p-ISSN : 2406-7733
e-ISSN : 2597-9922

PERANCANGAN JARINGAN *VIRTUAL PRIVATE NETWORK* BERBASIS *IP SECURITY* MENGGUNAKAN *ROUTER MIKROTIK*

Ayu Purnama Sari[1], Sulistiyono[2], Naga Kemala[3]
[1]Program Studi Sistem Informasi Fakultas Teknologi Informasi Universitas Serang Raya
[2]Program Studi Teknik Informatika Fakultas Teknologi Informasi Universitas Serang Raya
[3]Program Studi Rekayasa Sistem Komputer Fakultas Teknologi Informasi Universitas Serang Raya
ayupurnamasarifalizah@gmail.com[1], sulistiyonoputro@gmail.com[2], naga.kemala@gmail.com[3]

Abstrak – Perkembangan teknologi yang semakin maju mempengaruhi suatu sistem dan efisiensi dalam dunia pekerjaan. Oleh karena itu sangat dibutuhkan sekali jaringan internet, selain pentingnya jaringan *internet* juga perusahaan sangat membutuhkan adanya jaringan pribadi (*VPN*) yang aman, sebagai jalur khusus untuk mengakses ke jaringan lokal perusahaan. Untuk mengatasi hal ini maka penulis akan merancang sebuah *VPN IPsec* dengan menggunakan *Router MikroTik*. *VPN* memungkinkan untuk mengakses jaringan lokal perusahaan menggunakan koneksi *internet* publik. Dari hasil riset yang penulis lakukan telah membuktikan bahwa dengan adanya *VPN IPsec* jalur komunikasi menggunakan jaringan publik menjadi lebih aman dengan adanya proses *tunneling VPN* dan enkripsi dari *IPsec*

Kata Kunci : *VPN, IPsec, internet, MikroTik*

I. PENDAHULUAN

Virtual Private Network (*VPN*), merupakan salah satu alternatif untuk pengamanan data karena bersifat privat. *VPN* memungkinkan pengguna dapat masuk ke dalam jaringan lokal, memungkinkan pengguna untuk mengambil data dari dalam jaringan lokal serta melakukan *remote* pada perangkat yang ada di jaringan tersebut.

Salah satu toko di daerah pertokoan di pusat kota serang, Toko gunung jati merupakan toko yang bergerak di jual beli perabotan rumah tangga seperti furnitur, *sofa*, kasur, dan lain lain. Sering kali pemilik tidak berada di toko, dan membutuhkan data yang berada di jaringan lokal. Dikarenakan data-data harga disimpan di dalam komputer lokal. Oleh karena itu dibutuhkan jalur khusus yang bersiftat *private*. Keamanan data juga dapat ditingkatkan dengan adanya *VPN*. Digunakannya *protocol Internet protocol security* (*IPsec*) agar terciptanya perlindungan data dari orang lain yang tidak berhak, dan bahkan perlindungan data dari dibaca oleh orang yang tidak berhak. Penelitian ini dilakukan untuk mengantisipasi adanya kejadian yang tidak diinginkan. Contohnya adanya kebocoran data dari pihak pihak yang tidak berhak, dan mengakibatkan data privasi jadi tersebar.

VPN merupakan suatu bentuk jaringan privat yang melalui jaringan publik dengan berfokus pada keamanan data yang dienkripsi di dalamnya. (*cloudwards.net*: 2017). Hubungan ini dibangun melalui sebuah sistem *tunneling virtual* antar 2 *node*. Salah satu jenis *tunnel* yang akan digunakan adalah *tunnel L2TP*. Dengan menggunakan jaringan publik, pengguna dapat terhubung ke dalam jaringan lokal, mendapatkan hal dan pengaturan yang sama seperti pengguna berada di dalam lokasi kerja.

Untuk mengatasi masalah keamanan dalam berbagi komunikasi dan informasi, maka diperlukan teknologi *Virtual Private Network* (*VPN*). *VPN* merupakan suatu jaringan *LAN* yang terhubung dengan *internet*. Salah satu teknik pengamanan teknologi *VPN* adalah dengan *Internet Protocol Security* (*IPsec*). *IPsec* dibangun berdasarkan teknologi *Internet Protocol* (*IP*) yang bekerja pada lapisan jaringan dan menyediakan layanan kriptografi untuk keamanan dalam transmisi data. *IPsec* juga mendukung layanan autentifikasi, integritasi, kontrol akses, dan kerahasiaan dengan cara *tunnel* pada jaringan dan memproteksi serangan dengan menyembunyikan alamat *IP*.

Dalam membangun sebuah koneksi *VPN*, diperlukan sebuah *Server* yang terkoneksi dengan *IP Public*, sehingga dapat dilakukan *remote* dari jaringan publik ke jaringan lokal pada suatu lokasi, untuk mengatasi hal tersebut dapat menggunakan *Cloud Hosted Router* (*CHR*), yang merupakan suatu *RouterOS* yang berada dalam *Cloud* dan terkoneksi ke *IP public* dan akan menjembatani koneksi *VPN IPsec* yang akan dirancang.

Rancang bangun jaringan *VPN* dengan teknologi *IPsec* dapat diterapkan pada *MikroTik Routerboard*. *MikroTik Routerboard* adalah sebuah sistem operasi *router* yang dapat menjalankan dan mengatur aktifitas jaringan secara menyeluruh, mulai dari manajemen *bandwith*, *routing*, *firewall* dan lain sebagainya. (*MikroTik*.co.id , 2020)

Keamanan data saat berkomunikasi sangatlah penting untuk menjaga *privacy* dari setiap perusahaan. Dengan adanya jalur *Private* pihak dari luar tidak akan bisa masuk kedalam jalur tersebut.

Berdasarkan permasalahan yang telah dibahas maka pada penelitian ini akan berfokus pada membuat jalur komunikasi yang aman mengggunakan *VPN IPsec*. Karena kemampuan dari *IPsec* untuk mengenkripsi data menjadi lebih aman. Dan juga dengan adanya *VPN* komunikasi *data* antara *user* dan *server* yang berada di tempat yang berbeda menjadi

p-ISSN : 2406-7733
e-ISSN : 2597-9922

aman, karena menggunakan *tunnel* khusus yang diberikan oleh jaringan *VPN*.

Sesuai dengan latar belakang, masalah yang akan diteliti dapat dirumuskan sebagai berikut:

1. Bagaimana membangun jalur komunikasi yang aman pada jalur publik sehingga keamanan data dapat terjamin?
2. Bagaimana membangun jaringan *VPN* yang dapat berjalan dengan baik?

Tujuan penelitian ini antara lain sebagai berikut:

1. Terciptanya jalur komunikasi yang aman dengan menggunakan *VPN IPsec*.
2. Terciptanya Komunikasi data secara privat.

II. KAJIAN PUSTAKA

Dhio (2016) dalam penelitiannya yang dilakukan pada Sistem Informasi Pengelolaan Keuangan Daerah (SIPKD). *VPN* digunakan karena aplikasi SIPKD yang berbasis *web base* memiliki *server* yang terpusat berlokasi di kantor gubernur Riau. Sedangkan beberapa kantor ada di daerah di Pekanbaru dan luar Pekanbaru, dan aplikasi ini harus aman dan hanya bisa diakses oleh beberapa orang. Oleh karena itu *VPN* diimplementasikan untuk meningkatkan keamanan dan efisiensi.

Ilyas dan Samsumar (2018) dalam penelitiannya membangun jaringan *internet* berbasis jaringan *LAN* dan *hotspot wifi*, menggunakan *router MikroTik rb750r2* di SMA Negri Labuapi. Dengan *mikrotik*, dapat mengatur segala hal dalam pembangunan jaringan contohnya seperti pembangunan *hotspot*, memanajemen *bandwidth*, manajemen *user*. Topologi yang digunakan pada perancangan jaringan ini adalah topologi *star* karena jaringan *internet* terpusat pada *modem* dan dikonfigurasikan pada *mikrotik* melalui *PC*, kemudian internet disebarkan dari *mikrotik* yang terhubung pada *switch* dan *access point* ke *client*. Penggunaan *MikroTik* sangat membantu efisiensi dari penelitian ini.

Bambang dan Suharyanto (2019) dalam penelitiannya, menggunakan *VPN* dengan *PPTP* untuk mendukung rancangan infrastruktur jaringan komputer antar kantor pusat berada di Jakarta Barat dan kantor cabang yang berada di Jakarta Utara. Proses *tunneling* dengan *PPTP* akan membuat jalur dan komunikasi *data* yang lebih aman dengan proses enkripsi pada setiap pengirman paket datanya. Karena sebelumnya permasalahan yang ada pada PT. Hail Otis Logistik yaitu belum terkoneksi antara kantor pusat yang berada di Jakarta Barat dengan kantor cabang yang berada di Jakarta Utara hal ini menyebabkan sulitnya *transfer data* atau *sharing data* dan juga dalam *transfer data* ini *user* masih menggunakan *media internet* seperti *email* karena banyak *data* penting yang terdapat di dalamnya yang sangat rentan jika email itu sendiri diretas oleh pihak yang tidak bertanggung jawab.

Ikhwan dan Uray (2019) dalam penelitian menggunakan *VPN* dengan *protocol SSTP* (*Secure Socket Tunneling Protocol)*, untuk sebuah *server* pada fakultas MIPA karena data-data tersebut hanya boleh diakses oleh kalangan tertentu saja. Dan bisa diakses di luar fakultas MIPA itu sendiri. Konfigurasi *SSTP* dapat dilakukan menggunakan perangkat router mikrotik yang dihubungkan menggunakan perantara *Virtual Private Server* (*VPS*) yang ada di *internet*, kemudian diintegrasikan pada router *mikrotik*, sehingga kedua kondisi tersebut dapat saling berinteraksi seolah-olah pengguna berada di lingkungan FMIPA.

Swapna, Sri, Nikila, dan Sravani (2017) dalam penelitiannya menggunakan jaringan pribadi virtual (*VPN*) menggunakan teknik enkripsi canggih seperti *AES* (standar enkripsi lanjutan) dan penerowongan untuk mengizinkan organisasi membangun koneksi jaringan pribadi yang aman, ujung ke ujung, melalui jaringan pihak ketiga seperti Internet daripada menggunakan jalur sewa terpisah. Protokol ini mengenkripsi *data* dan memasukkannya ke dalam paket dengan membuat terowongan yang menyediakan komunikasi aman melalui *LAN* atau *WAN*. Karena enkapsulasi data itu, enkripsi dan otentikasi yang diperlukan, aman untuk mengirimkan data itu bahkan melalui jaringan publik seperti *internet*.

