

PEMANFAATAN VPN DENGAN IP CLOUD MIKROTIK MENGGUNAKAN JARINGAN 3G (STUDI KASUS : PT. BPRS MUAMALAT HARKAT BENGKULU)

¹Rozali Toyib, ²Muntahanah

¹²³Prodi Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Bengkulu

Jl. Bali Kota Bengkulu, telp (0736) 22765/fax (0736) 26161

Email: rozalitoiyib@umb.ac.id, muntahanah@umb.ac.id

ABSTRAK

Salah satu teknologi penting dan menjadi trend dalam jaringan komputer maupun handphone adalah teknologi jaringan nirkabel/ Wireless LAN, teknologi ini adalah perkembangan dari teknologi jaringan local yang memungkinkan efisiensi dalam implementasi dan pengembangan jaringan komputer karena dapat meningkatkan mobilitas dan Fleksibilitas user, saat ini, jaringan wireless menjadi target yang paling menarik bagi hacker). Untuk mengatasi permasalahan keamanan data di jaringan internet ada suatu metode yaitu Virtual Private Network (VPN), merupakan jaringan lokal yang terhubung melalui jaringan publik (Internet) dengan metode tunneling, enkripsi dan dekripsi yang menjamin keamanan data walaupun data melewati jaringan public, maka kerahasiaan data menjadi lebih terjaga, biarpun ada pihak yang dapat menyadap data yang lalu lalang, walaupun terlihat tetapi tidak bisa dibaca dengan mudah karena sudah diacak, dengan menerapkan sistem enkripsi ini, tidak ada satupun orang dapat mengakses dan membaca isi jaringan data dengan mudah, VPN menggantikan alamat IP ISP lokal dengan IP public VPN, mengatur dan menentukan lalu lintas data untuk mengoptimalkan keamanan di dalam jaringan dengan membatasi daerah jaringan yang satu dengan yang lainnya, mengatur port atau paket yang diperbolehkan atau ditolak dan mengautentikasi terhadap akses dari dalam dan luar jaringan menjadi personal komputer dan Kelemahan dari koneksi Internet (jaringan Publik) tidak bisa diprediksi, hal ini disebabkan terkoneksi pada jaringan pihak lain sehingga otomatis tidak mempunyai kontrol terhadap jaringan tersebut.

Keywords: Wireless, Fleksibilitas, Jaringan, Virtual Private Network

1 PENDAHULUAN

Salah satu teknologi penting dan menjadi trend dalam jaringan komputer maupun handphone adalah teknologi jaringan nirkabel/ Wireless LAN, teknologi ini adalah perkembangan dari teknologi jaringan local yang memungkinkan efisiensi dalam implementasi dan pengembangan jaringan komputer karena dapat meningkatkan mobilitas dan Fleksibilitas user, dengan adanya teknologi wireless transaksi perbankan dapat dilakukan dimana saja selama masih terjangkau

Terhubungnya LAN (Local Area Network) atau komputer ke internet membuka potensi adanya lubang keamanan (security hole) yang tadinya bisa ditutup dengan mekanisme keamanan secara fisik. Ini sesuai dengan pendapat bahwa kemudahan mengakses informasi berbanding terbalik dengan tingkat keamanan sistem informasi itu sendiri. Semakin tinggi tingkat keamanan, semakin sulit untuk mengakses informasi. Keamanan informasi adalah bagaimana cara kita dapat mencegah penipuan (cheating) atau mendekati adanya penipuan di sebuah sistem berbasis informasi, di mana informasinya sendiri tidak memiliki arti fisik. (Arifin, Zaenal, 2005)

Jaringan nirkabel telah menjadi salah satu target paling menarik untuk peretasan hari ini (saat ini, jaringan wireless menjadi target yang paling menarik bagi hacker). Pernyataan tersebut mengindikasikan bahwa semua aspek selalu mempunyai resiko, ada aspek baik dan buruk yang selalu saja mengikutinya. Keamanan selalu saja menjadi isu menarik dalam perkembangan komunikasi, interaksi, dan sosialisasi manusia. Perkembangan jaringan wireless yang begitu pesat dan populer menjadikan pihak-pihak lain yang kurang bertanggung jawab mencoba mencari celah-celah untuk dapat memanfaatkannya secara ilegal dan tidak bermaksud bagi kebaikan. Bukan mustahil bahwa saat ini jaringan wireless menjadi salah satu target utama bagi para hacker. Beberapa organisasi dan perusahaan semakin gencar mengembangkan jaringan wireless karena kemudahan, kenyamanan, dan harga peralatan yang semakin terjangkau. Di pasaran, peralatan-peralatan wireless ini secara default tidak mempunyai fitur keamanan yang memadai, sehingga keberadaan peralatan wireless menjadi target

Toyib, Pemanfaatan VPN Dengan IP Cloud Mikrotik Menggunakan Jaringan 3G (Studi Kasus : PT. BPRS Muamalat Harkat Bengkulu)

utama para hacker untuk mencoba memanfaatkan berbagai kelemahannya. Hal ini didukung lagi dengan dokumen-dokumen peralatan wireless yang dengan mudah diperoleh di website secara bebas, baik dari segi teknis detail hingga operasionalnya.

Untuk mengatasi permasalahan keamanan data di jaringan internet ada suatu metode yaitu Virtual Private Network (VPN). VPN merupakan jaringan lokal yang terhubung melalui jaringan publik (Internet). Di dalam VPN terdapat metode tunneling dan enkripsi yang menjamin keamanan data walaupun data melewati jaringan publik. Hal ini yang membuat VPN handal dalam mengatasi permasalahan ini. Untuk dapat mengimplementasikan VPN perusahaan wajib memiliki IP Publik yang Static, namun kenyataannya untuk mendapatkan IP Public yang Static kadang menjadi kendala bagi perusahaan skala kecil yang baru mengembangkan cabang nya karena mahal nya paket yang di tawarkan provider yang menyediakan ip Static.

2 TINJAUAN PUSTAKA

2.1 Jaringan Komputer

Sebuah jaringan biasanya terdiri dari dua atau lebih komputer yang saling berhubungan diantara satu dengan yang lainnya, dan saling berbagi sumber daya misalnya CDROM, Printer, Pertukaran File, atau memungkinkan untuk saling berkomunikasi secara elektronik. Komputer yang terhubung tersebut dimungkinkan berhubungan dengan media kabel, saluran telepon, gelombang radio, satelit atau infrared (Muhammad Dedy Haryanto, Imam Riadi 2014).

