# **BAB IV**

# **RANCANGAN JARINGAN USULAN**

### 1.1. Jaringan Usulan

Konsep jaringan yang penulis usulkan untuk permasalahan yang ditemukan di PT. Metalogix Infolink Persada adalah dengan penggunaan konsep jaringan VPN dengan metode L2TP/IPsec. Dengan konsep ini diharapkan akan dapat menjadi solusi keamanan jaringan yang diakses dari luar kantor pusat dan untuk mempermudah pekerjaan para pegawai yang memiliki mobilitas tinggi.

### 1.1.1. Topologi Jaringan

Penggunaan konsep VPN ini tidak banyak merubah topologi LAN kantor pusat yang ada. Dikarenakan konsep ini biasanya digunakan untuk topologi jaringan MAN ataupun WAN. Topologi VPN ini menghubungkan jaringan lokal kantor pusat ke jaringan kantor lainnya melewati jaringan publik.



Gambar 4.1. Topologi VPN

### 1.1.2. Skema Jaringan

Skema jaringan VPN ini mempunyai dua jenis koneksi. Yang pertama adalah *site-to-site* VPN, yaitu menghubungkan dua buah jaringan lokal yang berjauhan lokasi gedungnya dengan menggunakan jaringan publik sebagai penghubungnya dan menggunakan sebuah VPN *server* pada jaringan lokal kantor pusat dan sebuah VPN *client* pada jaringan kantor cabang.



Gambar 4.2.*site-to-site* VPN

Yang kedua adalah *remote-access* VPN, yaitu menghubungkan sebuah komputer yang berada diluar jaringan lokal kantor pusat yang menggunakan koneksi internet dan aplikasi VPN *client* yang sudah dikonfigurasi pada komputer *remote* yang digunakan.



Gambar 4.3. remote access VPN

Tetapi untuk skripsi ini penulis khusus membahas hanya tentang site-to-site VPN dengan metode L2TP/IPsec saja.

### 1.1.3. Keamanan Jaringan

Seperti yang sudah dijelaskan di bab-bab sebelumnya, bahwa keamanan jaringan adalah suatu hal yang penting dalam penggunaan konsep VPN ini. Dikarenakan koneksi yang digunakan untuk menghubungkan antar jaringan adalah koneksi publik yang bisa diakses oleh banyak orang.

Konsep VPN yang ada biasanya sudah memiliki protokol khusus seperti *IPsec* yang dapat mengamankan data saat melewati jaringan publik tersebut.*IPSec* (singkatan dari *IP Security*) adalah sebuah protokol yang digunakan untuk mengamankan transmisi data dalam sebuah *internetwork* berbasis TCP/IP. *IPSec* melakukan enkripsi terhadap data pada lapisan yang sama dengan protokol IP dan menggunakan teknik *tunneling* untuk mengirimkan informasi melalui jaringan internet atau dalam jaringan Intranet secara aman.

Rancangan VPN yang penulis buat menggunakan metode L2TP/IPsec. Perbedaan dari metode VPN lain adalah keamanan yang cukup baik dengan menggunakan tambahan protokol IPsec pada *layer network*.

## 1.1.4. Rancangan Aplikasi

Rancangan yang akan penulis terapkan adalah penggunaan *router* mikrotik sebagai VPN *server* dikantor pusat yang dihubungkan ke *switch* utama di jaringan lokal dan terhubung juga ke *modem* untuk koneksi ke internetnya.

Untuk konfigurasi *router* tersebut, penulis menggunakan aplikasi pendukung mikrotik berbasis GUI yaitu *Winbox* yang penulis *install* di perangkat komputer dengan sistem operasi *Windows* 7. Penggunaan *winbox* akan mempermudah dari pengkonfigurasian VPN *server* tersebut.

Berikut adalah skema yang penulis buat untuk mensimulasikan teknologi VPN ini pada kantor pusat PT. Metalogix Infolink Persada.