Putra, Indriyani, dan Angraini (2018) dalam penelitiannya menyatakan keamanan jaringan komputer menggunakan *VPN* dengan metode *PPTP* yang dapat mempermudah pekerjaan bagian *IT* untuk mengontrol dan mengatasi permasalahan-permasalahan jaringan yang ada di perusahaan dari jarak yang jauh, tanpa harus datang langsung ke tempat. Selain itu pertukaran *file* juga dapat dilakukan dengan adanya jaringan *VPN* ini. Sehingga pekerjaan juga menjadi lebih efisien.

Zamalia, Aksara, dan Yamin (2018) dalam penelitiannya, melakukan analisis perbandingan performa dari beberapa protokol *VPN* menggunakan *MikroTik.* Berikut ada *PPTP*, *L2TP*, *SSTP*, dan *IPSec*. Berdasarkan hasil analisis menunjukkan bahwa tingkat keamanan yang dibangun oleh *tunnel IPsec* lebih baik dari *tunnel PPTP*, *L2TP*, dan *SSTP*. Sedangkan untuk hasil pengujian terhadap performa, keamanan serta temuan-temuan pengujian diperoleh bahwa *tunnel VPN IPsec* lebih baik dibandingkan *tunnel VPN*, *PPTP*, *L2TP*, dan *SSTP*.

Mufida, Irawan, dan Chrisnawati (2017) dalam penelitiannya menggunakan *VPN* dengan metode *PPTP*, *user* dapat mengakses sumber daya yang berada dalam jaringan lokal, mendapatkan hak dan pengaturan yang sama seperti secara fisik berada di tempat dimana jaringan lokal itu berada. Keamanan data dan ketertutupan transmisi data dari akses yang tidak berhak dalam transmisinya pada internet menjadi standar utama dalam *VPN*, sehingga dalam *VPN* selalu disertakan akan fitur utama yaitu enkripsi dan *tunneling*.

Arlan, Munandi, dan Andini (2016) dalam penelitiannya menggunakan *protocol* keamanan *IPsec*

p-ISSN : 2406-7733
e-ISSN : 2597-9922

dalam *MPLS-VPN*. Dikarenakan *IPSec* pada *MPLS-VPN* merupakan solusi yang sangat tepat untuk meningkatkan kemanan pada layanan berbasis *IP Multimedia Subsystem* (*IMS*). Dari hasil pengujian upaya *network scanning* dari luar *core* ke dalam *core MPLS-VPN* tidak berhasil, hal ini karena propagasi paket di dalam *core* menggunakan metode *virtual routing* and *forwarding* (*vrf*) dan ditambahkannya *route distinguisher* (*rd*) pada *MPLS-VPN*. Dari upaya *sniffing* trafik *voice* dan *chat* di dalam *core MPLS-VPN* didapatkan bahwa paket-paket dapat di-*capture* dan dibuka isinya, namun dengan *IPSec tunnel* komunikasi *client* tidak dapat dibuka karena sudah dienkripsi oleh protokol *ESP*.

Alezi, dan Raufi (2015) dalam penelitiannya menyatakan pengelolaan kunci enkripsi sebagai bagian penting dari keamanan komunikasi. Menjalankan kueri jarak jauh pada *platform* sistem operasi yang berbeda yaitu untuk membandingkan keamanan lebih dari kecepatan aktif.

Jaringan Komputer

Jaringan komputer adalah koneksi antara dua *device* atau lebih, yang terhubung secara fisik maupun secara logika sehingga bisa saling bertukar informasi. Jaringan komputer dapat dikatakan terkoneksi apabila *device* yang ada dalam jaringan tersebut bisa saling bertukar data/informasi dan berbagi *resource* yang dimiliki (Sahari, 2015).

Sebuah jaringan komputer biasanya terdiri dari dua buah komputer atau lebih dan melakukan data *sharing* antar komputer. Informasi dan data bergerak melalui media komunikasi. Media komunikasi yang dipakai dalam membuat jaringan antara lain adalah kabel, jaringan telepon, gelombang radio, satelit, *Bluetooth*, dan inframerah. Pemakaian ini akan tergantung pada kegunaan dan ukuran jaringan (Sahari, 2015).

Adapun beberapa kemampuan dari jaringan komputer:

a. *Resource Sharing*

Dengan adanya jaringan komputer, berbagi *resource* bisa dilakukan tanpa terkendala jarak. *Resource sharing* meliputi:

1. *Data Sharing*. Dengan adanya jaringan komputer bisa dengan mudah berbagi *data* seperti dokumen, gambar, video, dll dengan kolega yang ada di lokasi yang jauh bahkan di negara yang berbeda.
2. *Hardware Sharing*. Jika dulunya satu komputer satu *printer*, dengan jaringan komputer, satu *printer* bisa digunakan oleh beberapa komputer sekaligus. Tidak hanya *printer*, bisa *sharing storage* dan banyak *hardware* lainnya.
3. *Internet Access Sharing*. Jaringan komputer kecil memungkinkan beberapa komputer berbagi satu koneksi *internet*. *Device* khusus seperti *router*, memiliki kemampuan mengalokasikan *bandwidth* dengan mudah untuk komputer *user* yang membutuhkan.

b. *Connectivity dan Communication*

Individu dalam sebuah gedung atau *workgroup* dapat dikoneksikan dalam jaringan *LAN*. Beberapa *LAN* dengan lokasi yang berjauhan terkoneksi kedalam jaringan *WAN*. Ketika jaringan sudah terbentuk dan terhubung, maka komunikasi antar *user* bisa terjadi, misalnya dengan menggunakan teknologi *email*.

c. *Data Security and Management*

Dalam dunia bisnis, jaringan memberikan kemudahan bagi *administrator* untuk melakukan *management* data penting perusahaan dengan lebih baik. Daripada data penting ini ada di setiap perangkat komputer karyawan yang bisa pengelolaan data dilakukan secara serampangan, akan lebih aman dan lebih mudah ketika data tersebut disimpan secara terpusat dengan menggunakan *Shared Server*. Dengan cara seperti ini, karyawan perusahaan lebih mudah dalam mencari data. *Administrator* juga dapat memastikan bahwa data di *backup* secara *reguler*, dan memungkinkan untuk menerapkan *security* dengan cara menentukan siapa yang boleh membaca atau menulis data yang bersifat penting (Sahari, 2015).

***Local Area Network* (*LAN*)**

LAN (*Local Area Network*) adalah suatu kumpulan komputer, dimana terdapat beberapa unit komputer (*client*) dan satu unit komputer untuk *bank data* (*server*). Antara masing-masing *client* maupun antara *client* dan *server* dapat saling bertukar *file* maupun saling menggunakan printer yang terhubung pada unit-unit komputer yang terhubung pada jaringan *LAN* (Sugeng & Putri, 2014).

***Wide Area Network* (WAN)**

WAN (*Wide Area Network*) adalah kumpulan dari *LAN* atau *Workgroup* yang dihubungkan dengan menggunakan alat komunikasi, umumnya menggunakan *modem* untuk membentuk hubungan dari atau ke kantor pusat dan kantor cabang, maupun antar kantor cabang. Dengan sistem jaringan ini, pertukaran data antar kantor dapat dilakukan dengan cepat serta dengan biaya yang relatif murah. Untuk menghemat biaya infrastruktur, sistem jaringan *WAN* dapat pula menggunakan jaringan umum (*public*) yang ada, yaitu *Internet* hanya saja perlu diperhatikan masalah sekuritas datanya, karena menggunakan jaringan umum, untuk menghubungkan antara kantor pusat dan kantor cabang (Sugeng & Putri, 2014).

Topologi Jaringan

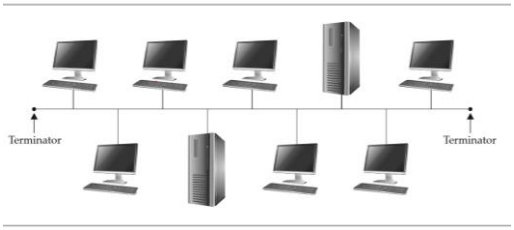
Kata topologi pada dasarnya berarti bentuk, dan istilah topologi jaringan mengacu pada bentuk jaringan bagaimana semua titik jaringan dihubungkan bersama. Jaringan mungkin ditransfer dalam beberapa topologi yang berbeda, dan pilihan topologi seringkali

p-ISSN : 2406-7733
e-ISSN : 2597-9922

merupakan keputusan terpenting ketika merencanakan jaringan. Topologi memiliki biaya yang berbeda, tingkat kinerja, dan tingkat keandalan (Hallberg, 2014).

Topologi *Bus*

Topologi *bus*, yang lebih lengkap disebut topologi *multipoint* bus umum, adalah jaringan dimana, pada dasarnya, kabel jaringan tunggal digunakan dari satu ujung jaringan ke yang lain, dengan perangkat jaringan yang berbeda yang terhubung ke kabel di berbagai lokasi (Hallberg, 2014).



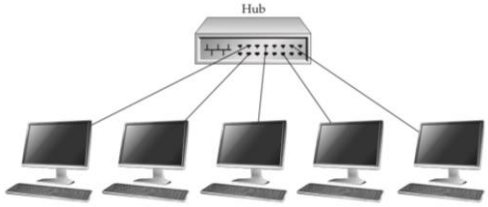
Sumber : dokumen pribadi

Gambar 1. Topologi *Bus*

Topologi *Star*

Topologi *star* adalah salah satu dimana unit pusat, yang disebut hub, host satu set kabel jaringan yang menyebar ke setiap *node* di jaringan. Secara teknis, hub disebut sebagai unit akses *multistation*, tetapi terminologi tertentu cenderung digunakan dengan hanya jaringan Ring Token, yang menggunakan topologi *ring logic* (Hallberg, 2014).

