

Implementasi Virtual Private Network Menggunakan L2TP/IPsec pada BBPK Jakarta

Sumarna, Aditya Maulana*

STMIK Nusa Mandiri

Jakarta, INDONESIA

sumarna@nusamandiri.ac.id, adityamaulana759@gmail.com*

Abstract – Some companies already use computer networks as a tool to communicate, including companies that already have subsidiaries in various regions. This is inseparable from the use of an internet network that can be interconnected. In BBPK Jakarta network, data delivery and exchange conducted between Cilandak building employees and Hang Jebat building still use email and WhatsApp facilities. In addition to being less secure or having the possibility of being hacked by irresponsible parties, it is also constrained by the capacity limit of files to be sent in one delivery. VPN network is one of the facilities in microtic hardware that allows to create a network within an internet network. VPN network with L2TP/IPsec tunnel is expected to help communication, employee activities at head office and branch offices, increase shipping security and reduce the possibility of threats that can occur when sending data in the network.

Keywords: VPN; Mikrotik; Internet; L2TP; IPsec.

Abstrak – Beberapa perusahaan banyak yang sudah menggunakan jaringan komputer sebagai alat untuk berkomunikasi, termasuk perusahaan yang sudah memiliki anak cabang di berbagai daerah. Hal ini tidak terlepas dari penggunaan jaringan internet yang dapat saling terhubung. Pada jaringan BBPK Jakarta, pengiriman dan pertukaran data yang dilakukan antara pegawai gedung Cilandak dengan gedung Hang Jebat masih menggunakan sarana email dan WhatsApp. Selain kurang aman atau memiliki kemungkinan diretas oleh pihak yang kurang bertanggung jawab, juga terkendala batasan kapasitas file yang akan dikirim dalam sekali pengiriman. Jaringan VPN adalah salah satu fasilitas yang ada pada perangkat keras mikrotik yang memungkinkan untuk membuat sebuah jaringan didalam sebuah jaringan internet. Dengan adanya jaringan VPN dengan tunnel L2TP/IPsec ini diharapkan dapat membantu komunikasi, kegiatan pegawai pada kantor pusat dan kantor cabang, meningkatkan keamanan pengiriman dan mengurangi kemungkinan ancaman yang dapat terjadi saat pengiriman data dalam jaringan.

Kata Kunci: VPN; Mikrotik; Internet; L2TP; IPsec.

1. Pendahuluan

Dengan semakin berkembangnya teknologi informasi, komunikasi dan transfer data, penggunaan komputer menjadi salah satu kebutuhan pokok dalam menunjang pekerjaan. Beberapa perusahaan banyak yang sudah menggunakan jaringan komputer sebagai alat untuk berkomunikasi, termasuk perusahaan yang sudah memiliki anak cabang di berbagai daerah. Hal ini tidak terlepas dari penggunaan jaringan internet yang dapat saling terhubung.

Hampir semua instansi atau perusahaan baik pemerintah ataupun swasta menggunakan teknologi komputerisasi untuk operasionalnya, dan komputer 1 dengan komputer lainnya saling terhubung di dalam sebuah jaringan baik secara intranet (lokal) maupun internet. Jaringan pada BBPK Jakarta, dimanfaatkan untuk membantu menghubungkan komputer karyawan dan peserta pelatihan agar dapat mengakses internet. Serta dipergunakan mempermudah saat melakukan pekerjaan mereka seperti, bertukaran dan penyimpanan data. BBPK Jakarta sebagai pusat pendidikan dan pelatihan kesehatan terpadu yang berlokasi dan berpusat

di Cilandak, Jakarta Selatan memiliki cabang kampus yang berada di daerah Hang Jebat, Jakarta Selatan.

Pada jaringan di BBPK Jakarta belum adanya penghubung antar kantor pusat dan cabang sehingga pegawai mengalami kesulitan untuk mendapatkan informasi yang *up to date*, cepat dan aman dari kantor pusat atau cabang. kebutuhan informasi harus dapat diakses melalui jaringan komputer yang di desain untuk dapat mendapatkan informasi yang diperlukan dengan cepat, mudah, aman dan akurat [1]. Pengiriman dan pertukaran data yang dilakukan antara pegawai gedung Cilandak dengan gedung Hang Jebat masih menggunakan sarana *E-Mail*, *WhatsApp* dan *Google Drive*. Selain kurang aman atau memiliki kemungkinan diretas oleh pihak yang kurang bertanggung jawab, juga terkendala batasan kapasitas file yang akan dikirim dalam sekali pengiriman. Dalam jaringan komputer, “pengamanan saat mengirim atau menerima data sangat penting dilakukan agar data yang dikirim tidak jatuh ke pihak ketiga atau pihak yang tidak mempunyai kepentingan, apalagi jika data tersebut bersifat mendesak atau rahasia” [1].

