### **BAB IV**

### **RANCANGAN SISTEM JARINGAN USULAN**

#### 4.1. Manajemen Jaringan Usulan

Setelah penulis menganalisa sistem jaringan berjalan pada PT. Trixten Global internasional, maka penulis mengusulkan sebuah jaringan menggunakan VPN (*Virtual Private Network*) dengan metode L2TP dan IPSec untuk menghubungkan kantor pusat dengan cabang. Dan di fungsikan untuk menjembatani antara kantor dan karyawan-karyawan yang sering bepergian (*mobile workers*) dengan memanfaatkan koneksi *internet* yang dimiliki tersebut.

Dengan menggunakan *router* Mikrotik yang sudah ada, kemudian dikonfigurasi untuk menerapkan sistem jaringan VPN. Untuk kantor pusat dikonfigurasi VPN *server* dengan metode L2TP/IPSec, sedangkan kantor cabang L2TP/IPSec *Client*. Dengan ini antara kantor pusat, kantor cabang dan *remote client* akan lebih mudah untuk melakukan komunikasi, pengiriman data perusahaan serta memonitoring jaringan akan lebih aman.

#### 4.1.1. Topologi Jaringan

Dalam mengusulkan topologi jaringan yang akan diimplementasikan pada perusahaan, penulis tidak akan merubah bentuk topologi yang sudah ada pada PT. Trixten Global Internasional, hal ini karena bentuk topologi yang ada sekarang sudah sangat baik. Topologi jaringan kantor pusat dan cabang menggunakan topologi *star*. Penulis mengusulkan untuk menggunakan VPN (*Virtual Private Network*) untuk berkomunikasi atau pertukaran data antar kantor menjadi lebih aman.



#### **Topologi Jaringan Usulan**

#### 4.1.2. Skema Jaringan

Pada skema jaringan usulan ini penulis menggambarkan secara detail dalam *IP Address* hanya tidak meletakkan seluruh perangkat komputer. Untuk simulasi implementasi jaringan penulis menggunakan *software Graphical Network Simulator* dan *VirtualBox*. Karena jaringan pada PT. Trixten Global Internasional menggunakan jenis *router Mikrotik router OS* dan pada kantor cabang *Mikrotik Router Board*. Dalam implementasi ini dibutuhkan sebuah *router* untuk dapat menghubungkan antara kantor pusat, kantor cabang dan akses *remote client* untuk membuat jaringan *virtual private network* (VPN), dimana kantor pusat sebagai *server* dan kantor cabang sebagai *client*. Sedangkan untuk *remote access* atau untuk *client* yang berada di luar kantor dapat melakukan koneksi VPN dengan setingan yang terdapat pada perangkat yang digunakan.



#### Skema Jaringan Usulan

#### 4.1.3. Keamanan Jaringan

Untuk keamanan jaringan yang diterapkan pada PT. Trixten Global Internasional menurut penulis sudah cukup bagus. Dengan memanfaatkan *software* anti virus dan membangun *firewall* pada konfigurasi *router*.

Sedangkan 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 (*Internet Protocol Security*) 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:

- 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*.

#### 4.1.4. Rancangan Aplikasi

Dalam rancangan aplikasi penulis merancang dan mengimplementasikan suatu jaringan VPN dengan metode L2TP/IPSec untuk menghubungkan antara kantor pusat dan kantor cabang, sehingga dalam pertukaran data akan lebih cepat dan aman.

Tahapan konfigurasi yang harus dilakukan sebagai berikut:

1. Instalasi Mikrotik Router OS

Setting BIOS komputer server dan atur booting agar CD/DVD bisa terdeteksi sistem komputer. Kemudian siapkan file instalasi Mikrotik, dan tunggu sampai muncul tampilan seperti dibawah.

X] system	[X] ipv6	[X] routerboard
X1 dhen		
1 aduanced_tools		[Y] ups
Yl caloa		[Y] upor-Managor
x1 ans	[Y] multicast	[Y] wireless
X] hotspot	[X] ntp	tal Mileless

### Gambar IV.3

#### Tampilan Instalasi Mikrotik

Lakukan proses instalasi Mikrotik dengan memilih (*check*) semua pilihan yang ada dengan tombol **'a'**. Kemudian tekan tombol **'i'** untuk memulai proses instalasi, setelah itu ikuti langkah selanjutnya sampai instalasi selesai dan tekan **'Enter'** untuk *Restart*.

ммм	ммм		ккк					TTTTTTTTTTT	r.	ккк	
MMMM	MMMM		ККК					TTTTTTTTTTT	r	KKK	
MMM MMMM	MMM	III	KKK KKK	RRRR	RR	000	1000	TTT	III	KKK	KKK
MMM MM	MMM	III	KKKKK	RRR	RRR	000	000	ТТТ	III	KKK	KK
MMM	MMM	III	KKK KKK	RRRR	RR	000	000	TTT	III	KKK	KKK
MMM	MMM	III	KKK KKK	RRR	RRR	000	1000	TTT	III	KKK	KKK
)UTER HAS	NO S	OFTWA	RE KEY								
bu have 1 nd to ent urn off t ee www.mi	.1h56m .er th .he de .kroti	to c e key vice k.com	onfigure by pasti to stop ti vkey for i	the ro ng it he tim more d	uter in a er. etail	to be Telne s.	remo twi	otely access ndow or in k	sible, Jinbox		
irrent in	stall	ation	softwar	e ID":	ØASI	-7006					

#### Gambar IV.4

Tampilan Mikrotik

#### 2. Instalasi Winbox dan Login

Untuk konfigurasi Mikrotik, penulis menggunakan software Winbox. Setelah Winbox.exe tersimpan di komputer, dapat langsung dijalankan dengan memasukkan *MAC Address* mikrotik, misal 08:00:27:DA:2C:F8, isi juga *Login* dengan *admin* sedangkan *password* kosong saja.

