ANALISIS DAN DESAIN JALUR TRANSMISI JARINGAN ALTERNATIF MENGGUNAKAN VIRTUAL PRIVATE NETWORK (VPN)

Amarudin[1)], Sampurna Dadi Riskiono[2)]

[1,2)] Teknik Elektro, Fakultas Teknik dan Ilmu Komputer, Universitas Teknokrat Indonesia
[1,2)] Jl. ZA Pagaralam, No 9-11, Labuhanratu,Bandarlampung
Email : [1]amarudin@teknokrat.ac.id, [2]sampurna.go@teknokrat.ac.id

Abstrak

Penelitian ini bertujuan untuk menganalisis pemanfaatan jalur transmisi jaringan dan keamanan jaringan pada Universitas Teknokrat Indonesia khususnya pada jalur jaringan di gedung pusat (Gd.A) dengan gedung Fakultas Sastra dan Ilmu Pendidikan (Gd.B). Berdasarkan hasil observasi dan wawancara dengan tim IT Pustik, penulis menemukan sebuah kelemahan dalam membangun sistem jaringan tersebut. Kelemahan dari implementasi jaringan yang digunakan selama ini yaitu jalur transmisi data antar gedung (Gd.A dan Gd.B) tidak dilengkapi dengan jalur alternatif untuk mengakses kedua gedung tersebut. Sehingga jika media transmisi antar gedung (Gd.A dan Gd.B) ada trouble, maka antar gedung tersebut tidak bisa saling askses. Padahal masing-masing gedung bisa terkoneksi ke jalur internet. Jadi, secara tidak langsung pemanfaatan jalur internet antar gedung tersebut belum maksimal. Oleh karena itu, perlu dirancang sebuah jalur alternatif yaitu menggunakan protokol Virtual Private Network (VPN). Dimana jalur ini akan digunakan jika jalur normal (eksisting) ada masalah. Jalur alternatif ini juga dilengkapi dengan sistem keamanan jaringan yang dapat berfungsi untuk mengenkripsi semua data yang ditransmisikan pada jalur tersebut. Berdasarkan hasil eksperiman dan analisis yang dilakukan, penulis menemukan bahwa penerapan jalur alternatif menggunakan protocol Virtual Private Network (VPN) sangat cocok untuk diterapkan. Walaupun protokol VPN ini lebis secure, akan tetapi pemanfaatan VPN ini juga terdapat kelemahan lain yang ditemukan. Yaitu ketika pada Gd.B tidak bisa mengakses internet, maka jalur alternatif (jalur VPN) tidak bisa digunakan. Sehingga pada Gd.B tersebut dibutuhkan perangkat tambahan (Modem), agar bisa mengakses internet sehingga dapat mengakses jalur VPN yang telah dibangun.

Kata Kunci: *Virtual Private Network (VPN), Jalur Alternatif, Keamanan Jaringan.*

1. Pendahuluan

Universitas Teknokrat Indonesia adalah salah satu universitas swasta ternama di kota Bandarlampung. Universitas ini memiliki visi "Menjadi universitas unggul di Sumatra yang berstandar internasional dan mampu berperan aktif dalam pembangunan bangsa melalui tri darma perguruan tinggi" [1]. Adapun bidang keilmuan di Universitas Teknokrat Indonesia mencakup bidang komputer, pendidikan, olahraga dan bahasa. Sesuai dengan bidang komputer yang dimiliki oleh Universitas Teknokrat Indonesia, maka pemanfaatan teknologi jaringan sudah mulai diimplementasikan di kampus tersebut. Pemanfaatan jaringan komputer di Universitas Teknokrat Indonesia sudah menyeluruh di semua area dan gedung yang ada di kampus tersebut. Salah satunya ialah jaringan komputer yang dibangun di gedung utama (Gd.A) dan gedung Fakultas Sastra dan Ilmu pendidikan (Gd.B). Tanpa adanya jaringan komputer yang dibangun antar gedung tersebut, maka berdampak pada lemahnya komunikasi yang dapat dilakukan antar staf yang bekerja pada masing-masing gedung tersebut. Akan tetapi berdasarkan hasil observasi yang dilakukan oleh penulis, ternyata penerapan jaringan komputer tersebut belum menerapkan sistem kemanan, misal *Secure Socke Layer* (SSL). Sehingga transmisi data yang terkirim melalui jaringan tersebut sangatlah berbahaya dari adanya *sniffing* (penyadapan) oleh pihak yang tidak bertanggung jawab. Dimana untuk melakukan *sniffing* ini bisa dilakukan oleh *sniffer* menggunakan aplikasi Wireshark. Wireshark adalah program *Network Protocol Analyzer* yang bisa digunakan untuk menganalisa protokol jaringan dengan lengkap. Program ini dapat merakam semua paket yang lewat serta menyeleksi dan menampilkan data tersebut sedetail mungkin, misalnya postingan komentar di blog atau bahkan *username* dan *password* [2]. Selain tidak adanya penerapan SSL, pada jaringan tersebut juga belum dilengkapi dengan jalur alternatif, misalnya VPN. Sehingga pemanfaatan jalur komunikasi antar gedung tersebut kurang maksimal.