Menurut Muhammad Ibrahim Hasan (2016) Jaringan diklasifikasikan berdasarkan jarak dan lokasi, yaitu Local Area Network (LAN), Metropolitan Area Network (MAN), Wide Area Network (WAN), Internet, dan jaringan tanpa kabel (Wireless). Hubungan antara jarak, lokasi, dan jenis jaringan berikut:

Tabel 1 Jenis Jaringan Berdasarkan Jarak

Jarak	Lokasi	Jenis Jaringan
10 m	Ruangan	LAN
100 m	Gedung	LAN
1 km	Kampus	LAN
10 km	Kota	MAN
100 km	Negara	WAN
1.000 km	Benua	WAN
10.000 km	Planet	INTERNET

2.2 Pengertian Mikrotik

Mikrotik Router, merupakan sistem operasi linux base yang diperuntukkan sebagai network router. Didesain untuk memberikan kemudahan bagi penggunaannya. Administrasinya bisa dilakukan melalui windows application (winbox). Selain itu instalasi dapat dilakukan pada standard komputer PC (Personal Computer). PC yang akan dijadikan router mikrotik tidak memerlukan resource yang cukup besar untuk penggunaan standard, misalnya hanya sebagai gateway. Untuk keperluan beban yang besar (network yang kompleks, routing yang rumit) disarankan untuk mempertimbangkan pemilihan resource PC yang memadai (Eko Purwanto, 2015),

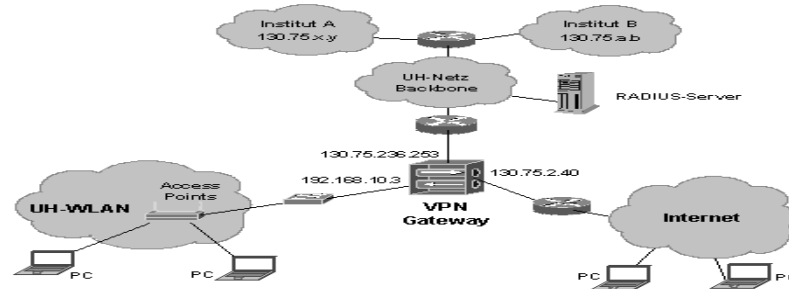
Mikrotik merupakan sebuah perusahaan yang bergerak di bidang produksi perangkat keras (Hardware) dan perangkat lunak (Software) yang berhubungan dengan sistem jaringan komputer yang berkantor pusat di Latvia, bersebelahan di Rusia. Mikrotik didirikan pada tahun 1995 untuk mengembangkan router dan sistem ISP (Internet Service Provider) nirkabel. Mikrotik adalah router yang dibangun dari sistem operasi Linux, hanya saja dimodifikasi sedemikian rupa sehingga fungsinya spesifik ke arah routing dan fungsi jaringan. Alat ini dapat digunakan untuk routing static, routing dinamik, hotspot, firewall, VPN, DHCP Server, DNS cache, dan web proxy Santi Dwi Ratnasari, Dwi safiroh Utsalana, 2017).

2.3 Pengertian Virtual Private Network (VPN)

Virtual Private Network (VPN) adalah jaringan *private* yang menggunakan jaringan publik seperti internet untuk menghubungkan *remote access* dan *user* secara bersama-sama dengan memberikan tingkat

Toyib, Pemanfaatan VPN Dengan IP Cloud Mikrotik Menggunakan Jaringan 3G (Studi Kasus : PT. BPRS Muamalat Harkat Bengkulu)

level privasi, *security*, *Quality of Service (QoS)*, dan pengelolaan dimana jaringan tersebut dibangun seluruhnya dalam fasilitas yang dimiliki secara pribadi dan *dedicated* (Purbo, Onno, 2016).



Gambar 1 Virtual Private Network

2.4 Teknologi Jaringan 3G

Sekarang lagi ramai dibicarakan tentang generasi ketiga teknologi bergerak atau yang sering disebut 3G. Teknologi 3G didapatkan dari dua buah jalur teknologi telekomunikasi bergerak. Pertama adalah kelanjutan dari teknologi GSM/GPRS/EDGE dan yang kedua kelanjutan dari teknologi CDMA (IS-95 atau CDMAOne). UMTS (Universal Mobile Telecommunication Service) merupakan lanjutan teknologi dari GSM/GPRS/EDGE yang merupakan standard telekomunikasi generasi ketiga dimana salah satu tujuan utamanya adalah untuk memberikan kecepatan akses data yang lebih tinggi dibandingkan dengan GPRS dan EDGE. Kecepatan akses data yang bisa didapat dari UMTS adalah sebesar 384 kbps pada frekuensi 5KHz sedangkan kecepatan akses yang didapat dengan CDMA 1x ED-DO Rel0 sebesar 2.4 Mbps pada frekuensi 1.25MHz dan CDMAx ED-DO relA sebesar 3.1Mbps pada frekuensi 1.25MHz yang merupakan kelanjutan dari teknologi CDMAOne. Berbeda dengan GPRS dan EDGE yang merupakan overlay terhadap GSM, maka 3G sedikit berbeda dengan GSM dan cenderung sama dengan CDMA. 3G yang oleh ETSI disebut dengan UMTS (Universal Mobile Telecommunication Services) memilih teknik modulasi WCDMA (wideband CDMA). Pada WCDMA digunakan frekuensi radio sebesar 5 Mhz pada band 1.900 Mhz (CdmaOne dan CDMA 2000 menggunakan spectrum frekuensi sebesar 1.25 MHz) dan menggunakan chip rate tiga kali lebih tinggi dari CDMA 2000 yaitu 3.84 Mcps (Mega Chip Per Second). Secara teknik dalam jaringan UMTS terjadi pemisahan antara circuit switch (cs) dan packet switch (ps) pada link yang menghubungkan mobile equipment (handphone) dengan BTS (RNC) sedangkan pada GPRS dan CDMA 2000 1x tidak terjadi pemisahan melainkan masih menggunakan resource yang sama di air interface (link antara Mobile Equipment dengan Base Station). HSPDA (High Speed Packet Downlink Access) merupakan kelanjutan dari UMTS dimana ini menggunakan frekuensi radio sebesar 5MHz dengan kecepatan mencapai 2Mbps (Parlin Pasaribu, 2006).

3 METODOLOGI PENELITIAN

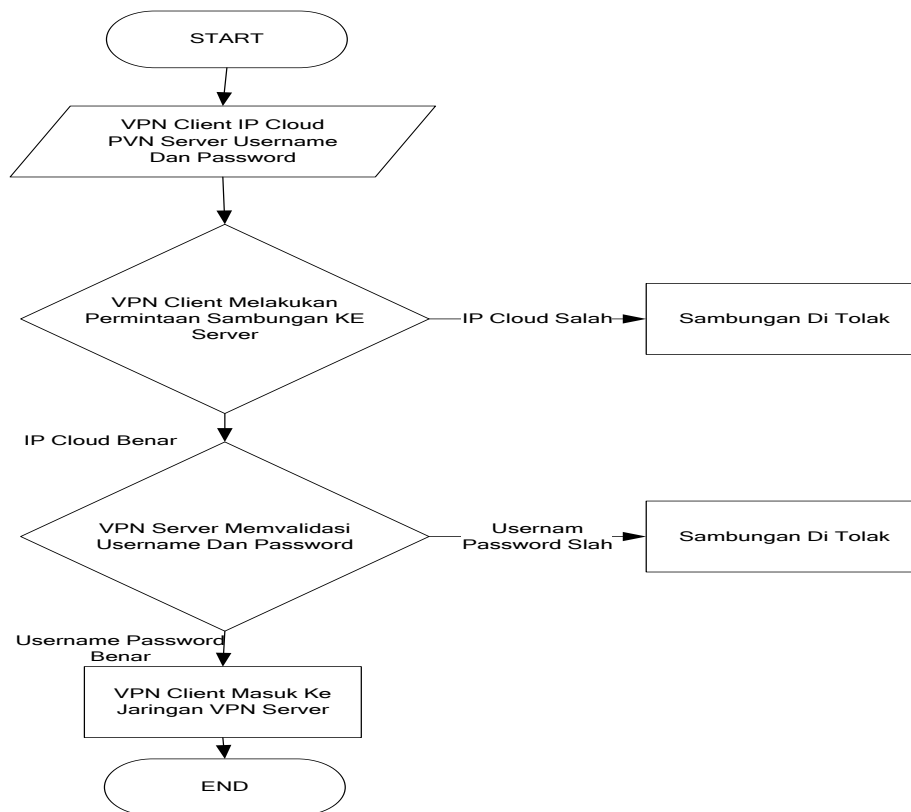
3.1 Tempat dan waktu penelitian

Penelitian di PT BPRS Muamalat Harkat Bengkulu yang beralamat di Jalan Bengkulu seluma Bengkulu selatan