Connect To:	08:00:27:DA:2C:	:F8	Connect
Login:	admin		
Password:	1		]
	🔲 Keep Passwo	ord	Save
	E Secure Mode	9	Remove
	🔽 Load Previou	is Session	Tools
Note:	Pusat		
Address /	User	Note	

Gambar IV.5

### Tampilan Winbox dan Login Mikrotik

### 3. Pengaturan IP Address

Pada *router* ini penulis menggunakan 2 *ether*, *ether* 1 untuk IP *Public* dan *ether* 2 untuk IP *Local*. Langkah memberikan IP *Address* pada masing-masing *interface* dengan klik Menul IP Address pada tampilan Address List klik tombol + warna biru.



### **Pengaturan IP Address**

#### 4. Pengaturan Route Table

*Set Route* pada Mikrotik Router bertujuan untuk menentukan jalur *gateway* dari jaringan lokal ke jaringan yang terkoneksi *internet*. Dengan cara klik Menu IP| Routes| pada tampilan *Route List* klik tombol + warna biru untuk menambahkan *gateway* seperti gambar:

Routes Nexthor	os Rules VRF					
+ - /	× 🗆 🍸			Find	al 🔻	
Dst. Addr	ess 🧭 Gateway			Distance	Routing Mark 💌	
AS ▶ 0.0.0.	0/0 192.168.1.1	reachable Public		1	4	
DAC 192.1	68.1.0/24 LAN reacha	able		0	1	
Route <0.0.0.0/0>	;					
General Attribut	es					ОК
Dst. Address:	0.0.0.0/0					Cancel
Gateway:	192.168.1.1	🔻 reacha	able Public		\$	Apply
Check Gateway:					•	Disable
Type:	unicast					Comment
Distance:	1					Сору
C	20					Remove
Scope:	30					
Target Scope:	10					÷
Routing Mark:					•	
Pref. Source:					•	
nabled			active		static	

### Pengaturan Route Table

5. Pengaturan DNS

Pengaturan DNS bertujuan untuk menentukan *network server* dari Mikrotik, dengan cara klik menu IP|DNS.

DNS Settings			
Servers:	8.8.8.8	\$	ОК
	8.8.4.4	\$	Cancel
Dynamic Servers:			Apply
	Allow Remote Requ	Jests	Static
Max UDP Packet Size:	4096		Cache
Cache Size:	2048	KiB	
Cache Used:	9		

### Gambar IV.8

## **Pengaturan DNS**

Isikan *IP address* google apabila settingan DNS nya diarahkan ke google, atau bisa juga ke *IP address speedy* maupun Nawala.

### 6. Pengaturan Firewall NAT

NAT atau disebut juga dengan *Network Address Translation* adalah suatu metode menghubungkan lebih dari satu komputer ke jaringan *internet* dengan menggunakan satu alamat IP. Klik Menu IP| Firewall| NAT. Setting seperti gambar:

eneral Advanced Extra Action Statistics	ОК
Chain: pronat	
Srn Address:	
Det Address	
Dst. Address.	Disable
Protocol:	✓ Comment
Src. Port:	- Сору
Dst. Port:	Remove
Any. Port:	Reset Count
In. Interface:	Reset All Cour
Out. Interface: 🗌 Public	<b>₹</b> ▲
Packet Mark:	· · · · · · · · · · · · · · · · · · ·
onnection Mark:	<b>▼</b>
Routing Mark:	
Routing Table:	
onnection Type:	
T Rule ⇔	
T Rule 🗢 eneral Advanced Extra Action Statistics	ОК
T Rule <> eneral Advanced Extra Action Statistics Action: masquerade	OK Cancel
T Rule <> eneral Advanced Extra Action Statistics Action: masquerade	OK Cancel Apply
T Rule <> eneral Advanced Extra Action Statistics Action: masquerade	OK Cancel Apply Disable
T Rule <> eneral Advanced Extra Action Statistics Action: masquerade	Cancel Cancel Disable Comment
T Rule <> eneral Advanced Extra Action Statistics Action: masquerade	OK Cancel Apply Disable Comment Copy
T Rule <> eneral Advanced Extra Action Statistics Action: masquerade	OK Cancel Apply Disable Comment Copy Remove
T Rule <> eneral Advanced Extra Action Statistics Action: masquerade	OK Cancel Apply Disable Comment Copy Remove Reset Court

#### **Gambar IV.9**

### **Pengaturan NAT**

#### 7. Konfigurasi VPN L2TP Server

Untuk mengaktifkan *router* sebagai *L2TP server* caranya pun cukup mudah. Pada menu **PPP** | Pilih **L2TP Server.** Kemudian centang opsi '**Enabled**', secara otomatis L2TP Server telah aktif.