Penelitian ini dilatarbelakangi pada permasalahan yang ditemukan penulis yakni adanya kekurangan pada pengembangan jaringan eksisting sebelumnya. Sistem jaringan yang dibangun di Universitas Teknokrat Indonesia khususnya pada jaringan antar Gd.A dan Gd.B tidak dilengkapi dengan jalur alternatif. Hal ini berdampak pada pemanfaatan media transmisi antar gedung tersebut kurang maksimal. Untuk itu, sangatlah penting untuk dibangun sebuah jalur alternatif dengan memanfaatkan dan menerapkan protokol *Virtual Private Network* (VPN) dengan syarat masih tetap mempertimbangkan tingkat keamanan data yang ditransmisikannya. Dengan demikian bila jalur utama ada masalah, maka bisa memanfaatkan jalur alternatif yang aman ini sebagai solusi komunikasi antar gedung tersebut.

1.1. *Virtual Private Network* (VPN)

VPN dalah sebuah jaringan komputer dimana koneksi antar perangkatnya (*node*) memanfaatkan jaringan *public* sehingga yang diperlukan hanyalah koneksi internet di masing-masing site. Ketika mengimplementasikan VPN, interkoneksi antar *node* akan memiliki jalur *virtual* khusus di atas jaringan *public* yang sifatnya independen. Metode ini biasanya digunakan untuk membuat komunikasi yang bersifat *secure*, seperti *system ticketing online* dengan *database* server terpusat [3].

1.2. *Point to Point Tunnel Protocol* (PPTP)

Salah satu *service* yang biasa digunakan untuk membangun sebuah jaringan VPN adalah *Point to Point Tunnel Protocol* (PPTP). Sebuah koneksi PPTP terdiri dari Server dan Client. Mikrotik RouterOS bisa difungsikan baik sebagai server maupun client atau bahkan diaktifkan keduanya bersama dalam satu mesin yang sama. *Feature* ini sudah termasuk dalam *package* PPP sehingga bisa dicek di menu *system package* apakah paket tersebut sudah ada di router atau belum. Fungsi PPTP Client juga sudah ada dihampir semua OS, sehingga bisa menggunakan Laptop/PC sebagai PPTP Client. Biasanya PPTP ini digunakan untuk jaringan yang sudah melewati multihop router (*Routed Network*). Jika ingin menggunakan PPTP pastikan di Router tidak ada rule yang melakukan *blocking* terhadap protocol TCP 1723 dan IP Protocol 47/GRE karena *service* PPTP menggunakan *protocol* tersebut [3].

1.3. Wireshark

Wireshark adalah program penganalisa jaringan yang sangat populer saat ini, walaupun program ini kebanyakan dikenal bukan karena fungsi utamanya melainkan karena sering digunakan untuk keperluan *hacking* pemula. Dengan kata lain bahwa Wireshark adalah program *Network Protocol Analyzer* alias penganalisa protokol jaringan yang lengkap. Program ini dapat merakam semua paket yang lewat serta menyeleksi dan menampilkan data tersebut sedetail mungkin, misalnya postingan komentar di blog atau bahkan *username* dan *password* [2].

1.4. Hacking

Hacking merupakan aktivitas penyusupan ke dalam sebuah sistem komputer ataupun jaringan dengan tujuan untuk menyalahgunakan ataupun merusak sistem yang ada. Definisi dari kata "menyalahgunakan" memiliki arti yang sangat luas, dan dapat diartikan sebagai pencurian data rahasia, serta penggunaan e-mail yang tidak semestinya seperti spamming ataupun mencari celah jaringan yang memungkinkan untuk dimasuki [4].

2. Penelitian Terkait

Ada beberapa penelitian sebelumnya yang membahas terkait keamanan jaringan, yakni penelitian yang dilakukan oleh Basim Mahbooba, *et al*. [5], yang membahas penguncian port berbasis sertifikat digital untuk menghubungkan sistem yang *embedded* pada IoT. Pada penelitian tersebut bertujuan memperkuat metode port knocking yang ada dengan sertifikat digital untuk otentikasi alternatif diantara perangkat IoT. Konsep-konsep tersebut akan menjadi pelengkap konsep-konsep kriptografi lainnya (yaitu kunci enkripsi bersama sebagaimana yang diadopsi dalam ZigBee).