Semua lalu lintas jaringan yang digunakan pada salah satu koneksi jaringan ke hub diteruskan ke semua titik terhubung lainnya pada hub tertentu. Karena itu, semua *bandwidth* koneksi *node* tunggal dibagi dengan semua koneksi *node* lain. Misalnya, jika salah satu node yang terhubung ke hub menggunakan setengah dari *bandwidth* yang tersedia, semua node lain harus bersaing dengan penggunaan itu. Dengan kata lain, jika menggunakan tipe jaringan dengan kapasitas 100 *Mbps*, itu adalah jumlah total *bandwidth* yang tersedia untuk semua node yang terhubung ke hub (Hallberg, 2014).



Sumber : Dokumen Pribadi

Gambar 2. Topologi *Star*

VPN

VPN adalah sebuah jaringan pribadi yang dibangun melalui sistem *tunneling* menggunakan jaringan *internet* (linuxconfig.org: 2013). *VPN* digunakan agar para pengguna dapat menggunakan sistem klien *VPN* untuk masuk ke *server* lokal saat berada di luar jalur lokal seolah-olah sedang berada di jalur yang sama dengan *server* yang sedang diakses. *VPN* juga rnenjadikan para penggunanya mengakses *server* lokal secara aman dikarenakan lalu lintas data yang terbaca bukanlah alamat tujuan dari situs yang sedang diakses pengguna, namun alamat *VPN* itu sendiri yang akan terbaca (*cloud*wards.net: 2017).

VPN dengan metode *site-to-site* adalah metode *VPN* yang menghubungkan antar jaringan yang berada di lokasi yang berbeda seolah-olah menggunakan akses intranet untuk bisa saling berkomunikasi. *VPN* bekerja dengan cara memberikan akses terhadap para penggunanya. *VPN* dijadikan *gateway* yang berfungsi untuk mengenkapsulasi dan mengenkripsi lalu lintas dari satu pengguna ke pengguna lainnya melalui tunnel *VPN* yang rnenggunakan jalur *internet* (Zornitsa Yakova: 2013).

VPN site-to-site

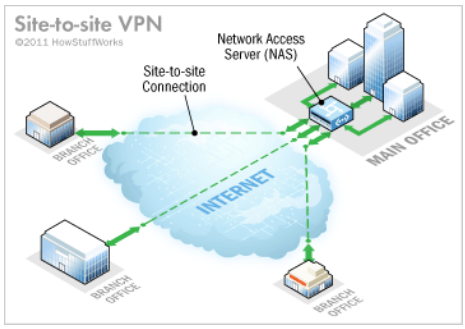
VPN site-to-site memungkinkan toko di beberapa lokasi tetap untuk membuat koneksi aman satu sama lain melalui jaringan publik seperti *internet*. *VPN* situs-ke-situs memperluas jaringan perusahaan, membuat sumber daya komputer dari satu lokasi tersedia untuk karyawan di lokasi lain (Jeff,Chris, dan Stephanie, 2011).

Ada dua jenis *VPN site-to-site* :

1. Berbasis *intranet* - Jika perusahaan memiliki satu atau lebih lokasi terpencil yang ingin digabungkan dalam satu jaringan pribadi, dapat membuat *VPN* intranet untuk menghubungkan setiap *LAN* yang terpisah ke satu WAN (Jeff, Chris, dan Stephanie, 2011)
2. Berbasis *extranet* - Ketika suatu perusahaan memiliki hubungan dekat dengan perusahaan lain (seperti mitra, pemasok atau pelanggan), dapat membangun *VPN* ekstranet yang menghubungkan *LAN* perusahaan-perusahaan tersebut. *VPN* ekstranet ini memungkinkan perusahaan untuk bekerja sama dalam lingkungan jaringan yang aman dan dibagikan sekaligus mencegah akses ke intranet mereka yang terpisah (Jeff, Chris, dan Stephanie, 2011).

Meskipun tujuan dari *site-to-site VPN* berbeda dari *VPN remote accsess*, itu bisa menggunakan beberapa perangkat lunak dan peralatan yang sama. Namun, idealnya, *VPN* dari satu lokasi ke lokasi lainnya harus menghilangkan kebutuhan setiap komputer untuk menjalankan perangkat lunak klien *VPN* seolah-olah menggunakan *VPN remote accsess* (Jeff, Chris, dan Stephanie, 2011).

p-ISSN : 2406-7733
e-ISSN : 2597-9922

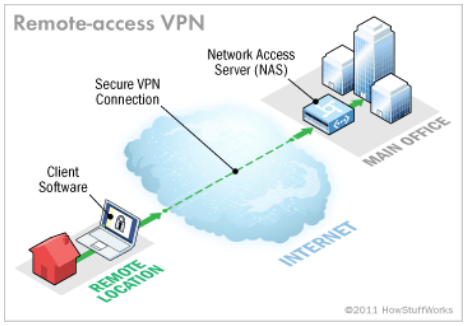


Sumber: computer.howstuffworks.com

Gambar 3. *VPN Site-to-Site*

VPN Remote Access

VPN remote access memungkinkan pengguna individu untuk membuat koneksi aman dengan jaringan komputer jarak jauh. Para pengguna dapat mengakses sumber daya aman di jaringan itu seolah-olah mereka langsung terhubung ke *server* jaringan. Contoh perusahaan yang membutuhkan *VPN* akses jarak jauh adalah perusahaan besar dengan ratusan tenaga penjualan di lapangan. Nama lain untuk jenis *VPN* ini adalah *virtual dial-up network* (*VPDN*) *virtual*, mengakui bahwa dalam bentuknya yang paling awal, *VPN* akses jarak jauh diperlukan untuk melakukan panggilan ke *server* menggunakan sistem telepon *analog* (Jeff, Chris, dan Stephanie, 2011).



Sumber : computer.howstuffworks.com

Gambar 4. *VPN Remote Access*

Keamanan *VPN*

Terdapat beberapa fitur penting yang ada dalam *VPN*:

a. *Enkripsi* adalah sebuah proses yang melakukan perubahan sebuah kode dari yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti. Dengan enkripsi, berfungsi mengubah isi dari data yang dikirim sehingga data tersebut tidak dapat dibaca oleh orang yang tidak berhak mendapatkannya (Mufida, 2017).

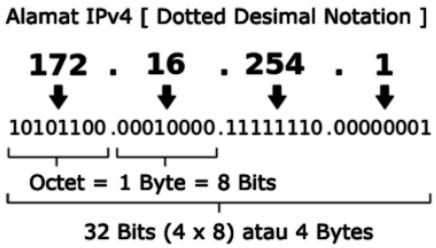
b. *Tunneling*. Teknologi *tunneling* merupakan teknologi yang bertugas untuk menangani dan menyediakan koneksi *point to point* dari sumber ke tujuannya. Disebut *tunnel* karena koneksi *point to point* tersebut sebenarnya terbentuk melewati jaringan umum, namun seolah-olah koneksi tersebut menjadi bersifat *private* karena tidak mempedulikan paket-paket data milik orang lain yang sama-sama menggunakan jalur tersebut (Mufida, 2017).

c. *IPsec* menyediakan layanan-layanan keamanan tersebut dengan menggunakan sebuah metode pengamanan yang bernama *Internet Key Exchange* (*IKE*). *IKE* bertugas untuk menangani protokol yang bernegosiasi dan algoritma pengamanan yang diciptakan berdasarkan dari *policy* yang diterapkan (Frankel Dkk, 2005). *IPSec* adalah pengembangan dari protokol *IP* yang bertujuan untuk menyediakan keamanan pada suatu *IP* dan *layer* yang berada di atasnya. Pada dasarnya paket *IP* tidak memiliki keamanan, sehingga tidak ada jaminan bahwa paket yang diterima sama dengan paket ketika ditransmisikan oleh si pengirim paket. Paket *IP* yang tidak memiliki keamanan atau *security*, sangat mudah untuk diketahui isinya dan alamat *IP* itu sendiri (Zamalia Dkk, 2018). *IPsec* adalah metode yang bertujuan untuk menjaga keamanan *IP datagram* ketika paket diransmisikan pada *traffic*. Sehingga *IPsec* menjadi suatu mekanisme yang diimplementasikan pada *VPN*. *IPSec* berada pada *layer* tiga *OSI* yaitu *network layer* sehingga dapat mengamankan data dari *layer* yang berada di atasnya (Zamalia Dkk, 2018).

IP address

IP Address adalah suatu alamat yang diberikan ke peralatan jaringan komputer untuk dapat diidentifikasi oleh komputer yang lain. Dengan demikian masing-masing komputer dapat melakukan proses tukar-menukar data/informasi, mengakses *intemet*, atau mengakses ke suatu jaringan komputer dengan menggunakan protokol *TCP/IP*. (Kurniawan, 2007)

IP address bisa dianalogikan seperti sebuah alamat rumah. Ketika sebuah datagram dikirim, informasi alamat inilah yang menjadi acuan datagram agar bisa sampai ke *device* yang dituju. *IP Address* terbagi dalam 2 versi, *IPv4* dan *IPv6*. Sebuah *IP address* versi 4 atau *IPv4* terbentuk dari 32 *binary bits*. Dari 32 *binary bits* tersebut terbagi lagi menjadi 4 *octet* (1 *octet* = 8 *bits*). Nilai tiap *oktet* diatara 0 sampai 255 dalam *format* desimal, atau 00000000 - 11111111 dalam *formal binary*. Setiap octet dikonversi menjadi desimal dan dipisahkan oleh tanda titik (*dot*). Sehingga format akhir *IP address* biasanya berupa angka desimal yang dipisahkan dengan tanda titik.



Sumber : MikroTik.co.id

Gambar 5. *IP Address*

p-ISSN : 2406-7733
e-ISSN : 2597-9922

IP Public

IP Adresss Public merupakan alamat-alamat *IP* yang disediakan untuk digunakan pada jaringan *internet* (Madcoms, 2009). Karena kelas *IP address* ini digunakan di dalam jaringan *internet* maka *IP* ini bisa diakses melalui jaringan *internet* secara langsung. Perangkat yang menggunakan *IP public*, seperti *web server*, *mailserver*, *DNS server*, *game server* ataupun perangkat lain dapat diakses dari jaringan manapun di dunia ini yang terkoneksi ke *internet* (Madcoms, 2009). Untuk dapat menggunakan *IP public*, suatu organisasi biasanya dapat mendaftarkan diri ke salah satu *ISP* (*Internet Service Provider*) (Madcoms, 2009).