+ 7 1	PPP Scanner PPTP S	Server SSTP Ser	ver	L2TP Server	OVPN Server	PPPoE Scan
Name / Type	L2 MTU Tx		Rx		Tx Packet (p/s	) Rx Packet
	L2TP Server					
		Enabled		ОК		
	Max MTU:	1450		Cancel		
	Max MRU:	1450		Apply		
	MRRU:		•	7600		
	Keepalive Timeout:	30				
	Default Profile:	default-encryption	Ŧ			
	- Authentication					
	🗹 pap	🗹 chap				
	mschap1	🗹 mschap2				

#### Gambar IV.10

#### Mengaktifkan L2TP

Selanjutnya melakukan setting pada Tab Secrets. Pilih Tab Secrets | klik Add [+]. Disini akan mengisi beberapa parameter standar yang utama untuk melakukan koneksi. Seperti '*Name & Password*' diisikan untuk dial koneksi L2TP dari *Client*. Kemudian Service bisa diisikan dengan 'L2TP' dan bisa juga dengan 'any' untuk semua jenis *service* PPP. Dan parameter selanjutnya yang juga penting adalah *setting IP Address* pada *Local Address* dan *Remote Address*. *IP Address* inilah yang nantinya akan ditambahkan secara otomatis ketika koneksi L2TP terbentuk dan sebagai *gateway* komunikasi data. Untuk parameter *Route* bisa juga ditambahkan dengan mengisikan *network* dari kantor cabang, sehingga akan ditambahkan *rule routing* baru secara otomatis.

Name:	Pusat		OK
Password:		<b>▲</b>	Cancel
Service:	l2tp	₹	Apply
Caller ID:		<b></b>	Disable
Profile:	default	Ŧ	Comment
Local Address:	172.16.10.1	-	Сору
Remote Address:	172.16.10.2	<b></b>	Remove
emote IPv6 Prefix:		<b></b>	
Routes:	192.168.10.0/24		
Limit Bytes In:		•	
Limit Bytes Out:		•	
Last Logged Out:	Jul/20/2016 06:43:09		

#### Menambahkan PPP Secret

8. Konfigurasi IPSec untuk L2TP Server

Untuk meningkatkan keamanan akan memadukan L2TP dengan IPSec. Pilih pada menu IP | IPSec. Kemudian penulis akan melakukan setting terlebih dahulu pada Tab **IPsec Proposal**, pada parameter yang tersedia isikan seperti gambar berikut.

Name:	defaul				OK
- Auth. Algo	ithms -				Cancel
md5		✓ sl	ha1		Apply
Encr. Algo	ithms -				Disable
I null			es es-128 ch		Сору
aes-192	2 cbc	✓ a	es-256 cb	ic	Remove
blowfish	ı	🗌 tv	vofish		
camellia	a-128		amellia-19 es-128 ctr	12	
aes-192	2 ctr	a	es-256 ctr	t.	
aes-128	3 gcm 6 gcm	<b>a</b>	es-192 go	m	
Lifetime:	00:30	00		•	
Comuna	none				

Gambar IV.12

## **Pengaturan IPsec Proposal**

Selanjutnya melakukan setting pada Tab **IPsec Policy**, tambahkan juga parameter pada tampilan berikut.

Policies	Groups F	eers	Remote Peers	Mode Configs	Proposals	Installed SAs	Keys	Users
+ -	× ×		T Stati	stics			Fir	id
Src	c. Address 🧳	Src. I	ort Dst. Addres	s Dst. Port P	roto Action	n Level	Tunnel	
IP	sec Policy <1	92.16	8.1.2:0->192.16	8.1.20:0>			no	
G	General Acti	ion			OK			
s	Grc. Address:	192.	168.1.2		Cano	cel		
	Src. Port:			•	Арр	ly		
D	Ost. Address:	192.	168.1.20		] Disat	ble		
	Dst. Port:			•	Comm	ient		
	Protocol:	255 (	all)	₹	Cop	y I		
			emplate		Remo	ove		
	Group:	defau	ult	Ŧ	]			
item								
_						-	_	_
en	nabled		1	[emplate				



Polici	es Groups Peers	Remote Pe	ers Mod	e Configs	Proposals	Installe	d SAs	Keys	Users
+	- 🗸 🗶 (	• T •	Statistics					Fin	d
	Src. Address 🧭 Src	. Port Dst. Ad	dress I	Dst. Port Pr	oto Actio	n Lev	vel	Tunnel	•
T	IPsec Policy <192.	168.1.2:0->192	2.168.1.20	:0>			uire	yes	
	General Action				0	к			
	Action:	encrypt		Ŧ	Can	icel			
	Level:	require		₹	App	oly			
	IPsec Protocols:	esp		₹	Disz	ble			
		✓ Tunnel							
	SA Src. Address:	172.16.10.1			Comr	nent			
	SA Dst. Address:	172.16.10.2			Co	ру			
	Proposal:	default		Ŧ	Rem	ove			
	Priority:	0							
1 item									

Gambar IV.14

Pengaturan IPSec Policy pada tab Action

Setelah konfigurasi pada Tab *IPSec Proposal* dan *IPSec Policy* telah dilakukan, penulis melanjutkan konfigurasi pada Tab *IPSec Peer*. Isikan sesuai dengan parameter seperti pada tampilan gambar berikut.