Adapun penelitian yang dilakukan oleh Amarudin [6], membahas desain keamanan jaringan pada Mikrotik Router OS menggunakan metode port knocking. Dimana pada penelitian tersebut mengusulkan desain keamanan jaringan mengguakan port knocking. Pemanfaatan metode Port Knocking pada keamanan jaringan sangat cocok diterapkan untuk menjaga Router dari akses orang lain yang tidak berhak mengaksesnya. Walaupun pengguna PC1 mengetahui *user* dan *password* untuk login ke Router, akan tetapi jika pengguna PC1 tersebut tidak mengetahui *role* (*route*) *ping request* ke Router, maka ia tidak bisa login ke Router. Dengan demikian untuk mengakses admin Router harus melewati dua gerbang *security*. Gerbang pertama yaitu *user* dan *password* admin Router. Sedangkan gerbang kedua yaitu *role (route) ping request* yang dipakai untuk mengakses admin Router.

Sedangkan penelitian lain yang dilakukan oeh Amarudin [7], membahas analisis dan implementasi keamanan jaringan pada mikrotik Router OS menggunakan metode port knocking. Dimana dalam penelitian tersebut dilakukan analisis dan implementasi keamanan jaringan pada area Universitas Teknokrat Indonesia. Berdasarkan hasil analisis dan pengujian implementasi sistem yang dilakukan, didapatkan hasil bahwa sistem dapat berjalan dengan baik dan dapat meningkatkan keamanan sistem jaringan yang dibangun dibandingkan pada jaringan yang tidak menerapkan keamanan Port Knocking. Hal ini dibuktikan dengan adanya autentikasi yang tepat saat mengakses Router. Yaitu autentikasi yang sesuai dengan role yang telah dibangun.

Penelitian lain terkait dengan pembahasan keamanan jaringan yakni sebuah penelitian yang dilakukan oleh Y. Hendriana [8], yang membahas evaluasi implementasi keamanan jaringan VPN pada CV.Pangestu Jaya. Dimana dalam penelitian tersebut dilakukan evaluasi terhadap implementasi VPN. Adapun hasil yang diperoleh dalam penelitian tersebut bahwa hasil pengujian konektivitas jaringan VPN antara kantor pusat dengan kantor cabang di CV. Pangestu Jaya bisa berjalan dengan baik dan stabil, dengan tingkat loss dan round trip dalam jumlah kecil, tetapi tetap dipengaruhi oleh bandwidth yang dimiliki oleh masing-masing komputer client. Adapun kelemahan yang diperoleh yakni masih adanya kelemahan terhadap serangan *Denial of Service* (DoS) dengan pingflood attack. Selain itu jaringan VPN masih rentan terhadap serangan penyusup, dengan telah dibobolnya *username* dan *password* vpn melalui eksperimen *hacking* menggunakan Linux Backtrack.

Berikutnya penelitian yang dilakukan oleh H. Supriyono, *et.al.* [9], membahas penerapan jaringan *virtual private network* untuk keamanan komunikasi data

bagi pt. mega tirta alami. Sehingga komunikasi data antar kantor pusat dan kantor cabang dapat terhubung dengan aman dari sniffing. Dalam penelitian tersebut telah dilakukan beberapa pengujian terhadap penerapan VPN. Beberapa percobaan teknis yang dilakukan pada tahap ini antara lain: pengujian konektifitas antar router yang dipasang, pengujian fungsionalitas router yang difungsikan sebagai server, pengujian IP route, pengujian *trace route*, pengujian ping dan pengujian download. Berdasarkan beberapa beberapa pengujian tersebut dapat berjalan dengan baik.

3. Metode

3.1. Rancangan Penelitian

Metode yang digunakan pada penelitian ini adalah metode kualitatif sehingga data yang diperoleh akan lebih lengkap dan bermakna dan tujuan penelitian dapat dicapai. Desain penelitian kualitatif ini dibagi dalam empat tahap, yaitu:

1. Perencanaan
   Kegiatan yang dilakukan dalam tahap ini adalah menyusun rancangan penelitian dan menyusun instrumen penelitian.
2. Pelaksanaan
   Pada tahap ini penulis sebagai pelaksana dan sebagai pencari informasi data melakukan wawancara dengan Staf IT (admin Pustik) dan melakukan kajian pustaka dari berbagai sumber buku dan jurnal.
3. Analisis Data
   Analisis data dilakukan setelah penulis melakukan wawancara terhadap Staf IT (admin Pustik).
4. Evaluasi
   Semua data yang sudah dianalisis kemudian dievaluasi sehingga diketahui kebutuhan yang dapat membuat sistem jaringan di Universitas Teknokrat Indonesia menjadi lebih baik.

