# **BAB IV**

# RANCANGAN JARINGAN USULAN

### 4.1. Jaringan Usulan

### 4.1.1. Topologi Jaringan

Untuk topologi jaringan penulis tidak akan merubah topologi jaringan yang sudah ada pada PT. Citra Selaras Jaya karena topologi yang sekarang digunakan sudah sangat baik dan berjalan sesuai apa yang diharapkan. Jaringan usulan yang penulis usulkan hanya membahkan Virtual Private Network(VPN) untuk dapat mengakses jaringan LAN kantor pusat dan cabang PT. Citra Selaras Jaya dengan membuat jalur yang aman dan rahasia dari jaringan public.

## 4.1.2. Skema Jaringan



#### Gambar IV.1

#### Skema Jaringan Usulan

Pada skema jaringan usulan dapat dilihat bahwa menambahkan Virtual Private Network (VPN) yang nantinya akan digunakan untuk kemudahan pengiriman data keserver ataupun monitoring yang dilakukan oleh pihak IT yang akan mengakses jaringan lokal melalui jaringan public seperti internet, dan membuat jalur aman dan rahasia, dengan begitu sistem jaringan PT. Citra Selaras Jaya dengan adanya VPN , pihak IT akan mendapatkan kemudahan untuk mengakses ke jaringan lokal walaupun posisi pegawai tersebut sedang berada di cabang lain.

#### 4.1.3. Keamanan Jaringan

Keamanan jaringan yang ada di PT. Citra Selaras Jaya sudah sangat bagus dengan membuat firewall pada beberapa konfigurasi hardware seperti router dan mengandalkan software antivirus. Akan tetapi pada saat ini sebaik apapun firewall yang dibuat masih bisa ditembus virus, spam, dan sebagainya. Karena itu penulis memberikan saran jika dalam jaringan Wide Area Network PT. Citra Selaras Jaya ditambah dengan hardware firewall yang memang dirancang untuk melindungi jaringan dari ancaman virus, hacker, dan sebagainya. Ada banyak vendor yang menyediakan hardware firewall diantaranya Cisco Pix Firewall keluaran dari cisco yang terkenal dengan routernya.

#### 4.1.4. Rancangan Aplikasi

Pada perancangan aplikasi ini, penulis mencoba menggunakan software simulasi yang digunakan untuk perancangan jaringan VPN, yang berguna untuk menghubungkan kedua jaringan yang ada cempaka putih maupun di glodok sampai bisa terkoneksi melalui jaringan public seperti internet software yang digunakan sebagai simulasi adalah GNS3 (Graphic Network Simulator).



Gambar IV.2

Desain simulasi jaringan menggunakan GNS

Perfoma jaringan :

- Sebelum menggunakan VPN, sering terjadi kegagalan komputer client mengirimkan data transaksi ke server dikarenakan banyaknya noise, sehingga data yang diterima oleh server bukan merupakan data Real Time.
- Sesudah menggunakan VPN, data yang di transmisikan melalui VPN akan mengalami kompresi, sehingga transmisi data dapat berjalan baik dan lancer. Serta adanya peningkatan keamanan dalam komunikasi data.
- 1. Router pada kantor pusat (cempaka putih )
  - a. Router

