e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed)
Vol.8 No.2 (December 2024)
Journal of Information System, Informatics and Computing
Website/URL: http://journal.stmikjayakarta.ac.id/index.php/jisicom
Email: jisicom@stmikjayakarta.ac.id , jisicom2017@gmail.com

Implementing Virtual Private Network (VPN) Network Security Using A Mikrotik Router

(*Implementasi Keamanan Jaringan Virtual Private Network (VPN) Menggunakan Router Mikrotik)*

Sari Dewi[1], Dwi Yuni Utami[2]

Program Studi Sistem Informasi (D3) PSDKU Kota Pontianak,
Program Studi Teknologi Komputer[2],
Fakultas Teknik dan Informatika
Universitas Bina Sarana Informatika; Jalan Kramat Raya No 98
Kwitang, Jakarta Pusat, 10450, Jakarta, Indonesia

Sari.sre@bsi.ac.id[1], dwi.dyu@bsi.ac.id[2]

Received: 2024-10-30. **Revised:** 2024-11-25. **Accepted:** 2024-11-29.
Issue Period: Vol.8 No.2 (2024), Pp. 220-231

Abstrak: Setiap aspek dalam perusahan membutuhkan jaringan lokal dan jaringan internet untuk mengolah data dan mempermudah pekerjaan kantor selalu membutuhkan teknologi jaringan komputer. Seiring berkembangnya teknologi, tuntutan terhadap keamanan data dan informasi pun ikut berkembang. Virtual Private Networks (VPN) adalah teknologi yang sering digunakan yang dapat menawarkan tingkat perlindungan ekstra terhadap transfer data melalui jaringan publik. Tujuan dari penelitian ini adalah menggunakan MikroTik Router OS sebagai gateway untuk menyelidiki dan mengimplementasikan keamanan jaringan VPN. PT. Tifico Fiber Indonesia berfungsi sebagai lokasi studi kasus. Untuk menjamin keamanan data yang dikirimkan melalui jaringan publik, MikroTik Router OS dikonfigurasi sebagai server VPN. Penelitian ini menggunakan (IP) publik Dimungkinkan untuk membuat jaringan pribadi virtual pada perangkat Mikrotik, menghubungkan perangkat jaringan di jaringan lokal satu sama lain, dan mengaktifkan akses jarak jauh. Sejumlah perangkat jaringan di tempat kerja diakses, koneksi jaringan pribadi virtual dicoba, dan pertukaran atau pengambilan data pada perangkat laptop di jaringan lokal bisnis yang sepenuhnya dapat diakses oleh pengguna yang tidak berada dalam lokasi kantor diuji. Menurut temuan penelitian, operasional kantor dapat memperoleh manfaat besar dari penggunaan VPN untuk mengakses data yang terletak di jaringan lokal dan dapat diakses sepenuhnya dari jarak jauh.
Kata kunci: VPN, Mikrotik, Web proxy

Abstract: *Very aspect of a company requires a local network and internet network to process data and make office work easier, always requiring computer network technology. As technology develops, demands for data and information security also grow. Virtual Private Networks (VPN) is a frequently used technology that can offer an extra level of protection against data transfer over public networks. The aim of this research is to use MikroTik Router OS as a gateway to investigate and implement VPN network security. PT. Tifico Fiber Indonesia serves as a case study*

DOI: 10.52362/jisicom.v8i2.1653

e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed)
Vol.8 No.2 (December 2024)
Journal of Information System, Informatics and Computing
Website/URL: http://journal.stmikjayakarta.ac.id/index.php/jisicom
Email: jisicom@stmikjayakarta.ac.id , jisicom2017@gmail.com

location. To ensure the security of data sent over public networks, MikroTik Router OS is configured as a VPN server. This research uses public (IP). It is possible to create a virtual private network on Mikrotik devices, connect network devices on a local network to each other, and enable remote access. A number of workplace network devices were accessed, virtual private network connections were attempted, and exchange or retrieval of data on laptop devices on a business local network that was fully accessible to users not within the office premises was tested. According to research findings, office operations can greatly benefit from using a VPN to access data that is located on the local network and can be accessed completely remotely.

Keywords: VPN, Mikrotik, Web proxy

I. PENDAHULUAN

Perkembangan teknologi komputer yang semakin pesat mengakibatkan badan usaha maupun lembaga akademik mengimplementasika teknologi ini untuk banyak keperluan-keperluannya., untuk koneksinya harus bisa menghubungkan antara kota, atau wilayah yang berjauhan dengan kabel jaringan. Pembangunan jaringan komputer seperti itu akan sangat mahal sekali untuk saat ini harus bisa bagaimana caranya membangun infrastruktur jaringan yang menghubungkan antara wilayah yang berjauhan seperti antar kota, provinsi bahkan berbeda negara sekalipun. Pembangunan *Wide Area Network* menjadi tidak efektif lagi, untuk saat ini dibutuhkan bagaimana memanfaatkan jaringan public yang sudah ada yaitu jaringan internet yang bisa menghubungan seluruh dunia [1]. Komputer *client* banyak yang terinsfeksi virus, ini karena terbukanya *port-port* untuk membaca dan menyimpan data pada komputer-komputer yang diperuntukkan untuk user, Banyak situs yang dilarang perusahaan tetapi masih bisa di buka contoh *facebook* dan *twitter*, Sering terputus ditengah jalan mengirim *email*, komputer *client* terkadang tidak dapat mengakses *server* pusat. Banyaknya kemungkinan aksi hacking dan data-sniffing membuat suatu pertanyaan. Apakah pertukaran data yang di lakukan di internet dengan media LAN maupun nirkabel benar – benar aman.

