BAB IV

RANCANGAN JARINGAN USULAN

4.1. Jaringan Usulan

Setelah penulis analisa sistem jaringan di Rumah Sakit Abdi Waluyo maka penulis menambahkan jaringan *Virtual Private Network* (VPN) untuk menghubungkan jaringan yang ada di kantor pusat ke kantor cabang atau sebaliknya.

Pada instansi pemerintah atau perusahaan swasta lainnya pasti memiliki kantor cabang di beda lokasi. Kantor cabang tersebut memiliki kebutuhan untuk saling berhubungan dengan kantor pusat. Solusi yang biasa digunakan adalah dengan membangun jaringan *private* yang menghubungkan kantor pusat dengan kantor cabang atau sebaliknya, yaitu *Wide Area Network* (WAN). Dengan berkembangannya jaringan public atau disebut dengan internet, solusi dengan membangun WAN ini adalah solusi yang efektif dan efisien. Dengan berkembangnya *Virtual Private Network* (VPN), sebuah organisai dapat membangun jaringan *private* diatas jaringan publik untuk menghubungkan antara kantor pusat dan kantor cabang atau sebaliknya.

4.1.1. Topologi Jaringan

Topologi jaringan saat ini memungkinkan terjadinya kejahatan komputer pada sisi *client* yaitu *manipulation computer* akan mengganti informasi dalam data yang dikirimkan. Jaringan distribusi yang telah dijabarkan penulis pada gambaran umum pada Rumah Sakit Abdi Waluyo sehingga untuk mengetahui komunikasi diantara perangkat jaringan yang berkomunikasi dan dapat memanipulasi data yang diterima.

Hal ini lah yang menjadi kekhawatiran untuk *client* yang mengerti kinerja dan sebuah jaringan dan ancaman bagi kerahasian informasi yang dimiliki Rumah Sakit Abdi Waluyo. Permasalahan inilah yang harus disadari oleh penggunaan internet yang memiliki kerentanan data dan ini bisa saja menjadi kerugian instansi itu sendiri, apalagi Rumah Sakit Abdi Waluyo memiliki data data pasien yang tidak boleh di sebarluaskan. VPN *site to site* merupakan solusi dari permasalahan yang ada untuk mengamankan jalur distribusi jaringan. Berikut adalah gambar topologi usulan dari penulis.



Sumber : Rumah Sakit Abdi Waluyo Gambar IV.1 Topologi Jaringan Usulan

4.1.2. Skema Jaringan

Skema jaringan yang hendak diusulkan tidak jauh berbeda dengan skema jaringan dalam sistem berjalan. Ditambah sebuah mikrotik untuk membuat jaringan VPN yang berfungsi sebagai penyambung jaringan di kantor pusat dan kantor cabang yang terjamin keamanannya. Berikut adalah gambar skema jaringan usulan.



Sumber : Rumah Sakit Abdi Waluyo Gambar IV.2 Skema Jaringan Usulan

4.1.3. Keamanan Jaringan

Pada keamanan jaringan di Rumah Sakit Abdi Waluyo masih kurang baik, karena setiap *user* yang dapat mengakses jaringan *wifi* dapat langsung terhubung dengan jaringan lokal pada Rumah Sakit Abdi Waluyo, sehingga memberikan kemudahaan pada *user* untuk mengakses *server* dan data yang tidak diinginkan yang berada pada jaringan tersebut, meskipun untuk megakses *server* tersebut harus memasukan *user* dan *password*. Tentu saja dengan menggunakan VPN dengan *protocol* PPTP semua *client* diharuskan ,masuk terlebih dahulu menggunakan *username* dan *password* selain itu ada juga pengaturan untuk melakukan pembatasan *IP Address* yang diperbolehkan untuk masuk ke jaringan tersebut.

Maka dari itu Rumah Sakit Abdi Waluyo menggunakan sistem keamanan jaringan berupa *Enkripsi MAC Addres* pada *PC Client* yang tujuannya hanya satu *user* dan satu *PC Client* yang dapat terkoneksi ke VPN *Server*.

4.1.4. Rancangan Aplikasi

Rancangan aplikasi jaringan yang dapat diusulkan untuk menghadapi permasalahan yang ada di Rumah Sakit Abdi Waluyo adalah diimplementasikan jaringan VPN yang berfungsi menghubungkan antar kantor yang berbeda yaitu kantor pusat dan kantor cabang. Hal ini dapat membuat karyawan yang di kantor cabang dapat mengakses server yang ada di kantor pusat. Baik menambahkan data atau mengambil data tanpa perantara seperti *flashdisk* atau melalui *e-mail*.

Berikut ini adalah langkah-langkah konfigurasi VPN menggunakan *mikrotik*.

1. Setelah kita mendapatkan IP Standard dari Transmitter,masuk ke IP tersebut melalui Browser,masukan default user dan passwordnya dalam hal ini adalah ubnt



2. .Setelah masuk user interface,pilih "Wireless",hal yang perlu di perhatikan untuk setting transmitter ini adalah,

Setting Wireless Mode ke Access point WDS SSID = ganti SSID sesuai dengan yang kita inginkan