Gambar 4.4. Skema Jaringan Usulan

1. Konfigurasi L2TP VPN Server

Pertama kita buka aplikasi *winbox* pada PC yang sudah terhubung ke VPN *server*. Lalu arahkan ke menu **PPP** >**L2TP** *Server*. Lalu akan muncul tampilan berikut:

L2TP Server		
	Enabled	ОК
Max MTU:	1450	Cancel
Max MRU:	1450	Apply
MRRU:	▼	
Keepalive Timeout:	30	
Default Profile:	default-encryption	
Authentication:	✓ mschap2 ✓ mschap1 ✓ chap ✓ pap	
IPsec Secret:	✓ Use IPsec ******	

Gambar 4.5. Mengaktifkan L2TP server

Kita *setting* seperti pada gambar lalu klik tombol OK untuk mengaktifkan L2TP *Server*.

Selanjutnya pilih tab *Secret>Add* [+]. Disini akan kita isi parameter standar seperti *name* dan *password* untuk *dial* koneksi dari VPN *client* dan juga beberapa parameter seperti dalam gambar.

New P	PP Secret			
	Name:	PPP		ОК
	Password:	***	•	Cancel
	Service:	l2tp	₹	Apply
	Caller ID:		▼	Disable
	Profile:	default	₹	Comment
Lo	cal Address:	172.16.31.1	•	Сору
Remo	te Address:	172.16.3.2	•	Remove
	Routes:	192.168.88.0/24		

Gambar 4.6. Membuat Secret

2. Konfigurasi IPsec VPN Server

Untuk menambah keamanan, penulis akan memadukan L2TP dengan *IPsec*. Pilih pada menu **IP>IPSec**. Ada beberapa parameter yang dikonfigurasi seperti didalam gambar.

IPsec Proposal <default></default>	
Name: default	ОК
Auth. Algorithms:md5 🛛 🗹 sha1	Cancel
null sha256	Apply
Encr. Algorithms: null des	Disable
aes-192 cbc aes-256 cbc	Сору
blowfish twofish	Remove
camella-256 aes-128 cr	
aes-192 ctr aes-256 ctr aes-128 gcm aes-192 gcm aes-256 gcm	1
Lifetime: 00:30:00	
PFS Group: modp1024	:
enabled default	

Gambar 4.7. IPSec Proposal Server

IPsec Policy <::/0:0->::/0:0>			IPsec Policy <::/0:0	->::/0:0>	
General Action		ОК	General Action		ОК
Src. Address: 192.168.128.1	103	Cancel	Action:	encrypt	Cancel
Src. Port:		Apply	Level:	require	▼ Apply
Dst. Address: 192.168.128.1	105	Disable	IPsec Protocols:	esp	▼ Disable
Dst. Port:	•	Comment		✓ Tunnel	Comment
Protocol: 255 (all)	<b>.</b>	Сору	SA Src. Address:	172.16.31.1	Сору
✓ Template		Remove	SA Dst. Address: Proposal:	172.16.31.2 default	Remove
Group: [default			Priority:	0	
enabled default	Templat	te	enabled	default	Template

Gambar 4.8. IPsec Policy Server

New IPsec Peer	
Address:	172.16.31.2
Port:	500
Local Address:	<b></b>
Auth. Method:	pre shared key
	Passive
Secret:	
Policy Template Group:	default
Exchange Mode:	main
	Send Initial Contact
	NAT Traversal
My ID:	auto 🗧 :
Proposal Check:	obey 두
Hash Algorithm:	shal 🔻
Encryption Algorithm:	des 🕑 3des 📃 aes-128
	aes-192 aes-256 blowfish
	camellia-128 camellia-192 camellia-256
Mode Configuration:	▼
DH Group:	modp1024
Generate Policy:	no Ŧ
Lifetime:	1d 00:00:00

Gambar 4.9. IPsec Peer Server

# 3. Konfigurasi L2TP VPN Client

Selanjutnya setelah selesai mengkonfigurasi VPN *server*, dilanjutkan dengan konfigurasi L2TP di VPN *client*. Kita hanya melakukan *dial* ke L2TP *server*. Buka menu **PPP**>*Add* [+]> pilih L2TP *client*.

New Inter	New Interface				
General	Dial Out	Statu	us Traffic		
	Connect	t To:	192.168.128.103		
	User:		ррр		
	Passw	ord:	***		
	Pro	ofile:	default-encryption 🔻		
Kee	Keepalive Timeout:		60		
			Dial On Demand		
Default (	Route Dista	nce:	1		
	A	llow:	✓ mschap2 ✓ mschap1 ✓ chap ✓ pap		

Gambar 4.10. Setting L2TP Client

Isikan parameter sesuai dengan jaringan yang ada. *Connect* to diisi dengan alamat IP publik *router* kantor pusat. Untuk *user* dan *password* isikan sesuai dengan yang sudah kita buat di VPN *server*.