3.2. Teknik Pengumpulan Data

Untuk mendapatkan informasi yang sesuai, penulis menggunakan teknik penilaian data sebagai berikut:

a. Teknik Observasi
   Metode observasi berguna bagi peneliti untuk mengumpulkan data dalam berbagai cara [10]. Metode observasi memberikan informasi bagi peneliti dengan cara memeriksa desain dan konfigurasi jaringan eksisting, memahami bagaimana cara kerja keamanan jaringan yang diterapkan sebelumnya, dan memeriksa apakah masih ada celah yang memungkinkan untuk dilakukan penetrasi terhadap sistem eksisting.
b. Teknik Wawancara
   Wawancara pada penelitian ini menggunakan pertanyaan-pertanyaan terbuka, yaitu pertanyaan yang membutuhkan lebih dari jawaban ya atau tidak. Selain itu, pertanyaan-pertanyaan yang dibuat juga dapat dipahami dengan mudah oleh responden yakni Staf IT Pustik. Kemudian menghasilkan data yang representatif dan berkembang menjadi wawancara lebih lanjut [11].
c. Studi Kepustakaan
   Merupakan cara pengumpulan data dengan mempelajari literatur, paket modul dan panduan, buku–buku pedoman, buku-buku perpustakaan dan segala kepustakaan lainnya yang dianggap perlu dan mendukung.

3.3. Sumber data

Sumber data dalam penelitian adalah subjek dari mana data ini diperoleh. Adapun yang dijadikan sumber data antaralain:

a. Wawancara terhadap Admin jaringan (Staf IT) di Universitas Teknokrat Indonesia.
b. Wawancara terhadap Staf Tata Usaha yang bekerja pada bagian Gd.A dan Gd.B.
c. Wawancara terhadap mahasiswa aktif yang sedang menggunakan internet kampus.

3.4. Teknik Analisa Data

Analisis data adalah proses mencari dan menyusun data yang diperoleh dari hasil wawancara atau catatan lapangan dengan cara mengorganisasikan data kedalam kategori. Kemudian memilih mana yang penting dan membuat kesimpulan sehingga mudah dipahami oleh diri sendiri dan orang lain. Komponen dari analisis data antara lain [12]:

1. Reduksi Data
   Mereduksi data berarti mencatat secara rinci dan teliti, merangkum, memilih hal–hal pokok, memfokuskan pada hal-hal yang penting, dicari tema dan polanya.
2. Penyajian Data
   Penyajian data pada penilaian kualitatif bisa dilakukan dalam bentuk bagan, uraian singkat, hubungan antar kategori dan sejenisnya.
3. Penyimpulan Data
   Kesimpulan awal yang di kemukakan masih bersifat sementara dan akan berubah jika di temukan bukti-bukti yang kuat yang mendukung pada tahap berikutnya. Tetapi apabila kesimpulan yang dikemukakan pada tahap awal sudah didukung oleh bukti-bukti yang valid dan konsisten maka kesimpulan yang dikemukakan merupakan kesimpulan kredibel.

4. Hasil dan Pembahasan

4.1. Kelebihan Implementasi VPN

Dalam perkembangan teknologi jaringan komputer saat ini telah bayak metode sistem keamanan data yang dapat diterapkan untuk mengamankan data yang ada di dalamnya. Salah satu metode untuk mengamankan data yaitu dengan cara membangun enkripsi pada sebuah data yang bersifat rahasia. Keamanan data ini bisa dibangun di dalam server tempat data berada maupun juga bisa dibangun pada koneksi jaringan yang berfungsi sebagai media transmisi data antar *device*. Dengan menerapkan sistem keamanan data, maka dapat meningkatkan kerahasiaan data yang ditransmisikan maupun data yang masih tersimpan dalam server tersebut. Dan hal ini pula

yang menjadikan dasar pengembangan sistem keamanan jaringan menggunakan *virtual private network* (VPN).

Dalam penelitian ini penulis menemukan beberapa kelebihan ketika menerapkan sistem keamanan jaringan menggunakan *Virtual Private Network* (VPN). Salah satu kelebihannya yaitu tansmisi data yang dikirimkan melalui jalur VPN lebih aman dibandingkan dengan jaringan tanpa menerapkan VPN. Dari sisi *user*/pengguna jaringan, sudah jelas sangat bermanfaat yaitu data yang diakses oleh *user* tersebut lebih aman sehingga *user* merasa lebih nyaman ketika bertransaksi menggunakan jaringan tersebut. Adapun bagi lembaga (Universitas Teknokrat Indonesia), sangat bermanfaat untuk mengamankan data yang diakses maupun data yang dikirimkan melalui jaringan tersebut. Sehingga dapat mengurangi dari adanya penyalahgunaan data dari pihak yang tidak bertanggung jawab. Selain itu juga bermanfaat sebagai jalur alternatif ketika pada jalur utama ada masalah atau *trouble*.