Addeese	172 16 10 2		OK
Address:	172.16.10.2		OK
Port:	500		Cancel
Local Address:	l)	<b>▼</b>	Apply
Auth. Method:	pre shared key	Ŧ	Disable
Secret:			Commen
			Сору
			Remove
Policy Group:		-	
Exchange Mode:	main	₹	
	Send Initial Contact     NAT Traversal		
My ID User FQDIN:			
Proposal Check:	obey	<b>*</b>	
Proposal Check: Hash Algorithm:	obey sha 1	  ▼   ▼	
Proposal Check: Hash Algorithm: Encryption Algorithm:	obey sha1 3des		
My ID Oser Fordin: Proposal Check: Hash Algorithm: Encryption Algorithm: Mode Configuration:	obey sha1 3des		
Proposal Check: Hash Algorithm: Encryption Algorithm: Mode Configuration: DH Group:	obey sha1 3des modp1024		
Proposal Check: Hash Algorithm: Encryption Algorithm: Mode Configuration: DH Group: Generate Policy:	obey sha1 3des modp1024 port override		
My ID Oser RdDN: Proposal Check: Hash Algorithm: Encryption Algorithm: Mode Configuration: DH Group: Generate Policy: Lifetime:	obey sha1 3des modp1024 port override 1d 00:00:00		
My ID Oser FQDN: Proposal Check: Hash Algorithm: Encryption Algorithm: Mode Configuration: DH Group: Generate Policy: Lifetime: Lifetytes:	obey sha1 3des modp1024 port override 1d 00:00:00		
My ID Oser FQDN: Proposal Check: Hash Algorithm: Encryption Algorithm: Mode Configuration: DH Group: Generate Policy: Lifetime: Lifetytes: DPD Interval:	obey sha1 3des modp1024 port override 1d 00:00:00		

Gambar IV.15 Pengaturan *IPSec Peer* 

#### 9. Konfigurasi L2TP Client

Setelah melakukan setting pada sisi L2TP *Server* yang berada pada kantor pusat, kita akan membuat L2TP *Client* yang berada pada kantor cabang. Untuk L2TP Client kita tinggal *dial* ke L2TP *server*. Pilih Menu **PPP** | klik **Add** [+] | pilih **L2TP Client**. Kemudian akan muncul tampilan seperti berikut.

General Dial	Out Stat	us Traffic		OK
Co	nnect To:	192.168.1.2		Cancel
	User:	Pusat		Apply
F	<sup>p</sup> assword:	*****		Disable
	Profile:	default-encryption	Ŧ	Comment
Keepalive	e Timeout:	60	-	Сору
Default Route	Distance:	<ul> <li>Dial On Demand</li> <li>Add Default Route</li> <li>1</li> </ul>		Torch
Allow				
<ul> <li>✓ pap</li> <li>✓ mschap1</li> </ul>		<ul> <li>✓ chap</li> <li>✓ mschap2</li> </ul>		

### Gambar IV.16

### Pengaturan L2TP Client

Isikan pada parameter '**Connect to'** dengan IP public dari router di kantor pusat yang menjadi L2TP server. Kemudian parameter '**User & Password**' kita isikan seperti konfigurasi *Secret* di L2TP *server*.

#### 10. Konfigurasi IPSec untuk L2TP Client

Sebelumnya penulis sudah melakukan konfigurasi *IPSec* untuk L2TP Server. Dan sekarang penulis juga akan melakukan konfigurasi untuk sisi L2TP Client. Pada dasarnya parameter yang digunakan antara *IPSec* baik sisi L2TP Server maupun Client sama, namun akan sedikit melakukan perubahan pada parameter *IP Address*.

Pada Tab *IPSec Proposal* tidak ada perbedaan dengan konfigurasi *IPSec* untuk L2TP *Server*.

Psec Propos	al <default></default>			
Name:	default			OK
- Auth. Algo	rithms		— 1	Cancel
md5		l sha1	ļ	Apply
Encr. Algo	rithms —	M	<u> </u>	Disable
☐ null ✓ 3des		des aes-128 cb	c İ	Сору
aes-192	2 cbc 🔽	aes-256 cb	c	Remove
blowfish camellia aes-192 aes-256	n	twofish camellia-19 aes-128 ctr aes-256 ctr aes-192 gc	2 m	
Lifetime:	00:30:00			
PFS Group:	modp1024		₹	
enabled		default	455 22	

Gambar IV.17

### Pengaturan IPSec Proposal pada Client

Kemudian untuk selanjutnya pada Tab *IPSec Policy* penulis akan mengganti IP Address dan untuk parameter yang lain samakan dengan *IPSec* di sisi L2TP *server*.