4. Konfigurasi IPSec VPN Client

Pada dasarnya parameter yang digunakan untuk *IPSec client* ini tidak jauh berbeda dari yang sudah kita setting di sisi *server*. Hanya ada perbedaan di konfigurasi IP *Address* saja.

Pada tab IPSec proposal tidak ada perbedaan dengan konfigurasi di sisi IPSec server.



Gambar 4.11. IPsec Proposal client

Selanjutnya pada tab *IPSec Policy*. Sesuaikan IP *address* asal dan tujuan yang digunakan.

IPsec Policy <::/0:0->::/0:0>		IPsec Policy <::/0:	0->::/0:0>	
General Action	ОК	General Action		ОК
Src. Address: 192.168.128.105	Cancel	Action:	encrypt	Cancel
Src. Port:	▼ Apply	Level:	require	Apply
Dst. Address: 192.168.128.103	Disable	IPsec Protocols:	esp	▼ Disable
Dst. Port:	Comment	SA Sec. Address	✓ Tunnel	Comment
Protocol: 255 (all)	▼ Copy	SA Dst. Address:	172.16.31.1	Сору
✓ Template	Remove	Proposal:	default	₹ Remove
Group: default	₹	Priority:	0	
enabled default	Template	enabled	default	Template

Gambar 4.12. IPsec Policy Client

Setelah setting IPSec Policy, dilanjutkan dengan setting IPSec Peer.

New IPsec Peer	
Address:	172.16.31.1
Port:	500
Local Address:	<b></b>
Auth. Method:	pre shared key
	Passive
Secret:	*****
Policy Template Group:	default
Exchange Mode:	main
	Send Initial Contact
	NAT Traversal
My ID:	auto
Proposal Check:	obey 🗧
Hash Algorithm:	shal 🔻
Encryption Algorithm:	des 🗹 3des 📃 aes-128
	aes-192 aes-256 blowfish
	camellia-128 camellia-192 camellia-256
Mode Configuration:	▼
DH Group:	modp1024
Generate Policy:	no
Lifetime:	1d 00:00:00

Gambar 4.13.IPsec Peer Client

# 5. Interkoneksi Jaringan

Agar jaringan dari kedua sisi bisa saling terkoneksi. Maka dibuat *routing* statik secara manual di L2TP *client*.

Re	oute <192.168.1	.0/24>	
6	ieneral Attribut	es	
	Dst. Address:	192.168.1.0/24	
	Gateway:	l2tp-out1	▼ reachable
(	Theck Gateway:		•
	Туре:	unicast	
	Distance:	1	
	Scope:	30	
	Target Scope:	10	

Gambar 4.14. Routing Statik Client

Setelah itu baru dipastikan bahwa jaringan kantor sudah saling terkoneksi bisa dengan menggunakan perintah ping dari masing-masing kantor ke kantor lainnya.

### 1.1.5. Manajemen Jaringan

Manajemen jaringan yang diusulkan tidak jauh berbeda dari manajemen jaringan yang sudah ada. Perbedaannya hanya pada pemberian hak akses untuk karyawan kantor untuk bisa mengakses jaringan lokal kantor pusat dari luar.

Pemberian hak akses tersebut adalah berupa pemberian *username* dan *password* VPN *client* kepada karyawan untuk digunakan saat ingin membuka koneksi ke kantor pusat melalui jaringan VPN.

Tidak semua karyawan yang bisa atau dapat mengakses jaringan dari luar kantor untuk menjaga keamanan data. Hanya beberapa karyawan yang dikira sangat membutuhkan yang akan diberikan hak akses tersebut.

## 4.2. Pengujian Jaringan

Pada sub-bab ini akan dijelaskan perbedaan yang ditemukan antara jaringan awal sebelum memakai L2TP/IPsec dan jaringan akhir setelah memakai L2TP/IPsec berdasarkan simulasi yang dilakukan oleh penulis.