Interface FastEth 0/0 =10.32.152.5

Subnet mask = 255.255.255.252

Interface FastEth 0/1 =192.168.1.1

Subnet mask = 255.255.255.0

- b. Server = 192.168.1.10
- c. Client

PC1 = 192.168.1.2 PC2 = 192.168.1.3 PC3 = 192.168.1.4 PC4 = 192.168.1.5 PC5 = 192.168.f0.6 PC6 = 192.168.1.7

2. Cara Konfigurasi VPN pada router kantor pusat :

Cempaka (config-if) #aaa new-model

Cempaka (config-if) #aaa authentication login userauthen local

Cempaka (config-if) #aaa authorization network groupauthor local

Cempaka (config-if) #username glodok password 123456

===konfigurasi EzVPN===

Cempaka (config) #crypto isakmp policy 10

Cempaka (config-isakmp) #encr 3des

Cempaka (config-isakmp) #authentication pre-share

Cempaka (config-isakmp) #group 2

Cempaka (config-isakmp) #crypto ipsec transf myset eps-3esp-sha-

Cempaka (config-crypto-transform) #model tunnel

Cempaka (config-crypto-transform) #exit

Cempaka (config) #crypto isakm client config group vpngrp

Cempaka (config-isakmp-group) #key cisco123

Cempaka (config-isakmp-group) #exit

Cempaka (config) #crypto dynamic-map dynmap 10

Cempaka (config-crypto-map) #set transform-set myset

Cempaka (config-crypto-map) #exit

Cempaka (config) #cryp map clientmap client authen list userauthen

Cempaka (config) #cryp map clientmap isakmp autho list groupauthor

Cempaka (config) #cryp map clientmap 10 ipsec-isakmp dynamic dynmap

===apply EzVPN===

Cempaka (config) #int gi0/0

Cempaka (config-if) #crypto map clientmap

=== EzVPN client mode ===

Cempaka (config) #crypto isakmp policy 1

Cempaka (config-crypto-isakmp) #encryption 3des

Cempaka (config-crypto-isakmp) #authentication pre-share

Cempaka (config-crypto-isakmp) #group2

Cempaka (config-crypto-isakmp) #exit

Cempaka (config) #crypto isakmp client config address local mypool

Cempaka (config) #crypto isakmp client config group ezvpn

Cempaka (config-isakmp-group) #key 123456

Cempaka (config-isakmp-group) #pool mypool

Cempaka (config-isakmp-group) #exit

Cempaka (config) #crypto ipsec transf myset esp-3desesp-sha-hmac Cempaka (config) #crypto dynamic-map mymap1 Cempaka (config-crypto-map) #set transform-set myset Cempaka (config-crypto-map) #reverse-route Cempaka (config) #crypto-map) #exit Cempaka (config) #crypto map mymap isakmp author list groupauthor Cempaka (config) #crypto map mymap client config address respond Cempaka (config) #crypto map mymap 1 ipsec-isakmp dynamic mymap Cempaka (config) #int g0/0 Cempaka (config-if) #crypto map mymap Cempaka (config-if) #crypto map mymap

## 3. Router pada kantor cabang (glodok )

a. Router

Interface FastEth 0/0 =10.32.152.9

Subnet mask = 255.255.255.252

Interface FastEth 0/1 =192.168.2.1

Subnet mask = 255.255.255.0

- b. Server = 192.168.2.2
- c. Client

PC1 = 192.168.2.10

PC2 = 192.168.2.11

PC3 = 192.168.2.12 PC4 = 192.168.2.13 PC5 = 192.168.2.14

4. Cara Konfigurasi VPN pada router kantor cabang :

Glodok

=== konfigurasi EzVPN ===

Glodok (config) #crypto ipsec client ezvpn ez

Glodok (config-crypto-ezvpn) #connect auto

Glodok (config-crypto-ezvpn) #group vpngrp key cisco123

Glodok (config-crypto-ezvpn) #mode network-extension

Glodok (config-crypto-ezvpn) #peer 10.32.152.5

Glodok (config-crypto-ezvpn) #xauth userid mode interactive

Glodok (config-crypto-ezvpn) #exit

=== apply EzVPN ===

Glodok (config) # int f0/0

Glodok (config-if) #crypto ipsec client ezvpn ez

Glodok (config-if) #int f0/1

Glodok (config-if) #crypto ipsec client ezvpn ez inside

Glodok (config) #crypto ipsec client ezvpn ezvpn

Glodok (config-crypto-ezvpn) #connect auto

Glodok (config-crypto-ezvpn) #group ezvpn key 123456

Glodok (config-crypto-ezvpn) #mode client

Glodok (config-crypto-ezvpn) #exit

Glodok (config) #int f0/0

Glodok (config-if) #crypto ipsec client ezvpn ezvpn inside Glodok (config-if) #exit Glodok (config) #int f0/1 Glodok (config-if) #crypto ipsec client ezvpn ezvpn

