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

<sup>1</sup>Rozali Toyib, <sup>2</sup>Muntahanah

<sup>123</sup>Prodi Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Bengkulu Jl. Bali Kota Bengkulu, telp (0736) 22765/fax (0736) 26161 Email: *rozalitoyib@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 efesiensi 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 tuneling, enskripsi dan deskripsi vang 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 enskripsi 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 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 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 efesiensi 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 ditutupdengan mekanisme keamanan secara fisik.Ini sesuai dengan pendapat bahwakemudahan mengakses informasi berbanding terbalik dengan tingkat keamanansystem informasi itu sendiri.Semakin tinggi tingkat keamanan, semakin sulit untuk mengakses informasi. Keamanan informasi adalah bagaimana cara kita dapatmencegah penipuan (cheating) atau mendekati adanya penipuan di sebuah sistemberbasis 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 sajamenjadi isu menarik dalam perkembangan komunikasi, interaksi, dan sosialisasimanusia. Perkembangan jaringan wireless yang begitu pesat dan popular menjadikan pihak-pihak lain yang kurang bertanggungjawab 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 semakinterjangkau. 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 yangterhubung melalui jaringan publik (Internet).Di dalam VPN terdapat metode tuneling dan enkripsi yang menjamin keamanan data walaupun data melewati jaringan publik.Hal iniyang membuat VPN handal dalam mengatasi permasalahan ini. Untuk dapat mengimplementasikan VPN perusahaan wajib memiliki IP Publik yang Static ,namun kenyataan nya untuk mendapatkan IP Public yang Static kadang menjadi kendala bagi perusahaan sekala kecil yang baru mengembangkan cabang nya karena mahal nya paket yang di tawarkan provider yang meyediaakan 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:

Del 1 Jems J	ai ingan D	ci uasai kali Jai
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

### Tabel 1 Jenis Jaringan Berdasarkan Jarak

#### 2.2 Pengertian Mikrotik

Mikrotik Router, merupakan sistem operasi linux base yang diperuntukkan sebagai network router. Didesain untuk memberikan kemudahan bagi penggunanya. 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 (Sofware) 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 publikseperti internet untuk menghubungkan remote access dan user secarabersama-sama dengan memberikan tingkat

level privasi, *security*, *Qualityof Service* (QoS), dan pengelolaan dimana jaringan tersebutdibangun 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 GRPS dan EDGE. Kecepatan akese data yang bisa didapat dari UMTS adalah sebesar 384 kbps pada frekuensi 5KHz sedangkan kecepatan akses yang didapat dengan CDMA1x 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 (Higth 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

- a) Observasi, yaitu memperoleh data dengan melakukan pengamatan langsung teknologi jaringan yang digunakan di PT. BPRS Muamalat Harkat Bengkulu
- b) Wawancara, yaitu pengumpulan data dengan melakukan wawancara secara langsung kepada Pimpinan dan Staf karyawan
- c) 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 :

- a. Client adalah User yang menggunakan layanan jaringan VPN yang terhubung ke router di setiap cabang di PT. BPRS Muamalat Harkat
- b. 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

- a) Pengaturan IP perangkat / Interfaces di Mikrotik.
- b) Mengkonfigurasi Point to Point Protocol over Ethernet (PPP) dengan Modem USB
- c) Mengkonfigurasi Point to Point Tunneling Protocol Server (PPTP)
- d) Membuat Authenticated User / VPN User.
- e) 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

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 membukan aplikasi Winbox.

S MikroTik WinBox Loader v2.2.16	
<u>C</u> onnect To: 4C:5E:0C:5C:58:27	Connect
Login: admin	
Password: Keep Password Secure Mode Load Previous Session	Save Remove Lools
<u>N</u> ote: MikroTik	
Address 🛆 User Note	

Gambar 4 Tampilan pertama saat membuka winbox

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

dm	in@4C:5E:0C:	C:58:27 (MikroTik) - WinBox v6.27 on RB951Ui-2HnD (mipsbe)	
0	Safe Mode	▼ H	ide Pas
20	Quick Set		
()enn	Interfaces		
Î	Wireless		
38	Bridge		
	PPP		
00000	Switch		
°78	Mesh		
255	IP		
-	MPLS	1 · · · · · · · · · · · · · · · · · · ·	
	Routing		
(8)	System		
-	Queues		
$\times$	Files		
8	Log		
<u> </u>	Radius		
$\geq$ $\times$	Tools		
0	New Terminal		
e 🖻	MetaROUTER		
3 🕗	Partition		
2	Make Supout.n		

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.