Berdasarkan uraian permasalahan diatas penulis mengusulkan jaringan *Virtual Private network* menggunakan *Layer 2 Tunneling Protocols* pada Balai Besar Pelatihan Kesehatan Jakarta.

Jaringan komputer adalah sekumpulan komputer yang terhubung satu dan lainnya dan bekerja sama secara otomatis dengan menggunakan media transmisi sebagai jalur koneksi [2]. Pengguna jaringan komputer bisa saling bertukar dokumen maupun data melalui kabel atau *nirkabel*, dan menggunakan perangkat keras atau perangkat lunak yang terhubung ke jaringan yang sama secara bersama-sama.

Virtual Private Network (VPN) adalah suatu teknologi dari jaringan komputer yang dikembangkan sebuah perusahaan besar yang menggunakan internet membutuhkan keamanan komunikasi untuk dapat terhubung ke jaringan pada jaringan lain [3]. VPN adalah teknik pengaman jaringan yang bekerja dengan cara membuat suatu tunnel sehingga jaringan yang terpercaya dapat terhubung dengan jaringan yang ada di luar melalui internet [4].

Layer 2 Tunneling Protokol (L2TP) adalah salah satu *protocol tunneling* yang bias digunakan dan mendukung VPN [5]. L2TP juga merupakan *tunnel* yang standar dari satu *router* ke *router* lain atau dari *client* ke *host gateway* melalui *Network Access Server (NAS)* ISP yang pertama dianalisa oleh *server NAS* ISP dan jika autentikasi itu berhasil, lalu ISP membuatkan saluran dari *client* ke *host gateway* secara *Point-to-Point*. Untuk mendapatkan tingkat keamanan yang lebih baik, L2TP dapat dikombinasikan dengan *protocol tunneling IPsec* pada layer 3 [6].

IPsecurity (IPsec.) bisa juga disebut dengan rangkaian protokol yang menambahkan keamanan komunikasi pada tingkat IP [3].

2. Metodologi

A. Metode Pengumpulan Data

Dalam melakukan pengumpulan data untuk penulisan ini maka diperlukan data yang baik dan akurat sehingga penulis menggunakan beberapa metode pengumpulan data sebagai berikut:

- 1) Metode Observasi; Observasi pada penelitian ini dilakukan dengan cara pengamatan langsung terhadap proses kerja yang dilakukan di BBPK Jakarta khususnya bagian IT untuk mengumpulkan data dan informasi mengenai penggunaan dan perancangan VPN dengan L2TP/IPsec.
- 2) Wawancara; Untuk mendapatkan informasi secara

lengkap maka pada penelitian ini dilakukan dengan cara melakukan suatu metode tanya jawab langsung kepada bagian IT Support dan kepala BBPK Jakarta.

- 3) Studi Pustaka; Sementara untuk memperoleh tambahan materi pada penelitian ini yaitu dengan cara menganalisis buku-buku, majalah dan artikel yang berkaitan dengan *Virtual Private Network*.

B. Analisis Penelitian

Sebelum melakukan perancangan VPN, penelitian ini dilakukan analisis yang terbagi menjadi beberapa bagian yaitu:

- 1) Analisis Kebutuhan; Pada tahap ini dilakukan analisis kebutuhan apa saja yang digunakan untuk merancang Jaringan private untuk transfer data yang lebih aman dengan L2TP/IPsec seperti router mikrotik dan winbox.
- 2) Desain; Tahap ini penulis mulai merancang skema jaringan VPN dengan L2TP/IPsec menggunakan Microsoft Office Visio.
- 3) Testing; *Testing* yang dilakukan adalah mensetting PC yang ada di kantor pusat dan cabang dengan sistem jaringan VPN dengan metode L2TP/IPSec sehingga dapat selalu terkoneksi dan terhubung.
- 4) Implementasi; Pada tahap ini penulis menerapkan jaringan *Virtual Private Network* pada BBPK Jakarta menggunakan Mikrotik untuk implementasi jaringannya.