÷	-		×		7	S	tatistic	s			
	Src.	Address	: / S	irc. Po	ort Dist	. Add	ress	Dst	. Por	t Prote	o Action
	IPse	ec Policy	<192	168.	1.20:0	->192	.168.1	.2:0>			
	Ge	neral 🖉	Action								OK
	Src	. Addres	ss: 1	92.16	8.1.20	)					Cancel
		Src. Po	ort:							•	Apply
	Dst	t. Addres	ss: 1	92.16	8.1.2				16		Disable
		Dst. Po	ort:							•	Commen
		Protoc	ol: 2	55 (al	Ŋ					Ŧ	Сору
				Ten	nplate						Remove
		Grou	ip: di	efault	9					Ŧ	L
iter Poli	enal cies	bled Groups	Pee	ers F	Remot	e Pee	Temp rs M	olate ode C	Config	js Pi	roposals Ir
iter Poli	enal cies	Groups	Pee	ers F	Remot	e Pee S	Temp rs M tatistic	olate ode C s	Config	js P	roposals Ir
iter Poe Poli	enal cies Src.	Groups	Pee \$ 4 S	ers F 20 irc. Po	Remot	e Pee Si t. Add	Temp rs M tatistic ress	ode C s Dst.	Config	gs Pi	roposals Ir Action
iter Poli <b>+</b>	enal cies Src. IPse	Groups Groups Address c Policy meral 4	Pee X S V S V S V S V S V S V S V S	ers F E	Remot	e Pee Si t. Add	Temp rs M tatistic ress .168.1	ode C s Dst. .2:0>	Config Por	gs P t Proto	roposals Ir p., Action
iter Poe Poli	enal c cies Src. IPse Ge	bled Groups Address c Policy meral 4	Pee X S <192 Action	ers F E irc. Pr 168.	Remot	e Pee S t. Add	Temp rs M tatistic ress 168,1	ode C s Dst .2:0>	Confi <u>c</u> Por	js Pi t Proto	roposals Ir o Action
iter Pac Poli	enal cies Src. IPse Ge	bled Groups Address ec Policy eneral A A	Pee X S <192 Action Action: Level:	ers F irc. Pr 168 enc req	Remotion Tost 1.20:0	e Pee S t. Add ⇒192	Temp rs M tatistic ress 168.1	ode C s Dst .2:0>	Config Port	js Pi Proto	roposals Ir o Action OK Cancel Apply
iter Poli	enal cies Src. IPse Ge	Groups Groups Address ec Policy eneral A A sec Prot	Pee X S V <192 Action Action: Level: cocols:	ers F C. Po irc. Po enc req esc	Remot	e Pee S t. Add	Temp rs M tatistic ress 168.1	ode C s Dst. 2:0>	Config Port	js Pi	roposals Ir Action OK Cancel Apply Disable
iter Poli	cies Cies Src. IPse Ge	bled Groups Address ec Policy meral A sec Prot	Pee X S V <192 Action Action: Level: bocols:	ers F C Pr irc. Pr req esc v	Remoti Tunne	e Pee S t. Add ⇒192	Temp rs M tatistic ress	ode C s Dst .2:0>	Config Port	js Pi t Proto ₹	roposals Ir Action OK Cancel Apply Disable
iter Poli	cies Cies Src. IPse Ge	bled Groups Address ec Policy meral A sec Prot	Pee X S 	ers F C. Pr 168 req esp V 172	Remoti Tunne 2.16.11	e Pee S t. Add > 192	Temp rs M tatistic ress 168.1	ode C s Dst .2:0>	Config Port	js Pi	roposals Ir Action OK Cancel Apply Disable Comment Conv
iter Pse Poli	enal cies Src. IPse Ge IP SA	bled Groups Address ec Policy meral A sec Prot sec Prot	Pee X S / S <192 Action Action: Level: locols: Idress:	ers F 	Remot	e Pee S t. Add >192	Temp rs M tatistic ress 168 1	ode C s Dst .2:0>	Config Port	js P t Prote ₹	roposals Ir Action OK Cancel Apply Disable Comment Copy Remove
ite Poli	enal cies Src. IPse Ge IP SA SA	bled Groups Address c Policy meral A Sec Prot Sec Prot	Pee Pee Action Action: Level: idress: posal: biol	ers F enc. Provide a second s	Remoti Tunne 2.16.11 ault	e Pee S t. Add >>192	Temp rs M tatistic ress .168.1	ode C s Dst .2:0>	Port	ps Proto	roposals Ir Action OK Cancel Apply Disable Comment Copy Remove

Gambar IV.18

Pengaturan IPSec Policy pada Client

Setelah *setting IPSec Policy* maka kita akan melakukan *setting* juga untuk *IPSec Peer*. Kita juga tinggal mengganti *IP Address* dan set parameter yang lain seperti halnya pada *IPSec* di sisi *L2TP server*.

sec Peer (172,16,10,1	>		
Address:	172.16.10.1		OK
Port:	500		Cancel
Local Address:		•	Apply
Auth. Method:	pre shared key	Ŧ	Disable
Secret	******		Comment
			Сору
			Remove
Exchange Mode:	main	Ŧ	
Exchange Mode:	main ✓ Send Initial Contact ○ NAT Traversal		
Exchange Mode: My ID User FQDN:	main ✓ Send Initial Contact NAT Traversal		
Exchange Mode: My ID User FQDN: Proposal Check:	main Send Initial Contact NAT Traversal obey		
Exchange Mode: My ID User FQDN: Proposal Check: Hash Algorithm:	main Send Initial Contact NAT Traversal obey sha1		
Exchange Mode: My ID User FQDN: Proposal Check: Hash Algorithm: Encryption Algorithm:	main  Send Initial Contact  NAT Traversal  obey sha1 3des		
Exchange Mode: My ID User FQDN: Proposal Check: Hash Algorithm: Encryption Algorithm: Mode Configuration:	main  Send Initial Contact  NAT Traversal  obey sha1 3des		

#### Gambar IV.19

### Pengaturan IPSec Peer pada Client

Terakhir kita akan memeriksa apakah interkoneksi jaringan L2TP/IPSec telah tersambung atau belum antara kantor pusat dengan kantor cabang. Apabila konfigurasi benar dan tersambung maka akan tercantum pada info Status: *Connected* serta akan muncul sebuah *interface* baru dari L2TP.