Akan dilakukan beberapa tahap pengujian yaitu *packetloss* dengan menggunakan perintah '*ping*' pada *command prompt*, lalu akan dilakukan *denial of service* menggunakan aplikasi *pingflood.exe* dan terakhir akan dilakukan *sniffing* menggunakan aplikasi *wireshark*.

### 4.2.1. Pengujian Jaringan Awal

Pada pengujian jaringan awal akan dilakukan tes terhadap jaringan kantor yang sedang berjalan tanpa VPN.

1. Packet Loss Test

Pengujian packet *loss* dilakukan beberapa kali tes dengan perintah '*ping*' ke *IP* tujuan menggunakan *command prompt* untuk melihat stabilitas koneksi di jaringan tanpa menggunakan VPN. Dan didapatkan hasil sebagai berikut:

Reply from Reply from	n 192.168.10.2: n 192.168.10.2:	bytes=32 butes=32	time=1ms	TTL=128 TTL=128
Reply from	n 192.168.10.2:	bytes=32	time<1ms	TTL=128
Reply from	n 192.168.10.2:	bytes=32	time<1ms	TTL=128
Reply from	n 192.168.10.2:	bytes=32	time<1ms	TTL=128
Ping stat: Packet Approximat Minimu Control-C	istics for 192.1 ts: Sent = 269, te round trip ti um = 0ms, Maximu	68.10.2: Received imes in m im = 5ms,	= 269, La illi-seco Average	ost = 0 (0% loss), nds: = 0ms

Gambar 4.15 Packet loss jaringan awal

2. Denial of Service Test

Pengujian ini untuk mengetahui ketahanan koneksi saat dibanjiri paket. Pengujian dilakukan dengan aplikasi *pingflood.exe*. Setelah dilakukan pengujian didapatkan hasil sebagai berikut:

Reply from 192.168.10.2: bytes=32 time<1ms TTL=128 Reply from 192.168.10.2: bytes=32 time<1ms TTL=128 Reply from 192.168.10.2: bytes=32 time<1ms TTL=128 Reply from 192.168.10.2: bytes=32 time<1ms TTL=128	
Ping statistics for 192.168.10.2: Packets: Sent = 1442, Received = 1442, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 21ms, Average = 0ms Control-C	×
^C	

Gambar 4.16 DoS Attack jaringan awal

Pengujian dilakukan dengan mengirimkan 10000 paket data sebesar 25kb didapatkan hasil, bahwa jaringan tidak terputus dan maksimum *round trip* sebesar 21ms.

3. Sniffing Test

Pada test kali ini akan dilakukan *sniffing* pada *user* dan *password* FTP. Saat salah satu PC mengakses sebuah FTP di dalam kantor. Berikut adalah hasil *sniffing username* dan *password* FTP.

🚺 ttp.cep	- Wireshark		- 10 <b>- X</b>
Els Edi	View Go Capture	Analyze Statistics	Telephony Iools Help
		* 2 8 3	****
Filter		APP	MARKOUN *
	Destination	Protocol	info .
23	192,168.0,208	TCP	54026 > ftp [SYN] SAC-0 w
20.8	102.168.8.12	TCP	ftp > 34026 [SYN, ACE] 50
12	192,168,0,208	TCP	54026 > ftp [ACK] Seg=1 A
208	197.168.6.12	A CONTRACTOR OF THE OWNER	te honse: 220 Serv-u FTP
(2)	197.168.0.208	Useman	10 ET USER TANK
08	192.165.6.12		Reiponse: 331 User name o
2	192.168.0.208	Pasaword	Aquest: PASS sand
208	192,168,6,12		Response: 230 User Togged
12	192,168.0.208	FTP	Request: SYST
208	192.168.6.12	FTP	Response: 215 UNIX Type:

Gambar 4.17. Hasil sniffing password

Seperti yang terlihat klien PC dengan IP 192.168.6.12 me*request* koneksi FTP *server* di IP 192.168.0.208 dengan *username* dan *password* dan semuanya bisa terlihat melalui *sniffing* dengan aplikasi Wireshark.

### 4.2.2. Pengujian Jaringan Akhir

Pada pengujian jaringan akhir ini akan dilakukan beberapa tes seperti yang sudah dilakukan di pengujian jaringan awal tadi. Dengan begitu nanti akan bisa dilihat perbedaan dari kedua jaringan ini anatar yang menggunakan VPN dan yang tidak menggunakannya.