3. Hasil dan Pembahasan

Pada pembahasan ini penulis menjelaskan jaringan yang sedang diterapkan dan jaringan usulan, yaitu:

A. Jaringan yang Sedang Diterapkan

- 1) Topologi Jaringan

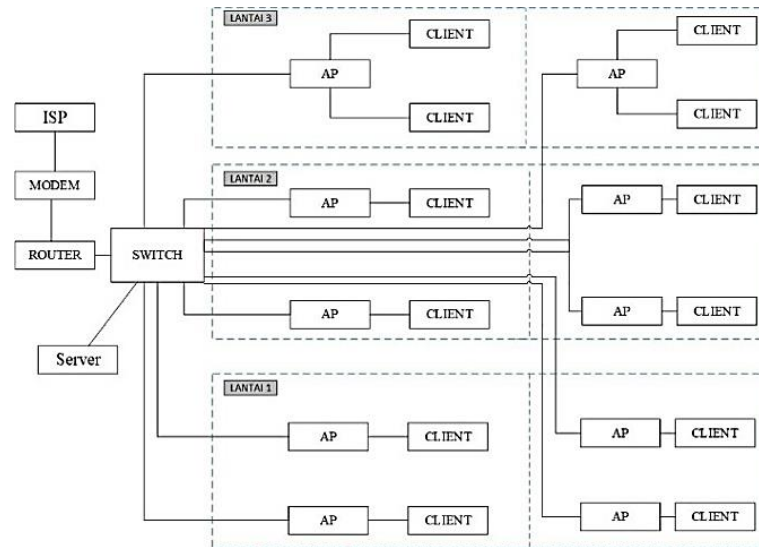
Jaringan BBPK Jakarta menggunakan topologi *extended star* dimana setiap *client* berkomunikasi langsung dengan *access point*, sedangkan *access point* berkomunikasi dengan *switch* yang kemudian terhubung dengan router. Akses internet didapat oleh sebuah ISP. Kemudian dihubungkan ke router. Router inilah yang menjadi pusat kontrol jaringan yang ada di BBPK Jakarta. Terdapat tiga lantai di BBPK Jakarta, ruangan pada tiap lantai memperoleh akses internet yang didapat dari ISP melalui *Access Point* yang dipasang pada masing-masing ruangan.

Tabel 1. Komponen Kantor Pusat Cilandak

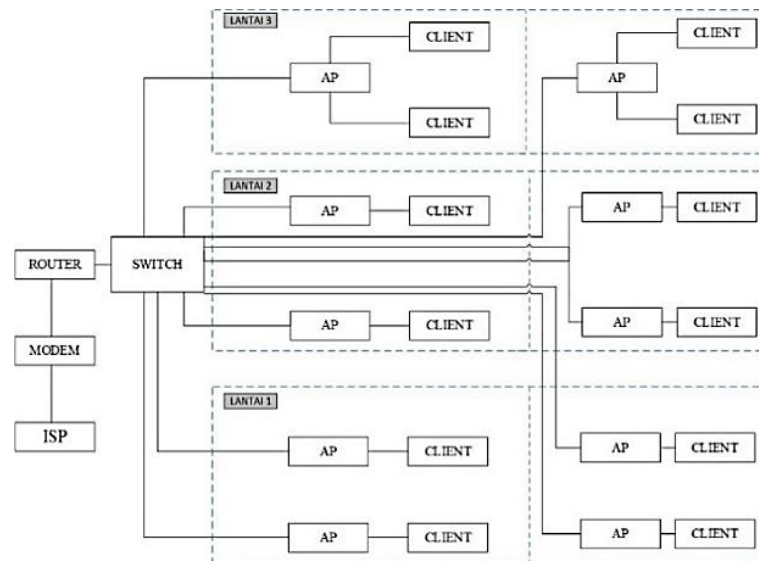
No	Komponen	Jumlah
1.	Router RB 1100AHx2	1
2.	Modem <i>ADSLHuaweiHG532G</i>	1
2.	Switch <i>Cisco Catalys 2960 48PSTL</i>	1
3.	Server HP Pro Liant ML 110	1
4.	Access Point Aruba IAP 303	10
5.	PC Pengguna	100

Tabel 2. Komponen Kantor Cabang Hang Jebat

No	Komponen	Jumlah
1.	Router RB 1100AHx2	1
2.	Modem <i>ADSLHuaweiHG532G</i>	1
2.	Switch <i>Cisco Catalysts 2960 48PSTL</i>	1
3.	Access Point Aruba IAP 303	10
4.	PC Pengguna	100