#### 4.2. Pengujian Jaringan

Dalam hal membangun jaringan komputer perlu dilakukan sebuah pengujian terhadap jaringan yang telah dibangun sebelumnya, hal ini berguna untuk memastikan bahwa semua sistem yang telah dibuat berjalan dengan baik dan sesuai dengan yang direncanakan.

#### 4.2.1 Pengujian Jaringan Awal

Pada sub bab ini akan dilakukan beberapa pengujian awal diantaranya tes koneksi dari *client* ke *gateway*, dari *client* ke *router* dengan cara *ping*.

1. Ping dari client ke gateway pada kantor pusat.

Pada pengujian ini penulis mencoba melakukan tes koneksi dari salah satu *client* ke *gateway* dengan cara ping pada kantor pusat.

C:\Windows\system32\cmd.exe	23
<pre>Microsoft Windows GyternS2(Mdexe Microsoft Windows [Uersion 6.1.7600] Copyright (c) 2009 Microsoft Corporation. All rights reserved. C:\Users\USER&gt;ping 192.168.0.1 Pinging 192.168.0.1 with 32 bytes of data: Reply from 192.168.0.1: bytes=32 time(ins TIL=64 Reply from 192.168.0.1: bytes=32 time(ins TIL=64 Ping statistics for 192.168.0.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms C:\Users\USER&gt;</pre>	* m
	-

#### Gambar IV.20



2. *Ping* dari *client* ke *router* pada kantor pusat

Pada percobaan kali ini penulis akan mencoba menghubungkan atau melakukan tes koneksi antara *client* dengan *router* yang berada pada jaringan lokal.



#### Ping dari Client ke Router Kantor Pusat

Dari hasil pengujian diatas terlihat bahwa hasil tes koneksi dapat terhubung dengan baik dan tidak ada data yang *lost*.

3. Tes Pengiriman Data

Pada pengujian ini penulis mencoba melakukan pengiriman data dalam jaringan lokal, kemudian dilakukan analisa paket data jaringan mengunakan Wireshark. Hasil dari paket data sebelum menggunakan VPN dengan aplikasi wireshark yaitu terlihat bahwa isi data yang dikirim bisa terbaca, seperti gambar dibawah:

📕 Wireshark - Follow TCP Stream (tcp.stream eq 0) - wireshark_pcapng_FF98D9E2-E542-42E7-BA0
@d.SMB
.NHjP.PHj         8
@D#VB \.n.a.m.at.x.tB 2 client pkt(s). 52 server pkt(s). 42 turns.
Entire conversation (7568 bytes)    Show data as ASCII  Find:  Find Next Hide this stream Print Save as Close Help

### Gambar IV.22

Analisa sebelum menggunakan VPN

#### 4.2.2. Pengujian Jaringan Akhir

Pada pengujian jaringan akhir penulis akan mencoba melakukan tes koneksi dengan melakukan *ping* dari *client* yang berada di kantor pusat ke *client* kantor cabang, dari *client* kantor pusat ke router kantor cabang begitu juga sebaliknya, dan melakukan tracert dari kantor pusat ke kantor cabang.

1. *Ping* dari *client* kantor pusat ke *router* kantor cabang

C:\Windows\system32\cmd.exe	
Microsoft Windows [Version 6.1.7600] Copyright (c) 2009 Microsoft Corporation. All rights reserved. C:\Vsers\VSER>ping 192.168.1.20 Pinging 192.168.1.20 with 32 bytes of data: Reply from 192.168.1.20: bytes=32 time=3ms TIL=63 Reply from 192.168.1.20: bytes=32 time=3ms TIL=63	
Reply from 192.168.1.20: bytes=32 time=1ms TTL=63 Reply from 192.168.1.20: bytes=32 time=1ms TTL=63 Ping statistics for 192.168.1.20: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 3ms, Average = 1ms	
C:\Users\USER>	

Gambar IV.23

Ping dari client kantor pusat ke router kantor cabang

2. *Ping* dari *client* kantor pusat ke *client* kantor cabang

C:\Windows\system32\cmd.exe	
icrosoft Windows [Version 6.1.7600] opyright (c) 2009 Microsoft Corporation. All rights reserved.	
::\Users\USER>ping 192.168.10.10	
inging 192.168.10.10 with 32 bytes of data: eply from 192.168.10.10: bytes=32 time=15ms TTL=126 eply from 192.168.10.10: bytes=32 time=5ms TTL=126 eply from 192.168.10.10: bytes=32 time=2ms TTL=126 eply from 192.168.10.10: bytes=32 time=2ms TTL=126	
ing statistics for 192.168.10.10: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), pproximate round trip times in milli-seconds: Minimum = 2ms, Maximum = 15ms, Average = 6ms	
::\Users\USER>	

Gambar IV.24

Ping dari client kantor pusat ke client kantor cabang

3. Tes koneksi dengan *tracert* dari kantor pusat ke kantor cabang



#### Gambar IV.25

### Tes Trecert dari Kantor Pusat ke Kantor Cabang

Pada pengujian diatas telihat bahwa koneksi berjalan dengan baik, dari client kantor pusat bisa terhubung langsung ke kantor cabang, hal ini bisa saling melakukan tukar menukar data. Pengujian dengan *traceroute* untuk melihat rute yang dilewati sebuah data ke tempat tujuan dan ini terlihat bahwa rute melewati *tunnel* yang telah dibuat dengan VPN.