Untuk itu dibutuhkan alternatif untuk masalah-masalah yang ada yaitu dengan membangun *Virtual Private Network (VPN)*. Oleh karena itu VPN dapat digunakan sebagai teknologi alternatif untuk menghubungkan jaringan lokal yang luas dengan biaya yang relatif kecil, karena transmisi data teknologi VPN menggunakan media jaringan publik yang sudah ada yaitu internet. Integritas Data, paket data yang dilewatkan di jaringan publik perlu penjaminan integritas data / kepercayaan data apakah terjadi perubahan atau tidak Pemanfaatan jaringan internet dengan *VPN* merupakan jalan keluar dari kebutuhan jaringan komputer [2]. dengan adanya VPN dimungkinkan seorang pengguna atau jaringan yang berjauhan dapat berhubungan seperti dalam satu jaringan lokal. VPN – WAN dapat mengurangi biaya pembuatan infrastruktur jaringan dan memotong biaya operasional dengan memanfaatkan failitas *internet* sebagai media komunikasinya. [3]. Atas dasar tersebut diatas maka penulis memanfaatkan teknologi RoutersOS Mikrotik untuk jaringan *Virtual Private Network* (VPN) untuk digunakan untuk meremot jaringan via *internet* yang digunakan sewaktu-waktu *Technical Support* atau IT berada diluar gedung untuk mengontrol jaringan atau mengkonfigurasi *server* atau keperluan lainnya [4]. Karena hal tersebut diatas, penulis merasa pada PT. TIFICO FIBER INDONESIA perlu membangun dan mengembangkan jaringan computer.

II. METODE DAN MATERI

Analisa Penelitian

a. Analisa Kebutuhan

DOI: 10.52362/jisicom.v8i2.1653

e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed)
Vol.8 No.2 (December 2024)
Journal of Information System, Informatics and Computing
Website/URL: http://journal.stmikjayakarta.ac.id/index.php/jisicom
Email: jisicom@stmikjayakarta.ac.id , jisicom2017@gmail.com

VPN merupakan perpaduan dari teknologi tunneling dengan teknologi enkripsi. Teknologi tunneling bertugas untuk menangani dan menyediakan koneksi point-to-point dari sumber ke tujuannya. Sedangkan teknologi enkripsi menjamin kerahasiaan data yang berjalan di dalam tunnel [5].
untuk membangun VPN, ada beberapa tahap yang harus dilakukan:
1. Pemilihan jenis implementasi VPN
2. Pemilihan protokol VPN

b. Desain

Teknologi VPN (*Virtual Private Network*) didasarkan pada strategi *tunneling. Tunneling* yang menyertakan paket enkapsulasi yang dikonstruksi dalam sebuah format protokol dasar dalam beberapa protocol lainnya. Dalam kasus dimana VPN berjalan melewati Internet, dipakai dalam satu dari beberapa protocol VPN di enkapsulasi dalam paket IP [6].

c. Testing

Teknologi VPN (*Virtual Private Network*), mengklarifikasikan identitas *client* sesuai dengan otoritasnya, dan akan mendapatkan IP *address Client intranet* yang bersifat rahasia, setelah sukses akan masuk ke IP lokal jaringan tersebut dan dapat mengakses jaringan yang bersifat lokal.

d. Implementasi

Dilihat dari jaringan yang digunakan, termasuk dalam kategori Site-to-site VPN. Site-to-site VPN merupakan jenis implementasi VPN yang menghubungkan antara dua tempat atau lebih yang letaknya, berjauhan, seperti halnya menghubungkan kantor pusat dengan kantor cabang, baik kantor yang dimiliki perusahaan itu sendiri maupun kantor perusahaan mitra kerjanya.
VPN yang digunakan untuk menghubungkan kantor pusat dengan kantor cabang suatu perusahaan disebut intranet site-to-site VPN. sedangkan bila VPN digunakan untuk menghubungkan suatu perusahaan dengan perusahaan lain (misalnya mitra kerja atau pelanggan), implementasi ini termasuk jenis ekstranet [7].dengan implemetasinya, untuk dapat menghubungkan kantor pusat dengan kantor cabang, pada masing-masing kantor dibutuhkan sebuah router (gateway), yang dalam penelitian ini digunakan mikrotik RB 450 sebagai server VPN di kantor pusat.Teknologi VPN (*Virtual Private Network*) memungkinkan seorang pengguna atau jaringan yang berjauhan dapat berhubungan seperti dalam satu jaringan lokal.