C* Safe Mo	ode									~	Hide Pag	aswords 🛛 📕 🧯
Quick Set												
Num Interfaces												
T Wireless		Interface I										
Bridge		Interface	Ethemet	EoIP Tunnel	IP Tunnel	GRE Tunnel	VLAN	VRRP	Bonding	LTE		
PPP				2 m 7	-							Find
Switch		- Nor			Trees		1.2 MTU	Ter			Pu	
°T <sup>2</sup> Mesh		R 11	oridae-local		Bridge		1598	1.8	78.	6 kbpa	ruk -	3.2 kbr
100	D.	41+	ether1-gates	way	Ethemet		1598			0 bps		0 br
1 IP		RS 41+	ether2-mast	er-local	Ethemet		1598		80.	8 kbps		3.2 kb
MPLS		S 41+	ether3-slave	local	Ethemet		1598			0 bps		0 br
and Routing	1	S 41+	ether4-slave	local	Ethemet		1598			0 bps		0 br
(0) <b>O</b>	D.	5 41+4	ether5-slave	Hocal	Ethemet		1598			0 bps		0 bp
488 System	12	5 9921	Man 1		Wireless (A	theros AR9	2290			0 bps		0 bp
Queues												
Files												
<b>I</b> 100												
Log												
🥵 Radius												
💥 Tools	1											
IIIII New Termina	1											
		+										
control and a second second		100 at 1										
	in i	/ items										

Gambar 6 Jendela interfaces yang perangkat Ethernet yang tersedia

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

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

Safe Mode	
	🖌 Hide Passwords 🛛 🔳 🛅
Courte Set     Interface     Viveless     Viveles     Viveles	<ul> <li>✓ Hide Passwords</li> <li>■ ■</li> <li>■ ■</li></ul>

Gambar 7 Jendela Address List

Ganti Address yang secara default terisi dengan "192.168.88.1/0" menjadi IP untuk interface "bridge locall", 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".

	Uptime:	00:27:	10		ОК	
	Free Memory:	17.8 M	iВ		PCI	
	Total Memory:	29.0 M	iB		USB	
USB	CDU	THRE S		115		
				1		
7					Find	
<b>T</b>	Vendor		Name	Serial Nu	Find Speed	
D /	Vendor		Name RB400	Serial Nu rb400_usb	Find Speed • 480 Mb.	

**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.

iterface <pp< th=""><th>o-out1&gt;</th><th></th></pp<>	o-out1>						
General PF	P Status Traffic	ок					
Nam	e: ppp-out1	Cancel					
Тур	e: PPP Client	Apply					
Po	Port: usb1						
API	l: 3data	Comment					
PI	4:	Сору					
nterface <pp< td=""><td>o-out1&gt;</td><td></td></pp<>	o-out1>						
General PF	P Status Traffic	ок					
	User: 3data	Cancel					
Pas	sword: 3data	Apply					
Remote Ad	idress:	- Enable					
	Dial On Demand	Comment					
	Add Default Route	Сору					
Keepalive Ti	meout:	- Remove					
		Torch					

### **Gambar 9 Jendela Interface PPP Out1**

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

New NAT Rule		
General Advanced Extra Action Statistics		ОК
Chain: Const	[¥]	Cancel
Src. Address:	•	Apply
Dst. Address:	· · ·	Disable
Protocol		Comment
Src. Pott:		Сору
Dat. Port:		Remove
Any. Pot:	· ·	Reset Counters
In. Interface:		Reset All Counter
Out Interface: ppp-out1	<b>[</b> ₹] ▲	
ew NAT Rule		
General Advanced Extra Action Statistics		OK
Action: Instructore	Ŧ	Cancel
		Apply

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.