1. Sebelum menggunakan VPN, komputer kantor pusat terkoneksi ke kantor cabang hanya menggunakan e-mail.

Yang dimana penerimaan dan pengiriman data tidak terlalu besar dan memerlukan waktu yang cukup lama.

 Setelah menggunakan VPN, komputer Pusat bisa terkoneksi ke knator cabang dan bisa menerima dan mengirim file dengan waktu yang lebih cepat dan dengan data yang lebih besar.

🔂 user1 [Running] - Oracle V	VM VirtualBox put Devices Help				x
					x
♥ ↓ \\192.168.0.	2\Sharing	<b>- €</b>	Search Sharing		٩
Organize 🔻 Include in	n library 🔻 New folder			:≡ - □ (	?
🔆 Favorites	Name	Date modified	Туре	Size	
Desktop	🕌 Key levelő 🍥 winbox	8/1/2017 8:18 PM 1/24/2015 12:28 PM	File folder Application	112 KB	
<ul> <li>Libraries</li> <li>Documents</li> <li>Music</li> <li>Pictures</li> <li>Videos</li> <li>Computer</li> <li>Local Disk (C:)</li> <li>Network</li> </ul>		2			
2 items ( Offlin	Offline status: Online ne availability: Not available				
👌 🙆 [		0.		8:58 PM 8/1/2017	
			) 🔮 🌽 🛄 🚍 🛅	🛄 🕖 💌 Right Ct	<b>п</b>

Gambar IV.26

Tampilan Kantor Pusat setelah terkoneksi ke Kantor Cabang

### 4. Grafik Transer Data

General Status T	raffic		OK
Tx/Rx Rate:	14.5 Mbps	/ 225.5 kbps	Copy
Tx/Rx Packet Rate:	1 268 p/s	/ 650 p/s	Remove
Tx/Rx Bytes:	25.2 MiB	/ 606.0 KiB	
Tx/Rx Packets:	19 344	/ 10 634	Iorch
Tx/Rx Drops:	0	/0	
Tx/Rx Errors:	0	/0	
Tx: 14.5 Mbps Rx: 225.5 kbps			
Tx Packet: 1 20 Rx Packet: 650	58 p/s ) p/s		





nterface <l2tp-out1></l2tp-out1>	6		
General Dial Out	Status Traffic		OK
Tx/Rx Rate	: 204.1 kbps	/ 12.3 Mbps	Cancel
Tx/Rx Packet Rate	: 564 p/s	/ 1 082 p/s	Apply
Tx/Rx Byte:	: 1119.4 KiB	/ 55.7 MiB	Disable
Tx/Rx Packets	: 22 477	/ 41 721	Comment
Tx/Rx Drops	: <b>0</b>	/0	Сору
Tx/Rx Errors	ε 0	/ 0	Remove
Tx: 204.1 kbp	\$		Torch
Tx Packet: 56	)4 p/s 082 p/s		
enabled r	unning	slave Status:	connected

Gambar IV.27

Grafik Transfer Data pada Router Cabang

### 5. Tes Pengiriman Data

Dalam pengujian ini penulis mencoba melakukan pengiriman data dari PC kantor cabang ke PC kantor Pusat dengan koneksi VPN L2TP/IPSec. Dan setelah dilakukan konfigurasi dengan benar, akhirnya pengiriman berhasil.

Dibawah ini merupakan gambar dari analisa paket data yang melewati jaringan kantor pusat menggunakan wireshark. Dari hasil analisa ini bahwa data yang dikirim telah terenkripsi.