Metode Pengumpulan Data

Metode penelitian yang dilakukan penulis dalam proses penulisan Penelitian ini adalah sebagai berikut:

a. Observasi

Dalam metode ini penulis mengadakan kunjungan langsung ke PT. Tifico Fiber Indonesia, dimana segala yang berhubungan dengan teknologi dan sistem informasi berpusat disini.

b. Wawancara

Untuk mendapatkan informasi atau data yang diperlukan dalam penulisan Penelitian ini penulis melakukan wawancara dengan orang-orang IT di PT. Tifico Fiber Indonesia

Penelitian yang dilakukan penulis dalam menyusun Penelitian menganalisa tentang penggunaan Mikrotik sebagai pusat pengelola jaringan lokal dan komunikasi data. Adapun ruang lingkup dari Penelitian ini adalah Mengkonfigurasikan VPN (*Virtual Private Network*) dengan menggunakan RouterOS Mikrotik.

III. PEMBAHASA DAN HASIL

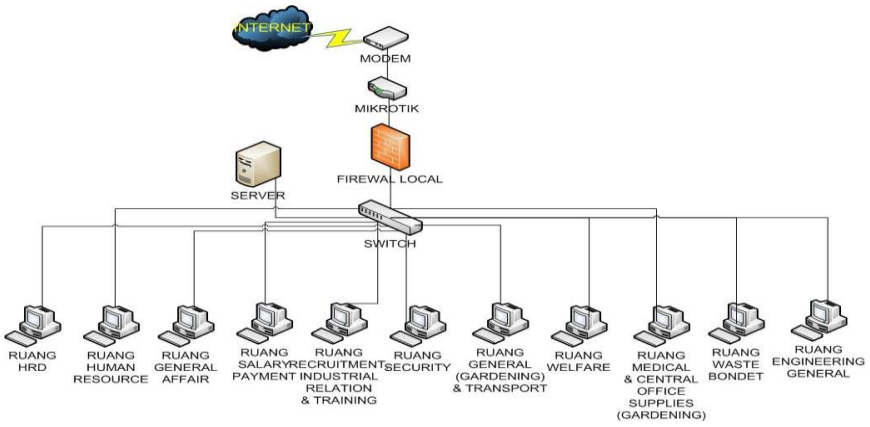
Dalam membangun sebuah jaringan *Virtual Private Network* (VPN) tidak hanya terpusat pada transfer atau akses datanya saja tapi infrastruktur sebuah jaringan harus lebih diperhatikan, karena infra struktur ini akan membuktikan apakah sebuah jaringan akan bertahan lama atau sebaliknya.Dalam penjelasan secara menyeluruh dari sistem jaringan yang sedang berjalan, maka penulis mencoba menggambarkan keadaan jaringan komputer yang ada di dan infrastrukturnya sebagai berikut:

DOI: 10.52362/jisicom.v8i2.1653

e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed)
Vol.8 No.2 (December 2024)
Journal of Information System, Informatics and Computing
Website/URL: http://journal.stmikjayakarta.ac.id/index.php/jisicom
Email: jisicom@stmikjayakarta.ac.id , jisicom2017@gmail.com

3.3.1 Topologi Jaringan

Topologi jaringan adalah sebuah bentuk gambaran secara logika dalam suatu infrastruktur sebuah jaringan baik itu LAN, MAN maupun WAN. Sebelum membuat jaringan maka diperlukan suatu bentuk jaringan atau topologi. Di PT. Tifico Fiber Indonesia menggunakan tipe star, karena di tiap-tiap gedung setiap *client* nya terhubung dengan switch. hanya komputer yang tidak terhubung dengan jaringanlah yang mempunyai keamanan yang sempurna [8]. Teknologi QoS adalah teknologi yang memungkinkan *administrator* jaringan untuk dapat menangani berbagai efek akibat terjadinya konjesti pada lalu lintas aliran paket dari berbagai layanan. Penanganan QoS dilakukan dengan memanfaatkan sumber daya jaringan secara optimal, dibandingkan dengan menambah kapasitas fisik jaringan tersebut. Meningkatnya berbagai layanan akan meningkatkan lalu lintas aliran paket dengan berbagai laju kecepatan, yang akan membutuhkan kemampuan jaringan melalukan aliran paket pada laju kecepatan tertentu [9].



Gambar 1. Topologi Jaringan

Secara umum model layanan untuk memberikan fungsi QoS adalah sebagai berikut:

1. *Best Effort Service*

Best Effort merupakan model pelayanan QoS yang paling sederhana, di mana paket-paket dapat dikirimkan setiap waktu, tanpa terlebih dahulu bernegosiasi dengan kemampuan jaringan. Jaringan akan memberikan kemampuan terbaiknya mengirimkan paket-paket tersebut [15].