IP Private

IP Adresss Private merupakan alamat-alamat IP yang disediakan untuk digunakan pada jaringan *local* (*LAN*). (Madcoms, 2009) misalnya digunakan di jaringan sekolah, kantor, toko, warnet dan sebagainya. Perangkat yang terhubung ke jaringan lokal seperti *printer*, komputer, *laptop*, *smartdevice* menggunakan biasanya akan mendapatkan *IP address private*. Agar *IP private* dapat terhubung ke *internet* maka diperlukan *router* yang mempunyai kemampuan untuk melakukan *NAT* (*Network Address Translation*) agar semua *device* dengan *IP private* dapat terkoneksi ke *internet* dengan menggunakan *IP public* yang terkoneksi langsung ke *internet*). Meskipun sudah terkoneksi ke *internet*, *IP private* tetap tidak bisa diakses langsung dari jaringan *internet* (Madcoms, 2009).

Server

Server adalah komputer yang mendukung aplikasi dan telekomunikasi dalam jaringan, serta pembagian peralatan *software*, dan *database* di antara berbagai terminal kerja dalam jaringan (O'brien (2011:190).

Ada banyak jenis *server*, termasuk *server web* , *server email*, dan *server file*. Setiap jenis menjalankan perangkat lunak khusus untuk tujuan *server*. Misalnya, *server Web* dapat menjalankan *Apache HTTP Server* atau *Microsoft IIS*, yang keduanya menyediakan akses ke situs *web* melalui *internet*. *Server* email dapat menjalankan program seperti *Exim* atau *iMail*, yang menyediakan layanan *SMTP* untuk mengirim dan menerima email . *Server file* mungkin menggunakan Samba atau layanan berbagi *file* bawaan sistem operasi untuk berbagi *file* melalui jaringan.

Server dapat berjalan di berbagai jenis komputer, penting bahwa perangkat kerasnya cukup untuk mendukung permintaan *server*. Misalnya, *server web* yang menjalankan banyak skrip *web* secara *real-time* harus memiliki prosesor yang cepat dan RAM yang cukup untuk menangani "memuat" tanpa melambat. *Server file* harus memiliki satu atau lebih *hard drive* cepat atau SSD yang dapat membaca dan menulis data dengan cepat. Apa pun jenis *server*nya, koneksi jaringan yang cepat sangat penting, karena semua data mengalir melalui koneksi itu.

Sumber : dell.com

Gambar 6. *Server*

Router

Router beroperasi pada lapisan jaringan (*Layer* 3) dari model *OSI*. Karena *router* beroperasi pada *layer network*, koneksi melintasi *router* hanya memerlukan *layer* yang lebih tinggi menggunakan protokol yang sama. *Router* dapat menerjemahkan dari salah satu protokol di *Layer* 1 hingga 3 ke protokol lain di *Layer* 1 hingga 3 (Hallberg, 2014). *Router* dapat menghubungkan jaringan yang sama dan yang berbeda. Mereka sering digunakan untuk tautan *Wide Area Network* (WAN). *Router* sebenarnya menjadi *node* di jaringan, dan mereka memiliki alamat jaringan sendiri. *Node* lain mengirim paket ke *router*, yang kemudian memeriksa isi paket dan meneruskannya dengan tepat. Untuk alasan ini, *router* sering memiliki mikroprosesor cepat dan memori dibangun ke dalamnya untuk melakukan pekerjaan ini. *Router* juga dapat menentukan rute terpendek ke suatu tujuan dan menggunakannya. Mereka dapat melakukan trik lain untuk memaksimalkan *bandwidth* jaringan dan secara dinamis menyesuaikan diri dengan masalah yang berubah atau pola lalu lintas pada jaringan (Hallberg, 2014).

Sumber : MikroTik.co.id

Gambar 7. *Router*

MikroTik

MikroTik adalah perusahaan Latvia yang didirikan pada tahun 1996 untuk mengembangkan *router* dan sistem *ISP* nirkabel (*MikroTik*.co.id, 2020). *MikroTik* sekarang menyediakan perangkat keras dan lunak untuk konektivitas *Internet* di sebagian besar negara di dunia. Pengalaman dalam menggunakan perangkat keras *PC* standar industri dan sistem perutean lengkap memungkinkan pada tahun 1997 untuk membuat sistem peranti lunak *RouterOS* yang

p-ISSN : 2406-7733
e-ISSN : 2597-9922

menyediakan stabilitas, kontrol, dan fleksibilitas yang luas untuk semua jenis antarmuka data dan perutean. Pada tahun 2002 memutuskan untuk membuat perangkat keras sendiri, dan merek *Routerboard* lahir.

Sumber : MikroTik.com

Gambar 8. Logo *MikroTik*

MikroTik RouterOS

MikroTik RouterOS adalah sebuah sistem operasi pengembang *Linux* yang secara *independent* difungsikan sebagai sistem operasi yang menjadikan sebuah perangkat komputer difungsikan sebagai sebuah perangkat *router* jaringan (*MikroTik*.co.id, 2020). *MikroTik* menyediakan 2 versi pilihan terhadap *RouterOS*, yaitu *router* yang sudah diinstalasi dengan *RouterOS* khusus dengan lisensi yang sudah tertanam di dalamnya, maupun *file* instalasi *RouterOS* yang nantinya dapat dilakukan instalasi terhadap komputer yang akan dijadikan *router* dengan tambahan pembelian lisensi tergantung pada peruntukannya.

CHR

CHR adalah versi *RouterOS* yang dimaksudkan untuk berjalan sebagai mesin *virtual*. Ini mendukung arsitektur x86 64-*bit* dan dapat digunakan pada sebagian besar *hypervisor* populer seperti *VMWare*, *Hyper-V*, *VirtualBox*, *KVM*, dan lainnya (*MikroTik*.co.id, 2020). *CHR* memiliki fitur *RouterOS* lengkap yang diaktifkan secara *default* tetapi memiliki model lisensi yang berbeda dari versi *RouterOS* lainnya. Pada dasarnya fitur ini bukanlah fitur yang terdapat pada menu *RouterOS*, melainkan sebuah *file image* yang digunakan di aplikasi *VM* (*Virtual Machine*). *MikroTik* ingin memberikan solusi bagi pengguna *RouterOS* yang berbasis *Virtual Machine*. Salah satu fungsinya adalah melakukan interkoneksi antar jaringan *LAN* via *internet*. Tapi jaringan tersebut tidak memiliki alokasi *IP Public* untuk koneksi internetnya. Untuk itu sebagai alternatif bisa mengkoneksikan kedua *LAN* tersebut ke *service VPN* yang dibuat pada *MikroTik* yang diinstall di *Public Cloud Server*.

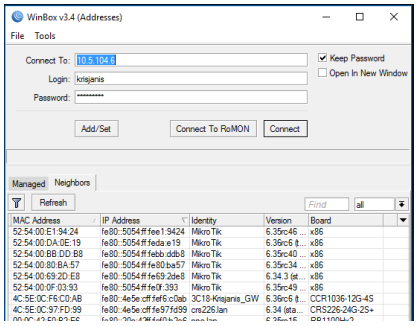
Winbox

Winbox adalah sebuah *software* atau *utility* yang digunakan untuk me-*remote* sebuah *server MikroTik* ke dalam mode *GUI* (*Graphical User Interface*) melalui *operating system windows*. Kebanyakan teknisi banyak mengkonfigurasi *MikroTik* OS atau *MikroTik routerboard* menggunakan *winbox* dibanding dengan yang mengkonfigurasi langsung lewat *mode CLI* (*Command Line Interface*). Hal ini karena menggunakan *winbox* dirasa lebih mudah dan *simple* dibanding melalui *browser*. Dan hasilnya pun juga lebih cepat (*wirelessmode.net*, 2015).

Mengkonfigurasi *MikroTik* melalui *winbox* ini lebih banyak digunakan karena selain penggunaannya yang mudah, pengguna juga tidak harus menghafal perintah – perintah *console*.

Fungsi Umum *Winbox*:

a. *Interface* pengaturan *router MikroTik* secara *remote*.
b. Memberikan akses kepada *admin* untuk mengatur *bandwidth* jaringan.
c. Memblokir situs tertentu.
d. Membatasi kecepatan jaringan.
e. Mengetahui dan mengatur alamat *IP* dan akses ke situs tertentu.
f. Mengatur *proxy*



Sumber: wiki.MikroTik.com

Gambar 9. Tampilan *Winbox*

III. METODE PENELITIAN

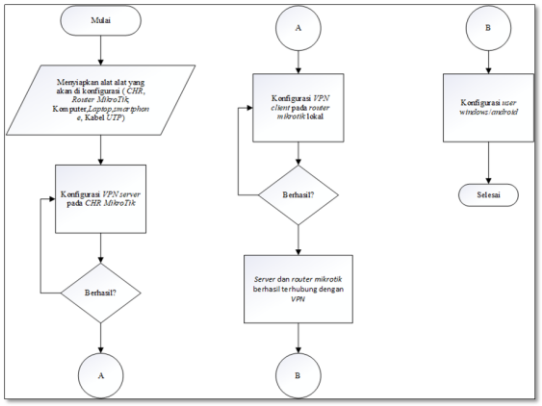
Tipe penelitian yang dipakai adalah tipe penelitian terapan, dan yang dideskripsikan di dalam penelitian ini adalah penelitian rancang bangun jaringan *VPN* dengan menggunakan *IPsec (IP Security)* dengan *Router MikroTik.*

Tahapan ini berisi tahapan yang dilakukan dalam proses penelitian termasuk di dalamnya menjelaskan bagaimana penerapan metode pengembangan sistem atau metode komputasi pada penelitian yang sedang dilakukan.

Berikut tahapan-tahapan penelitian yang akan dipaparkan:

1. Studi literatur. Kegiatan ini dilakukan sebagai acuan guna memperkuat penelitian dan menyelesaikan permasalahan yang ada pada salah satu toko di Royal.
2. Pengumpulan data. Tahapan ini dilakukan untuk mengumpulkan dan mengoreksi data dari berbagai sumber, informasi atau data. Menggunakan metode observasi atau pengamatan langsung ke objek penelitian serta metode wawancara kepada pihak yang berkaitan dengan objek yang akan diteliti.
3. Pengujian alat.
4. Analisis hasil pengujian.
5. Pembuatan Laporan.