4.2. Kelemahan Implementasi VPN

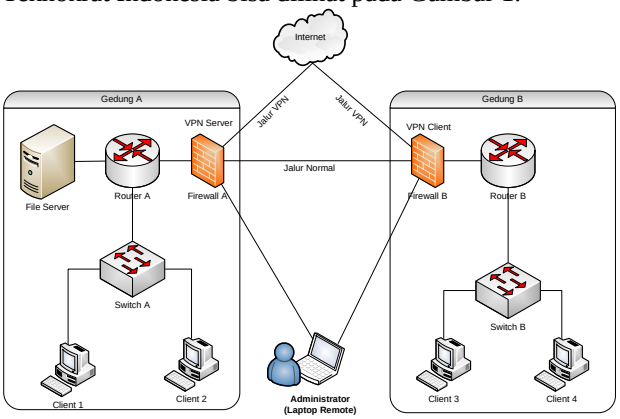
Dalam sistem jalur transmisi jaringan yang dibangun menggunakan protokol *Virtual Private Network* (VPN) ini juga memiliki kelemahan disamping kelebihan sebagaimana yang dijelaskan sebelumnya. Salah satunya adalah masih adanya ketergantungan keamanan data dari pemilik VPN. Karena data yang ditrasnmisikan menggunakan VPN dapat diketahui oleh pemilik VPN.

Selain itu, kelemahan lain dari penerapan protokol *Virtual Private Network* (VPN), yaitu muncul masalah baru jika pada sisi VPN Client tidak bisa terhubung ke internet. Sehingga diperlukan perangkat tambahan misalnya berupa Modem sebagai koneksi ke internet.

4.3. Solusi dari Permasalahan

a) Desain Topologi Jaringan

Berdasarkan permasalahan yang ditemukan, maka untuk membangun jalur transmisi alternatif pada jaringan tersebut, perlu diterapkan protokol *Virtual Private Network* (VPN). Adapun desain penerapan *Virtual Private Network* (VPN) yang dibangun di Universitas Teknokrat Indonesia bisa dilihat pada Gambar 1.



Gambar 1. Desain Penerapan Jalur Alternatif VPN

b) Konfigurasi VPN

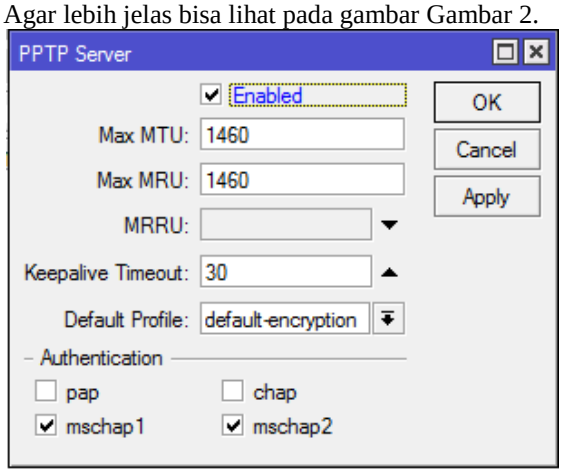
Berikut ini langkah-langkah konfigurasi VPN:

1. Konfigurasi PPTP Server

Berdasar topologi Gambar 1, yang menjadi pusat dari link PPTP (konsentrator) adalah Router A, maka harus dilakukan setting PPTP Server pada router tersebut.

2. Enable PPTP Server

Langkah pertama yang harus dilakukan adalah mengaktifkan PPTP server. Masuk pada menu **PPP->Interface>PPTP Server**. Gunakan profile "Default-encryption" agar jalur VPN terenkripsi.
Agar lebih jelas bisa lihat pada gambar Gambar 2.



Gambar 2. Enable PPTP Server

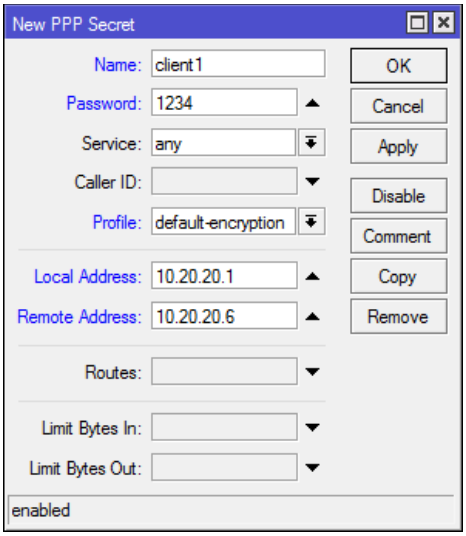
3. Secret

Pada tahap ini, tentukan *user name* dan password untuk proses autentikasi Client yang akan terkoneksi ke PPTP server. Penggunaan huruf besar dan kecil akan berpengaruh.

-**Local Address** adalah alamat IP yang akan terpasang pada router itu sendiri (Router A / PPTP Server) setelah link PPTP terbentuk

-**Remote Address** adalah alamat IP yang akan diberikan ke Client setelah link PPTP terbentuk. Arahkan agar menggunakan profile "Default-Encryption".