3.2 Metode pengumpulan data

- Observasi, yaitu memperoleh data dengan melakukan pengamatan langsung teknologi jaringan yang digunakan di PT. BPRS Muamalat Harkat Bengkulu
- Wawancara, yaitu pengumpulan data dengan melakukan wawancara secara langsung kepada Pimpinan dan Staf karyawan
- Studi pustaka, yaitu membaca, mempelajari buku-buku literatur yang berhubungan dengan penelitian.

3.3 Flowchart Konfigurasi Server VPN



Gambar 2 Flowchart Cara Kerja VPN

Keterangan :

- Client adalah User yang menggunakan layanan jaringan VPN yang terhubung ke router di setiap cabang di PT. BPRS Muamalat Harkat
- Administrator Server Adalah orang yang mengelola, memonitor dan mengontrol kinerja VPN yang ada di PT. BPRS Muamalat Harkat

4 HASIL DAN PEMBAHASAN

4.1 Konfigurasi PVN Server Pada Router Menggunakan WinBox

Dalam tahapan Konfigurasi Mikrotik Router OS ini, tahapan tahapan yang akan kita lakukan yaitu mencakup

- Pengaturan IP perangkat / *Interfaces* di Mikrotik.
- Mengkonfigurasi Point to Point Protocol over Ethernet (PPP) dengan Modem USB
- Mengkonfigurasi Point to Point Tunneling Protocol Server (PPTP)
- Membuat Authenticated User / VPN User.
- Mengaktifkan Fitur IP Cloud

4.2 Pengaturan IP / Interfaces di Mikrotik

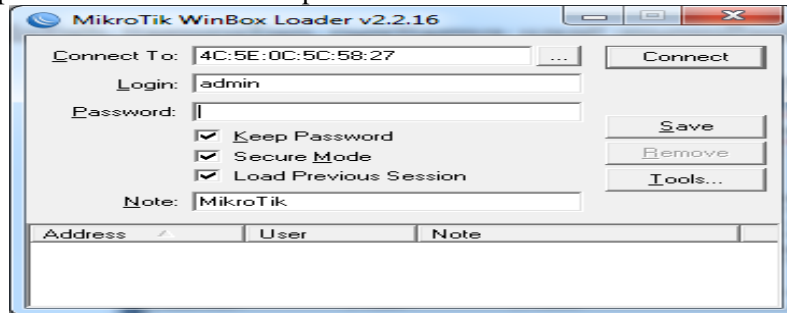
Pertama kali yang dibutuhkan dalam mengkonfigurasi Mikrotik Router OS adalah Winbox. Winbox adalah sebuah software utility yang digunakan untuk melakukan remote ke server mikrotik dalam mode Graphic User Interface (GUI). Berikut adalah gambar icon Mikrotik yang telah didownload.



Gambar 3 Icon aplikasi Winbox yang sudah di download

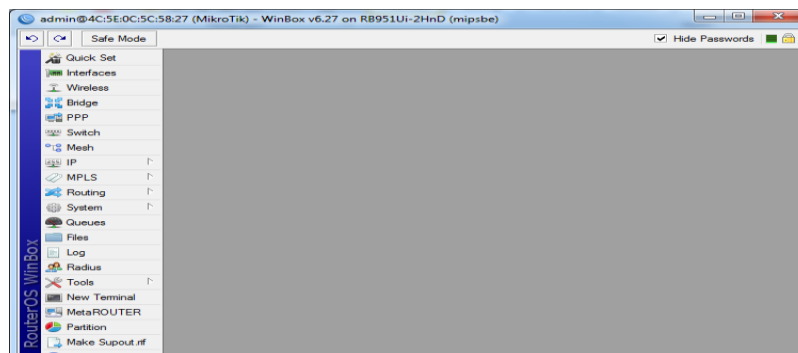
Toyib, Pemanfaatan VPN Dengan IP Cloud Mikrotik Menggunakan Jaringan 3G (Studi Kasus : PT. BPRS Muamalat Harkat Bengkulu)

Maka untuk dapat menggunakan Winbox, harus mendownloadnya terlebih dahulu dari www.mikrotik.co.id. Setelah Winbox terdownload, sekarang buka Aplikasi Winbox. Kemudian akan muncul dialog box seperti gambar dibawah. Pada jendela yang tampil seperti pada gambar, “Connect To” adalah kolom alamat IP atau alamat Media Access Control (MAC Address) perangkat Mikrotik yang akan dikonfigurasi lewat Winbox. Dibawahnya, “Login” dan “Password” adalah tempat identitas user yang akan mengakses Mikrotik lewat Winbox. Dikarenakan Mikrotik OS-nya masih baru dan belum pernah di konfigurasikan sebelumnya, maka User ID & Password untuk Login di Mikrotik masih default yaitu User ID = “admin” dan Password = tidak ada. Untuk memulai masuk pada tampilan GUI dari Mikrotik Klik Connect seperti yang ditunjukkan pada gambar dihalaman sebelumnya. Berikut adalah tampilan pertama saat membuka aplikasi Winbox.



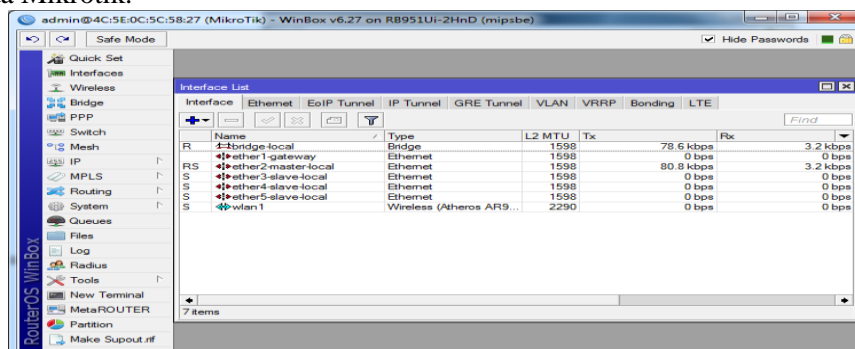
Gambar 4 Tampilan pertama saat membuka winbox

Berikut adalah gambar jendela dari aplikasi Winbox yang keluar setelah Winbox terhubung dengan Mikrotik.