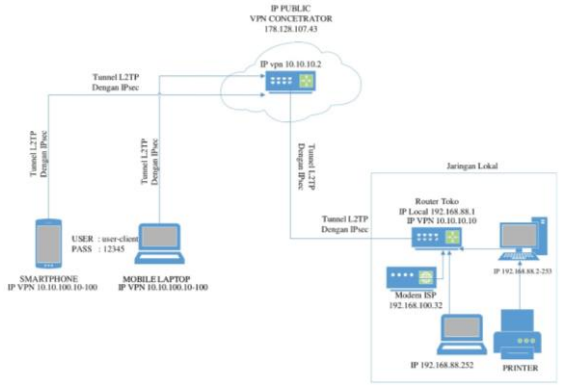
p-ISSN : 2406-7733
e-ISSN : 2597-9922



Sumber : Dokumen Pribadi

Gambar 10. *Flowchart* penelitian

IV HASIL DAN PEMBAHASAN



Sumber: Dokumen Pribadi

Gambar 11. Topologi Jaringan

Dalam mengusulkan topologi jaringan yang akan diimplementasikan, tidak akan merubah bentuk topologi yang sudah ada hal ini karena bentuk topologi yang ada sekarang sudah sangat baik. Topologi jaringan toko menggunakan topologi *star*. Dan diusulkan untuk menggunakan *VPN* untuk berkomunikasi atau pertukaran data menjadi lebih aman.

Keamanan jaringan

Keamanan dalam jaringan usulan ini dengan sistem *VPN L2TP/IPsec*. *VPN* merupakan suatu metode pengamanan dengan membentuk koneksi logical antar beberapa *node* dalam jaringan yang bersifat *public*. Koneksi yang dibentuk dalam *VPN* merupakan koneksi *virtual* dalam bentuk *tunnel* dan bersifat *private* dengan adanya fitur *authentication* serta *policy-policy* yang dibentuk oleh setiap *router* yang terlibat. Dan *IPsec* menyediakan layanan-layanan keamanan tersebut dengan menggunakan sebuah metode pengamanan yang bernama *Internet Key Exchange* (*IKE*). *IKE* bertugas untuk menangani protokol yang bernegosiasi dan algoritma pengamanan yang diciptakan berdasarkan dari *policy* yang diterapkan.

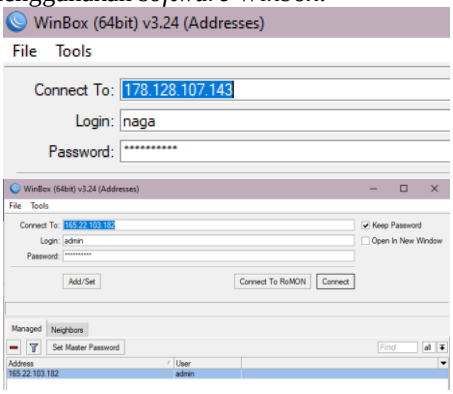
IPsec mendukung dua buah sesi komunikasi keamanan, yaitu sebagai berikut:

1. Protokol *Authentication Header* (*AH*), menawarkan autentikasi pengguna dan perlindungan dari beberapa serangan (umumnya serangan *man in the middle*), dan juga menyediakan fungsi autentikasi terhadap data serta integritas terhadap data. Protokol ini mengizinkan penerima untuk merasa yakin bahwa identitas pengirim adalah benar adanya, dan data pun tidak dimodifikasi selama transmisi.
2. Protokol *Encapsulating Security Payload* (*ESP*), Protokol ini melakukan enkapsulasi serta enkripsi terhadap data pengguna untuk meningkatkan kerahasiaan data. *ESP* juga dapat memiliki skema autentikasi dan perlindungan dari beberapa serangan dan dapat digunakan secara sendirian atau bersamaan dengan *Authentication Header*.

Rancangan Jaringan

Dalam rancangan aplikasi berikut merancang dan mengimplementasikan suatu jaringan *VPN* dengan metode *L2TP/IPsec* untuk menghubungkan antara *mobile user* dan *client* di Toko, sehingga dalam pertukaran data akan lebih cepat dan aman. Berikut adalah tahapan konfigurasi pada sisi *router* (*CHR*) *server*.

1. Instalasi *winbox* dan *login* konfigurasi *MikroTik*, menggunakan *software Winbox*.



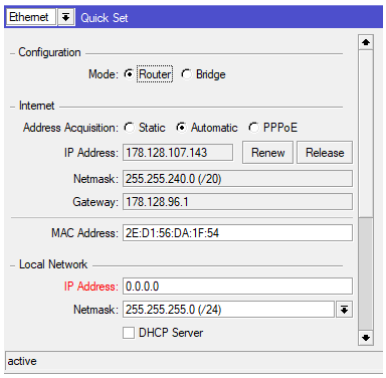
Sumber: dokumen pribadi

Gambar 12. Tampilan *winbox*

Masukan *IP public* dari *MikroTik* yang ada di *CHR* , 178.128.107.43, untuk *login* dapat diisi naga pada *form login*, dan *password* dapat disesuaikan dengan konfigurasi *router*, *password serang2020*.

2. Cek *IP public* dari *router*, di menu *quick settings*.

p-ISSN : 2406-7733
e-ISSN : 2597-9922



Sumber : dokumen pribadi

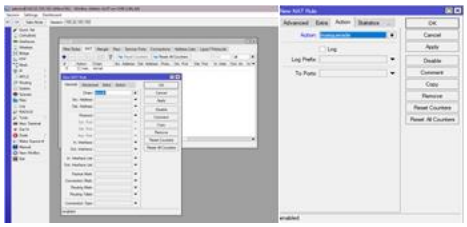
Gambar 13. *IP Router Server*

3. Lakukan *ping* ke *google.com* untuk memastikan *router server* terkoneksi ke *internet*. Untuk melakukan *ping* bisa klik di menu kiri, *New Terminal*, ketikkan seperti gambar berikut.

Sumber: dokumen pribadi

Gambar 14. Hasil *Ping*

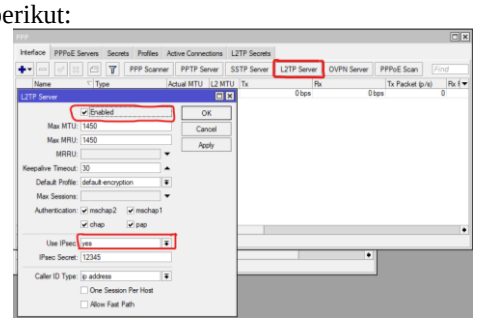
4. Konfigurasi *NAT*. Masuk ke menu *IP*, lalu Pilih *Firewall*, dan pilih *NAT*, klik tanda + berwarna biru, konfigurasi *chain* ke *srcnat* dan action ke *masquerade*. Agar antar *client* bisa saling berkomunikasi.



Sumber: dokumen pribadi

Gambar 15. Konfigurasi *NAT*

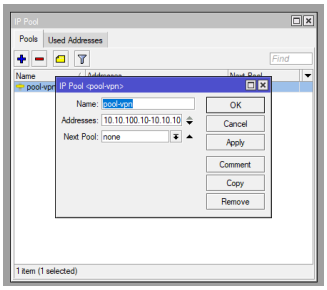
5. Konfigurasi *L2TP server* pada sisi *Server*. Masuk ke *menu PPP*, pada bagian *interface* pilih *L2TP Server* dan klik lalu centang *enabled*. Dan klik pada *box use IPsec*, pilih yes, *input* juga *IPsec Secret*, memasukan 12345, seperti pada gambar berikut:



Sumber: dokumen pribadi

Gambar 16. Konfigurasi *L2TP Server dan IPsec*

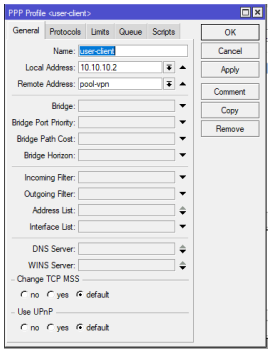
6. Konfigurasi *IP Pool*. *IP pool* dapat dikonfigurasi dari menu *IP*, lalu pilih *Pool*. *IP Pool* ini akan digunakan pada *secret VPN user* dan *client*, yang fungsinya akan memberikan alamat *IP* dinamis dari *range* yang ditentukan, gunakan *range* dari 10.10.100.10-100.



Sumber: dokumen pribadi

Gambar 17. Konfigurasi *IP Pool*

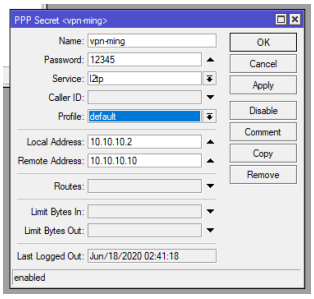
7. Konfigurasi *Profiles* Masuk ke menu PPP dan pilih *Profiles*,klik tanda + berwarna biru. Dan akan muncul tampilan seperti ini. Isikan *local address* 10.10.10.2, ini akan berfungsi sebagai *local address* untuk *VPN Server* saat *VPN* telah berhasil terkoneksi, dan *Remote address* gunakan *pool* tadi, maka *IP* dalam *Pool* akan diberikan pada *user* dan *client* yang berhasil terkoneksi di *VPN*



Sumber: dokumen pribadi

Gambar 18. Konfigurasi *Profiles*

8. Membuat *Secret. Secret* ini akan digunakan pada proses *login* atau *dial up* nanti. Diperlukan nama dan *password*, dan *service* yang digunakan adalah *L2TP*.



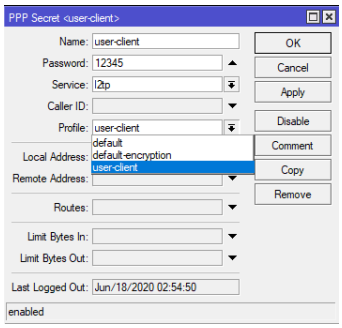
Sumber: dokumen pribadi

Gambar 19. Konfigurasi *Secret*

Ada 2 *secret*, yang pertama adalah *secret* untuk *dial* dari *router* toko, dan satu lagi untuk *dial* dari sisi *user*. Berikut adalah konfigurasi kedua *secret* tsb. Pada *secret VPN-ming* ini akan digunakan untuk menghubungkan *router* toko dengan *router server*, jadi dikonfigurasi *local address* 10.10.10.2

p-ISSN : 2406-7733
e-ISSN : 2597-9922

yang akan diberikan pada *server*, dan *remote address* 10.10.10.10 akan diberikan pada *Router* Toko.