Gambar 1. Topologi Kantor Pusat Cilandak



Gambar 2. Topologi Kantor Cabang Hang Jebat

2) Skema Jaringan

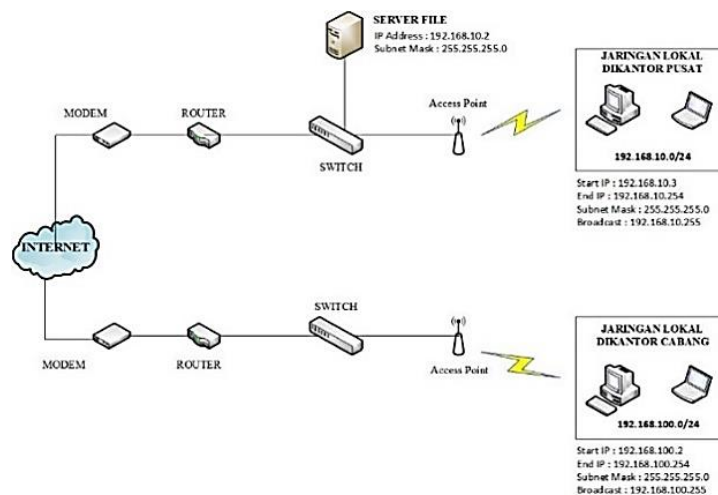
Secara umum jaringan pada BBPK Jakarta baik kantor pusat maupun kantor cabang dijelaskan di dalam skema jaringan Gambar 3. Jaringan pada Balai Besar Pelatihan Kesehatan Jakarta telah dijelaskan di dalam skema jaringan sebagai berikut:

- ISP; Akses internet yang didapatkan oleh pengguna di lingkungan jaringan BBPK Jakarta untuk menunjang pekerjaan sehari-hari, maka BBPK Jakarta berlangganan dengan salah satu penyedia

- layanan internet yaitu *Hypernet* dengan kecepatan *upload* dan *download* masing-masing *up to 100 Mbps*.
- Router; Router yang digunakan pada BBPK Jakarta adalah router Mikrotik RB 1100 AHx2. Router ini bertindak sebagai pusat kontrol jaringan yang berjalan. Ether 1 router terhubung dengan ISP lalu ether 2 terhubung ke *switch* nantinya akan terhubung ke *acces point* sebagai penghubung dengan PC *client* atau pengguna.

- c. *Server file*; Sever yang digunakan pada BBPK Jakarta adalah server HP Pro Liant ML 110. Server ini terdapat pada ruang *server* yang ada pada kantor pusat BBPK Cilandak. Server ini akan menjadi basis data yang akan mempermudah karyawan dalam mencari serta bertukar informasi yang berhubungan dengan kepentingan Pada BBPK Jakarta.
- d. *Switch*; *Switch* yang digunakan pada BBPK Jakarta adalah *Cisco Catalysts 2960 48PST-L*. *switch* ini terhubung dengan ether 2 router yang kemudian menjadi penghubung ke *access point* pada di tiap lantai yang ada di BBPK Jakarta.
- e. *Access Point*; *Access point* yang digunakan pada BBPK Jakarta adalah Aruba IAP 303. *Access point* ini terhubung pada perangkat sebelumnya yaitu *switch* yang kemudian akan terhubung ke pengguna untuk mendapatkan akses *internet*. Setiap PC atau *client*

- yang terhubung pada BBPK Jakarta melalui perantara *wireless* baik karyawan ataupun PC peserta pelatihan. PC atau laptop karyawan yang ingin terhubung ke dalam jaringan dapat melakukan koneksi ke dalam jaringan *wireless* dengan SSID “BBPK Jakarta” dengan *password* “kusuma2020”. Sebelum itu PC atau laptop karyawan harus didaftarkan *Mac Address* perangkat tersebut pada router mikrotik, karena keamanan jaringan *wireless* yang diterapkan adalah *Mac Address Filtering*.
- f. PC Pengguna; PC karyawan yang digunakan pada BBPK Jakarta adalah *HP Pavilion All-in-One 24 r0xx*. Akses internet didapat dengan melakukan koneksi ke perangkat *Wireless Access Point* yang terdapat di tiap ruangan. Komputer ini digunakan oleh pegawai untuk membantu kegiatan mereka sehari-hari seperti membuat, mengetik atau membuat laporan pada BBPK Jakarta.