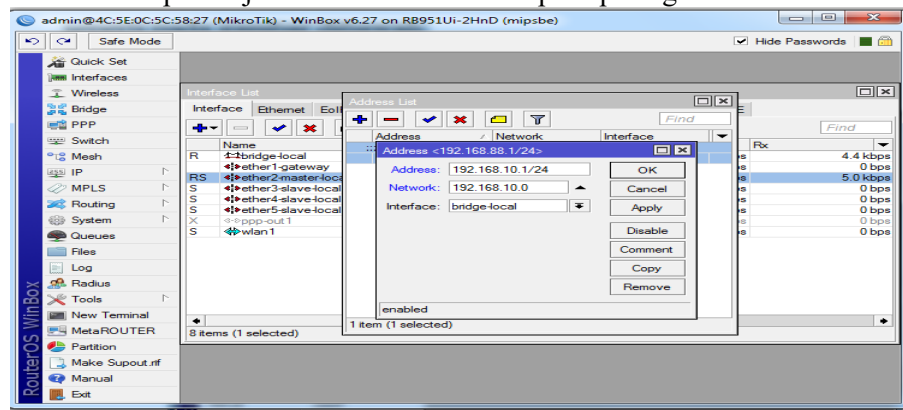
Gambar 5 Jendela aplikasi Winbox

Selanjutnya, Klik menu Interfaces untuk menampilkan semua Interface LAN Card yang telah terpasang. Berikan nama untuk memudahkan dalam membedakan setiap Port kabel LAN, suatu misal menggunakan “Modem Three” pada interface “ether1”, dan “lokal” untuk interface “ether2”, klik dua kali pada Interface Name “ether1” dan “ether2” tersebut dan ganti dengan nama “Three” dan “local”. Klik dua kali pada tiap Interface untuk mengganti nama setiap Interface. Berikut adalah gambar menu interfaces pada Mikrotik.



Gambar 6 Jendela interfaces yang perangkat Ethernet yang tersedia

Selanjutnya setting IP dari Interfaces Bridge local, buka Menu IP > Kemudian Addresses, lalu klik tombol “+” untuk menampilkan jendela “New Adress” seperti pada gambar dibawah.

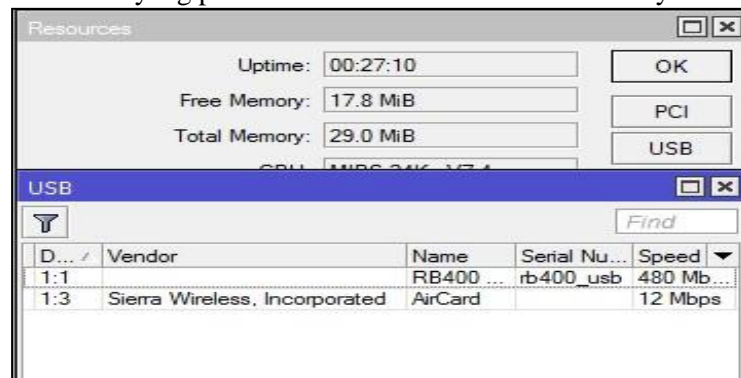


Gambar 7 Jendela Address List

Ganti Address yang secara default terisi dengan “192.168.88.1/0” menjadi IP untuk interface “bridge local”, yaitu “192.168.10.1/24”, isi Network dengan IP Network dari IP lokal, yaitu “192.168.10.0”. Jika sudah simpan konfigurasi dengan mengklik Apply, lalu klik OK.

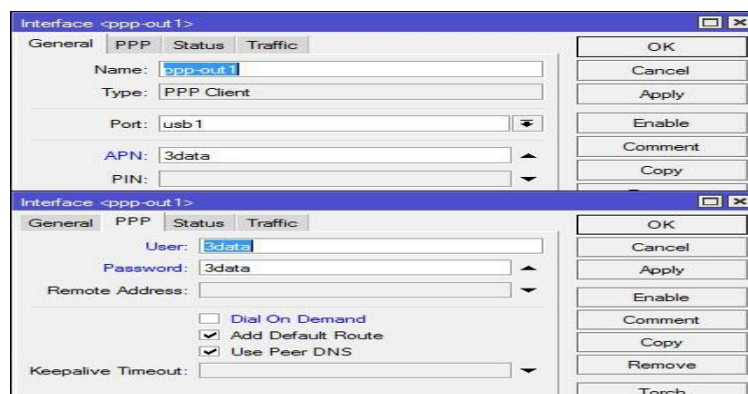
4.3 Seting USB Modem Sebagai Koneksi Internet.

Jika IP, interface (ethernet dan wireless) dan DNS sudah dikonfigurasi, kita pasangkan 3G modem kita ke port usb di router. Hal yang perlu kita cek kembali adalah menu “/system resource usb”.



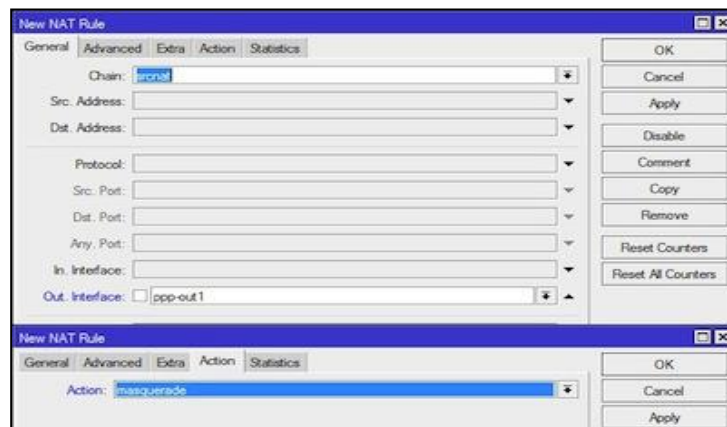
Gambar 8 Jendela Resource USB

Untuk perangkat yang sudah disupport Mikrotik, biasanya akan muncul USB device baru secara otomatis. Mikrotik juga akan membuatkan interface baru “ppp-out1”, Untuk memasukkan Username, Password dan APN dari provider kita, kita masukan di interface ppp-out1 yang sudah dibuat oleh Mikrotik.



Gambar 9 Jendela Interface PPP Out1

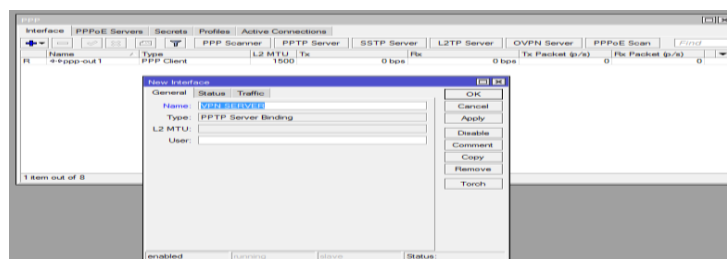
Langkah terakhir, kita harus menambahkan srcnat masquerade untuk interface ppp-out1 supaya client bisa akses ke internet.