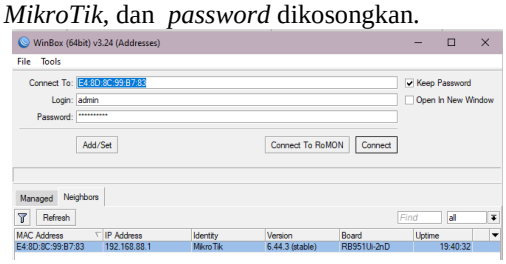
Sumber: dokumen pribadi

Gambar 20. Daftar *Secret*

Untuk *Secret* ini, menggunakan nama *user-client*, karena *secret* ini akan digunakan untuk sisi *user* dan *client*. Tidak perlu *setting local* dan *remote address*, cukup gunakan *profiles* yang sebelumnya sudah dibuat, dan akan otomatis *tersetting* sesuai *IP Pool* yang telah dibuat tadi.

Konfigurasi akan dilanjutkan pada sisi *router* toko.

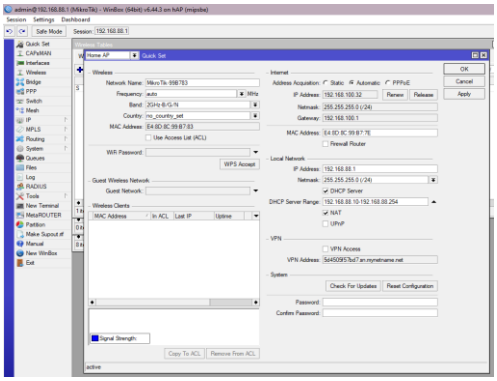
1. Buka *winbox* dan *login router*. Buka aplikasi *winbox* dan klik pada MAC *address router*. Contoh E4:8D:8C:99:B7:83, untuk *user* diisikan admin, dan *password* mengikuti konfigurasi pada *MikroTik*, dan *password* dikosongkan.



Sumber: dokumen pribadi

Gambar 21. Tampilan *winbox router* toko

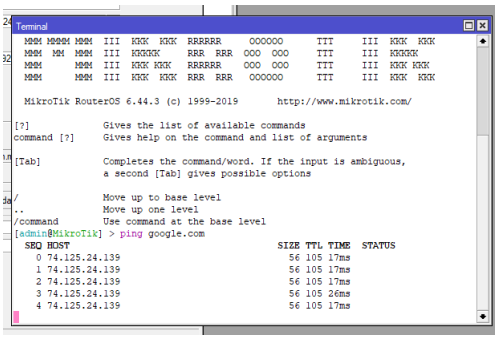
2. Konfigurasi *IP* menggunakan *Quick set.* Lakukan konfigurasi cepat dan simpel dengan menu *Quick Set*. Di situ bisa dilihat *ip internet*, dan juga *ip* lokal. *Ip* lokal milih *router* toko adalah 192.168.88.1



Sumber: dokumen pribadi

Gambar 22. *Menu quick set winbox*

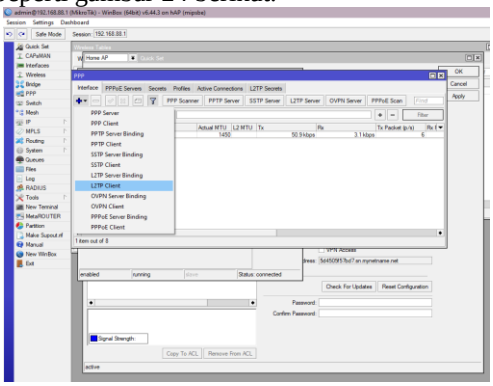
3. Lakukan *ping* ke *google.com* untuk memastikan *router server* terkoneksi ke *internet*. Untuk melakukan *ping* bisa klik di menu kiri, *New Terminal*, ketikkan seperti gambar berikut.



Sumber: dokumen pribadi

Gambar 23. *Test Ping google*

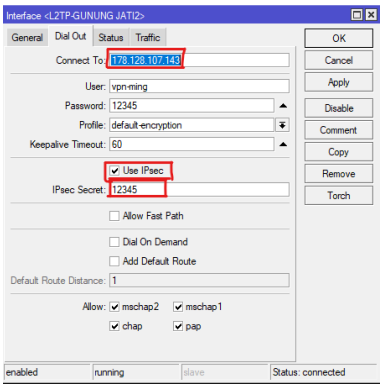
4. *Setting L2TP Client.* Masuk ke menu PPP, di *interface* ada tanda + berwarna biru, klik maka akan muncul beberapa pilihan, pilih *L2TP Client*. Seperti gambar 24 berikut.



Sumber: dokumen pribadi

Gambar 24. Konfigurasi *L2TP Client*

Dan pada tab general bisa untuk mengubah nama *interface*, di sini digunakan *L2TP*-GUNUNG JATI.



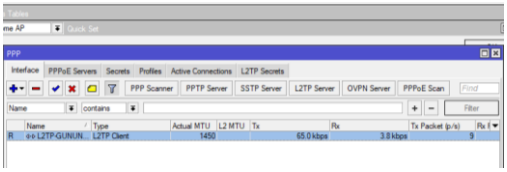
Sumber: dokumen pribadi

Gambar 25. Konfigurasi *Dial Out* dan *IPsec*

Input IP Publik milik *router server* di *box Connect to:* dengan 178.128.107.43 Isi *user* dengan *Secret* yang telah dibuat untuk *tunnel VPN* ini, yaitu *VPN-ming* dengan *password* 12345. Dan centang *box Use IPsec*, karena di penelitian ini berfokus pada pengamanan data dengan *IPsec*. Masukan juga *IPsec secret* sesuai dengan yang di *router server* yaitu 12345.

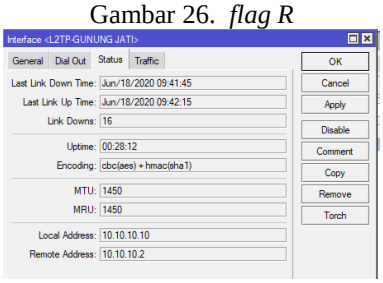
Setelah berhasil dibuat, akan muncul *flag* R yang berarti *running.*

p-ISSN : 2406-7733
e-ISSN : 2597-9922



Sumber: dokumen pribadi

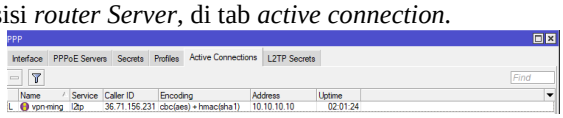
Gambar 26. *flag R*



Sumber: dokumen pribadi

Gambar 27. *Status Interface Client VPN*

Berikut pada Gambar 28 adalah contoh *tunnel VPN IPsec* yang telah berhasil dibuat, menggunakan *encoding cbc (aes) + hmac (sha1)*, dapat dilihat dari sisi *router Server*, di tab *active connection.*

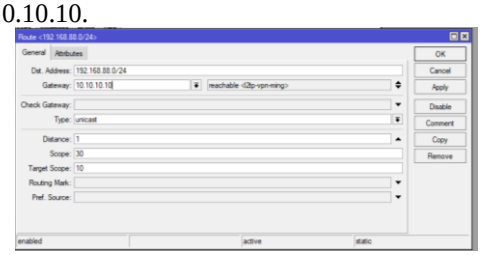


Sumber: dokumen pribadi

Gambar 28. *Tunnel VPN IPsec*

Langkah terakhir untuk konfigurasi *server* dan *client*, dapat dilakukan di sisi *router Server*, yaitu melakukan konfigurasi *static routes* ke *ip local* yang ada di sisi *router* toko, agar dapat berkomunikasi dari *user* dan *client.*

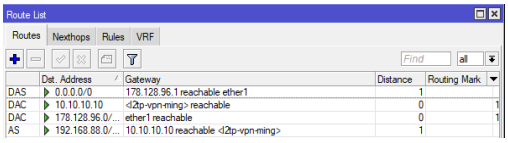
Masuk ke *router server*, ke menu *IP* dan pilih *Routes*. Dan klik *icon* + berwarna biru. Isikan dst. *address* sesuai dengan jaringan lokal yang ada, di sini menggunakan 192.168.88.0/24. Dan masukan *gateway* dengan *remote address* yang diberikan *server* kepada *VPN client*. Sesuai konfigurasi menggunakan 10.10.10.10.



Sumber: dokumen pribadi

Gambar 29. Konfigurasi *Routes*

Pada gambar 30 adalah h *routes* yang sudah terhubung.

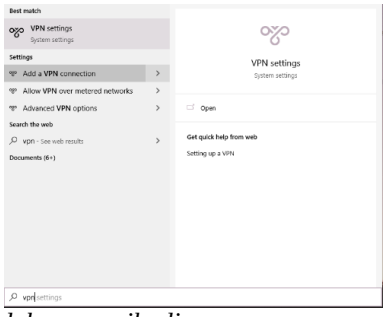


Sumber: dokumen pribadi

Gambar 30. *Routes*

Konfigurasi pada sisi *User* atau pengguna pada *windows*

1. Buat koneksi *VPN* dari *setting*, apabila menggunakan *windows* bisa mengikuti gambar berikut ini. Ketik *VPN* pada *start menu*, dan *add VPN connection*



Sumber: dokumen pribadi

Gambar 31. *VPN* pada *windows*

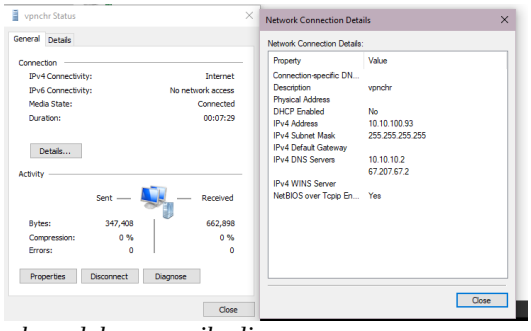
2. Masukan *IP Address Public* dari *server MikroTik* CHR, lalu pilih *VPN type* ke *L2TP*, sesuai yang dibuat, masukan *pre-shared key*, ini sama dengan *IPsec Secret*. Masukan 12345. Dan bisa *login user name* sesuai dengan yang di *secret*.