Contoh konfigurasi bisa dilihat pada Gambar 3.



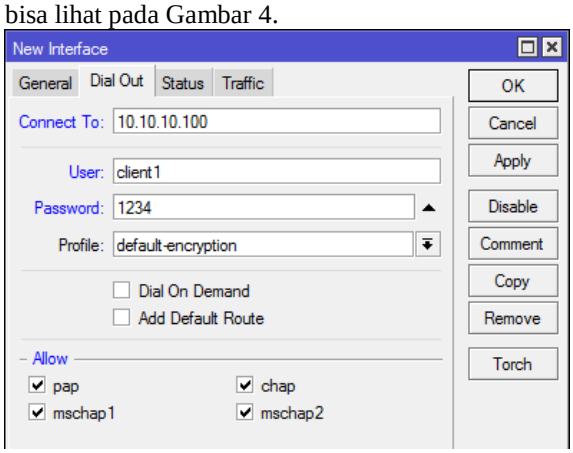
Gambar 3. Secret

Sampai disini, konfigurasi pada Router A (PPTP Server) sudah selesai, langkah selanjutnya adalah melakukan konfigurasi di sisi client (Router B).

4. Client Router Gedung B

Langkah-langkah untuk melakukan konfigurasi Client PPTP pada Router Mikrotik adalah sebagai berikut :

Tambahkan interface baru PPTP Client, lakukan dial ke IP Public Router A (PPTP server) dan masukkan *username* dan *password* sesuai pengaturan secret PPTP Server. Konfigurasinya bisa lihat pada Gambar 4.



Gambar 4. Interface baru

Catatan: IP 10.10.10.100 adalah *ip public* dari server.

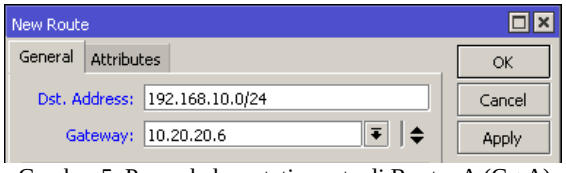
Setelah koneksi PPTP terbentuk, akan muncul IP Address baru di kedua Router dengan flag #D# yang menempel di interface pptp sesuai dengan pengaturan Secret pada PPTP server.

Sampai disini koneksi VPN antar router sudah terbentuk, akan tetapi antar jaringan lokal belum bisa saling berkomunikasi. Agar antar jaringan local bisa saling berkomunikasi, kita perlu menambahkan routing static dengan konfigurasi

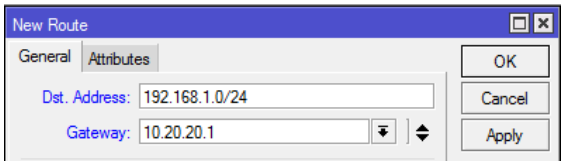
5. Static Route

- **dst-address** : Jaringan local Router tujuan.
- **gateway** : IP PPTP Tunnel pada kedua router.

Konfigurasi tersebut bisa dilihat pada Gambar 5 dan Gambar 6.



Gambar 5. Penambahan static route di Router A (Gg.A)



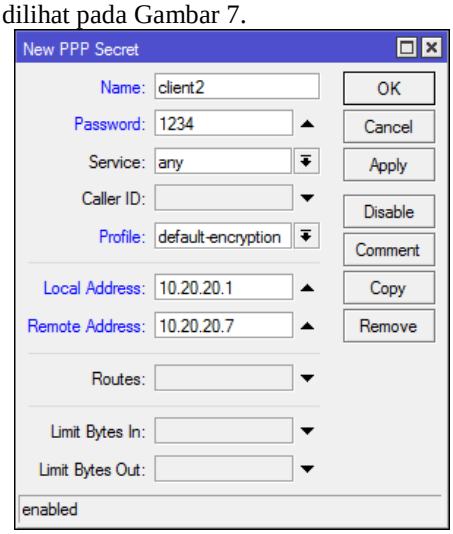
Gambar 6. Penambahan static route di router B (Gd.B)

6. Mobile Client

Client PPTP tidak harus menggunakan Router. Sebagaimana pada topologi jaringan Gambar 1, ada sebuah Laptop Administrator (*Remote Client*) yang akan melakukan koneksi VPN ke Router A. Maka perlu dibbuat Secret baru pada PPTP server untuk autentikasi *remote client* tersebut.

7. Secret

username= client2; *password*= 1234; Local Address= 10.20.20.1; Remote Address= 10.20.20.7 bisa dilihat pada Gambar 7.