Gambar 10 Jendela NAT Rule

4.4 Mengkonfigurasi Point to Point Tunneling Protocol Server (PPTP)

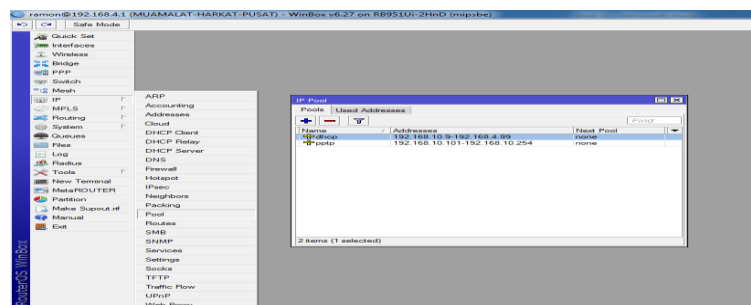
Selanjutnya, kembali ke jendela PPP. Klik tombol “+”, pilih PPTP Server, maka akan muncul jendela New Interface seperti gambar dibawah ini. Beri Nama “VPN-SERVER”. Kemudian klik Apply lalu OK.



Gambar 11 Jendela PPTP

Klik tombol “+”, pilih PPTP Server, maka akan muncul jendela New Interface seperti gambar dibawah ini. Beri Nama “VPN-SERVER”. Kemudian klik Apply lalu OK.

Berikut adalah gambar jendela dimana IP Pool akan di buat dan Range IP untuk VPN – Client akan ditentukan.



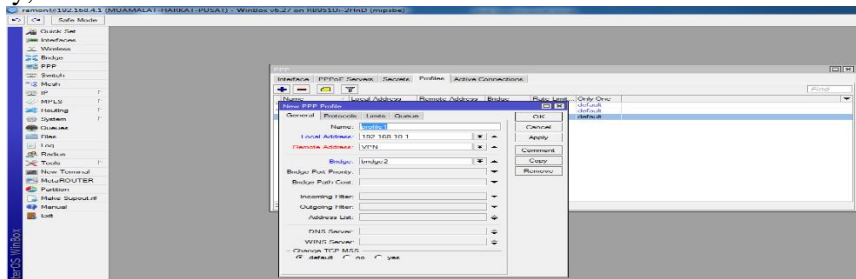
Gambar 12 Jendela IP pool

Beri nama “VPN” pada “Name”. Pada “Addresses”, diisi range IP yang diinginkan untuk dapat mengakses VPN Server. Karena yang dibutuhkan hanya 1 user untuk client, dan 1 untuk admin, maka diketikkan “192.168.10.1-192.168.10.25”. “Next Pool” dibiarkan “none”. Kemudian Klik Apply lalu OK.

4.5 Membuat Authenticated User / VPN User.

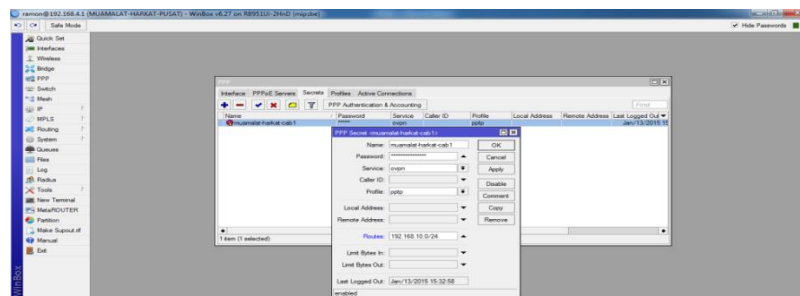
Kemudian kembali ke “PPP”, masuk tab “Profile”. Klik tombol “+”. Beri nama “VPN-PROFILE”, “Local Address” diisi dengan alamat IP dari Interface “lokal”, yaitu “192.168.10.1”, dan “Remote

Address” diisi dengan IP Pool yang sudah dibuat yaitu “VPN”, kemudian simpan konfigurasi dengan mengklik Apply, lalu OK.



Gambar 13 Jendela Profile

Kemudian pindah ke tab “Secrets” untuk membuat username dari setiap user VPN, klik tanda “+”. Masukkan “Name” & “Password” terserah, misalnya disini saya menentukan username = “muamalat_harkat_cab1” dan password = “m12345678, untuk “Service” pilih “pptp”, dan untuk “Profile” pilih yang sudah dibuat tadi, yaitu “VPN-PROFILE”. Selanjutnya simpan konfigurasi, klik Apply, lalu OK.

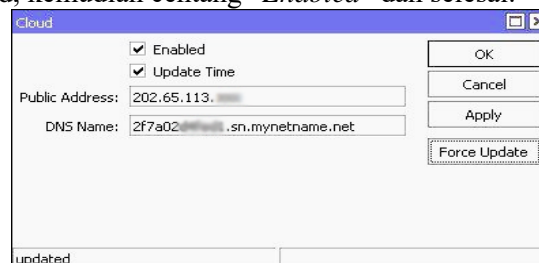


Gambar 14 Jendela Secret

Selanjutnya, pindah kembali pada tab “Interface” untuk mengaktifkan Point to Point Tunneling Protocol Server (PPTP Server). Klik tombol “PPTP Server”, beri tanda centang pada “Enabled” untuk mengaktifkan PPTP Server, lalu pada “Default Profile” pilih “VPN-PROFILE”, dan pada “Authentication”, pastikan “pap” dan “chap” tidak dicentang. Klik Apply untuk menyimpan konfigurasi, lalu OK.

4.6 Mengaktifkan Fitur IP Cloud

Jika sebelumnya kita telah menggunakan layanan DDNS dari pihak ketiga, kita membutuhkan script yang cukup rumit agar router melakukan update ke penyedia DDNS. Dengan fitur IP Cloud, cukup masuk ke menu IP → Cloud, kemudian centang “Enabled” dan selesai.



Gambar 15 Jendela IP Cloud

Sebelum menjalankan fitur Ip Cloud ini, pastikan router sudah terkoneksi ke internet, agar router dapat melakukan request DNS ke IP Cloud Server. Jika statusnya sudah “updated”, maka kita ias menggunakan nama Domain untuk remote Router atau mengakses service yang dijalankan oleh router seperti VPN dari jaringan internet. Setiap menit router akan selalu mengecek outgoing IP Router dan akan melakukan update IP ke IP Cloud Server. Dengan begitu, walau IP public router berubah-ubah, kita tetap ias remote atau VPN ke router menggunakan nama domain yang sama.

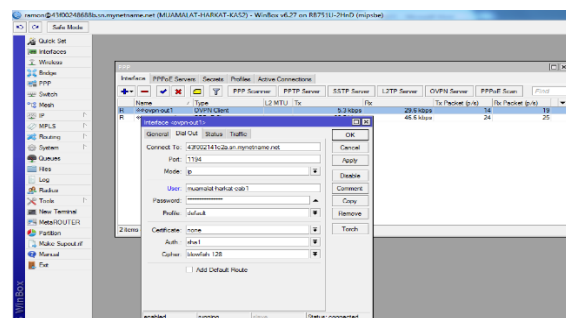
Toyib, Pemanfaatan VPN Dengan IP Cloud Mikrotik Menggunakan Jaringan 3G (Studi Kasus : PT. BPRS Muamalat Harkat Bengkulu)

4.7 Pembahasan

4.7.1 Pengujian Jaringan PVN

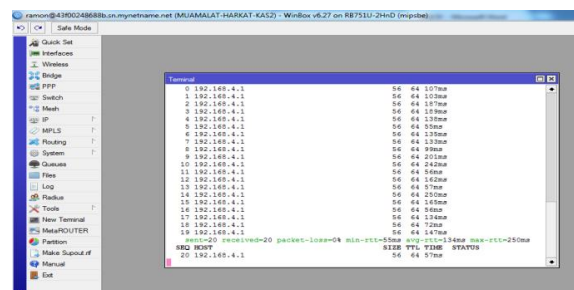
Untuk mengetahui apakah VPN Server berjalan dengan baik maka dibutuhkan pengujian pada beberapa poin berikut ini. Konfigurasi connect to arahkan ke IP cloud server PVN yang telah di buat, lengkapi dengan username dan password nya, proses ini mencega dan indetifikasi penggunaan yang tidak sah dari jaringan komputer dan mengantisipasi resiko jaringan komputer berupa ancaman fisik maupu logik baik langsung atau tidak langsung menggnggu aktivitas yang sedang berlangsung dalam jaringan komputer serta membuat tingkat akses mekanisme kendali terhadap rekayasa sosial untuk membedakan sumberdaya internal dan eksternal autentikasi user.