Gambar 3. Skema Jaringan Berjalan

B. Jaringan yang Diusulkan

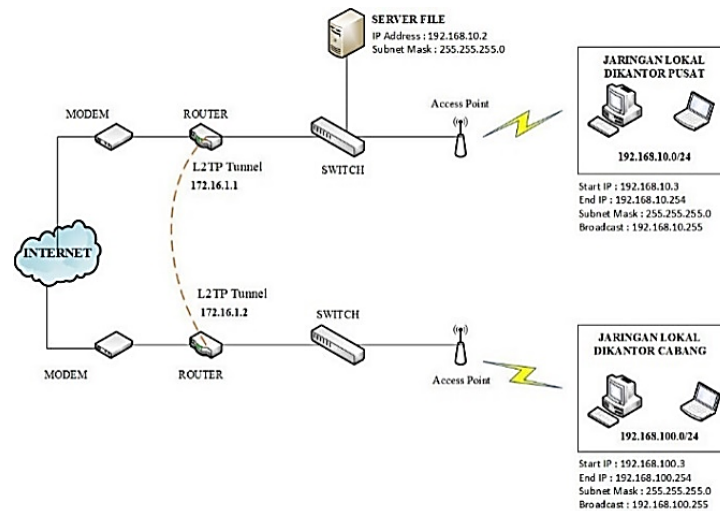
1) Topologi Jaringan Usulan

Penelitian ini tetap menggunakan topologi yang sudah berjalan, yakni topologi *extended star*, karena topologi *extended star* memiliki kelebihan dari segi infrastruktur jaringan, mudah dalam instalasi ketika adanya penambahan perangkat jaringan seperti *switch*, PC, *Access Point*. Konfigurasi yang diterapkan VPN (*Virtual Private Network*) menggunakan L2TP (*Layer 2 Tunneling Protocol*) antar Gedung Cilandak dan Gedung Hang Jebat sehingga dalam melakukan pengiriman atau pertukaran data menjadi lebih aman dan *private*

2) Skema Jaringan Usulan

Pada skema jaringan usulan direkomendasikan yaitu penerapan VPN L2TP dan IPSec yang dilakukan di *router*

mikrotik pada menu PPP untuk menghubungkan jaringan yang ada pada kantor cilandak (pusat) dan kantor Hang Jebat (cabang) dengan syarat masing-masing lokasi terdapat internet yang menghubungkan mereka. *Router* yang berada di kantor Cilandak akan bertindak sebagai *router L2TP server* dan *router* yang berada di kantor Hang Jebat akan bertindak sebagai *router L2TP client*. Kemudian untuk untuk *dial* koneksi L2TP dari *client* dibuatkan *username* dan *password* yang pada menu *Secret*. Agar kedua jaringan lokal pada jaringan pusat dan cabang bisa terkoneksi ditambahkan juga *routing static* pada *router server* dan *client*. Setelah kedua jaringan lokal ini terhubung maka pengguna pada kantor pusat dan pengguna pada kantor cabang dapat terjalannya berkomunikasi sehingga dapat melakukan kirim ataupun terima *file*.



Gambar 4. Skema Jaringan Usulan

Tabel 3. IP Address

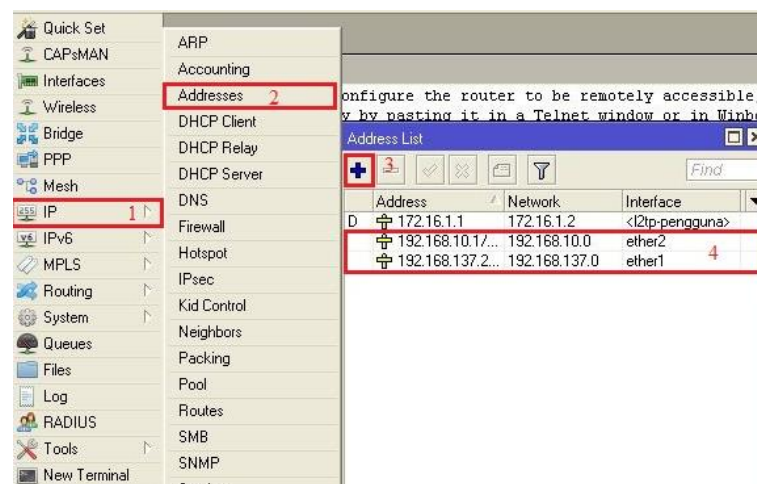
No	Perangkat	IP Address	Subnet
1	ISP(Pusat)	192.168.137.254	255.255.255.0
2	ISP(Cabang)	192.168.137.253	255.255.255.0
3	L2TP Tunnel router kantor pusat	172.16.1.1	255.255.255.0
4	L2TP Tunnel router kantor cabang	172.16.1.2	255.255.255.0
5	File Server	192.168.10.2	255.255.255.0
6	Client kantor pusat	192.168.10.3 s/d 254	255.255.255.0
7	Client kantor cabang	192.168.100.3 s/d 254	255.255.255.0