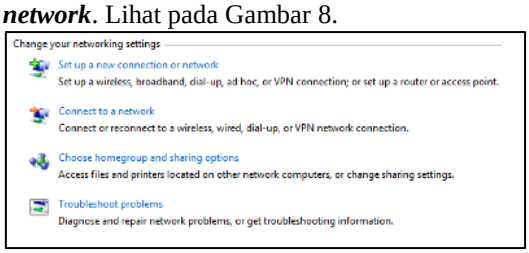
Gambar 7. PPP Secret

c) Konfigurasi PPTP Client Windows 7

Langkah selanjutnya adalah melakukan konfigurasi PPTP Client pada Laptop Administrator. Langkah-langkah tersebut disesuaikan dengan SO yang digunakan. Karena berbeda SO maka akan beda langkah konfigurasinya.

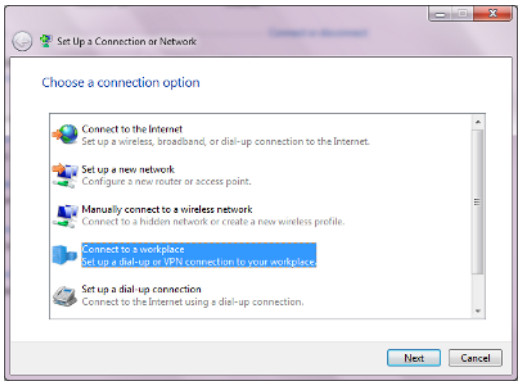
Berikut langkah-langkah konfigurasi PPTP Client untuk SO Windows 7.

1) Setelah Laptop Administrator sudah bisa akses internet, kemudian masuk pada menu *Network and Sharing Center*, kemudian *create* koneksi baru dengan memilih ***Set up new connection or network***. Lihat pada Gambar 8.



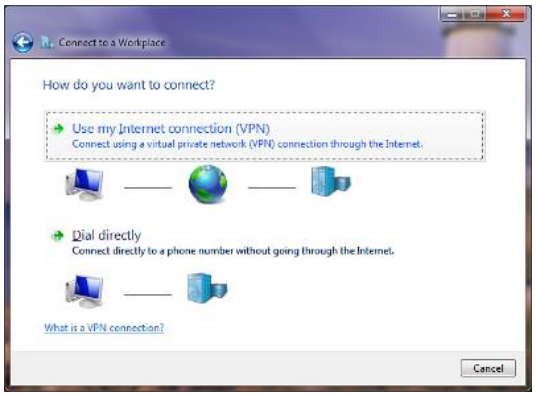
Gambar 8. Setup new connection

2) Kemudian pada tampilan window selanjutnya, pilih ***Connect to a workplace***, kemudian klik *next*. Lihat pada Gambar 9.



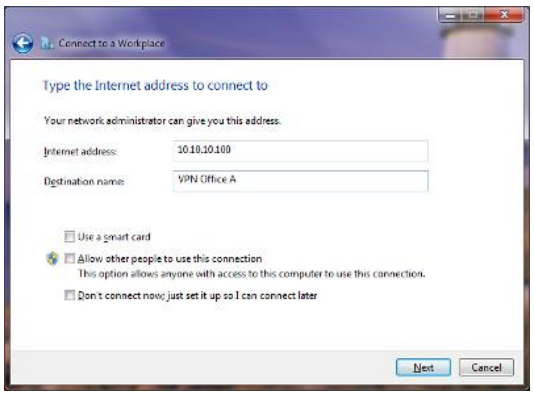
Gambar 9. Connect Workplace

3) Kemudian langkah selanjutnya pada form Coonection Workplace pilih ***Use My Internet Connec.*** Lihat pada Gambar 10**.**



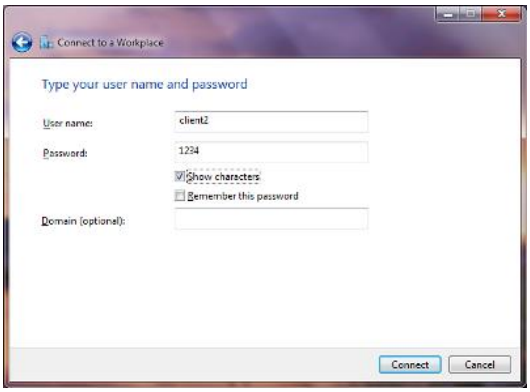
Gambar 10. Use My Internet Connection (VPN)

4) Pada langkah berikutnya memasukkan ke IP Address mana yang akan koneksikan. Sesuai topologi Gambar 1, maka masukkan IP Address public Router A. *Destination name* adalah parameter untuk memberikan nama pada interface VPN yang sedang dibuat. Lihat pada Gambar 11.



Gambar 11. IP Address Destination

5) Selanjutnya masukkan *username* dan *password* sesuai pengaturan Secret yang ada di PPTP server. Kemudian klik Connect. Lihat pada Gambar 12.



