. Skema usulan Kantor cabang semarang dan lapangan

E-ISSN : 2623-1700
P-ISSN : 1693-3672

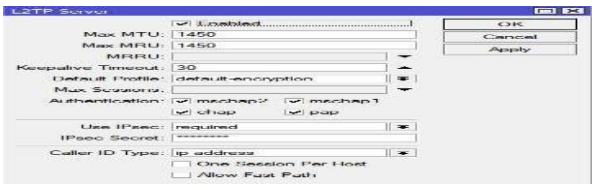
Pada skema gambar 3 di atas terdapat empat pembagian yang penulis bagi untuk kebutuhan skema topologi dan kebutuhan kedepannya yang di perlukan cabang semarang, kebutuhan ini penulis buat atas dasar hasil riset pada lapangan area jakarta yang sudah di observasi oleh penulis, adapun penjelasan skemanya sebagai berikut. Terdapat kantor semarang yang sudah memiliki akses internet yang di dapatkan dari ISP NEXA, dan untuk pembagiannya sendiri penulis mengusulkan untuk dilakukan penarikan kabel FO ke area Gudang, site office, dan gate in/out, dan dilakukan pemasangan masing-masing satu box panel dan perangkat seperti converter, switch POE dan switch unmanage. Adapun penulis mengusulkan skema topologi berdasarkan analisa kebutuhan kedepannya bila di perlukan cctv, internet lan, dan wifi di area gudang, lapangan dan gate in/out.

A. Rancangan Aplikasi

Pada perancangan yang akan dibuat oleh penulis bahwa akan diterapkan satu router yaitu sebagai *VPN L2TP Server* pada kantor MTI Pusat dan satu router lainnya sebagai *VPN L2TP Client*, dan akan di konfigurasi menggunakan aplikasi winbox dan dibuat jalur *VPN L2TP* dan *IPSec*.

1. Tahapan Konfigurasi *L2TP/IPSec Server kantor Pusat MTI*

Pertama kita buka aplikasi winbox, Trus ke bagian *PPP>L2TP Server*, centang pada bagian *enable***,** dan untuk bagian *use Ipseq* nya pilih *required* trus dilanjud ke bagian *IP Seq Secred* masukan *password* sesuai yang kita inginkan, trus klik *apply* dan ok, dan disisi server sudah kita setting untuk *VPN L2TP/Ipseq.*

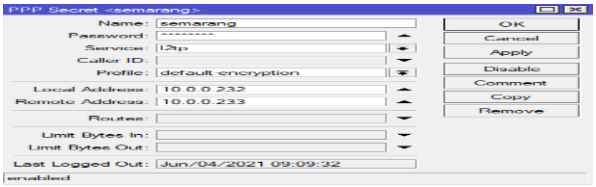


Gambar 4. Konfigurasi *L2TP/IPSec Server*

Langkah selanjudnya kita cek di bagian *IP>Ipseq>Peers* dan akan muncul *L2TP IN Server*, untuk sisi server sudah kita setting *VPN L2TP/IPSeq*, Tampilan gambar Sebagai berikut.

Gambar 5. *IPSec Peers*

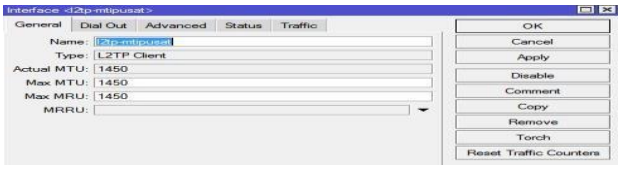
Kemudian langkah selanjutnya pembuatan *username* dan *password* pada menu *secret* pada router server dengan cara ke menu *PPP>Secrets>Tambah*, tampilan gambar sebagai berikut