### 4.1.5. Manajemen Jaringan

Seperti yang sudah dijelaskan dalam bab sebelumnya yaitu agar setiap toko client bisa mengirimkan paket data transaksi ke server tanpa terputus ataupun gagal, maka penulis mengusulkan untuk menambahkan Virtual Private Network(VPN) pada jaringan PT. Citra Selara Jaya. VPN menghubungkan komponen komponen dari satu jaringan diatas jaringan bersama yang lain melindungi proses pengirimannya. Suatu jaringan private yang dibangun pada suatu infrastruktur jaringan publik yang keamanan datanya terjamin.

# 4.2. Pengujian Jaringan

Dalam membangun sebuah jaringan komputer tentunya perlu dilakukan pengujian terhadap jaringan tersebut untuk memastikan semua sistem berjalan sesuai apa yang diharapkan.

#### 4.2.1. Pengujian Jaringan Awal

a. Ping dari client (192168.1.10) ke gateway (192.168.2.1)

VPCS> ping 192.168.2.1										
84	bytes	from	192.168.2.1	<pre>icmp_seq=1</pre>	tt1=254	time=98.171	ms			
84	bytes	from	192.168.2.1	<pre>icmp_seq=2</pre>	tt1=254	time=78.121	ms			
84	bytes	from	192.168.2.1	icmp_seq=3	tt1=254	time=78.035	ms			
84	bytes	from	192.168.2.1	icmp_seq=4	tt1=254	time=78.226	ms			
84	bytes	from	192.168.2.1	icmp_seq=5	tt1=254	time=78.122	ms			

b. Ping dari client (192.168.1.10) ke client (192.168.2.2)

VPC	VPCS> ping 192.168.2.2									
192	192.168.2.2 icmp seq=1 timeout									
84	bytes	from	192.168.2.2	icmp_seq=2	tt1=62	time=93.751	ms			
84	bytes	from	192.168.2.2	icmp_seq=3	tt1=62	time=93.751	ms			
84	bytes	from	192.168.2.2	icmp_seq=4	tt1=62	time=93.752	ms			
84	bytes	from	192.168.2.2	icmp_seq=5	tt1=62	time=93.749	ms			

c. Ping client (192.168.1.10) ke router (10.32.152.5)

VPO	CS> pir	ng 10.	32.152.5				
84	bytes	from	10.32.152.5	icmp_seq=1	tt1=255	time=15.625	ms
84	bytes	from	10.32.152.5	icmp_seq=2	tt1=255	time=15.623	ms
84	bytes	from	10.32.152.5	icmp_seq=3	tt1=255	time=15.624	ms
84	bytes	from	10.32.152.5	icmp_seq=4	tt1=255	time=15.625	ms
84	bytes	from	10.32.152.5	icmp_seq=5	tt1=255	time=15.629	ms