Sumber: dokumen pribadi

Gambar 32. Konfigurasi *VPN IPsec* pada *user*

Lalu klik *connect*, *VPN* akan terkoneksi. Maka secara otomatis perangkat anda akan terdeteksi di dalam Jaringan *local* dari *Client.*

Berikut ini adalah rincian dari jaringan *VPN* yang telah terkoneksi:



Sumber: dokumen pribadi

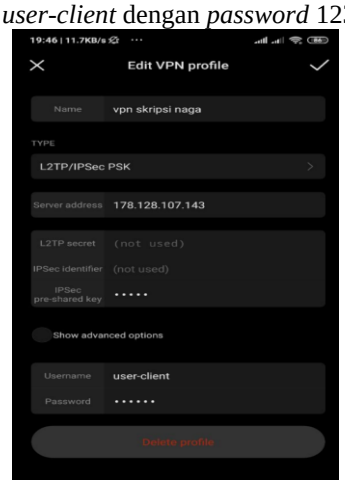
Gambar 33. Rincian *IP* dari *VPN* yang terkoneksi

Konfigurasi pada sisi *User* atau pengguna pada *Smartphone Android.*

1. Masuk ke *setting* kemudian pilih *VPN*, lalu *add VPN*. Ketikkan alamat *IP public server*. Lalu pilih *L2TP/IPsec psk* (*pre shared key*). Ketikkan

p-ISSN : 2406-7733
e-ISSN : 2597-9922

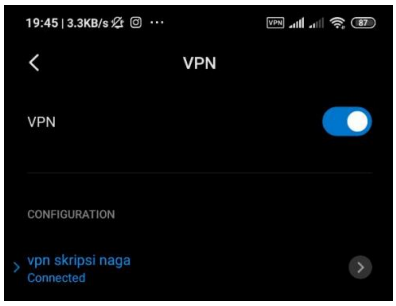
preshared key 12345, dan *login* menggunakan *secret user-client* dengan *password* 12345.



Sumber : dokumen pribadi

Gambar 34. *VPN pada Smartphone Android*

2. Koneksikan jaringan *VPN* yang sudah di buat. Akan muncul tulisan *connected*.

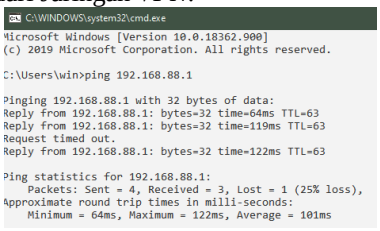


Sumber : dokumen pribadi

Gambar 35. Koneksi *VPN*

Pada rancangan pengujian akan dicoba melakukan tes koneksi dengan melakukan *ping* dari *user* yang berada di luar Toko ke *router* yang berada di Toko, melakukan *ping* dari *user* ke salah satu perangkat yang berada di dalam Toko, dan melakukan *tracert*. Lalu akan menguji keamanan dari jaringan dengan melakukan percobaan *login* ke jaringan *VPN* dan cek hasil enkripsi dari *IPsec*. Melakukan *remote router* lokal dan *file sharing* dengan jaringan *VPN* ini.

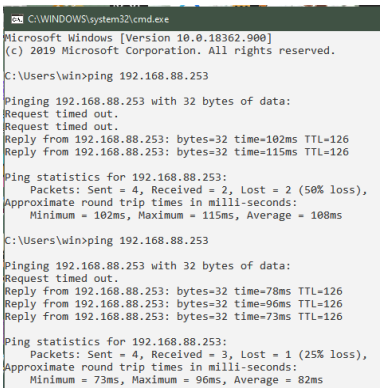
1. Melakukan *ping* ke *router* yang berada di jaringan *LAN* dari Jaringan *VPN*.



Sumber: dokumen pribadi

Gambar 36. Melakukan *ping* ke *router* toko

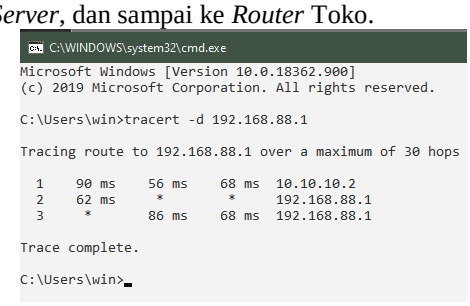
2. Melakukan *ping* ke salah satu perangkat di Jaringan Lokal.



Sumber: dokumen pribadi

Gambar 37. Melakukan *ping* ke perangkat lokal

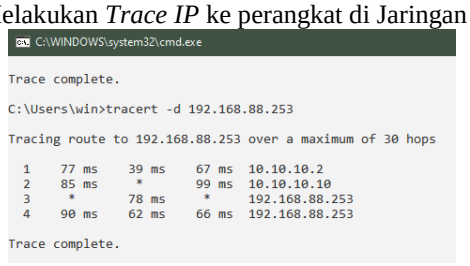
3. Melakukan *trace ip router* jaringan *LAN* 10.10.10.2 *IP VPN* dari *VPN Server* 192.168.88.1 *IP* lokal dari *Router* Toko Berarti paket yang dikirimkan dari *user*, berhasil melewati *VPN Server*, dan sampai ke *Router* Toko.



Sumber: dokumen pribadi

Gambar 38. Melakukan *Trace* ke *router* toko

4. Melakukan *Trace IP* ke perangkat di Jaringan *LAN*



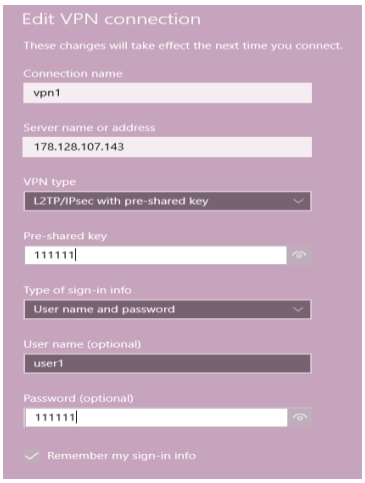
Sumber: dokumen pribadi

Gambar 39. melakukan *trace* ke perangkat lokal 10.10.10.2 *IP VPN* dari *VPN Server* 10.10.10.10 *IP VPN* dari *Router* toko 192.168.88.253 *IP* dari Perangkat *Laptop* di jaringan *LAN*. Berarti paket yang di kirimkan dari *user*, berhasil melewati *VPN Server*, melewati *tunneling* dari *router* toko dan sampai ke *Laptop* di jaringan *LAN*.

5. Percobaan *login* ke jaringan *VPN* .

Pada percobaan pertama ini pihak luar yang tidak mengetahui *user name*, *password* dan *Pre-shared key IPsec*. Mencoba untuk masuk ke dalam jaringan *VPN*.

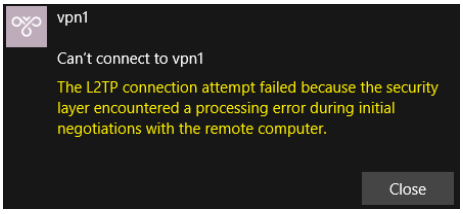
p-ISSN : 2406-7733
e-ISSN : 2597-9922



Sumber : dokumen pribadi

Gambar 40 Percobaan *login* pertama

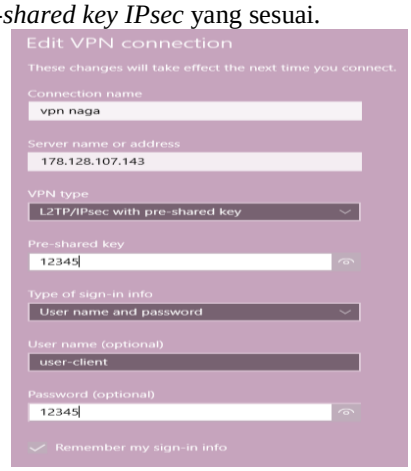
Hasilnya dapat di lihat pada Gambar 40, tidak bisa masuk ke dalam jaringan karena data yg di masukan pada Gambar 40 sebelum nya tidak sesuai dengan yang telah di konfigurasi di *server VPN*.



Sumber : dokumen pribadi

Gambar 41 Tidak berhasil *Connect*

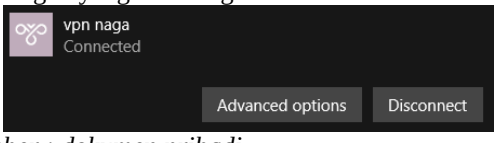
Pada percobaan kedua ,akan melakukan *login* ke jaringan menggunakan *user name*, *password*, dan *Pre-shared key IPsec* yang sesuai.



Sumber : dokumen pribadi

Gambar 42 Percobaan *login* kedua

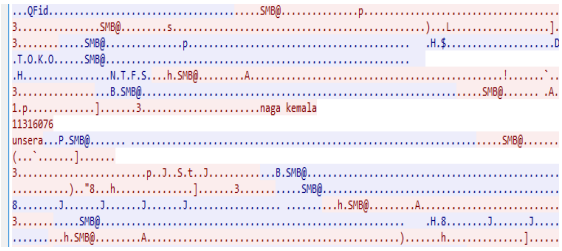
Hasil nya dapat masuk ke jaringan *VPN* , karena *username password*, dan *Pre-shared key* sesuai dengan yang di konfigurasikan di *server VPN*.



Sumber : dokumen pribadi

Gambar 43 Berhasil *Connect*

6. Pengujian enkripsi *IPsec*. Berikut adalah hasil pengiriman data dari jaringan lokal dan belum terkoneksi dengan jaringan *VPN*. *Data* tersebut masih dapat terbaca karena belum terenkripsi oleh *IPsec*



Sumber : dokumen pribadi

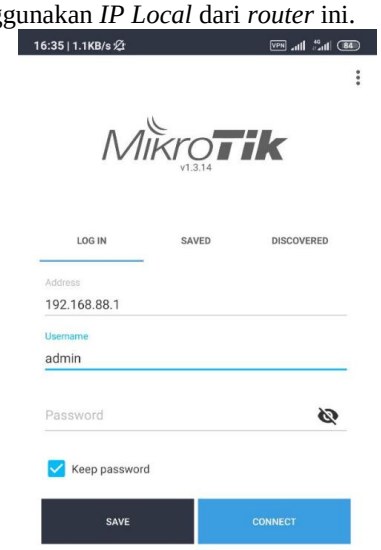
Gambar 44. Hasil pengiriman data tanpa *VPN Ipsec*

Dan yang berikut ini adalah hasil dari pengiriman data yang sudah terkoneksi dengan jaringan *VPN IPsec*.