Server kemudian melakukan verifikasi username dan password dan apabila berhasil, VPN server memberi IP Address baru pada komputer client dan selanjutnya sebuah koneksi/tunnet akan terbentuk.



Gambar 16 Jendela Client PVN Menggunakan IP Cloud

Setelah muncul tanda R pada router client, selajut nya dapat kita coba untuk mengecek koneksi dari router client ke router server dengan menggunakan terminal, ketikkan perintah “ ping 192.168.10.1”



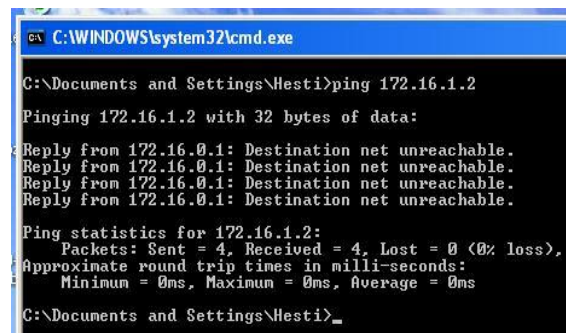
Gambar 17 Ping Ke PVN Server

Bila balasan nya Reply from 192.168.10.1 berarti alamat IP 192.168.10.1 membalas perintah ping yang telah dikirim ke alamat 3192.168.10.1 . Bytes menunjukkan besar request packet yang dikirimkan. Time menunjukkan nilai “round trip delay” yang menunjukkan waktu yang diperlukan packet yang dikirimkan untuk mencapai komputer/alamat IP yang dituju. Nilai ini dihitung dengan membagi dua selisih waktu Ping packet mulai dikirimkan dengan waktu response dari Ping packet diterima. Sedangkan TTL merupakan nilai “Time-To-Live” yang digunakan untuk mencegah adanya circular routing pada suatu jaringan.

IP address (alamat Internet) khusus untuk masing-masing komputer yang terhubung dalam jaringan tersebut, apa bila jaringan ini tidak terlindungi oleh tunnel atau firewall, IP address tadi akan dengan mudahnya dikenali atau dilacak oleh pihak-pihak yang tidak diinginkan, dengan adanya perlindungan seperti firewall, kita bisa menyembunyikan (hidden) address tadi sehingga tidak dapat dilacak oleh pihak-pihak yang tidak diinginkan.

4.7.2 Pengujian Koneksi Antar Client

Skenario yang dilakukan adalah : PC2 mengirimkan paket ICMP (ping) ke PC1 dan sebaliknya, sebelum dan sesudah di aktifkan koneksi VPN. Apakah ada perbedaan saat diaktifkan VPN dan saat tidak ada VPN



```

C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Hesti>ping 172.16.1.2

Pinging 172.16.1.2 with 32 bytes of data:

Reply from 172.16.0.1: Destination net unreachable.
Reply from 172.16.0.1: Destination net unreachable.
Reply from 172.16.0.1: Destination net unreachable.
Reply from 172.16.0.1: Destination net unreachable.

Ping statistics for 172.16.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Hesti>_

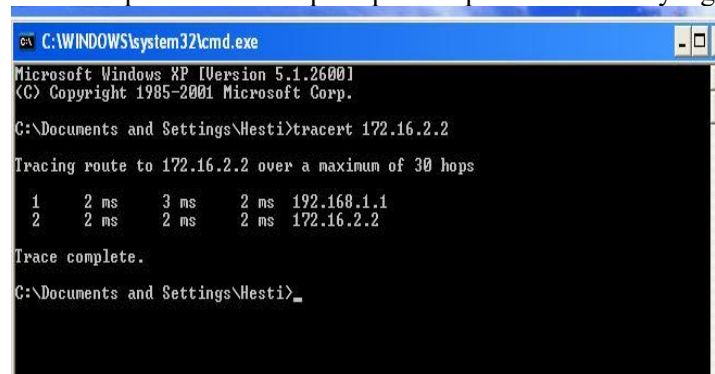
```

Gambar 18 Pengujian Koneksi antar client

VPN server kemudian memverifikasi username dan password dan apabila berhasil maka VPN server memberi IP address baru pada komputer Client dan selanjutnya sebuah koneksi/tunnel akan terbentuk, selanjutnya komputer client bisa digunakan untuk mengakses berbagai resource (komputer atau LAN) yang berada dibelakang VPN server misalnya melakukan tranfer data, ngeprint dokument, browsing dengan gateway yang diberikan dari VPN server, melakukan remote destop dan lain sebagainya. Dengan ada enkripsi dan deskripsi maka data yang dilewati jaringan internet inididak dapat diakses oleh orang lain bahkan oleh client lain yang terhubung ke server VPN yang sama sekalipun. Karena kunci untuk membuka enkripsinya hanya diketahui oleh server VPN dan client yang terhubung. Enkripsi dan deskripsi menyebabkan data tidak dapat dimodifikasi dan dibaca sehingga keamanannya terjamin.

4.7.3 Pengujian Routing

Skenario yang dilakukan adalah : dari PC2 dilakukan pengecekan jalur yang dilalui paket data menggunakan perintah “tracert” pada command prompt. Berapa kali loncatan yang dilalui oleh router



```

C:\WINDOWS\system32\cmd.exe

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Hesti>tracert 172.16.2.2

Tracing route to 172.16.2.2 over a maximum of 30 hops

  0  2 ms  3 ms  2 ms  172.168.1.1
  1  2 ms  2 ms  2 ms  172.16.2.2

Trace complete.

C:\Documents and Settings\Hesti>_

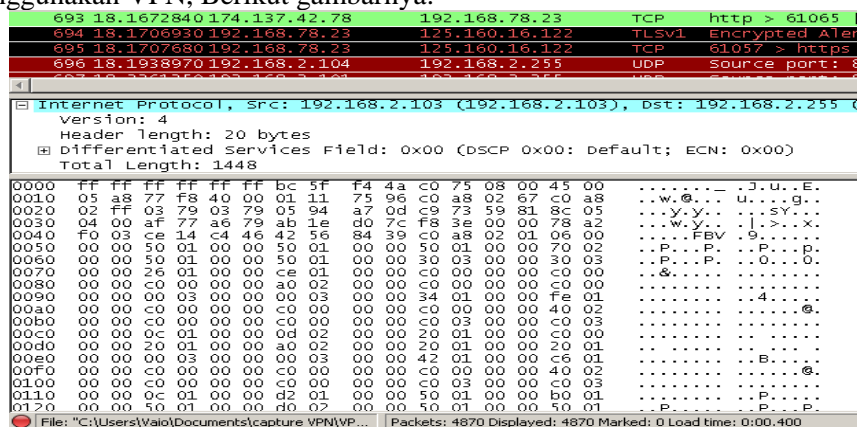
```