PPP								
Interface PPPoE Server	Secreta Profiles	Active Connection						
Internet PFPAE Server How in the server of	Secrets Portles Transformer Portes PP Clear Ceneral Status Name Carton L2 MTU: User:	Active Connection overver (PPTP 5) L2 MTU Tx 1500 Traffic Server Binding	na    SSTP Server    SSTP Server    Stops	er L2	TP Server 0 by OK Cancel Apply Disable Comment Copy Remove Toroh	OVPN Server    Tx Packet (p/s)	PPPOE Scart [ <i>Lind</i> 0 Psc Packet (9/3) 0	
	(another t							

**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.

Guide Set		
in interfaces		
🔟 Wreless		
🕰 Bidge		
PPP	200	
22 Switch	Interface PPPoP Servers Publics Active Connections	
18 Mosh		
us er in		
MPLS F	Name - Local Address Bender Address Bridge Bade Dark, Orle One	
Realing F	default	
Dystem /	OK default	
Cueune .	Name: Stoffoll Cancel	
Tiles.	Local Address 102 168 10 1 * Apply	
ing pol j	Flemate Address: VPN	
Radius	Cummun	
😴 Tools 🛛 🗠	Bridge: bridge:2 F A Copy	
New Terminal	Bidge Post Priority. Period	
MetaROUTER	Bindge Path Cost	
D Purtition		
Make Supout #	Incoming Herr 🛛 👻	
Manual	Outgoing Filter.	
E Lot	Address Lut.	
	DNS Server 😂	
	WINS Server 0	
	- Charge TCP M55	
	C default C on C yes	

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 Poing Tunneling Protocol Server (PPTP Server). Klik tombol "PPTP Server", beri tanda centang pada "Enabled" untuk mengaktifkan PPTP Server, lalu pada "Default Profile" pillih "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  $\rightarrow$  Cloud, kemudian centang "*Enabled*" dan selesai.

	Enabled     Indate Time	ОК
Public Address:	202.65.113.	Cancel
DNS Name:	2f7a02 .sn.mynetname.net	Apply
		Force Update

**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 mengecheck 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.

### 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 mengantisipsi 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.

C# Safe Mode										
🔏 Quick Set										
(en interfaces										
1 Weekse										In
3 Endos	hands	-								10
RE PPP		PITCE 38	Vers Secrets	Phones Active	s Connections					
- Swtch	+-	×		PPP Scorver	PPTP Server	SSTP Server	L2TP Server	OVPN Server	PPPaE Scan	
°12 Mesh	. N	leme	/ Type	12	MTU Tx	Fix	200.011	Tx Packet (p	/s) Rx Packet	(p/e)
2월 🕑 🔍 💱	B 4		O WHITE DE			0.5 Keps	45.6 k	bps .	24	25
MPLS D		Interface kovp	mout1>							
🚜 Routing 🛛 🗅		General Da	sout Status	Traffic		OK				
💮 System 🗈		Connect To:	43/002141c2	a an mynethame r	vet	Cencel				
🐢 Queues		Port:	1194			Apply				
🚞 Hes		Note	n							
E Log						Disable				
A Raku		User:	muomolat hark	at-cab1		Comment				
🔆 Tools 🛛 🗠		Password:			-	Сору				
III New Territol		Profile	defack		¥	Remove				
25 MetaROUTER										
😃 Fattion	2 items	Cettficate:	none		•	Terch				
All Make Supert of		Auh:	sha1		(W)					
😧 Marsal		Calver	blowfals 128							
📕 Est										
			and Defau	E PIOLEC						

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"

0	Safe Mode		
10	uick Set		
	tedaces		
-			
T	revess		
B	ridge	Taminal	
C P	PP	0 102 160 4 1 56 64 107mm	17
	witch	1 192,160,4.1 56 64 103mg	1
	WECH	2 192,168,4,1 56 64 187mg	
2 M	eeh	3 192.160.4.1 56 64 109ms	
(i) 15	E 15	4 192.168.4.1 56 64 138mm	
	a. e. b.	5 192.168.4.1 56 64 55ms	
1	PLS I	6 192.160.4.1 56 64 135ms	
\$ R	outing 1	7 192.168.4.1 56 64 133ms	
1.0	intern 1	8 192.168.4.1 56 64 99ns	
		9 192.168.4.1 56 64 201mm	
<b>e</b> o	URU68	10 192.160.4.1 56 64 242ma	
10	ins.	11 192.168.4.1 56 64 56ms	
1.1		12 192.165.4.1 56 64 162ms	
1.0	99	13 192.165.4.1 56 64 57mm	
8. R	adius	14 192.105.4.1 50 64 250ms	
S- 1	anda P	10 192.100.4.1 56 64 165ms	- 11
		10 122.100.4.1 36 64 3683	
E N	ew Terminal	17 172.100.111 No 64 134E3	
S M	HAROUTER	10 192.100.4.1 50 64 1/283	
		epite20 received=20 packet_loge=0% min_rtt=55me war_rtt=134me may_rtt=250me	
- P	antion	SEO HOST SIZE TTL THE STATUS	
1 M	lake Supout rf	20 192,165,4.1 56 64 57mm	
	tion of the second s		- 15