	Virtu	alBox Ho	st-Only N	letwork [V	Vireshark .	2.0.5 (v2.0	.5-0-ga3b	e9c6 from	master-2.0)	]			-		-									
Eile	E Ed	lit <u>V</u> iew	<u>Go</u> <u>C</u>	apture	Analyze	Statistics	Telepho	ny <u>T</u> ools	Internals	Help		-												
0	۲		ø	<b>B</b>	* 2	् ५	• 🛸 📫	• 7 ₹		]  €	ର୍ ପ		¥ 1	8	*	Ħ								
Filt	er: t	cp.strean	n eq 16						- Expre	ession	Clear	Apply	Save											
No.		Time	s	ource		0	estination	1	Prot	ocol	Le	ngth	Info											
	207	5 169.1	53856 :	192.168	3.0.10		192.168	.10.10	SME	3		238		2 Res	sponse	, FIN	D_FIRS	5T2, F	iles:	Ipse	ec.txt			
	2076	5 169.2	624761	192.168	8.10.10	) 1	L92.168	.0.10	TCF	•		54	1032	<ul> <li>44</li> </ul>	5 [ACK	] Sec	=10960	) Ack=	12123	Win=	65535	5 Len=	0	
	2094	4 170.6	84938 1	192.168	8.10.10	1 1	L92.168	.0.10	SME	3		162	NT Cr	eate	AndX	Reque	st, Fi	D: 0x	:400f,	Path	n: ∖na	ama.tx	t	
	209	5 170.6	85278 1	192.168	3.0.10	1	192.168	.10.10	SME	3		193	NT Cr	eate	AndX	Respo	nse, P	ID: C	x400f					
	2096	5 170.6	85305	192.168	3.0.10	1	192.168	.10.10	SME	3		158	NT Tr	ans P	Respon	ise, M	IT NOT	FY						
	2097	7 170.6	87088 1	192.168	8.10.10	) 1	192.168	.0.10	TCF	•		54	1032	- 44	5 [ACK	] Sec	=11068	B Ack=	12366	win=	65292	2 Len=	0	
	2098	8 170.6	87126	192.168	8.10.10		192.168	.0.10	SME	3		130	Trans	2 Red	quest,	QUEF	Y_FILE	_INFO	, FIC	: 0x4	100f,	Query	File	Internal
	2099	9 170.6	87178 :	192.168	3.0.10		192.168	.10.10	SME	3		126	Trans	2 Res	sponse	, FID	0: 0x40	00t, q	UERY_	FILE_	INFO			
	2100	0 170.6	88237 1	192.168	3.10.10		L92.168	.0.10	SME	3		128	Trans	2 Red	quest,	QUER	Y_FS_1	INFO,	Query	FS A	ttrib	oute I	nto	
	2101	1 1/0.6	88641	192.168	5.0.10		192.168	.10.10	SME	5		134	Trans	2 Res	sponse	, QUE	RY_F5	INFO						
	2104	2 1/0.6	91308.	192.168	5.10.10		192.168	.0.10	SMI	5		142	Trans	2 Red	quest,	SET_	FILE_	INFO,	FID:	0X400	JT			
	210:	3 1/0.0	91526.	192.108	5.0.10		192.168	.10.10	SME	5		118	Trans	2 Res	sponse	, FIL	0X40	JOT, S	EI_FI	LE_IN	IFO E			
	2104	+ 1/0.0	92019	192.100	.10.10		192.108	.0.10	500	-		1/4	-	2 Ret	quest,	DET_	FILE_:	INFO,	FID:	0.400				
	Fram En En En Ep [T [T Fr Ca	te 2075 trefac capsul rrival time shooch Ti time de time de time de time su ame Le apture	: 238 e id: ation Time: dift fo me: 14 lta fr lta fr nce re mber: Length: Length	Dytes 0 (\De type: I Aug 18 r this 714805: om pre om pre ferenc: 2075 238 by: : 238 l ad: ca c4 b2 (	on whre vice\NP Etherne , 2016 packet 95.6355 vious c vious d e or fi tes (19 bytes (1 lco]	2 (1904 PF_{FF91 et (1) 07:36: 573000 573000 captured displaydirst fr: 904 bit: (1904 bit:	b1ts), BD9E2-E 35.6355 0000000 seconds d frame ed fram ame: 16 s) its)	238 by 542-42E 73000 s second e: 0.000 ie: 0.000 i9.15385	tes capt 7-BAOD-F E Asia s 5] 277000 s 0277000 6000 sec	second second second second seconds]	(1904 894220 urd Tin Is] uds]	DIES  })  e	) on 1	nter	race u	,								
	LO 20 30 40 50 50 70 80 90 80 90 80	00 e0 0a 0a fb 4e 00 00 00 00 00 00 00 00 00 00 db 92 67 bf ile: "C:\U	11 85 01 bd 3e 44 00 98 02 08 00 38 04 08 00 00 e8 f8 84 f8 sers\ADM	40 00 4 04 08 0 00 00 0 07 c8 0 a8 05 0 00 00 0 01 00 0 d1 01 4 d1 01 7	po 30 80 06 00 05 00 00 00 00 00 08 00 70 01 00 17 10 4d 7f 00 pData\Loc	5d 2e 0 0f c7 0 00 b4 1 00 00 0 42 19 0 00 44 0 00 00 0 db 92 0 64 bf 1 00 00 0 cal\T	20 a8 0 20 a8 0 25 7b 9 25 7b 9 25 7b 9 25 7b 9 25 7b 9 20 00 0 20	0 0a c0 1 d5 50 d 42 32 0 00 00 0 70 00 0 00 00 0 00 00 1 01 c9 1 01 a0 0 00 80 207 · Display	a8 18 00 00 7d 00 17 5b 00 q. red: 261 (11	@. .>D. .8. .@	B p.D. M.d		Default											

Gambar IV.28

Analisa Paket Data

## Tabel IV.1

Indikator	Sebelum Implementasi	Sesudah Implementasi
	VPN	VPN
Besar data yang dapat	Batas data yang diupload	Tidak ada batasan
diupload	ke email tidak terlalu	ukuran file, karena file
	besar	diletakkan di server file
		sharing.
Penggunaan bandwidth	Bandwidth tidak efisien,	Bandwidth lebih efisien,
dan durasi pertukaran	karena pengiriman data	karena langsung
data	memerlukan waktu yang	terkoneksi VPN, dan
	lebih lama.	pengiriman lebih cepat.
Keamanan pengiriman	Pengiriman data masih	Pengiriman data lebih
data	rentan pembobolan.	aman, karena VPN telah
		mengenkripsi data yang
		dikirim.

# Tabel Perbandingan Sebelum dan Sesudah Implementasi VPN L2TP/IPSec