Gambar 19 Pengujian Routing

Tracer (jejak Rute) utilitas baris perintah yang dapat digunakan untuk melacak lintasan yang diambil paketprotokol internet (IP) ke tujuannya,sehingga tracer melaporkan alamat IP antarmuka di samping router, terlihat perintah tracer dan output, paket perjalanan melalui dua perute (192.168.1.1 dan 172.16.2.2), trecert ini berguna untuk pemecahan masalah jaringan besar yang mana beberapa lintasan dapat mengarah ke titik yang sama atau banyak komponen menengah (perute atau jembatan yang terlibat). Setelah mengetahui jalur yang dilewati paket data, *ICMP* pada perintah *PING* lalu jalur yang biasa dilewati diputus untuk mengetahui jalur backup yang dimiliki masing-masing. Routing protokol pada setiap topologi dan mengecek koneksi dari internet yang digunakan agar bisa terhubung ke server atau tidak, perangkat yang melakukan pengiriman mengenai adanya jaringan, tetapi kalau tidak menemukan alamat tujuan atau dalam waktu yang diberikan untuk melakukan ping sudah habis (time out). Data yang dikirim tidak sampai pada tujuan, namun berputar hingga masa tenggang keberadaan pada jaringan habis sebelum mencapai tujuan.

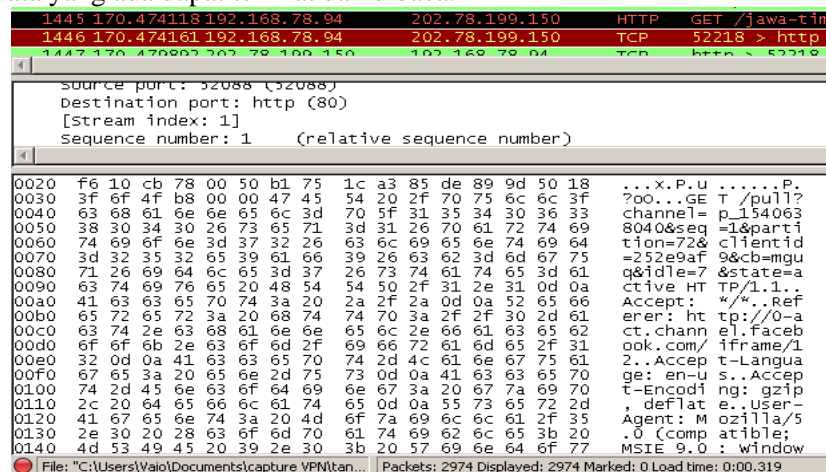
4.7.4 Pengujian Pengekripsian Data

Dengan adanya aplikasi Wire shark, dapat diketahui proses dari pengenkripsian semua data. dan dapat dibedakan diketahui jelas perbedaan yang ada antara koneksi internet dengan menggunakan VPN dan tanpa menggunakan VPN, Berikut gambarnya:



Gambar 20 Koneksi menggunakan VPN

Terlihat pada bagian response daripada perintah-perintah yang ada pada dibagian atas, data-data atau tulisan-tulisan yang ada terenkripsi dan sulit untuk membacanya. Lain halnya dengan pada gambar dibawah ini yang merupakan koneksi internet tanpa menggunakan internet PVN yang pada bagian response data-data yang ada dapat terlihat dan dibaca.



Gambar 4.17 Koneksi tanpa menggunakan VPN

VPN memiliki sistem kinerja mengenkripsi semua data yang lewat melalui, dengan adanya teknologi enkripsi ini, maka kerahasiaan data menjadi lebih terjaga, biarpun ada pihak yang dapat menyadap data yang lalu lalang, walaupun terlihat tetapi tidak bisa dibaca dengan mudah karena sudah diacak, dengan menerapkan sistem enkripsi ini, tidak ada satupun orang dapat mengakses dan membaca isi jaringan data dengan mudah.

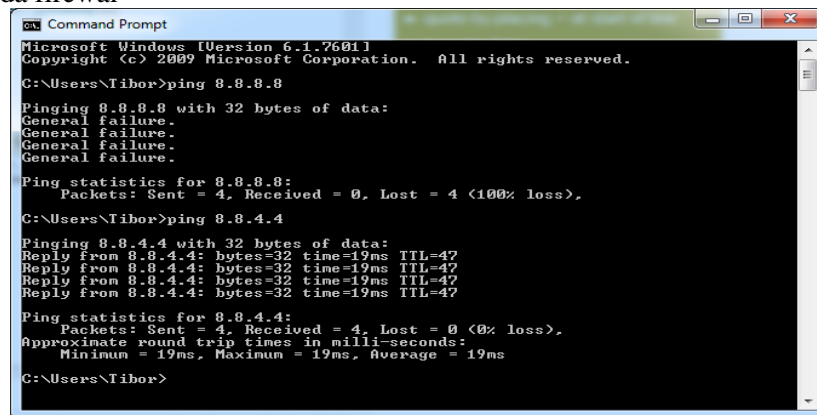
VPN ini juga dapat digunakan untuk meningkatkan kecepatan download dari internet, ketika menggunakan VPN, kita seolah-olah sedang menggunakan jaringan pribadi, yang mana sedikit digunakan oleh orang lain dan juga bisa terkoneksi langsung dengan arus data yang mengalir di internet, yang dapat meningkatkan kecepatan download, dengan VPN kita dapat mengakses komputer atau jaringan kantor, dari mana saja selama terhubung ke internet seperti misalnya mengambil data, membuka e-mail atau database dan sebagainya.

VPN dapat digunakan juga untuk mengakses situs yang diblokir atau konten yang disensor oleh host atau ISP yang biasanya terkait dengan regulasi negara atau kantor seperti misalnya pemblokiran situs sosial media pada jam kerja pemblokiran situs FB pada beberapa negara dan sebagainya.

VPN akan memastikan jalur data yang dilewati aman dari manipulasi dan melakukan autentikasi terhadap sumber-sumber pengirim data yang akan diterimanya, VPN akan melakukan pemeriksaan terhadap semua data yang masuk dan mengambil informasi source datanya. Kemudian alamat source data ini akan disetujui jika proses autentikasinya berhasil dan VPN menjamin semua data yang dikirim dan diterima berasal dari sumber yang semestinya.