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 firewal, IP address tadi akan dengan mudahnya dikenali atau dilacak oleh pihak-pihak yang tidak diinginkan, dengan adanya perlindungan seperti firewall, kita bisa menyembunyikan (hiden) address tadi sehingga tidak dapat dilcak 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 = 4, Lost = 0 (0% 1 Approximate round trip times in milli-seconds: Minimum = Oms, Maximum = Oms, Average = Oms	oss),
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 misalnyamelakukan tranfer data, ngeprint dokument,browsing dengan gateway yang diberikan dari VPN server, melakukan remote destop dan lain sebagainya. Dengan ada enskripsi dan deskripsi maka data yang dilewati jaringan internet initidak dapat diakses oleh orang lain bahkan oleh client lain yang terhubung ke server VPN yang sama sekalipun. Karena kunci untuk membuka enskripsinya hanya diketahui oleh server VPN dan client yang terhubung. Enskripsi 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

es C:\WIN	DOWS\s	- 🗆 ×			
Microsoft (C) Copyr	•				
C:\Docume	ents an	nd Setting	ys∖Hesti	i)tracert 172.16.2.2	
Tracing 1	route t	o 172.16	.2.2 ove	er a maximum of 30 hops	
1 2 2					
Trace cor	nplete.				
C:\Docume	ents an	nd Setting	ys∖Hesti	i>	

### **Gambar 19 Pengujian Routing**

Tracer (jejak Rute) utilitas baris perintah yang dapat digunakan untuk melacak lintasan yang diambil paketprotokol internet (IP) ke tujuannya,sehigga tracer melaporkan alamat IP antarmuka di samping router, terlihat perintah tracer dan output, paket perjalan 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:

0.	23 I	0. I	072	040		••••••		• ~ • •	0			2 · 1	50		23		T C P		cp ~	07000	- L-
69	94 1	8.1	706	930	197	2.10	58.1	78.2			12	5.1	60.:	16.:	122		TLSV1	L En	crypt	ed Al	er
69	95 1	8.1	707	680	192	2.10	58.1	78.2	3		12	5.1	60.:	16.1	122		TCP	61	057 >	- http	s
69	96-1	8.1	938	970	1.92	2.16	58.0	2.10	4		19	2.1	68.3	2.2	55		LIDP	50	unce	port:	8
	77.1	<u> </u>	262	350	10	2.24		1.1.0	-	_	10						110.0				
4										_		_	_								
TEL TOT	ern	et	Pro	toc	01.	Sr	<u>c:</u>	192.	168		103	- (1	92.1	168		1031.	DST	192	168.	2.255	-0
	ans	ion	· 4		- · ,				200			~~				,					~
1 .	e i s	2011	. 4 	at b		0 h		~													
1 _ 7	ieau.	er	ren	gun		0 0	yte	>				<i>c</i> -		~			7.			~	
1 ± 0	TTP	ere	ntı	ate	a s	erv	псе	S F1	iela	: 0	xoo	ζD	SCP	υ×	00:	рета	uιτ;	ECN:	0X00	1 <u>)</u>	
Т	ota	1 с	eng	th:	14	48															
0000	FF	FF	<del>ff</del>	FF	FF	FF	bc	SE	E4	1 2	<u></u>	75	08	00	45	00			7	E	_
0010	65	- a 8	22	fa	ά'n	hh	01	11	25	96	20	- A 8	ñ2	ĕž.	20	aB		a		<u>.</u> .	
0020	ŏž	ŤŤ.	δŚ	79	03	žğ	05	94	à7	бď	2ğ	73	59	8í	ãč.	05		. v		Y	
0030	04	òò	af	77	ã6	79	ăĥ	1e	бБ	70	Ťŝ	3ē	őő	õõ	78	až			11.5	× .	
0040	fó	ō3	ce	14	⊂4	46	42	56	84	39	<u>_0</u>	a8	ōž	õī	06	ōō		FBV	9		
0050	òō	ōō	50	01	ōó	ÓÖ	50	01	ōó	ōō	5Ö	Ōī	ōō	ōō	7ō	ōž	P.	P.	P.	p.	
0060	00	00	50	01	00	00	50	01	00	00	30	03	00	00	30	03	P .	P.	0.	ò.	
0070	00	00	26	01	00	00	ce	01	00	00	⊂0	00	00	00	⊂0	00	&.				
0080	00	00	C0	00	00	00	аO	02	00	00	C0	00	00	00	C0	00					
0090	00	00	00	03	00	00	00	03	00	00	34	01	00	00	fe	01			4.		
00a0	00	00	C0	00	00	00	C0	00	00	00	⊂0	00	00	00	40	02				@.	
0060	00	00	<u>_0</u>	00	00	00	<u>_0</u>	00	00	00	<u>_0</u>	03	00	00	<0	03					
0000	00	00	QC.	01	00	00	od	02	00	00	20	01	00	00	<0	00			· · ·		
0000	00	00	20	01	00	00	au	02	00	00	20	01	00	00	20	01			· · _ ·		
ooeo	00	00	00	03	00	00	00	03	00	00	42	01	00	00	C6	01			в.		
00000	00	00	CO.	00	00	00	CU.	00	00	00	CU.	00	00	00	40	02				œ.	
0100	00	00	<u>co</u>	00	00	00	C0	00	00	00	CO.	03	00	00	C0	03			· · <u>·</u> ·		
0120	80	88	50	01	80	80	do	85	80	80	50	01	80	80	50	01			· · · · ·	· ·	
	"CA	leorel	Unio!	Dee	100	telen	nture	UDA N		Dev	skoter	497	0.Dier	davia	4,49	70 Mark		and time			_
		sers	(valo	(DOCI	лпеп	usica	pedre	: VPINU	V 🗠	- Pac	-Nets:	. 4071	J DISD	лауе	u: 40	vo Mark	veu, U LC	au cime	: 0:00.4	100	