Gambar 6. *L2TP Secre*

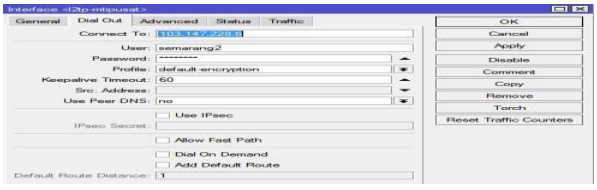
2. Tahapan Konfigurasi L2TP/IPSec Client Kantor Cabang Semarang

Dari sisi *Client* kita setting pada bagian *PPP>Tambah>L2TP Client* dan pada menu general kita kasih nama *L2TP MTI Pusat***.** dilanjut ke menu *Dial Out* dan kita isi *Connect To* yaitu ip public dari kantor MTI Jakarta dan isi *user* dan *passwordnya*, Tampilan gambar sebagai berikut:



Gambar 7. *L2TP MTI Pusat*

Pada gambar IV.8 penulis melakukan *Dial Out* pada sisi *router client* ke router kantor pusat, dan *Connect To* diisi *ip public* dari kantor MTI Jakarta dan isi *user* dan *passwordnya* yang telah dibuat pada router MTI Pusat, Tampilan gambar sebagai berikut:



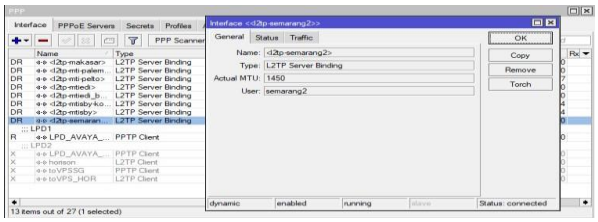
Gambar 8. *L2TP* MTI Pusat *Dial out*

Dibagian *Use IPSeq* kita centang dan isi *Password IPSeq Secrednya* yang sudah kita buat pada Router MTI Jakarta, Tampilan gambar sebagai berikut:

E-ISSN : 2623-1700
P-ISSN : 1693-3672

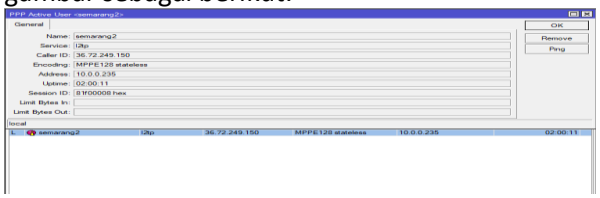
Gambar 9. *L2TP* MTI Pusat dan Use IPSec

Dan setelah proses *dial up* berhasil maka akan mendapatkan *interface* baru sesuai nama yang kita buat, dan di samping kiri akan muncul *flag DR* yang artinya *Dinamic Running*. Tampilan seperti gambar berikut:



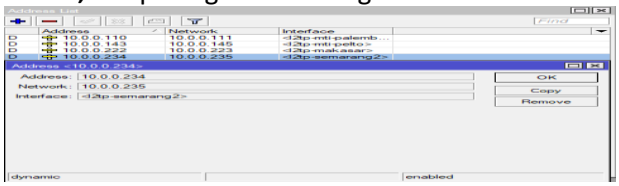
Gambar 9. *Interface L2TP* Semarang

Kemudian kita cek disisi router server kantor pusat pada menu *PPP>active connections* dan akan terlihat router *client* cabang melakukan *Dial up* menggunakan *username* Semarang2, tampilan gambar sebagai berikut:

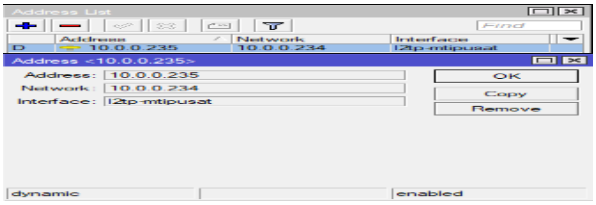


Gambar 10. *L2TP Active Connections Router Client*

Langkah selanjutnya kita cek pada masing-masing router server kantor pusat dan router *client* cabang pada menu *IP>Address* akan muncul ip baru yang bersifat *dinamis* pada sisi router server dan pada router *client* kita akan mendapatkan beberapa IP yaitu *remote address* dan *local address* yang sudah kita setting sebelumnya pada router server di menu *Secret*, tampilan gambar sebagai berikut:



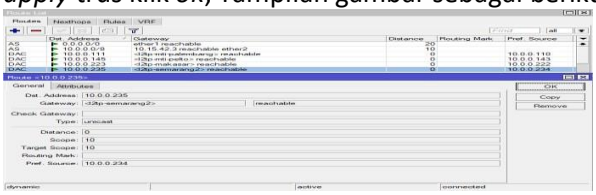
Gambar 11. *Address List L2TP* Cabang Semarang



Gambar 12. *Address List L2TP* Kantor Pusat

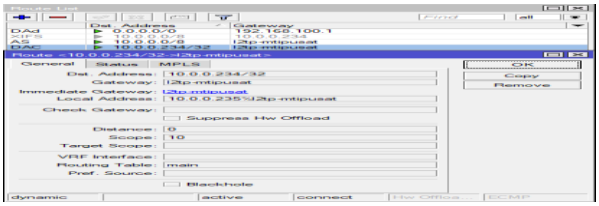
Kemudian langkah selanjutnya agar kedua LAN yang ada dimasing-masing kantor bisa saling terkoneksi kita harus menambahkan satu konfigurasi baru yaitu static routing pada setiap router masing-masing kantor dengan cara ke menu *IP>Route>Tambah.*

Setting disisi router server kantor Pusat, pada tab *Dst. Address* isikan alamat *IP Lan* pada kantor *Client* dan *Gateway* kita pilih *interface L2TP Client* trus klik *apply* trus klik *ok*, Tampilan gambar sebagai berikut:



Gambar 13. *Routing L2TP* Kantor Pusat

Setting disisi router *Client* Cabang, pada tab *Dst. Address* isikan alamat *IP Lan* pada kantor Pusat dan *Gateway* kita pilih *interface L2TP* Kantor Pusat trus klik *apply* trus klik *ok*, Tampilan gambar sebagai berikut:



Gambar 14. *Routing L2TP* Kantor Pusat

Pengujian Jaringan

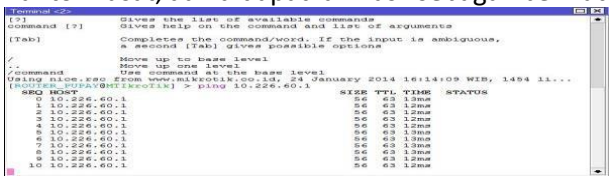
Pada pengujian jaringan ini tidak banyak pengujian yang dilakukan hanya pada *new terminal* yang ada pada *winbox* yaitu *ping ip* masing-masing router kantor pusat MTI dan router Kantor cabang semarang, adapun pengujian ini dilakukan untuk memastikan jalur VPN L2TP/IPSec sudah dalam satu jaringan.

A. Pengujian Jaringan Awal

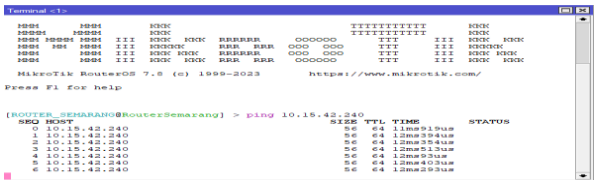
Pengujian *new terminal* pada *winbox* ke kantor pusat dan Kantor cabang semarang dengan mengakses *IP Router* Masing-masing dengan

E-ISSN : 2623-1700
P-ISSN : 1693-3672

menggunakan Router Kantor Cabang dan Router Kantor Pusat, dan didapatkan hasil sebagai berikut:



Gambar 15. Pengujian *Ping Router* Kantor Cabang



Gambar 16. Pengujian *Ping Router* Kantor Pusat

B. Pengujian Jaringan Akhir

Pada pengujian jaringan akhir ini akan dilakukan beberapa tes jaringan *VPN L2TP/IPSec* yaitu untuk pengujian apakah aplikasi SAP Keuangan, Telpon Avaya , dan Monitoring cctv bisa berjalan di area cabang maupun area pusat dan sudah melewati lalulintas jaringan pada kedua *ISP* dan dijadikan jaringan *local.*

Pengujian Aplikasi SAP Keuangan

Pada pengujian ini tentunya Penulis akan mencoba menginstal aplikasi SAP Keuangan di area cabang, dan ketika jalur internet sudah melewati jalur *VPN L2TP/IPSec* akan di tambahkan DNS Statik di router cabang sehingga aplikasi SAP bisa digunakan oleh Team Keuangan. Adapun penginstalan aplikasi SAP Keuangan di area cabang, pada tahap ini penulis akan menginstal aplikasi SAP Keuangan dan untuk penginstalan sendiri terdapat pada tampilan gambar sebagai berikut.

File Exe SAP

Pada gambar 17 file akan di extrac dan setelah selesai klik yes.

Gambar 17. Proses instal SAP

Kemudian pada gambar 18, klik next, dan next lagi.

Gambar 18. Proses lanjutan Instal SAP

Pada tampilan Gambar 19 akan dilanjutkan dengan klik next dan tunggu sampai proses instalasi selesai.

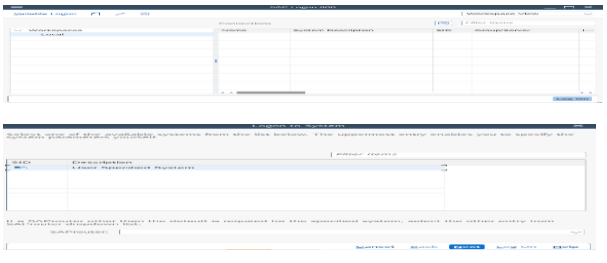
Gambar 19. Proses loading instalasi SAP

Setelah proses instalasi selesai pada gambar 20 akan muncul dibagian dekstop satu aplikasi SAP Logon.

Gambar 20. Tampilan Aplikasi SAP Logon

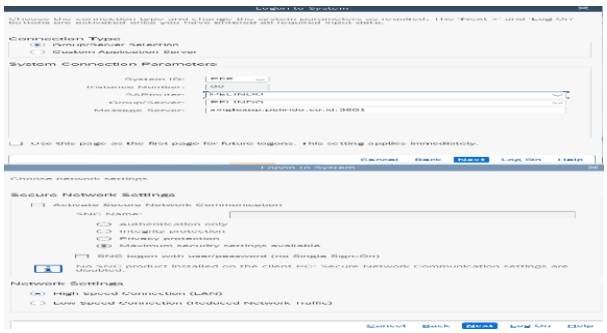
Konfigurasi aplikasi SAP Keuangan dan pengujian Jaringan *VPN L2TP IP/Sec*, tampilan pada gambar dibawah.

Untuk konfigurasi aplikasi SAP terdapat pada gambar 21 yaitu masuk aplikasi SAP Logon, Klik Log On, akan muncul tampilan baru dan klik next.



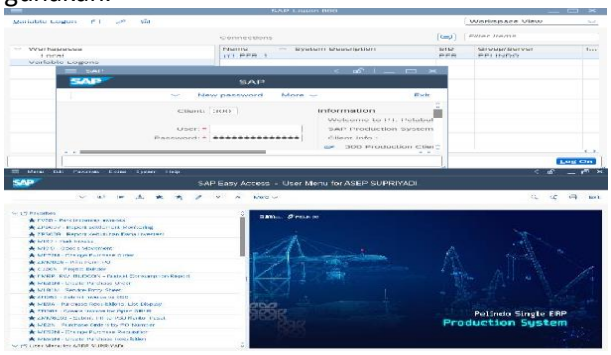
Gambar 21. Tampilan Awal SAP

Kemudian pada gambar 22 ini penulis mengsetting aplikasiSAP,PER>PELINDO>PELINDO>singlesap.pelindo.co.id:3601, klik next dan next.