4.7.5 Pengujian Firewall

Hak akses internet yang di batasi telah di batasi pada konfigurasi firewall, Skenario yang dilakukan adalah : PC mengirimkan paket ICMP (ping) ke google.com atau ipaddress 8.8.8.8, sebelum dan sesudah di aktifkan firewall pada koneksi VPN. Apakah ada perbedaan saat diaktifkan firewall VPN dan saat tidak ada firewall



Gambar 4.18 Pengujian Firewall

Firewall mengatur dan menentukan lalu lintas data untuk mengoptimalkan keamanan di dalam jaringan dengan membatasi daerah jaringannya satu dengan yang lainnya, mengatur port atau paket yang diperbolehkan atau di tolak dan mengautentikasi terhadap akses dari dalam dan luar jaringan menjadi personal komputer. Membatasi tingkat akses, pembatasan login, login hanya diperbolehkan pada terminal tertentu, ada waktu dan hari tertentu dan pembatasan dengan call-back (login dapat dilakukan siapapun, bila telah sukses login, sistem segera memutuskan koneksi dan memanggil nomor telepon yang telah disepakati, penyusup tidak dapat menghubungi lewat sembarang saluran telepon, tetapi hanya pada saluran telepon tertentu). Pembatasan jumlah usaha login dibatasi sampai tiga kali dan segera dikunci dan diberitahu ke administrator, semua login direkam dan sistem operasi melaporkan informasi-informasi berupa waktu pemakaian login dan terminal yaitu terminal dimana pemakai login tingkat akses yang diizinkan.

4.7.6 Hasil Pengujian

1. IP address (alamat Internet) khusus untuk masing-masing komputer yang terhubung dalam jaringan tersebut, apa bila jaringan ini tidak terlindungi oleh tunnel atau firewall, IP address tadi akan dengan mudahnya dikenali atau dilacak oleh pihak-pihak yang tidak diinginkan, dengan adanya perlindungan seperti firewall, kita bisa menyembunyikan (hidden) address tadi sehingga tidak dapat dilacak oleh pihak-pihak yang tidak diinginkan.
2. Dengan ada enkripsi dan dekripsi maka data yang dilewati jaringan internet ini tidak dapat diakses oleh orang lain bahkan oleh client lain yang terhubung ke server VPN yang sama sekalipun. Karena kunci untuk membuka enkripsinya hanya diketahui oleh server VPN dan client yang terhubung. Enkripsi dan dekripsi menyebabkan data tidak dapat dimodifikasi dan dibaca sehingga keamanannya terjamin.
3. Routing protokol pada setiap topologi dan mengecek koneksi dari internet yang digunakan agar bisa terhubung ke server atau tidak, perangkat yang melakukan pengiriman mengenai adanya jaringan, tetapi kalau tidak menemukan alamat tujuan atau dalam waktu yang diberikan untuk melakukan ping sudah habis (time out).
4. VPN memiliki sistem kinerja mengenkripsi semua data yang lewat melalui, dengan adanya teknologi enkripsi ini, maka kerahasiaan data menjadi lebih terjaga, biarpun ada pihak yang dapat menyadap data yang lalu lalang, walaupun terlihat tetapi tidak bisa dibaca dengan mudah karena

sudah diacak, dengan menerapkan sistem enkripsi ini, tidak ada satupun orang dapat mengakses dan membaca isi jaringan data dengan mudah

5. Firewall mengatur dan menentukan lalulintas data untuk mengoptimalkan keamanan di dalam jaringan dengan membatasi daerah jaringan yang satu dengan yang lainnya, mengatur port atau paket yang diperbolehkan atau di tolak dan mengautentikasi terhadap akses dari dalam dan luar jaringan menjadi personal komputer.
6. Kelemahan dari koneksi Internet (jaringan Publik) tidak bisa diprediksi, hal ini disebabkan terkoneksi pada jaringan pihak lain sehingga otomatis tidak mempunyai kontrol terhadap jaringan tersebut.

5 PENUTUP

5.1 Kesimpulan

- a. Lebih efisien dalam hal mengkoneksikan User ke Server. Karena koneksi di dial up langsung dari router , jadi setiap client langsung dapat koneksi ke VPN Server. Client tidak harus mendial up terlebih dahulu ke VPN Server agar terbentuk jalur tunneling. Waktu yang dibutuhkan untuk membentuk jalur tunneling ke VPN server tergolong cepat, karena langsung di dial up oleh router VPN Server.
- b. Menyembunyikan alamat IP nyata, VPN menggantikan alamat IP lokal dengan IP public VPN , semua situs web dikunjungi hanya akan tahu alamat daerah bukan IP lokal asli , itu sangat aman dan aman ketika pengguna membutuhkan akses data penting online.
- c. Mengatur dan membatasi daerah jaringan yang satu dengan yang lainnya, mengatur port atau paket yang diperbolehkan atau di tolak dan mengautentikasi terhadap akses dari dalam dan luar jaringan menjadi personal komputer
- d. Dengan ada enkripsi dan deskripsi maka data yang dilewati jaringan internet ini tidak dapat diakses oleh orang lain bahkan oleh client lain yang terhubung ke server VPN yang sama sekalipun. Karena kunci untuk membuka enkripsinya hanya diketahui oleh server VPN dan client yang terhubung. Enkripsi dan deskripsi menyebabkan data tidak dapat dimodifikasi dan dibaca sehingga keamanannya terjamin.
- e. Kelemahan dari koneksi Internet (jaringan Publik) tidak bisa diprediksi, hal ini disebabkan terkoneksi pada jaringan pihak lain sehingga otomatis tidak mempunyai kontrol terhadap jaringan tersebut.

5.2 Saran

Karena Faktor penggunaan jaringan publik, maka kita perlu memberi perhatian yang lebih untuk mencegah terjadinya hal-hal yang tidak diinginkan seperti penyadapan, hacking dan tindakan cyber crime pada jaringan NPN

REFERENSI

- Arifin, Zaenal. Langkah Mudah Membangun Jaringan Komputer, Yogyakarta, 2005
- Dedy Haryanto Muhammad, Riadi Imam (2014), Analisis Dan Optimalisasi Jaringan Menggunakan Teknik Load Balancing (Studi Kasus : Jaringan Uad Kampus 3), Jurnal Sarjana Teknik Informatika, Volume 2 Nomor 2.
- Eko Purwanto (2015), Implementasi Jaringan Hotspot Dengan Menggunakan Router Mikrotik Sebagai Penunjang Pembelajaran (Studi Kasus : Smk Sultan Agung Tirtomoyo Wonogiri), Jurnal INFORMA Politeknik Indonusa Surakarta, Vol. 1 No 2.
- Muhammad, Ibrahim Hasan (2016), Analisa Dan Pengembangan Jaringan Wireless Berbasis Mikrotik Router Os V.5.20 Di Sekolah Dasar Negeri 24 Palu, Jurnal Elektronik Sistem Informasi dan Komputer (JESIK), Sekola Tinggi Manajemen Informatika dan Komputer (STMIK) Bina Mulia, Vol.2 No. 1
- Pasaribu Parlin(2006)Evolusi Teknologi Telekomunikasi Bergerak: 1G to 4G, Komunitas eLearning IlmuKomputer.Com

Purbo, Onno W.Virtual Private Network (VPN) sebagai alternatif Komunikasi Data Pada Jaringan Skala Luas (WAN) . Dipetik Juni 2016 darihttp://kambing.ui.ac.id/onnopurbo/library/library-ref-ind/VPN_jurnal.pdf

Ratnasari Dwi Santi, Utsalina Safiroh Dwi (2017), Implementasi Penanganan Serangan Mac-Clone Pada Hotspot Mikrotik Di Stmik Pradnya Paramita Malang (Studi Kasus: Stmik Pradnya Paramitamalang), Jurnal Teknologi Informasi, Vol. 8 No. 1.