1. Packet Loss Test

Pengujian *packet loss* dilakukan beberapa kali tes dengan perintah '*ping*' ke *IP* tujuan menggunakan *command prompt* untuk melihat stabilitas koneksi di jaringan menggunakan L2TP/IPSecVPN. Dan didapatkan hasil sebagai berikut:

Reply from 192.168.10.2: bytes=32 time=4ms TTL=126 Reply from 192.168.10.2: bytes=32 time=4ms TTL=126 Reply from 192.168.10.2: bytes=32 time=5ms TTL=126 Reply from 192.168.10.2: bytes=32 time=2ms TTL=126 Reply from 192.168.10.2: bytes=32 time=5ms TTL=126	
Ping statistics for 192.168.10.2: Packets: Sent = 221, Received = 221, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 10ms, Average = 4ms Control-C ^C C:\Users\virtual1>	

Gambar 4.18. Packet Loss Jaringan VPN

Dari data diatas dapat kita lihat untuk data max dan *average round trip* suatu paket masih dalam nilai yang wajar. Dari percobaan 221 kiriman paket, max round trip = 10ms dan average round trip = 4ms.

Penulis juga melakukan *trace route* untuk melihat apakah paket yang dikirim sudah melewati jaringan L2TP yang dibuat. Dan seperti gambar dibawah, hasilnya adalah paket dikirim melalui *gateway* kantor cabang IP 60.10.10.1 dan diteruskan ke IP VPN *server* 172.16.31.1.

C:\Use	ers\	virtu	al1>	trace	ert 19	2.1	68.10.2	
Fraci	ng Pe	oute	to V	IRTUA	L1-P	C [1	92.168.10.21	
over a	a ya:	ximum	of :	30 hc	ps:			
-	$\gamma_{1}$		14		14		(0 10 10 1	
±	1	ms	1	ms	1	ms	00.10.10.1	
2	- 4	ms	2	ms	2	ms	172.16.31.1	
3	6	ms	4	ms	4	ms	VIRTUAL1-PC	[192.168.10.2]
сž.								
Trace	COM	olete						

Gambar 4.19. Trace Route VPN

2. Denial of Service Test

Pengujian ini untuk mengetahui ketahanan koneksi saat dibanjiri paket. Pengujian dilakukan dengan aplikasi *pingflood.exe*. Setelah dilakukan pengujian didapatkan hasil sebagai berikut:

Reply from 192.168.10.2 Reply from 192.168.10.2 Reply from 192.168.10.2	bytes=32 time=4ms TTL=126 bytes=32 time=4ms TTL=126
Ping statistics for 192.	168.10.2:
Packets: Sent = 497.	Received = 490. Lost = 7 (1% loss).
Approximate round trip t	imes in milli-seconds:
Minimum = 1ms, Maxim	um = 19ms, Average = 3ms
Control-C ^C C:\Users\virtual1>_	

Gambar 4.20. Pingflood Jaringan VPN

Data diatas adalah hasil dari pengujian dengan membanjiri VPN *server* dengan 10,000 paket data sebesar 25kb. Hasilnya menunjukan bahwa hanya terjadi beberapa kali *timeout* tetapi tidak sampai mematikan *service* VPN.

3. Sniffing Test

Pada kesempatan ini dilakukan pengetesan menggunakan aplikasi Wireshark. Dengan cara meng*capture traffic* pada jaringan antara kantor pusat dengan kantor cabang.

Setelah itu dilakukan pengaksesan FTP *server* pada kantor pusat dari komputer di kantor cabang. Hasilnya *traffic* protokol FTP berupa *username* dan *password* tidak terbaca pada aplikasi wireshark seperti yang ada pada pengujian jaringan awal.