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.

14	451	.70.	474	118	19,	2.10	oð.,	78.9	4		20	2.7	8.1	99.	150		HTTP	GE,	r ∕jawa-ti	1 mu
14	461	70.	474	161	192	2.10	58.3	78.9	4		20	2.7	8.1	99.	150		TCP	52.	218 > http	) C
, 14	171	70	470	רמסי	201	79	2 1 (	1 00	50		10	ר ר	60	70	04		TCD	htt	to 5 50010	2
	sour	ce	por	t:	520	88	toz	088,	,	_	_	_	_	_		_		_		_
	Dest	ina	tio	n p	ort	: h	ttp	(80	20											
	Estr	eam	in	dev	• 1	٦			-											
	EDCI	2000	- 'n	umb		1		(no	1 - + +	~	e 0 9	uon	~~	io Linn	hor	<u>`</u>				
1	sequ	enc	e 11	umo	er .	-		0 e	aci	ve	sey	uen	ce	riam	Der	, ,				
<u> </u>																		_		
0020	f6	10	ch	78	00	50	h1	75	1c	a3	85	de	89	9d	50	18		. 11	P.	
0030	3Ē	6f	4f	b8	ōō	ōō.	47	45	54	20	2f	70	75	6c	6c	3f	?00(	GE .	T /pull?	
0040	63	68	61	6e	6e	65	6c	3d	70	5Ē	31	35	34	30	36	33	channe	1=	p_154063	
0050	38	30	34	30	26	73	65	71	3d	31	26	70	61	72	74	69	8040&s	eq	=1&parti	
0060	74	69	6f	6e	Зd	37	32	26	63	6c	69	65	6e	74	69	64	tion=7	28	clientid	
0070	3d	32	35	32	65	39	61	66	39	26	63	62	3d	6d	67	75	=252e9	af	9&cb=mgu	
0080	71	26	69	64	6C	65	3d	37	26	73	74	61	74	65	3d	61	q&idle	=7	&state=a	
0090	63	74	69	76	65	20	48	54	54	50	2f	31	2e	31	0d	0a	ctive	ΗT	TP/1.1.	
OOaO	41	63	63	65	70	74	Зa	20	Za	21	Za	0d	0a	52	65	66	Accept		*/*Ret	
0000	65	12	65	72	3a	20	68	74	74	20	3a	21	21	30	2d	61	erer:	nt	tp://0-a	
UUCU	63	/4	2e	53	68	61	be	be Se	65	60	2e	66	61	63	55	62	ct.cna	nŋ,	el.Taceb	
0000	57	DT Od	00	2e	63	67	60	27	59	50	12	61	60	60	27	51 61	00K.CO	n/	itrame/i	
00e0	22	ou c c	24	4 <u>+</u>	65	60	20	20	- 4-	24	40	01 41	62	62	65	20	2ACC	≤p	c-Langua	
0100	74	24	45	60	62	6f	2U 64	60	60	67	25	30	67	75	60	20	t_Enco	-u di	sactep	
0110	24	2u	64	65	66	60	61	74	65	04	0.5	20	72	65	72	54	def1	41 51	a User-	
0120	71	67	65	60	74	25	20	Áđ.	6f	75	60	66	60	61	5Ê	25	Adent ·	- C	071112/5	
0130	20	30	20	28	63	6f	ъй	70	61	74	69	62	60	65	ξ'n	20		nn	atible:	
0140	4d	53	4ŏ	45	žõ	39	Ze	зŏ	зb	źō	57	69	6e	64	őf	77	MSIE 9	.б	window	
- File	:: "C:\L	Jsers	\Vaio	Doci	Jmen	ts\ca	pture	VPN\	tan	Pad	kets	: 297	4 Dis	playe	d: 29	74 M	arked: 0 Load	ime	: 0:00.319	