3) Rancang Aplikasi

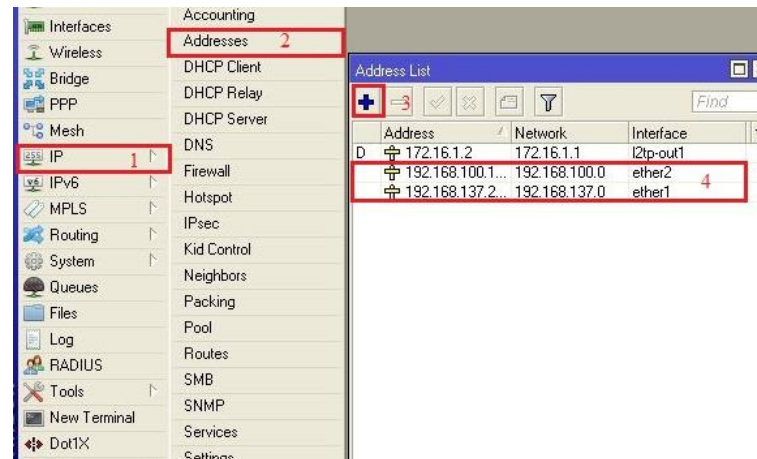
Dalam rancangan aplikasi ini penulis menggunakan *VirtualBox* sebagai simulasi yang digunakan. Aplikasi yang dibutuhkan dalam membangun jaringan usulan tersebut adalah sebuah Mikrotik dan *Software* pendukung yaitu *Winbox*, sebagai aplikasi untuk menunjang kinerja

perusahaan dalam mengkonfigurasi perangkat mikrotik.

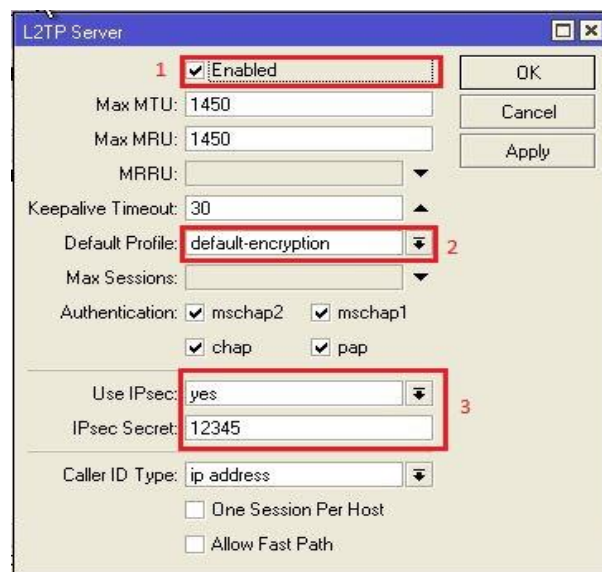
- Konfigurasi *IP Address Router* Pusat; Gambar 5.
- Konfigurasi *IP Address Router* Cabang; Gambar 6.
- Konfigurasi Router Pusat; Gambar 7, Gambar 8.
- Konfigurasi Router Cabang; Gambar 9.