Gambar 12. User dan Password Secret

6) Kemudian jika proses autentikasi sudah selesai, maka di laptop administrator akan muncul *interface* baru dengan nama VPN Gedung A dan terpasang IP address yang mengambil dari *ip-pool Remote Address* sesuai dengan pengaturan *profile* dan *Secret* pada PPTP Server..

5. Simpulan

Berdasarkan hasil dan pembahasan, dapat disimpulkan sebagai berikut:

1. Penerapan jalur alternatif menggunakan *Virtual Private Network* (VPN) sangat bermanfaat untuk menjaga keberlangsungan proses kerja transmisi data.
2. Berdasarkan hasil eksperimen yang dilakukan oleh peneliti, bahwasanya konfigurasi penerapan *Virtual Private Network* (VPN) tidak begitu kompleks dan tidak rumit, sehingga bisa dengan mudah untuk diterapkan dimana saja bagi yang ingin menerapkan protokol VPN ini pada jaringan yang dibangunnya.
3. Berdasarkan permasalahan yang ditemukan, bahwa untuk memaksimalkan penggunaan jaringan bisa diterapkan protokol VPN.
4. Selain itu, penulis juga menemukan beberapa kelemahan dari penerapan protokol VPN ini, yakni masih perlu adanya kewaspadaan terhadap keamanan data yang ditransmisikan dari penyalahgunaan oleh pihak pemilik VPN.

Ucapan Terimakasih

Terima kasih kepada Direktorat Riset dan Pengabdian kepada Masyarakat (DRPM) Dikti yang telah mendanai kegiatan penelitian ini yakni pada skema Penelitian Dosen Pemula (PDP) sesuai dengan SK Penetapan Pemenang Hibah PDP nomor: T/140/E3/RA.00/2019 tanggal 25 Februari 2019 dan Kontrak Pelaksanaan Penelitian Nomor: 005/LPPM-UTI/FTIK/PDP-MONO/V/2019 tanggal 2 Mei 2019.

Terima kasih juga peneliti sampaikan kepada LPPM Universitas Teknokrat Indonesia yang telah memfasilitasi kegiatan penelitia ini khususnya tim Pusat TIK atas fasilitas perangkat dan laboratorium yang telah digunakan.

Daftar Pustaka

[1] Teknokrat, "Visi Misi," *Universitas Teknokrat Indonesia*, 2015. [Online]. Available: https://www.teknokrat.ac.id/en/about-us/profile/visi-misi. [Accessed: 18-Apr-2019].

[2] Anom, "Pengertian dan Fungsi Wireshark, sisi Hacker vs Administrator Jaringan," 2017. [Online]. Available: https://meretas.com/wireshark-adalah/. [Accessed: 18-Feb-2019].

[3] Adyatma Yoga, "Mikrotik.ID : Konfigurasi VPN PPTP pada Mikrotik," 2018. [Online]. Available: http://www.mikrotik.co.id/artikel_lihat.php?id=43. [Accessed: 19-Mar-2019].

[4] Anom, "Definisi Hacking | Penjelasan Hacking," 2014. [Online]. Available: https://penjelasanhacking.wordpress.com/2014/06/27/definisi-umum-hacking/. [Accessed: 19-Mar-2019].

[5] B. Mahbooba and M. Schukat, "Digital certificate-based port knocking for connected embedded systems," *2017 28th Irish Signals Syst. Conf. ISSC 2017*, pp. 1–5, 2017.

[6] A. Amarudin, "Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking," *J. Teknoinfo*, vol. 12, no. 2, p. 72, 2019.

[7] A. Amarudin, "Analisis dan Implementasi Keamanan Jaringan pada Mikrotik Router OS Menggunakan Metode Port Knocking," pp. 1–7, 2018.

[8] Y. Hendriana, "Evaluasi Implementasi Keamanan Jaringan Virtual Private Network (VPN)(Studi Kasus pada CV. Pangestu Jaya)," *J. Teknol.*, vol. 5, no. 2, pp. 132–142, 2012.

[9] H. Supriyono, J. A. Widjaya, and A. Supardi, "Penerapan Jaringan Virtual Private Network Untuk Keamanan Komunikasi Data Bagi PT. Mega Tirta Alami," 2013.

[10] B. B. Deutsche Forschungsgemeinschaft., *Forum, qualitative social research*, vol. 6, no. 2. Deutsche Forschungsgemeinschaft, 2000.

[11] P. Gill, K. Stewart, E. Treasure, and B. Chadwick, "Methods of data collection in qualitative research: interviews and focus groups," *Bdj*, vol. 204, p. 291, Mar. 2008.

[12] A. Alamsyah and A. A. Arus, "Analisis Sistem Pendaftaran pada Web Forum Ilmiah Matematika Unnes 2014," *Sci. J. Informatics*, vol. 1, no. 1, pp. 107–117, 2015.