2. *Integrated Service (IntServ)*

Intserv merupakan model pelayanan yang terintegrasi untuk menangani kebutuhan beragam QoS. Sebelum mengirimkan paket data, model pelayanan ini akan mengaplikasikan layanan khusus ke dalam jaringan yang ditangani dengan proses signaling (Riskiono, 2019). *Diffserv* merupakan model yang memberikan multilayanan yang menghendaki kebutuhan QoS yang berbeda-beda. Berbeda dengan *Intserv*, *Diffserv* tidak mengaplikasikan RSVP sehingga tidak meminta *router-router* untuk menyediakan sumber daya jaringan untuk melakukan pengiriman paket. *Diffserv* menyediakan layanan khusus menurut QoS yang dikehendaki

DOI: 10.52362/jisicom.v8i2.1653

e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed)
Vol.8 No.2 (December 2024)
Journal of Information System, Informatics and Computing
Website/URL: http://journal.stmikjayakarta.ac.id/index.php/jisicom
Email: jisicom@stmikjayakarta.ac.id , jisicom2017@gmail.com

oleh masing-masing paket, misalnya dengan menggunakan teknik IP *Precedence*. Jaringan akan melakukan *packet classification, traffic shaping, traffic policing,* dan *queuing* berdasarkan informasi yang diberikan)[13]. *Quality of Service* (QoS) berarti *router* baru melakukan prioritas dan mengatur *traffic* jaringan. Qos tidak hanya membatasi saja tetapi lebih menjaga kualitas, untuk menjalankan QoS mikrotik mempunyai mekanis memengatur *bandwith* antara lain([11] jaringan private yang menghubungkan seluruh kantor cabang yang ada atau yang biasa disebut dengan *Wide Area Network (WAN).* Dengan berkembangnya jaringan publik atau biasa disebut dengan internet, solusi dengan membangun *WAN* menjadi solusi yang sangat mahal dan tidak fleksibel. Dengan berkembangnya *Virtual Private Network* (*VPN*), sebuah organisasi dapat membangun jaringan *private* maya diatas jaringan publik untuk menghubungkan seluruh kantor cabang yang dimilikinya [10].

PT. Tifico Fiber Indonesia menggunakan IP address kelas C yang lebih jelas ada pada tabel berikut:

Tabel 1. IP Address PT. Tifico Fiber Indonesia

Perangkat	IP Address	Subnet Mask	Gateway
Modem	192.168.1.1	255.255.255.0	-
Mikrotik	192.168.1.2	255.255.255.0	192.168.1.1
	192.168.10.1	255.255.255.0	-
Ruang HRD	192.168.10.50	255.255.255.0	192.168.10.1
Ruang Human Resource	192.168.10.90	255.255.255.0	192.168.10.1
Ruang General Affair	192.168.10.101	255.255.255.0	192.168.10.1
Ruang Salary Payment	192.168.10.121	255.255.255.0	192.168.10.1
Ruang Recruitment Industrial Relation & Training	192.168.10.131	255.255.255.0	192.168.10.1
Ruang Security	192.168.10.151	255.255.255.0	192.168.10.1
Ruang General (Gardening) & Transport	192.168.10.161	255.255.255.0	192.168.10.1
Ruang Welfare	192.168.10.171	255.255.255.0	192.168.10.1
Ruang Medical & Central Office Supplies	192.168.10.181	255.255.255.0	192.168.10.1
Ruang Waste Bondet	192.168.10.210	255.255.255.0	192.168.10.1
Ruang Engineering General	192.168.10.230	255.255.255.0	192.168.10.1
VPN Client 1	192.168.2.201	255.255.255.0	-
VPN Client 2	192.168.2.202	255.255.255.0	-

4.1.1 Analisa Kebutuhan

Topologi jaringan saat ini memungkinkan terjadinya kejahatan komputer pada sisi klien adalah Manipulation - komputer antara akan mengganti informasi dalam data yang dikirimkan. Jaringan distribusi yang telah dijabarkan peneliti pada gambaran umum pada Pt. Tifico Fiber Indonesia. Permasalahan seperti inilah yang harus disadari oleh pengguna internet yangmemiliki kerentanan data dan ini bisa saja menjadi kerugian bagi

DOI: 10.52362/jisicom.v8i2.1653

e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed)
Vol.8 No.2 (December 2024)
Journal of Information System, Informatics and Computing
Website/URL: http://journal.stmikjayakarta.ac.id/index.php/jisicom
Email: jisicom@stmikjayakarta.ac.id , jisicom2017@gmail.com

suatu perusahaan apabila tidak disikapi. Virtual Private Network (VPN) site to site merupakan solusi dari permasalahan yang ada untuk mengamankan jalur distribusi [12].

4.1.2 Desain

Sistem yang dibangun melibatkan beberapa tahapan, yaitu mengambil username dan password dari textbox, mengubah data text dari String menjadi ASCII, enkripsi data, mengirimkan data yang telah dienkripsi, dekripsi data yang telah diterima oleh server. Tahapan pembangunan sistem sebagai berikut :

1. Proses Pada Client.

   Pada tahap ini diawali dengan user pada sisi client mengetikkan username dan password pada textbox halaman login kemudian menekan tombol “Connect”. Kemudian data tersebut diubah ke bentuk ASCII lalu dilakukan proses encapsulasi dengan vpn menggunakan protocol *pptp*. Setelah itu data dikrimkan melalui jaringan.

2. Proses pada sisi server

   Pada tahap ini diawali dengan proses pembuatan user yang ingin berkomunikasi dengan jaringan yang satu jaringan dengan vpn-server. Vpn server berfungsi sebagai penyedia jalur khusus yang dibuat untuk melakukan koneksi secara privat dan untuk melakukan proses enkapsulasi data terhada suatu jaringan yang dilewati oleh *cient* [11].