d. Capture dengan Wireshark sebelum VPN

	📕 🙋 💿 📄 🛅	🕺 🖸   🍳 🗢 🖻 🖉 (	) 👲 🗐 📲 🔍 ପ୍ ସ୍	. 🎹						
Ap	pply a display filter <c< th=""><th>:trl-/&gt;</th><th></th><th></th><th></th><th></th><th></th><th></th><th><b>→</b></th><th>Expression</th></c<>	:trl-/>							<b>→</b>	Expression
۱o.	Time	Source	Destination	Protocol	Length I	info				
	7 29.995809	c2:01:0a:84:00:00	c2:01:0a:84:00:00	LOOP	60 R	Reply				
	8 31.974560	c2:02:10:38:00:00	c2:02:10:38:00:00	LOOP	60 R	Reply				
	9 37.667283	c2:02:10:38:00:00	CDP/VTP/DTP/PAgP/UD	CDP	359 D	Device I	D: R2	Port ID	: FastEthernet0/0	
	10 39.991078	c2:01:0a:84:00:00	c2:01:0a:84:00:00	LOOP	60 R	Reply				
	11 41.975830	c2:02:10:38:00:00	c2:02:10:38:00:00	LOOP	60 R	Reply				
	12 49.990348	c2:01:0a:84:00:00	c2:01:0a:84:00:00	LOOP	60 R	Reply				
	13 51.971600	c2:02:10:38:00:00	c2:02:10:38:00:00	LOOP	60 R	Reply				
	14 55.559055	c2:01:0a:84:00:00	CDP/VTP/DTP/PAgP/UD	CDP	359 D	Device I	D: R1	Port ID	: FastEthernet0/0	
	14 55.559055 15 59.992118	c2:01:0a:84:00:00 c2:01:0a:84:00:00	CDP/VTP/DTP/PAgP/UD c2:01:0a:84:00:00	CDP LOOP	359 D 60 R	Device I Reply	D: R1	Port ID	: FastEthernet0/0	
- Fr  - Et	14 55.559055 15 59.992118 16 61.970869 rame 1: 60 bytes thernet II, Src: Destination: c2 Source: c2:01:0 Type: Loopback	c2:01:0a:84:00:00 c2:01:0a:84:00:00 c2:02:10:38:00:00 on wire (430 bits), 6 c2:01:0a:84:00:00 (c2:02 :01:0a:84:00:00 (c2:01:0a:1 (0x9000) (c2:01:0a:1	CDP/VTP/DTP/PAgP/UD_ c2:01:0a:84:00:00 c2:02:10:38:00:00 0 bytes captured (480 b :01:0a:84:00:00) Dst: L:0a:84:00:00) 34:00:00)	CDP LOOP LOOP vits) on c2:01:0a	359 D 60 R 60 R interfa :84:00:	Device I Reply Replv Ace 0 00 (c2:	D: R1	Port ID 84:00:00	: FastEthernet0/0	
Fr Et Et	14 55.559055 15 59.992118 16 61.970869 rame 1: 60 bytes thernet II, Src: Destination: c2 Source: c2:01:0 Type: Loopback onfiguration Test skipCount: 0	c2:01:0a:84:00:00 c2:01:0a:84:00:00 c2:02:10:38:00:00 on wire (480 bits), 6 c2:01:0a:84:00:00 (c2:02 :01:0a:84:00:00 (c2:02 :a:84:00:00 (c2:01:0a:1 (0x:000) Protocol (loopback)	CDP/VTP/DTP/PAgP/UD c2:01:0a:84:00:00 c2:02:10:38:00:00 0 bytes captured (480 b :01:0a:84:00:00), Dst: l:0a:84:00:00) 34:00:00)	CDP LOOP LOOP vits) on c2:01:0a	359 D 60 R 60 R interfa :84:00:	Device I Reply Reply Acce 0 00 (c2:	D: R1	Port ID 84:00:00	: FastEthernet0/0	