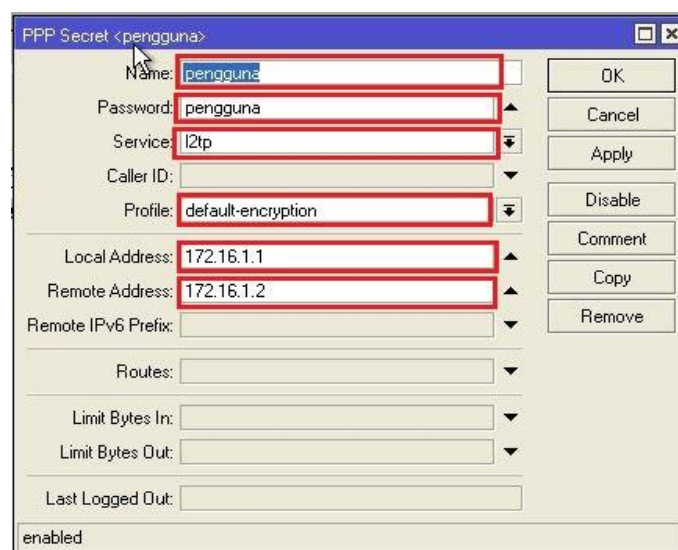
Gambar 5. IP Address Kantor Pusat



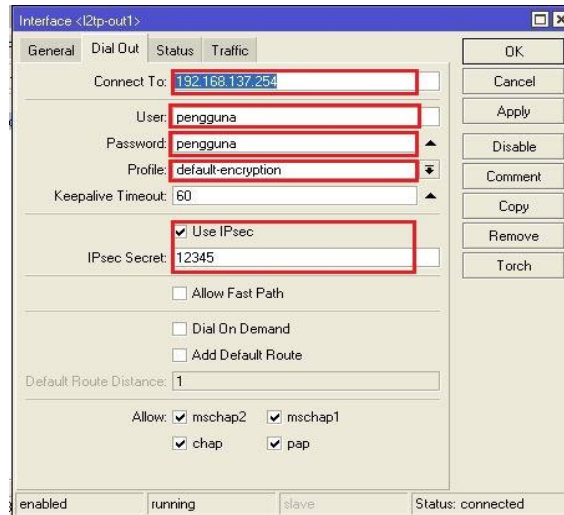
Gambar 6. IP Address Kantor Cabang



Gambar 7. L2TP Router Server



Gambar 8. PPP Secret Router Server



Gambar 9. Konfigurasi L2TP Router Pusat

4) Pengujian Jaringan

Dalam pengujian jaringan ini penulis mencoba melakukan perbandingan dari jaringan komputer pada Balai Besar Pelathan Kesehatan Jakarta pada saat belum menerapkan VPN dan saat sudah menerapkan VPN. Dan pengujian ini menggunakan simulator *VirtualBox* dengan beserta aplikasi-aplikasi pendukung seperti *winbox*.

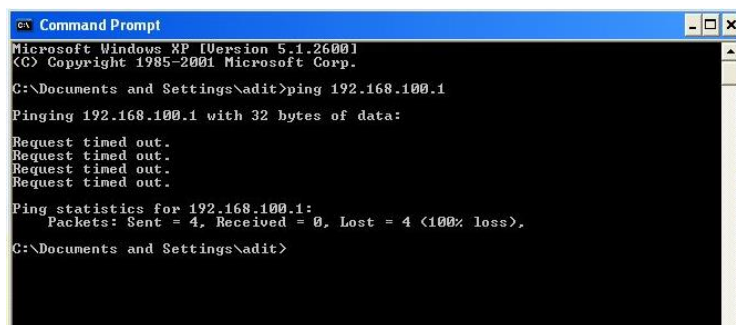
a. Pengujian Jaringan Awal

Pengujian jaringan awal merupakan pengujian jaringan dimana pengujian tersebut dilakukan sebelum adanya perubahan rancangan pada simulasi jaringan.

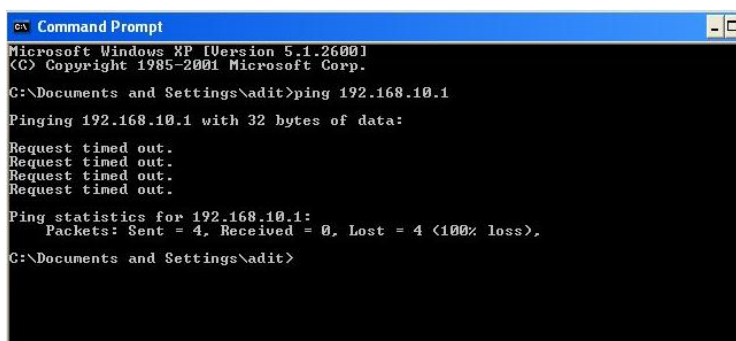
Pengujian jaringan awal dilakukan dengan menggunakan perintah dan *ping* pada *client* masing-masing cabang.

Pengujian Client pada Jaringan Lokal di Kantor Pusat. Pada Gambar 10 diketahui bahwa saat *client* pada jaringan lokal di kantor pusat melakukan test *ping* menuju *gateway* di kantor cabang hasilnya adalah *request time out*. Hal ini menunjukkan jaringan lokal di kantor pusat tidak terhubung pada jaringan lokal di kantor cabang.