Sumber : dokumen pribadi

Gambar 45. Hasil pengiriman data dengan *VPN IPsec*

7. Pengujian *remote router* local. Koneksikan perangkat dengan jaringan *VPN*, dan *remote router MikroTik* yang ada di jaringan lokal toko menggunakan aplikasi *winbox*. Contoh ini menggunakan *winbox* pada smarphone *android*. Berikut adalah tampilan awal, akan *meremote* menggunakan *IP Local* dari *router* ini.

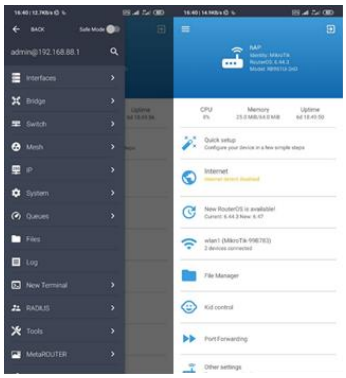


Sumber : dokumen pribadi

Gambar 46. Tampilan awal *Winbox android*

p-ISSN : 2406-7733
e-ISSN : 2597-9922

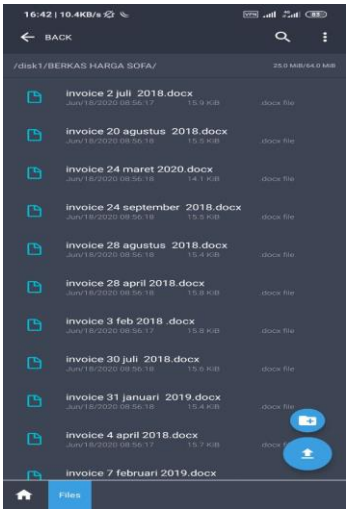
Selanjut berhasil terhubung ke dalam *router* tersebut.



Sumber : dokumen pribadi

Gambar 47. Tampilan *menu winbox android*

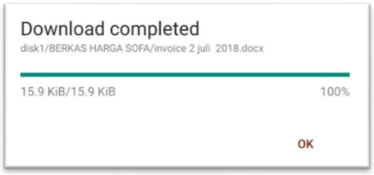
8. Pengujian *file sharing* dari *router* lokal menggunakan jaringan publik dengan *VPN*. Percobaan mengambil *file* yang ada di dalam *router* toko ini, masuk ke *file manager*. Diperlukan *user* name dan password untuk masuk ke *file server* ini. Untuk *username*: *user*, dan *password*: 12345.



Sumber : dokumen pribadi

Gambar 48. *File manager server router*

Selanjutnya klik salah satu *file* dan *download* ke *smartphone*.



Sumber : dokumen pribadi

Gambar 49. Hasil *download file*

9. Hasil *speedtest* jaringan *VPN*. Berikut adalah tabel dari hasil *speedtest* jaringan VPN

Tabel 1. Hasil *Speedtest*

No	*Download*	*Upload*	*Ping*
1	19.2*Mbps*	3.9*Mbps*	32*ms*
2	18.3*Mbps*	4.1*Mbps*	34*ms*
3	2.83*Mbps*	0.47*Mbps*	20*ms*
4	17.9*Mbps*	3.8*Mbps*	36*ms*

Sumber : Dokumen Pribadi

Pada hasil penelitian, telah diperoleh beberapa hasil yang dapat dijelaskan sebagai berikut.

1. Terciptanya jalur *VPN IPsec*. Dari yang sebelumnya menggunakan jaringan *internet* publik untuk pengiriman data yang diduga kurang aman untuk beberapa data sensitif seperti harga barang dan lain-lain. Kini dapat menggunakan jaringan *VPN IPsec* sebagai jalur khusus untuk pengiriman data.
2. Enksripsi data yang aman menggunakan *IPsec*. Dengan ini data jadi tidak mudah untuk dibaca oleh pihak tidak berwenang.
3. Remote *router* di jaringan lokal, dari jaringan publik menggunakan *VPN IPsec*.
4. *File sharing* yang dapat diakses dari luar jaringan lokal.

V. PENUTUP

Kesimpulan

Beberapa kesimpulan dari hasil yang didapat selama melakukan perancangan jaringan *VPN* berbasis *IPsec* menggunakan *router MikroTik*.

1. Dengan adanya jaringan *VPN IPsec* menjadikan jalur komunikasi data yang aman. Dan dapat diakses dari jaringan publik seperti, *wifi* dan *hotspot.* Ini dikarenakan *Tunneling* dari *VPN* yang memberikan jalur khusus untuk masuk ke jaringan lokal. Dan ditambah keamanan *data* dengan *protocol IPsec* yang dapat mengenkripsi *data* yang keluar masuk untuk menyembunyikan informasi yang dikirim dari pihak pihak yang tidak mempunyai hak, sehingga keamanan data dapat terjamin.
2. Perancangan jaringan *VPN* dengan memanfaatkan *IPsec* dapat membuat jaringan *VPN* menjadi lebih aman hal ini di disebabkan oleh tingkat keamanan yang lebih baik dari adanya enkripsi data pada fasilitas yang diberikan oleh *IPsec*, maka dengan demikian jaringan *VPN* dapat berjalan dengan baik.

Saran

Dari hasil penelitian yang telah dilakukan peneliti ada beberapa saran yang diberikan oleh peneliti sebagai berikut:

1. Perlu dilakukan penelitian lebih mendalam mengenai jaringan *VPN* agar memudahkan komunikasi secara aman.
2. Sebaiknya Menggunakan lisensi berbayar dari *MikroTik* untuk *CHR*. Dikarenakan adanya limitasi *bandwith* pada lisensi *free*. Khususnya untuk kepentingan *file sharing*. Karena *file sharing* membutuhkan *bandwith* yang besar.
3. Perlu dilakukan analisis terus menerus terhadap pengujian keamanan jaringan, karena semakin berkembangnya teknologi semakin tinggi pula tingkat ancaman keamanan terlebih dari serangan para peretas.

p-ISSN : 2406-7733
e-ISSN : 2597-9922

DAFTAR PUSTAKA

Arlan Reza, Munadi Rendy, dan Andini Nur. (2016) . "Implementasi Dan Analisis Sistem Keamanan *Ip* Security (*IPsec*) Di Dalam Multi *Protocol* Label Switching-*Virtual Private Network* (Mpls-*VPN*) Pada Layanan Berbasis *Ip* Multimedia Subsystem (IMS)" *e-Proceeding of Engineering* : Vol.3, No.3 December 2016. 4630-4640

Frankel, S., Kent, K., Lewkowski, R., D Orebaugh, A., W Richey, R., & R Sharma, S. (2005). Guide to IPsec VPNs Recommendations of the National Institute. *Nist Special Publication*, 126. https://doi.org/10.6028/NIST.SP.800-77

Hallberg, B. (2014). *Networking A Beginner's Guide Sixth Edition* (Sixth Edit). McGraw-Hill Education.

Ilyas, F. H., & Samsumar, L. D. (2018). MEMBANGUN JARINGAN INTERNET BERBASIS LOCAL AREA NETWORK DAN HOTSPOT WiFi PADA SMA NEGERI 1 LABUAPI. *Explore*, *8*(1), 41. https://doi.org/10.35200/explore.v8i1.24

Kurniawan, W. (2007). *Computer Starter Guide: Jaringan Komputer*. C.V Andi Offset.

Madcoms. (2009). *Panduan Lengkap Membangun Sistem Jaringan Komputer*. C.V Andi Offset.

Mufida, E., Irawan, D., & Chrisnawati, G. (2017). Remote Site Mikrotik VPN Dengan Point To Point Tunneling *Protocol* (PPTP) Studi Kasus pada Yayasan Teratai Global Jakarta. *Jurnal Matrik*, *16*(2), 9. https://doi.org/10.30812/matrik.v16i2.7

Putra, J. L., Indriyani, L., & Angraini, Y. (2018). Penerapan Sistem Keamanan Jaringan Menggunakan VPN Dengan Metode PPTP Pada PT. Asri Pancawarna. *IJCIT (Indonesian Journal on Computer and Information Technology) p-ISSN: 2527-449X, e-ISSN: 2549-7421*, *3*(2), 260–267. https://doi.org/https://doi.org/10.31294/ijcit.v3i2.4677

Ruslianto, I., & Ristian, U. (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

Saputra, D. (2016). Implementasi Virtual Private Network Pada Sistem Informasi Pengelolaan Keuangan Daerah Pemerintah Provinsi Riau. *Jurnal Teknologi*, *6*(2), 18–31.

Scott, C., Wolfe, P., Erwin, M., & Tunnel, A. (n.d.). *Virtual Private Networks , Second Edition*.

Supriyanto, B., dan Suharyanto. (2019). "Perancangan Jaringan *VPN* Menggunakan Metode Point To Point Tunneling *Protocol*." *Jurnal Teknik Komputer, Vol V No.2.* hal 235 – 240.

Sri, G. S. N., Kumari, G. N. S., & Devi, N. S. (2017). Secure Connection in VPN using AES. *International Research Journal of Engineering and Technology(IRJET)*, *4*(4), 949–952. https://www.irjet.net/archives/V4/i4/IRJET-V4I4195.pdf

Sugeng, W., & Putri, T. D. (2014). *Jaringan Komputer dengan TCP/IP "Membahas Konsep Implementasi TCP/IP Dalam Jaringan Komputer" Edisi Revisi*. Modula.

Yakova Zornitsa (2014) "A New *Virtual Private Network*s Access Model" Faculty of Mathematics and Informatics, Sofia University "St. Kliment Ohridski", 5, James Bourchier Blvd.

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

(2011; April 14). Jeff Tyson, Chris Pollette & Stephanie Crawford "How a *VPN* (*Virtual Private Network*) Works". Retrieved April 2, 2020 From HowStuffWorks: https://computer.howstuffworks.com/*VPN*.htm.

(2019; Juni 19) Retreived April 4, 2020 from *Cloud*Wards: https://www.*cloud*wards.net/what-is-a-*VPN*/