- Fr - Et - € - Cc	14 55.559055 15 59.992118 16 61.970869 rame 1: 60 bytes thernet II, Src: - Destination: c2 - Source: c2:01:0 - Type: Loopback onfiguration Test - skipCount: 0 - Relevant functi	c2:01:0a:84:00:00 c2:01:0a:84:00:00 c2:02:10:38:00:00 on wire (480 bits), 6 c2:01:0a:84:00:00 (c2:02 :01:0a:84:00:00 (c2:01:0a:10 (0x9000) Protocol (loopback) on: Reply (1)	CDP/VTP/DTP/PAgP/UD c2:01:0a:84:00:00 c2:02:10:38:00:00 0 bytes captured (480 b :01:0a:84:00:00), Dst: 1:0a:84:00:00) 34:00:00)	CDP LOOP LOOP vits) on c2:01:0a	359 C 60 R 60 R interfa :84:00:	Device I Reply Replv CCE 0 00 (c2:	D: R1	Port ID 84:00:00	: FastEthernet0/0	
- Fr - Et - Et - Et	14 55.559055 15 59.992118 16 61.970869 rame 1: 60 bytes thernet II, Src: Destination: c2 Source: c2:01:0 Type: Loopback onfiguration Test - skipCount: 0 Relevant functi - Function: Reply	c2:01:0a:84:00:00 c2:01:0a:84:00:00 c2:02:10:38:00:00 on wire (480 bits), 6 c2:01:0a:84:00:00 (c2:0 01:0a:84:00:00 (c2:0 a:84:00:00 (c2:01:0a:1 (0x9000) Protocol (loopback) on: Reply (1) (1)	COP/VTP/DTP/PAgP/UD c2:01:0a:84:00:00 c2:02:10:38:00:00 0 bytes captured (480 b :01:0a:84:00:00), Dst: 1:0a:84:00:00) 34:00:00)	CDP LOOP LOOP vits) on c2:01:0a	359 C 60 R 60 R interfa ::84:00:	Device I Reply Reply Cce 0 00 (c2:	D: R1	Port ID 84:00:00	: FastEthernet0/0	
Fr Et	14 55.559055 15 59.992118 16 61.9708069 rame 1: 60 bytes thernet II, Src: 2 Destination: c2 3 Source: c2:01:0 - Type: Loopback configuration Test - skipCount: 0 - Relevant functi - Function: Reply - Receipt number: 2 (20 hyter)	c2:01:0a:84:00:00 c2:01:0a:84:00:00 c2:02:10:38:00:00 on wire (480 bits), 60 c2:01:0a:84:00:00 (c2:01:0a: a:84:00:00 (c2:01:0a: (0x9000) Protocol (loopback) on: Reply (1) (1) 0	CDP/VTP/DTP/PAgP/UD c2:01:0a:84:00:00 c2:02:10:38:00:00 0 bytes captured (480 b :01:0a:84:00:00) Dst: L:0a:84:00:00) 34:00:00)	CDP LOOP LOOP wits) on c2:01:0a	359 C 60 R 60 R interfa ::84:00:	Device I Reply Reply Cce 0 00 (c2:	D: R1	Port ID 84:00:00	: FastEthernet0/0	
Fr Et Cc	14 55.559055 15 59.992118 16 61.970869 rame 1: 60 bytes thernet II, Src: 2 Destination: c2 3 Source: c2:01:0 - Type: Loopback configuration Test - skipCount: 0 - Relevant functi - Function: Reply - Receipt number: ata (40 bytes) - Data: @20000000	c2:01:0a:84:00:00 c2:01:0a:84:00:00 c2:02:10:38:00:00 on wire (430 bits), 6 c2:01:0a:84:00:00 (c2:02 :01:0a:84:00:00 (c2:02 :a:84:00:00 (c2:01:0a:1 (0x9000) Protocol (loopback) on: Reply (1) (1) 0	CDP/VTP/DTP/PAgP/UD. c2:01:0a:84:00:00 c2:02:10:38:00:00 0 bytes captured (480 b :01:0a:84:00:00) 34:00:00) 24:00:00	CDP LOOP LOOP wits) on c2:01:0a	359 C 60 R 60 R interfa :84:00:	Device I Reply Reply Cce 0 00 (c2:	D: R1	Port ID 84:00:00	: FastEthernet0/0	