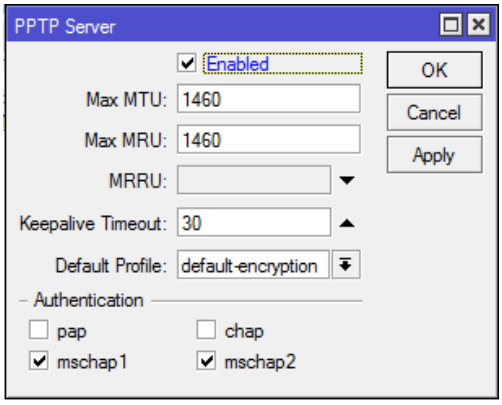
4.1.3 Testing.

Apabila semua telah terpasang dengan baik dan benar maka langkah selanjutnya adalah pengujian konektifitas jaringan.

1. Pengujian konektifitas jaringan, menguji atau mengetes jaringan dilakukan untuk mengutahui apakah komputer yang kita konektifitaskan telah berhasil masuk dalam jaringan yang dituju. Hal ini dapat dilakukan dengan cara berikut:
   Komputer *Router 1 (ISP 1)*
   a. *Router* disini merupakan sebuah di setting mempunyai fungsi sebagai ISP, VPN server
   b. VPN server ini menggunakan router Mikrotik RB 450. Supaya VPN server bisa berkomunikasi dengan berbagai client, maka di VPN server di install *PPTP Server*.
   c. Pada komputer client, Client menggunakan sistem operasi *Microsoft Windows* yang support terhadap *PPTP*.
   d. Konfigurasi PPTP Server
      Berdasar topologi di atas, yang menjadi pusat dari link PPTP (konsentrator) adalah Router Office A , maka kita harus melakukan setting PPTP Server pada router tersebut.
   e. -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.

DOI: 10.52362/jisicom.v8i2.1653

e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed)
Vol.8 No.2 (December 2024)
Journal of Information System, Informatics and Computing
Website/URL: http://journal.stmikjayakarta.ac.id/index.php/jisicom
Email: jisicom@stmikjayakarta.ac.id , jisicom2017@gmail.com



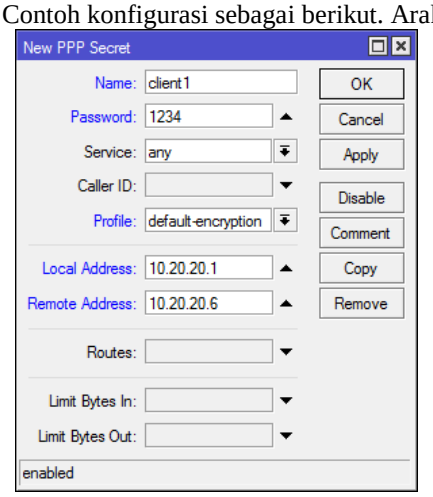
Gambar 2 , aktifasi VPN PPTP

f. Pada tahap ini, kita bisa menentukan **username** dan **password** untuk proses autentikasi Client yang akan terkoneksi ke PPTP server. Penggunaan huruf besar dan kecil akan berpengaruh.

g.

-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.

Contoh konfigurasi sebagai berikut. Arahkan agar menggunakan profile "Default-Encryption"



Gambar 3. Konfigurasi user

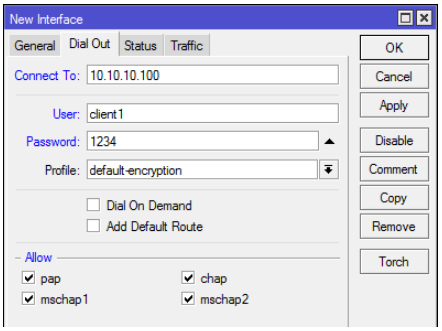
Sampai disini, konfigurasi Router A (PPTP Server) sudah selesai, sekarang kita lakukan konfigurasi di sisi client.

Client Router Office 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.

DOI: 10.52362/jisicom.v8i2.1653

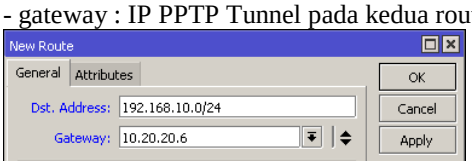
e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed)
Vol.8 No.2 (December 2024)
Journal of Information System, Informatics and Computing
Website/URL: http://journal.stmikjayakarta.ac.id/index.php/jisicom
Email: jisicom@stmikjayakarta.ac.id , jisicom2017@gmail.com



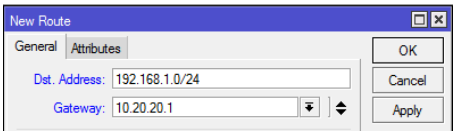
Gambar 4,Konfigurasi interface

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

- dst-address : jaringan local Router lawan
- gateway : IP PPTP Tunnel pada kedua router.