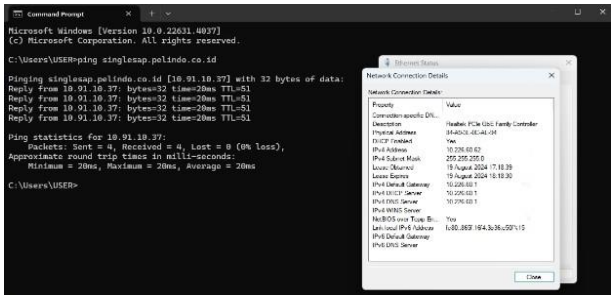
Gambar 22. Settingan alamat SAP

Tampilan Gambar 23, yaitu mencakup tampilan *login*. Setelah tampilan sudah seperti gambar dibawah aplikasi SAP Keungan sudah siap di gunakan.



Gambar 23. Tampilan Login Aplikasi SAP

Untuk pengujian sendiri mencakup *ping* alamat *DNS SAP* keuangan untuk mengetahui apakah aplikasi sudah melewati jaringan *VPN L2TP/IPSec*, tampilan pada gambar dibawah.

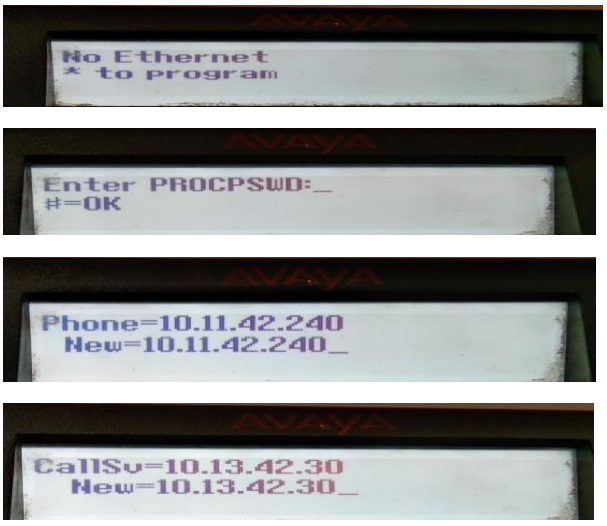


Gambar 24. Tampilan Login Aplikasi SAP

Pengujian Perangkat Telpon Avaya di area cabang

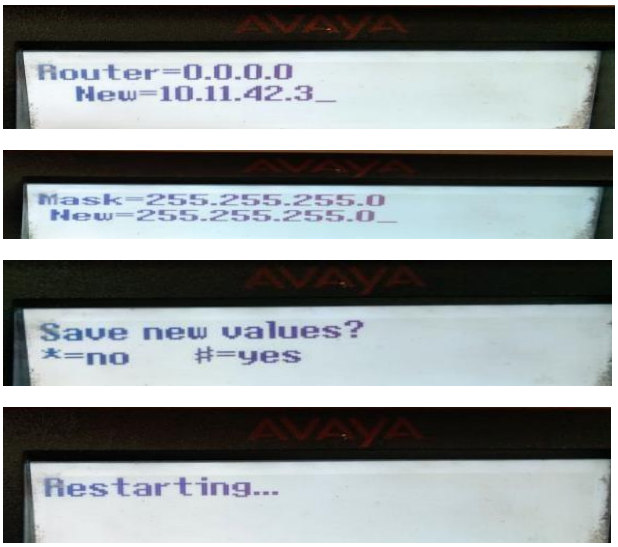
Seperti yang sudah di terapkan dibeberapa cabang yaitu untuk mempermudah komunikasi antar cabang dan kantor pusat perlu dilakukan settingan pada telpon avaya, tentunya pengujian pertama harus pada router yaitu jaringan sudah melewati jalur *VPN L2TP/IPSeq* yang telah di buat dan selanjutnya akan di lakukan setingan pada telpon avaya yaitu penyetingan ip address dan ip server avaya yang berada pada kantor pusat, setingan dan pengujian sebagai berikut:

Settingan Telpon Avaya berupa memasukan password untuk tampilan awal, dilanjut pada penyetingan ip address dan ip server avaya, tampilan seperti pada gambar dibawah:



Gambar 25. Konfigurasi avaya

selanjudnya masukan *gateway, subnetmask* nya trus tekan pagar dan telpon avaya akan terestart sendiri, tampilan pada gambar dibawah.

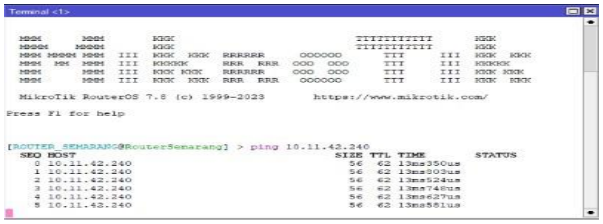


Gambar 26. Konfigurasi lanjutan avaya

tahap selanjutnya setelah disetting akan muncul tampilan seperti pada gambar dibawah, menandakan settingan sukses dan untuk mengecek

E-ISSN : 2623-1700
P-ISSN : 1693-3672

apakah telpon avaya sudah melewati jalur *vpn l2tp/ipseq* kita akan ping dari router ke ip server avaya.



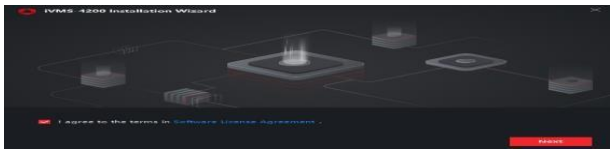
Gambar 27. Tampilan sukses dan pengujian

pengujian Monitoring CCTV Area Cabang

Pada pengujian Monitoring CCTV Area cabang ini yaitu hanya pada penginstalan Aplikasi IVMS 4200 untuk menampilkan CCTV pada area cabang, dan tentunya untuk keberhasilan pada pengujian ini jaringan harus sudah melewati jalur *VPN L2TP/IPSeq* yang telah di buat, dikarenakan ketika jaringan sudah dalan satu jaringan local kita bisa mengakses tampilan Monitoring CCTV dari jarak jauh, pengujian sebagai berikut:

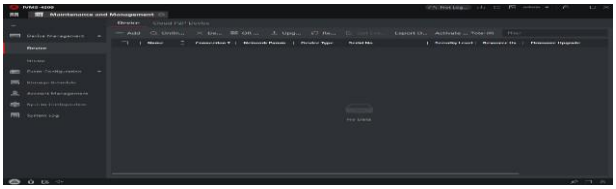
Instalasi Aplikasi Ivms Monitoring CCTV kantor Pusat.

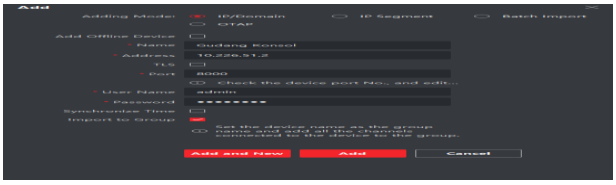
Klik file EXE Ivms , kemudian penulis melakukan instalasi dengan cara klik next>instal>Finish.