Fr Et	14 55.559055 15 59.992118 16 61.970869 rame 1: 60 bytes thernet II, Src: Destination: c2 Source: c2:01:0 Type: Loopback onfiguration Test skipCount: 0 Relevant functi Function: Reply Receipt number: ata (40 bytes) Data: 000000000 Liength: 401	c2:01:0a:84:00:00 c2:01:0a:84:00:00 c2:02:10:38:00:00 on wire (480 bits), 6 c2:01:0a:84:00:00 (c2:02 :01:0a:84:00:00 (c2:02 :a:84:00:00 (c2:01:0a:1 (0x:000) Protocol (loopback) on: Reply (1) (1) 0	CDP/TP/DTP/PAgP/UD C2:01:0a:84:00:00 c2:02:10:38:00:00 0 bytes captured (480 b :01:0a:84:00:00) 34:00:00) 34:00:00)	CDP LOOP LOOP vits) on c2:01:0z	359 C 60 R 60 R interfa :84:00:	Device I Reply Reply Cce 0 00 (c2:	01:0a:	Port ID	: FastEthernet0/0	
Fr Et	14 55.559055 15 59.992118 16 61.970869 rame 1: 60 bytes thernet II, Src: 2 Destination: c2 2 Source: c2:01:0 Type: Loopback onfiguration Test skipCount: 0 Relevant functi Function: Reply Receipt number: ata (40 bytes) Data: 000000000 [Length: 40]	c2:01:0a:84:00:00 c2:01:0a:84:00:00 c2:02:10:38:00:00 on wire (480 bits), 6 c2:01:0a:84:00:00 (c2:02 :01:0a:84:00:00 (c2:01:0a:10 (0x:000) Protocol (loopback) on: Reply (1) (1) 0	COP/VTP/DTP/PAgP/UD c2:01:0a:84:00:00 c2:02:10:38:00:00 0 bytes captured (480 b :01:0a:84:00:00), Dst: 1:0a:84:00:00) 34:00:00)	CDP LOOP LOOP vits) on c2:01:0e	359 C 60 R 60 R interfa :84:00:	Device I Reply Reply Cce 0 00 (c2:	01:0a:	Port ID	: FastEthernet0/0	
<ul> <li>Fr</li> <li>Et</li> <li>€</li> <li>€</li> <li>Cc</li> </ul>	14 55.559055 15 59.992118 16 61.9708069 rame 1: 60 bytes thernet II, Src: 2 Destination: c2 2 Source: c2:01:0 - Type: Loopback onfiguration Test - skipCount: 0 - Relevant functi - Function: Reply - Receipt number: ata (40 bytes) - Data: 000000000 - [Length: 40]	c2:01:0a:84:00:00 c2:01:0a:84:00:00 c2:02:10:38:00:00 c2:02:10:38:00:00 on wire (480 bits), 6 c2:01:0a:84:00:00 (c2:0 a:84:00:00 (c2:01:0a:1 (0x:900) Protocol (loopback) on: Reply (1) (1) 0	CDP/VTP/DTP/PAgP/UD. c2:01:0a:84:00:00 c2:02:10:38:00:00 0 bytes captured (480 b :01:0a:84:00:00), Dst: 1:0a:84:00:00) 34:00:00)	CDP LOOP LOOP wits) on c2:01:0a	359 C 60 R 60 R interfa :84:00:	Device I Reply Reply Cce 0 00 (c2:	D: R1	Port ID	: FastEthernet0/0	