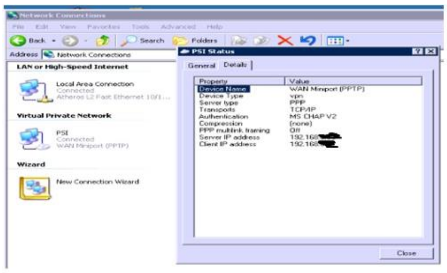


Gambar 5. Penambahan static route di Router A



Gambar 6. Penambahan static route di router B

h. Pengujian VPN dapat dilakukan melalui komputer client, untuk mendeteksi apakah hubungan komputer sudah berjalan dengan baik, maka dilakukan utilitas ping. Ping digunakan untuk mengetahui konektifitas yang terjadi dengan IP address yang tujuan. Dari Gambar Tersebut di dapat ip client



Gambar 7 Pengujian VPN PPTP

Setelah Connect tes Ping ke IP local VPN Server. Perintah ping untuk IP Address 192.168.10.1 (ip vpn server/lokal), jika kita lihat ada respon pesan balasan atas perintah ping yang kita berikan,. diperoleh informasi berapa kapasitas pengiriman dengan waktu berapa lama memberikan tanda bahwa perintah untuk menghubungkan ke IP Address telah berjalan dengan baik Setelah dilakukan pengujian pada

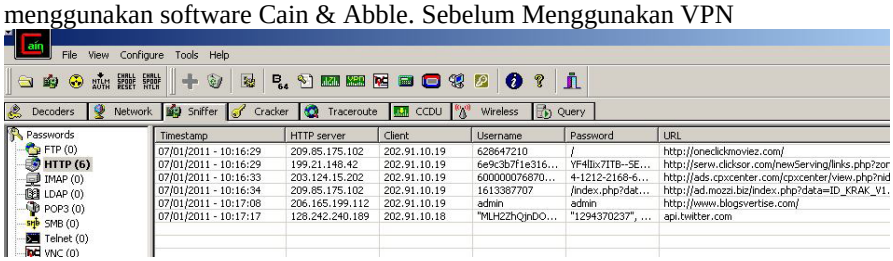
DOI: 10.52362/jisicom.v8i2.1653

e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed)
Vol.8 No.2 (December 2024)
Journal of Information System, Informatics and Computing
Website/URL: http://journal.stmikjayakarta.ac.id/index.php/jisicom
Email: jisicom@stmikjayakarta.ac.id , jisicom2017@gmail.com

sistem jaringan, di setiap komputer telah dapat terhubung dengan baik. Jadi jaringan tersebut dapat masuk ke jaringan lokal, serta dapat digunakan untuk sharing data, remote access, masuk ke web yang diakses secara lokal dan sebagainya.

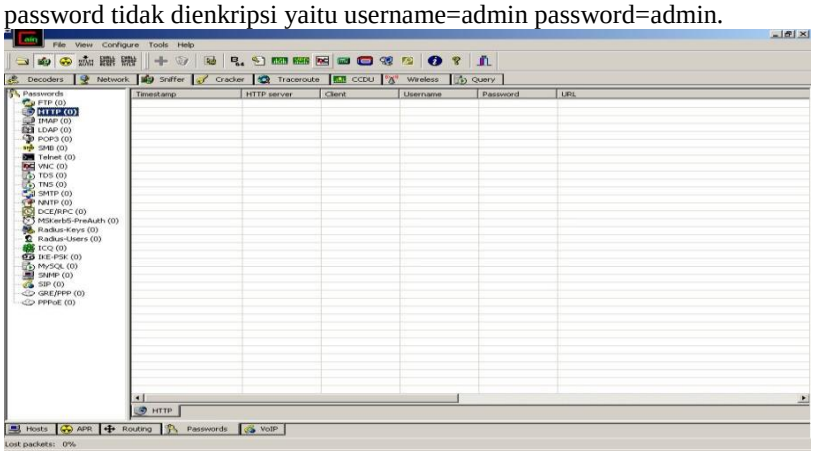
4.1.4 Implementasi Keamanan jaringan

Keamanan Data, Banyaknya data yang bisa disadap oleh hacker melalui teknik MIMA (Man In the Middle Attack) dikarenakan data yang dikirim kejaringan terbuka tidak dienkipsi. Ini bisa dibuktikan dengan menggunakan software Cain & Abble. Sebelum Menggunakan VPN



Gambar 8 Sniffing Menggunakan Cain & Abble

Gambar diatas adalah hasil dari proses sniffing terhadap sebuah website review www.blogvertise.com yang banyak digunakan oleh para blogger. Terlihat jelas username dan password tidak dienkripsi yaitu username=admin password=admin.



Gambar 9 Hasil Pengujian

Gambar diatas menunjukan bahwa tidak ada proses yang dilakukan oleh client,
padahal client melakukan banyak aktivitas seperti membuka website, tetapi pada sisi hacker tidak terbaca. Hal ini dikarenakan Client telah membangun sebuah tunnel atau terowongan langsung pada VPN Server dan data yang dikirim melalui client dienkripsi sehingga walaupun data yang dikirim berhasil disadap oleh hacker

4.3 Rancangan Sistem Keamanan Jaringan

Untuk merancang sebuag keamanan yang baik dan *secure* harus dilakukan secara baik dan benar. Agar jaringan ini dapat kuat dan bertahan lama. Dengan menggunakan VPN hanya jaringan tertentu aja yang bisa masuk ke dalam *server* atau pusatnya.