Gambar 4.17 Koneksi tanpa menggunakan VPN

VPN memilki sistem kinerja mengekripsi semua data yang lewat melalui, dengan adanya teknologi enskripsi ini, maka kerahasiaan data menjadi lebih terjaga, biarpun ada pihak yang dapat menyadap data yang lalu lalang, waalaupun terlihat tetapi tidak bisa dibaca dengan mudah karena sudah diacak, dengan menerapkan sistem enskripsi 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 jaringanpribadi, yang mana sedikit digunakan oleh orang lain dan juga bisa terkoneksi langsung dengan arus datayang mengalir di internet, yang dapat meningkatkan kecepatan download, dengan VPN kita dapat mengakses komputer ataujaringan kantor, dari mana saja selama terhbung ke internet seperti misalnya mengambil data,membuka e-mail atau databasedan sebagainya.

VPN dapat digunakan juga untuk mengakses situs yang dibelokir 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 utenentikasi terhadap sumber-sumber pengirim data yang akan diterimanya, VPN akan melakukan pemeriksaan terhadap semua data yang masuk dan mengambil informasi source datanya. Kemudin 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 firewal

Command Prompt	
Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation. All rights reserved.	Â
C:\Users\Tibor>ping 8.8.8.8	=
Pinging 8.8.8.8 with 32 bytes of data: General failure. General failure. General failure. General failure.	
Ping statistics for 8.8.8.8: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),	
C:\Users\Tibor>ping 8.8.4.4	
Pinging 8.8.4.4 with 32 bytes of data: Reply from 8.8.4.4: bytes 32 time=19ms TTL=47 Reply from 8.8.4.4: bytes 32 time=19ms TTL=47 Reply from 8.8.4.4: bytes 32 time=19ms TTL=47 Reply from 8.8.4.4: bytes=32 time=19ms TTL=47	
Ping statistics for 8.8.4.4: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 19ms, Maximum = 19ms, Average = 19ms	
C:\Users\Tibor>	
	-

### Gambar 4.18 Pengujian Firewall

Firewall mengatur dan menentukan lalulintas data untuk mengoptimalkan keamanan di dalam jaringan dengan membatasi daerah jaringanyang 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 pembatsan dengan call-back (login dapat dilakukan siapapun, bila telah sukses login, sistem segera memutuskan koneksi dan memanggil nomor telepon yang telah disepakati, penyusup tdak dapat menghubungi lewat semabanrangn saluran telepon, tetpi hanya pada saluran telepon tertentu). Pembatasan jumlah usaha login dibatasi sampai tiga kali dansegera dikunci dan diberitahu ke administrator, semua login direkam dan sistem operasimelaporkaninformasi-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 firewal, IP address tadi akan dengan mudahnya dikenali atau dilacak oleh pihak-pihak yang tidak diinginkan, dengan adanya perlindungan seperti firewall, kita bisa menyembunyikan (hiden) address tadi sehingga tidak dapat dilcak oleh pihak-pihak yang tidak diinginkan.
- 2. Dengan ada enskripsi 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 enskripsinya hanya diketahui oleh server VPN dan client yang terhubung. Enskripsi dan deskripsi 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 mengekripsi semua data yang lewat melalui, dengan adanya teknologi enskripsi 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 enskripsi 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 mempunyaikontrol 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 enskripsi 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 enskripsinya hanya diketahui oleh server VPN dan client yang terhubung. Enskripsi 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 mencega terjadinya hal-hal yang tidak diinginkan sperti 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

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

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.