- Fr - Et - Et - Da	14 55.559055 15 59.992118 16 61.9708069 rame 1: 60 bytes thernet II, Src: 2 Destination: c2 3 Source: c2:01:00 - Type: Loopback configuration Test - skipCount: 0 - Relevant functi - Function: Reply Receipt number: ata (40 bytes) Data: 00000000 - [Length: 40]	c2:01:0a:84:00:00 c2:01:0a:84:00:00 c2:02:10:38:00:00 c2:02:10:38:00:00 c2:02:10:38:00:00 c2:01:0a:84:00:00 c2:01:0a:84:00:00 c2:01:0a:84:00:00 c2:01:0a:84:00:00 c2:01:0a:84:00:00 c2:01 c0:000000000000000000000000000000000	CDP/VTP/DTP/PAgP/UD c2:01:0a:84:00:00 c2:02:10:38:00:00 0 bytes captured (480 b :01:0a:84:00:00) Dst: 1:0a:84:00:00) 34:00:00)	CDP LOOP LOOP sits) on c2:01:0a	359 C 60 R 60 R interfa :84:00:	Device I Reply Rep	D: R1	Port ID	: FastEthernet0/0	
Fr     Et     C     C     D     C     D     C     D     C     D	14 55.559055 15 59.992118 16 61.970869 rame 1: 60 bytes thernet II, Src: 2 Destination: c2 3 Source: c2:01:0 Type: Loopback onfiguration Test = skipCount: 0 - Relevant functi - Function: Reply - Data: 000000000 - [Length: 40] 0 c2 01 08 84 00 0 00 00 00 00	c2:01:0a:84:00:00 c2:01:0a:84:00:00 c2:02:10:38:00:00 on wire (430 bits), 6 c2:01:0a:84:00:00 (c2:02 :01:0a:84:00:00 (c2:02 :a:84:00:00 (c2:01:0a:1 (0x9000) Protocol (loopback) on: Reply (1) (1) 0 0 0000000000000000000000000000	CDP/VTP/DTP/PAgP/UD c2:01:0a:84:00:00 c2:02:10:38:00:00 bytes captured (480 b :01:0a:84:00:00) 34:00:00) 34:00:00) 30000000000000000000 0 90 00 00 00 0 90 00 00 00	CDP LOOP LOOP sits) on c2:01:0a	359 C 60 R 60 R interfa :84:00:	Device I Reply Rep	01:0a:	Port ID	: FastEthernet0/0	
Fr     Fr     C     C     C     D	14 55.559055 15 59.992118 16 61.970869 rame 1: 60 bytes thernet II, Src: 2 Destination: c2 5 Source: c2:01:0 Type: Loopback onfiguration Test skipCount: 0 Relevant functi Function: Reply Receipt number: ata (40 bytes) Data: 00000000 [Length: 40] 2 c2 01 0a 84 00 0 00 00 00 00	c2:01:0a:84:00:00           c2:01:0a:84:00:00           c2:01:0a:84:00:00           on wire (480 bits), 6           c2:01:0a:84:00:00 (c2:01           c1:0a:84:00:00 (c2:01:a:84:00:00 (c2:01:a:84:00:00 (c2:01:a:84:00:00 (c2:01:a:84:00:00)           Protocol (loopback)           on: Reply (1) (1) (1)           0           000 c2:01:0a:84:00:00           000 c2:01:0a:84:00:00           000 c2:01:0a:84:00:00           000 c2:01:0a:84:00:00           000 c2:01:0a:84:00:00           000 c2:01:0a:84:00:00           00:00:00:00:00:00:00:00:00:00:00:00:00:	CDP/VTP/DTP/PAgP/UD c2:01:0a:84:00:00 c2:02:10:38:00:00 0 bytes captured (480 b :01:0a:84:00:00), Dst: 1:0a:84:00:00) 34:00:00) 00000000000000000000 0 90 00 00 00 0 90 00 00 00 0 90 00 00 00	CDP LOOP LOOP vits) on c2:01:0a	359 C 60 R 60 R interfa ::84:00:	Device I Reply Reply Reply Cce 0 00 (c2:	D: R1	Port ID	: FastEthernet0/0	