	Edit	View	v Go	0 0	apture	Ar	alyze	Sta	tistics	s T	elepho	ny	Wire	less	Tools	Hel	р						
ſ.	<b>-</b> 🦪	۲		5 2		9	ر بھ	•	8	1			0	0,0	1								
Ţ,	pply a c	display I	filter	<ctr< th=""><th>ŀ-/&gt;</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>(</th><th></th><th>E</th><th>xpress</th><th>ion</th><th></th></ctr<>	ŀ-/>													(		E	xpress	ion	
	÷	Time			Source	e				Dest	ination				Prot	ocol	Length	Info	0				
	8955	1925.	1264	60	202.	10.1	0.1			202	.10.1	0.2			PPP	Comp	272	Cor	npress	ed	data		
	8956	1925.	1389	61	202.	10.1	0.1			202	.10.1	0.2			PPP	Comp	272	Cor	npress	ed	data		
	8957	1925.	1394	61	202.	10.1	0.1			202	.10.1	0.2			PPP	Comp	272	Cor	npress	ed	data		
	8958	1930.	.0375	83	202.	10.1	0.2			169	.254.	169.	254		TCP		74	468	835 →	80	[SYN	] Seq	ŀ
	8959	1930.	0385	64	202.	10.1	0.1			202	.10.1	0.2			ICM	P	102	Des	stinat	ior	unr	eacha	1
	8960	1930.	5076	43	202.	10.1	0.2			202	.10.1	0.1			ISA	KMP	134	Int	format	ior	al		
	8961	1930.	5091	43	202.	10.1	0.1			202	.10.1	0.2			ISA	KMP	134	Int	format	ior	nal		
	8962	1930.	5101	43	202.	10.1	0.1			202	.10.1	0.2			ISA	KMP	134	Int	format	ior	nal		
	8963	1930.	5111	44	202.	10.1	0.2			202	.10.1	0.1			ISA	KMP	134	Int	format	ior	nal		
	8964	1935.	0872	25	202.	10.1	0.2			202	.10.1	0.1			PPP	Comp	208	Cor	npress	ed	data		
	8965	1935.	0897	25	202.	10.1	0.1			202	.10.1	0.2			PPP	Comp	208	Cor	npress	ed	data		
	8966	1935.	1207	29	202.	10.1	0.1			202	.10.1	0.2			PPP	Comp	272	Cor	npress	ed	data		
	8967	1935.	1222	29	202.	10.1	0.1			202	.10.1	0.2			PPP	Comp	272	Cor	npress	ed	data		
	8968	1935.	1227	29	202.	10.1	0.1			202	.10.1	0.2			PPP	Comp	272	Cor	npress	ed	data		
	8969	1935.	1287	30	202.	10.1	0.2			202	.10.1	0.1			PPP	Comp	272	Cor	npress	ed	data		
	8970	1935.	1427	32	202.	10.1	0.1			202	.10.1	0.2			PPP	Comp	272	Cor	npress	ed	data		
	8971	1935.	1562	33	202.	10.1	0.1			202	.10.1	0.2			PPP	Comp	272	Cor	npress	ed	data		
	8972	1935.	1562	33	202.	10.1	0.1			202	.10.1	0.2	-		PPP	Comp	272	Cor	npress	ed	data	1000	
	8973	1935.	4992	77	Pese	ompu	_c1:	eb:0t	2	Pcs	Compu	_67:	0f:0	15	ARP		42	Who	o has	202	2.10.	10.2?	
	8974	1935.	4997	77	PcsC	ompu	_67:	Of:ds	5	Pcs	Compu	_c1:	eb:0	b	ARP		42	203	2.10.1	0.2	? is	at 08	
i.	_	_			_	01																	,
Î	rame	8946:	62	byte	s on 1	vire	(49	bit	s),	62 k	ytes	cap	ture	d (4	96 bi	ts) o	n inte	rfad	ce Ø				ĺ
	Int	erfac	e id:	: 0	(-)						10 I I I I I I I I I I I I I I I I I I I												
	Enc	apsul	ation	n ty	pe: Et	her	net (	1)															
	Arr	ival	Time:	: Au	g 2,	201	7 02:	04:0	6.26	4735	5000 1	SE As	ia	Stan	dard	Time							
	[Ti	me sh	ift f	for	this p	ack	:t: 0	.000	0000	100 5	second	ds]											
	Epo	ch Ti	me: 1	1501	514246	5.26	17356	100 s	econ	ds													
20	0 98											88											
	0 00	30 0	8 99		80 48			15 ca		08 0	n ca	Øa	- 0	@.			-						
91	0 01	82 8	6 45	06	35 80		81 (	a ca	02	60 1	4 88	61				-							
32	6 D.		_											_									
1 2 2	0 00	00 0	0 25	00	21 89	08	99.8	10 00		00.0	36												

Gambar 4.21. Sniffing Jaringan VPN