Pengujian Client pada Jaringan Lokal di Kantor Cabang. Pada Gambar 11 diketahui bahwa saat *client* pada jaringan lokal di kantor cabang melakukan test *ping* menuju *gateway* di kantor pusat hasilnya adalah *request time out*. Hal ini menunjukkan jaringan lokal di kantor cabang tidak terhubung pada jaringan lokal di kantor pusat.



Gambar 10. Ping Menuju Gateway di Kantor Cabang



Gambar 11. Ping Menuju Gateway di Kantor Pusat

b. Pengujian Jaringan Usulan

Pada pengujian jaringan akhir ini dimana pengujian tersebut dilakukan setelah perubahan rancangan jaringan dengan menggunakan VPN. Pengujian jaringan akhir dilakukan dengan menggunakan perintah *ping*.

Pengujian Client pada Jaringan Lokal di Kantor Pusat. Pada Gambar 12 ping dari *client* kantor pusat menuju *gateway* jaringan lokal di kantor cabang menunjukkan sudah terhubung, yang artinya *client* pada

kantor pusat sudah terkoneksi ke jaringan lokal di kantor cabang.

Pengujian Client pada Jaringan Lokal di Kantor Cabang. Pada Gambar 13 ping dari *client* kantor cabang menuju *gateway* jaringan lokal di kantor pusat menunjukkan sudah terhubung, yang artinya *client* pada kantor cabang sudah terkoneksi ke jaringan di kantor pusat.

```

C:\Documents and Settings\adit>ping 192.168.100.1

Pinging 192.168.100.1 with 32 bytes of data:

Reply from 192.168.100.1: bytes=32 time=8ms TTL=63
Reply from 192.168.100.1: bytes=32 time=2ms TTL=63
Reply from 192.168.100.1: bytes=32 time=5ms TTL=63
Reply from 192.168.100.1: bytes=32 time=14ms TTL=63

Ping statistics for 192.168.100.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 14ms, Average = 7ms
  
```

Gambar 12. Ping Menuju Gateway di Kantor Cabang

```

C:\Documents and Settings\adit>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time=6ms TTL=63
Reply from 192.168.10.1: bytes=32 time=5ms TTL=63
Reply from 192.168.10.1: bytes=32 time=4ms TTL=63
Reply from 192.168.10.1: bytes=32 time=3ms TTL=63

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 6ms, Average = 4ms
  
```

Gambar 13. Ping Menuju Gateway di Kantor Pusat

4. Kesimpulan

Berdasarkan hasil pengujian jaringan VPN yang telah dilakukan maka dapat diambil kesimpulan yaitu diterapkannya jaringan *Virtual Private Network* (VPN) L2TP pada BBPK Jakarta dapat menghubungkan dua jaringan yaitu BBPK Jakarta kantor pusat yang berada di Cilandak dengan kantor pusat kantor cabang di Hang Jebat. Dengan menggunakan VPN dengan metode L2TP pegawai yang ada di gedung pusat dan cabang dapat melakukan komunikasi dengan aman dan lancar.

5. Daftar Pustaka

- [1] E. Mufida, D. Irawan, and G. Chrisnawati, Remote Site Mikrotik VPN dengan *Point to Point Tunneling Protocol* (PPTP) Studi Kasus pada Yayasan Teratai Global Jakarta, *J. Matrik*, vol. 16, no. 2, p. 9, 2017, doi: 10.30812/matrik.v16i2.7.
- [2] D. Lumena, A. Anton, and E. R. Nainggolan, Analisis dan Perancangan Jaringan *Private Cloud Computing* Berbasis Web Eycos, *None*, vol. 13, no. 1, pp. 1–8, 2016.
- [3] T. Rahman and A. I. Haris, Rancang Bangun Jaringan Virtual Private Network (VPN) Berbasis IPSec Pada PT. Inner City Management, *Simp. Nas. Ilmu Pengetab. dan Teknol.* 2017, 2017.
- [4] S. N. Khasanah and L. A. Utami, Implementasi Failover Pada Jaringan WAN Berbasis VPN, vol. IV, no. 1, pp. 62–66, 2018.
- [5] A. Rachmawan, Perbandingan Protokol L2TP dan PPTP Untuk Membangun Jaringan Intranet di Atas VPN, *J. Manaj. Inform.*, vol. 8, no. 2, pp. 53–57, 2018.
- [6] B. Sutara and Sutrisno, Layanan Jaringan Internet Pada Virtual Private Network (VPN) Menggunakan L2TP Untuk Peningkatan Keamanan Jaringan, *J. ICT*, vol. 16, no. 1, pp. 1–6, 2017.