# 4.2.2. Pengujian Jaringan Akhir

Pada pengujian jaringan akhir penulis akan coba melakukan test jaringan

VPN di router dan memastikan enkripsi data agar data aman.

a. Pengujian untuk memastikan EzVPN sudah aktif

cempaka#sh cry IPv4 Crypto IS	/pto isakmp sa SAKMP SA					
dst	src	state	conn-id	slot	status	
10.32.152.5	10.32.152.9	QM_IDLE	1001	0	ACTIVE	
IPv6 Crypto IS	SAKMP SA					

b. Pengujian melihat konfigurasi EzVPN



c. Pengujian data yang terenkripsi melalui IPSec

empaka#sh crypto ipsec sa
nterface: FastEthernet0/0
Crypto map tag: mymap, local addr 10.32.152.5
<pre>protected vrf: (none) local ident (addr/mask/prot/port): (C.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port): (192.168.2.0/255.255.0/C/D) current_peer 10.32.152.9 port 500 PERMIT, flags=() forte concernent 15 forte concernent 15 forte dispert 15</pre>
<pre>#pxts encaps: 15, #pxts encrypt: 15, #pxts digest: 15 #pxts decaps: 14, #pxts decrypt: 14, #pkts verify: 14</pre>
<pre>#pkts compressed: 0, #pkts decompressed: 0</pre>
<pre>#pkts not compressed: 0, #pkts compr. failed: 0</pre>
<pre>#pkts not deccmpressed: 0, #pkts deccmpress failed: 0</pre>
#send errors C, #recv errors 0
local crypto endpt.: 10.32.152.5, remote crypto endpt.: 10.32.152.9 path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0 current outbound spi: 0x29107822(688945186)
inbound esp sas:
spi: 0x815098EB(2169542891)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 1, flow_id: SW:1, cryptc map: mynap
sa tining: remaining key lifetime (k/sec): (4416208/3523)
IV SIZE: 6 Dytes
Status, ACTIVE
Deloust Marrie

d. Capture dengan Wireshark sesudah VPN

🔏 Captu	ring from Standa	rd input					
File Edit	View Go Captu	ure Analyze Statistics	Telephony Wireless T	ools Help			
	🔬 💿 🚺 🛗	🗙 🖸 🔍 🗢 🗢 🖻	s 🐨 🕹 🗐 🗐	ର୍ ପ୍ ପ୍ 🎹			
Apply	a display filter <0	Ctrl-/>		~			Expression +
No.	Time	Source	Destination	Protocol	Length Info		<b>_</b>
-	1 0.000000	10.32.152.5	10.32.152.9	ESP	150 ESP	(SPI=0x94958042)	
	2 0.062007	10.32.152.9	10.32.152.5	ESP	150 ESP	(SPI=0xa9e48da1)	
	3 1.102640	10.32.152.5	10.32.152.9	ESP	150 ESP	(SPI=0x94958042)	
	4 1.129643	10.32.152.9	10.32.152.5	ESP	150 ESP	(SPI=0xa9e48da1)	
	5 2.140771	10.32.152.5	10.32.152.9	ESP	150 ESP	(SPI=0x94958042)	
	6 2.170275	10.32.152.9	10.32.152.5	ESP	150 ESP	(SPI=0xa9e48da1)	
	7 3.267414	10.32.152.5	10.32.152.9	ESP	150 ESP	(SPI=0x94958042)	
	8 3.357926	10.32.152.9	10.32.152.5	ESP	150 ESP	(SPI=0xa9e48da1)	
	9 4.481569	10.32.152.5	10.32.152.9	ESP	150 ESP	(SPI=0x94958042)	
	10 4.549577	10.32.152.9	10.32.152.5	ESP	150 ESP	(SPI=0xa9e48da1)	•
T P H S D	ime to live: 2 rotocol: Encap eader checksum ource: 10.32.1 estination: 10 Source Seorr. Destination Ge	<pre>155 9 Security Payload 1: 0x76a7 [validation 1:52.5 9.32.152.9 0 Ontoion ] toIP: Unknown]</pre>	(50) on disabled]				
Enca	psulating Secu	urity Payload	(				
E	SP SPI: 0x9495	8042 (2492825666)	)				
L L E	SP Sequence: 4	10	<i>6</i>				•
0000 0010 0020 0030 0040	02 01 11 5c 00 00 88 00 4e 00 98 09 94 95 80 c2 cb c3 9b cd 66 6e 83 ff 10	00 c2 02 01 e4 00 00 ff 32 76 a7 00 0 42 00 00 00 28 dd 0 3 2c bd 68 3c 3- 5 a e4 81 b7 9d 1:	0 00 08 00 45 00 a 20 98 05 0a 20 a 73 39 c5 fc 6a 4 62 cd 76 f7 aa 1 7d da e5 a5 1b	\	E.  9j .v		
7 Re	ady to load or captu	re				Packets: 202 · Displayed: 202 (100.0%)	Profile: Default
100							II

Jadi dengan VPN data menjadi aman karena setiap lalu lintas data terbungkus dengan aman sehingga data tidak disalah gunakan oleh orang yang tidak bertanggung jawab.