1. Konfigurasi Keamanan Winbox

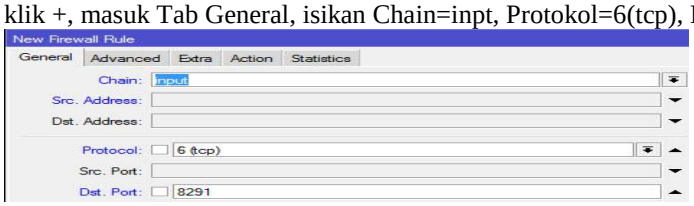
Untuk menjaga agar router ini lebih aman, maka penulis mengkonfigurasikan winbox ini, hanya bisa di setting lewat lokal saja. Jadi, agar tidak sembarang orang bisa mengkonfigurasikannya tanpa sepengetahuan orang IT tersebut. Untuk mengkonfigurasikannya adalah sebagai berikut:

a. Klik menu IP>Firewall
b. klik +, isikan name= our network, dan ip address 192.168.10.0/24

DOI: 10.52362/jisicom.v8i2.1653

e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed)
Vol.8 No.2 (December 2024)
Journal of Information System, Informatics and Computing
Website/URL: http://journal.stmikjayakarta.ac.id/index.php/jisicom
Email: jisicom@stmikjayakarta.ac.id , jisicom2017@gmail.com

c. Klik OK
d. Klik menu Firewall>Filter Rules
e. klik +, masuk Tab General, isikan Chain=inpt, Protokol=6(tcp), Dst Port=8291



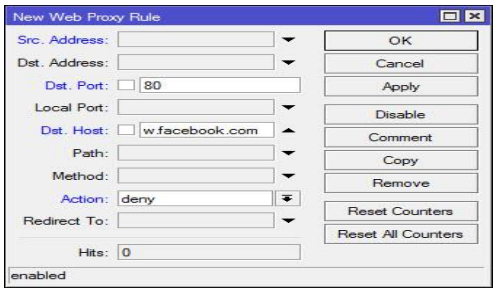
Gambar 10. Setting untuk web Proxy

f. Masuk ke Tab, Advance, isikan Src.Address=our network
g. Masuk ke Tab, Action, isikan Action=accept
h. lalu klik ok

2. Memblock situs-situs yang tidak diperbolehkan

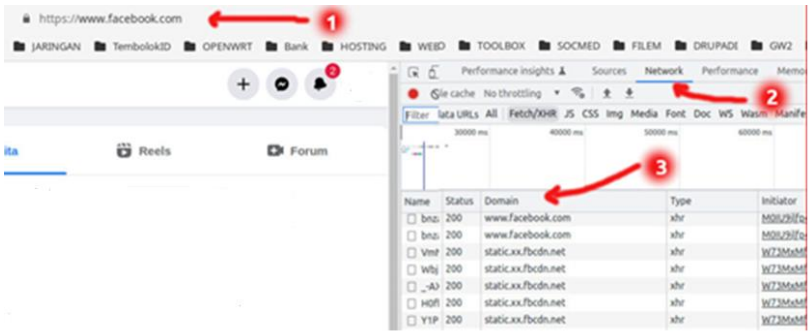
Untuk menjaga agar kinerja perusahaan ini tetap terjaga, maka penulis memblock situs-situs yang dilarang oleh PT. TIFICO FIBER INDONESIA. Jadi, agar tidak ada sembarang orang yang bisa mengakses situs-situs tersebut. Untuk mengkonfigurasikannya adalah sebagai berikut:

a. Klik IP> Pilih Web Proxy
Klik tanda +,
Isikan Dst.Port: 80
Dst.Host: "www.facebook.com" (catatan: saya akan memblok situs "www.facebook.com")
Action: deny
Lalu klik Apply dan pilih Ok



Gambar 11. Settingan untuk blok situs

Tampilan setelah dibokir situs



Gambar 12. Hasil Blok situs

DOI: 10.52362/jisicom.v8i2.1653

e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed)
Vol.8 No.2 (December 2024)
Journal of Information System, Informatics and Computing
Website/URL: http://journal.stmikjayakarta.ac.id/index.php/jisicom
Email: jisicom@stmikjayakarta.ac.id , jisicom2017@gmail.com

Untuk Blokir aplikasi, game dan website sudah tidak bisa menggunakan layer 7 protocol, karena koneksi sekarang sudah dienkripsi menggunakan SSL/HTTPS. Sehingga content yang ada di dalam traffic tidak bisa dibaca oleh mikrotik. Alternatifnya kita harus membuat list server yang akan diblokir lalu menandai koneksinya baru bisa kita ablokir.

IV. KESIMPULAN

Setelah mempelajari dan menganalisis sistem jaringan di PT. Tifico Fiber Indonesia maka penulis dapat mengambil kesimpulan bahwa Untuk itu sebaiknya perusahaan menggunakan Virtual Private Network (VPN) agar keamanannya lebih baik dari sebelumnya, serta memiliki kelebihan seperti fasilitas koneksi jarak jauh (access remote). Penggunaan *VPN* akan menjadi sangat populer saat ini karena *VPN* memberikan jaminan keamanan dan reliabilitas yang hampir sama dengan jaringan pribadi. *VPN* sangat mudah digunakan, dengan menginstalasikan *VPN client* pada komputer atau laptop pemakai, maka pemakai dapat akses ke *Lokal Area Network* dengan fasilitas *VPN* lewat jaringan internet Dengan adanya simulasi ini maka memudahkan untuk dilakukan pengujian bentuk model jaringan dan jenis *protocol routing* yang ingin di implementasikan pada PT. Tifico Fiber Indonesia.