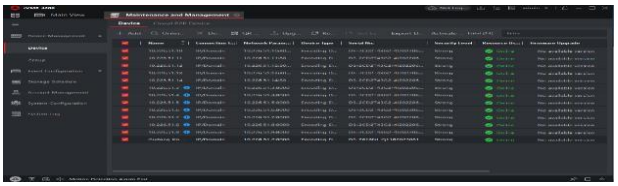


Gambar 28. Instal Aplikasi Ivms

Kemudian *Login* dan konfigurasi IP Address CCTV, NVR Cabang, pada konfigurasi ini kita akan *Add* ke aplikasi IVMS yaitu ditambahkan ip address NVR cabang, Tampilan pada gambar dibawah.

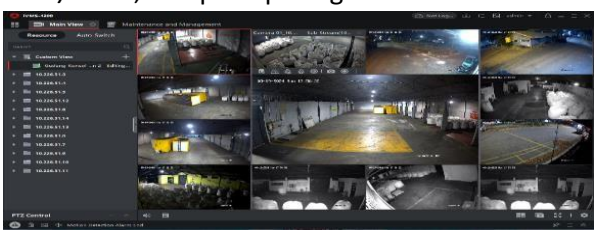




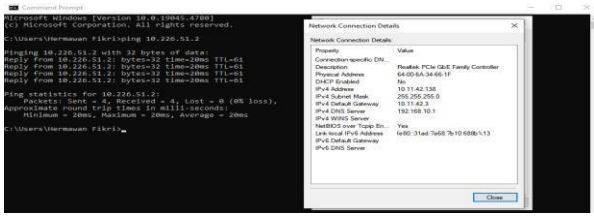


Gambar 29. Tampilan penyetingan ip address NVR

Tampilan CCTV Area Cabang dan Pengujian, pada pengujian Monitoring CCTV tidak banyak dilakukan yaitu hanya pada ping *IP Address* NVR, menunjukan jaringan sudah melewati jalur *VPN L2TP/IPSec*, Tampilan pada gambar dibawah.



E-ISSN : 2623-1700
P-ISSN : 1693-3672



https://ejournal.urindo.ac.id/index.php/TI/index

Gambar 29. Tampilan monitoring dan pengujian

KESIMPULAN DAN SARAN

Setelah dilakukan *Riset* pada PT Multi Terminal Indonesia, penulis menyimpulkan bahwa ada sedikit masalah pada jaringan. dan di antaranya penulis akan membahas pada skripsi ini tentang masalah aplikasi keuangan,telpon avaya, dan akses cctv cabang, maka bisa disimpulkan dengan diterapkannya jaringan *L2TP/IPSec* ini bisa di terapkan jaringan local dan bisa di akses di area cabang. Dan untuk akses karyawan dengan mobilitas tinggi yaitu penggunaan aplikasi keuangan di luar jaringan kantor pusat dan cabang. maka akan diterapkan yaitu VPN dengan Protocol L2TP dan IPSec. Adapun penulis menyimpulkan pada riset kali ini adalah sebagai berikut.

Setelah dilakukan Konsep *L2TP/IPSec* ini, Jaringan Pusat dan cabang sudah dalam satu jaringan local. Dan penggunaan aplikasi keuangan, telpon avaya, dan monitoring cctv bisa di gunakan di area cabang.

Pada menerapan *VPN* dengan *protocol L2TP* dan *IPSec* jaringan pada kantor Pusat MTI dan Cabang MTI bisa di akses darimanapun, selama perangkat client terhubung internet.

Pada penerapan VPN dengan *L2TP* dan *IPSec*, keamanan data akan terjaga. Yaitu dengan alamat IP tidak dapat terdeteksi pada saat client merequesh database keserver local.

Dari hasil riset dan pengamatan yang sudah dilakukan oleh penulis, dengan *VPN L2TP* dan *IPSec* ini dapat membantu dalam mempermudah karyawan dalam bekerja di luar area kantor dan keamanan dalam mengakses data, namun penulis menemukan bahwa ada beberapa router di area cabang yang belum menerapkan *IPSec*, oleh karena itu penulis menyarankan agar di lakukan settingan *IPSec* di router cabang-cabang yang belum menerapkan *IPSec*, dikarenakan penerapan *IPSec* sangat membantu untuk menjaga data diantaranya, menjaga keamanan router saat

mengirim data melalui internet public, mengenkripsi data aplikasi, mengautentikasi data dengan cepat jika data berasal dari pengirim yang dikenal, melindungi data jaringan dengan menyiapkan sirkuit terenkripsi, yang disebut terowongan IPSec yang mengenkripsi semua data yang dikirim Antara dua titik akhir.