REFERENASI

[1] Wardana, M. A., Nusri, A. Z., & Juliandika, J. (2022). Jaringan Virtual Private Network (Vpn) Berbasis Mikrotik Pada Kantor Kecamatan Marioriawa Kabupaten Soppeng. *Jurnal Ilmiah Sistem Informasi Dan Teknik Informatika (JISTI)*, *5*(2), 107–116. https://doi.org/10.57093/jisti.v5i2.135

[2] Arfind, R., Supendar, H., & Riza Fahlapi. (2023). Perancangan Virtual Private Network Dengan Metode PPTP Menggunakan Mikrotik. *Jka*, *1*(3), 108–116.

[3] Riskiono, S. D. (2019). *ANALISIS DAN DESAIN JALUR TRANSMISI JARINGAN ALTERNATIF MENGGUNAKAN VIRTUAL PRIVATE NETWORK (VPN)*. *13*(2), 100–106.

[4] Afrianto, N., Gusti, D., Candra, A., Putra, B. P., Meiditra, I., Fitriyanto, I., & Sugiantoro, B. (2024). *Perancangan Jaringan Vpn Dan Keamanan Data Menggunakan Tunelling Pada Laboratorium Komputer UIN Sunan Kalijaga Yogyakarta*. *12*(1), 27–38.

[5] Sulistiyono, S. (2020). Perancangan Jaringan Virtual Private Network Berbasis Ip Security Menggunakan Router Mikrotik. *PROSISKO: Jurnal Pengembangan Riset Dan Observasi Sistem Komputer*, *7*(2), 150–164. https://doi.org/10.30656/prosisko.v7i2.2523

[6] Ruslianto, I. (2019). Perancangan dan Implementasi Virtual Private Network (VPN) menggunakan Protokol SSTP (Secure Socket Tunneling Protocol) Mikrotik di Fakultas MIPA Universitas Tanjungpura. *Computer Engineering, Science and System Journal*, *4*(1), 74. https://doi.org/10.24114/cess.v4i1.11792

[7] Atmoko, A. T., Surya Budiman, A., & Nuraeni, N. (2024). Perancangan Dan Pengembangan Virtual Private Network (VPN) Menggunakan PPTP Pada PT Indobinatu Mitra Sejati Design and Development of Virtual Private Network (VPN) Using PPTP in PT Indobinatu Mitra Sejati. *Jtsi*, *5*(1), 160–170.

[8] Sari, L. O. (2024). *Virtual Private Network Implementation Using Mikrotik Based Layer 2 Tunneling Protocol Implementasi Virtual Private Network MenggunakanLayer 2 Tunneling Protocol Berbasis Mikrotik*. *4*(October), 1496–1504.

[9] Rahino, B. G., & Susila, A. (2022). *Implementasi Jaringan VPN (L2TP / Ipsec) Mikrotik Untuk Remote Access Sebagai Security Selama Work From Home*. *1*(11), 1911–1918.

[10] Eko Syah Putra Siahaan. (2021). VIRTUAL PRIVATE NETWORK DENGAN. *JURNALCOMASIE*, *05*(02).

[11] Dewi, S., & Teknik, F. (2022). ANALISA VIRTUAL PRIVATE NETWORK (VPN) IP MULTI PROTOCOL LABEL SWITCHING (MPLS) UNTUK JARINGAN WIDE AREA NETWORK (WAN). *Jisamar*, *6*(1), 16–25. https://doi.org/10.52362/jisamar.v6i1.662

[12] Christo, P., Mulyono, H., Yayasan, D., & Dasar, S. (2022). *PENERAPAN PRIVATE ACCESS MENGGUNAKAN METODE PPTP DAN OVPN DI YAYASAN UMMU ' L QURO DEPOK t : JIKA | 257*. *6*(3), 256–263.

DOI: 10.52362/jisicom.v8i2.1653

e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed)
Vol.8 No.2 (December 2024)
Journal of Information System, Informatics and Computing
Website/URL: http://journal.stmikjayakarta.ac.id/index.php/jisicom
Email: jisicom@stmikjayakarta.ac.id , jisicom2017@gmail.com

[13] Ekawati, I., & Irwan, D. (2021). *Implementasi Virtual Private Network Menggunakan PPTP Berbasis Mikrotik*. *9*(1), 41–48.

[14] Phang, V., & Setyaningsih, E. (2021). Perancangan Virtual Private Network Dengan Protokol Pptp Menggunakan Mikrotik Untuk Kebutuhan Remote Access. *Power Elektronik : Jurnal Orang Elektro*, *10*(2), 68. https://doi.org/10.30591/polektro.v10i2.2573

[15] Wulandari, T. P., Reza, N. R., & Deswana, E. Z. (2024). *Penerapan VPN Dalam Topologi Star Untuk Keamanan Pengiriman Data*. *2*(2).

DOI: 10.52362/jisicom.v8i2.1653