DAFTAR PUSTAKA

[1] M. A. Gunawan and S. Wardhana, "Implementasi dan Perbandingan Keamanan PPTP dan L2TP/IPsec VPN (Virtual Private Network)," *Resist. (Elektronika Kendali Telekomun. Tenaga List. Komputer)*, vol. 6, no. 1, p. 69, 2023, doi: 10.24853/resistor.6.1.69-78.

[2] S. Sumarna and A. Maulana, "Implementasi Virtual Private Network Menggunakan L2TP/IPsec pada BBPK Jakarta," *Expert J. Manaj. Sist. Inf. dan Teknol.*, vol. 11, no. 2, p. 90, 2021, doi: 10.36448/expert.v11i2.1829.

[3] B. G. Rahino and A. Susila, "Implementasi Jaringan VPN (L2TP / Ipsec) Mikrotik Untuk Remote Access Sebagai Security Selama Work From Home," vol. 1, no. 11, pp. 1911–1918, 2022.

[4] Prayogi Wicaksana, F. Hadi, and Aulia Fitrul Hadi, "Perancangan Implementasi VPN Server Menggunakan Protokol L2TP dan IPSec Sebagai Keamanan Jaringan," *J. KomtekInfo*, vol. 8, no. 3, pp. 169–175, 2021, doi: 10.35134/komtekinfo.v8i3.128.

[5] J. Safira, P. Teknologi Rekayasa Jaringan Telekomunikasi Jurusan Teknik Elektro, and P. Negeri Lhokseumawe, "Implementasi Jaringan Vpn L2Tp / Ipsec Menggunakan Linux Di Laboraturium Jaringan Komputer," *J. Tektro*, vol. 5, no. 1, pp. 59–63, 2021.

[6] D. Bahtiar *et al.*, "Pengenalan Dasar Instalasi Jaringan Komputer," *J. Kreat. Mhs. Inform.*, vol. 2, pp. 507–518, 2021.

[7] I. K. Astuti, "Fakultas Komputer INDAH KUSUMA ASTUTI Section 01," *Jar. Komput.*, p. 8, 2018, [Online]. Available: https://id.scribd.com/document/503304719/jaringan-komputer

[8] A. Sayuti, A. Harist, M. Informatika, T. Komputer, and A. Bina Sriwijaya, "JURNAL PRASETIYA KOMPUTER Implementasi Hotspot RB951 di PT. Alam Lestari Unggul

E-ISSN : 2623-1700
P-ISSN : 1693-3672

Menggunakan Metode Network Development Life Cycle (NDLC)," vol. 1, no. 1, p. 2023, 2023, [Online]. Available: https://ojs.politeknikdarussalam.ac.id/index.php/prastikom

[9] S. ÖCAL, "No 主観的健康感を中心とした在宅高齢者における　健康関連指標に関する共分散構造分析Title," vol. 3, no. 2, p. 6, 2021.

[10] Fachrurrazy, " LANDASAN TEORI 2."

[11] A. I. Ardhitya, "Pengertian dan Penjelasan Mikrotik Arse Irawhan Ardhitya," 20019.

[12] Prayogi Wicaksana, F. Hadi, and Aulia Fitrul Hadi, "Perancangan Implementasi VPN Server Menggunakan Protokol L2TP dan IPSec Sebagai Keamanan Jaringan," *J. KomtekInfo*, vol. 8, no. 3, pp. 169–175, 2021, doi: 10.35134/komtekinfo.v8i3.128.