Hide SSID = berfungsi agar SSID tidak go public atau di sembunyikan

Setting Security key ke WPA dan masukan password yang kita mau

(192.168.1 link.cgi			C Q Search	2	☆ 自	÷	命の	
NanoStation2 Main Wireless Networ	K ADVANCED	SERVICES	SYSTEM	Tools:	<u>air</u> 0 	S [™]		
BASIC WIRELESS SETTINGS								
Wireless Mode:[7]	Access Point W	DS 💌	Auto			- 1		
WDS Peers:						- 1		
SSID:	-		Hide SSID					
Country Code:	INDONESIA		-	Change				
IEEE 802.11 Mode:	B/G mixed 💌							
Channel Spectrum Width:[?]	20MHz 💌 Max	Datarate: 54	Mbps			- 1		
Channel Shifting:	Enabled 💌							
Channel:	3 - 2422 MHz	-						
Output Power:			10 dBm	Auto EIRP re	gulatory limiter			
Data Rate, Mbps:	54 💌 🗸 Auto	0						
WIRELESS SECURITY								
Security:	WPA 💌	1						
Authentication Type:	Open Sha	ared Key						
WEP Key Length:	64 bit 👻		Key Type:	HEX 👻				
WEP Key:			Key Index:	1 -				
WPA Preshared Key:								
MAC ACL:	Enabled		Policy:	Allow 👻				
				~				
				Remove				

3.lalu kita setting receiver,gunakan browser untuk masuk ke IP receiver dan masukan user dan password default dalam hal ini ubnt

◆ ◆ ③ 192.168.1 ■ login.cgi		C Search	☆	•	A	Q	≡
	<i>all</i> US	Username: Password:					
		Login					

4. setelah masuk user interface pilih "Wireless", lalu setting receiver seperti berikut,

Ganti Wireless Mode menjadi Station WDS

Isi ESSID sesuai dengan SSID yang kita berikan di transmitter

Lock to AP MAC berfungsi untuk mengunci mac address transmitter agar receiver tidak menerima sinyal dari pihak lain,isi dengan mac address transmitter Ganti security dengan WPA dan masukan password yang sama dengan yang kita gunakan di transmitter.

(192.168.1. Hink.cgi	C	Q. Search	☆ 自 🕹 合 오 💟	Ξ
NanoStation2			air OS [*]	
MAIN WIRELESS NETWORK A	DVANCED SERVICES SYSTE	EM Tools:	Logout	
BASIC WIRELESS SETTINGS				
Wireless Mode:[7]	Station WDS			
ESSID:	Se	lect		
Lock to AP MAC:				
Country Code:	INDONESIA	✓ Change		
IEEE 802.11 Mode:	B/G mixed 💌			
Channel Spectrum Width:[2]	20MHz 💌 Max Datarate: 54Mb	ops		
Channel Shifting:[2]	Enabled 💌			
Channel Scan List:	Enabled 10	Edit	THE REAL PROPERTY OF THE PROPERTY OF THE REAL PROPE	
Output Power:	26	dBm Auto EIRP regulate	ory limiter	
Data Rate, Mbps:	54 💌 🗸 Auto			
WIRELESS SECURITY				
Security:	WPA 💌			
Authentication Type:	Open Shared Key			
WEP Key Length:	64 bit 👻 Key	Type: HEX 👻		
WEP Key:	Key	Index: 1 -		
WPA Authentication:	PSK - EAP-TTLS - MSCH	HAPV2 =		
WPA Preshared Key:				
WPA Anonymous Identity:				
WPA User Name:				
WFA USCI Fassword.				
	Change		0100001000010100000	

4.2. Pengujian Jaringan

Dalam hal pengujian jaringan usulan, penulis mencoba melalukan pengujian jaringan dengan dua langkah, yaitu :

4.2.1. Pengujian Jaringan Awal

Menggunakan VPN akan memberikan keamanan yng maksimal karena akan dilakukan *enkripsi* pada paket data yang melaluinya.berikut hasil capture penulis mencoba jaringan awal,

C Windows syst	empi o	nd exe - Ping	5.5.8.5 -1		ш ц
ply from ply from quest times	out.	bytes=32 bytes=32	tine=44ms tine=49ms	TIL=46 TIL=46	
ly from ly from	aut.	bytes=32 bytes=32	tine=52ms tine=52ms	TTL=46 TTL=46	
ly from	out.	bytes=32 bytes=32	tine=45ms tine=44ms	TTL=46 TTL=46	
ly from uest timed uest timed uest timed	out.	bytes=32	tine=43ns	TTL=46	
ly from 8.8	.8.8:	bytes=32	tine=45ms	TTL=46	
ly from ly from		hytes=32 bytes=32	tine=44ms	TTL-46 TTL-46	
ly from ly from uest timed uest timed	out.	hytes=32 bytes=32	tine=44ns tine=44ns	TTL=46 TTL=46	
ly from	in a start	hytes=32	tine=43ms	TTL=46	

4.2.2. Pengujian Jaringan Akhir

Evaluasi jaringan dengan VPN ini dilakukan dengan melihat posisi transmitter dan receiver, berikut hasil capture penulis setelah evaluasi,

1000		and the second s		and the second
ply	from	bytes=32	time<1ms	TTL=64
ply	from	bytes=32	time<1ms	TTL=64
ply	from	bytes=32	time<1ms	TTL=64
ply	from	bytes=32	time<1ms	TTL=64
ply	from	bytes=32	time<1ms	TTL=64
ply	from	bytes=32	time<1ms	TTL=64
ply	from	bytes=32	time<1ms	TTL=64
ply	from	bytes=32	time<1ms	TTL=64
ply	from	bytes=32	time<1ms	TTL=64
ply	from	bytes=32	time<1ms	TTL=64
ply	from	bytes=32	time<1ms	TTL=64
ply	from	bytes=32	time<1ms	TTL=64
ply	from	bytes=32	time<1ms	TTL=64
ply	from	bytes=32	time<1ms	TTL=64
ply	from	bytes=32	time<1ms	TTL=64
ply	from	bytes=32	time<1ms	TTL=64
ply	from	bytes=32	time<1ms	TTL=64
ply	from	bytes=32	time<1ms	TTL=64
ply	from	bytes=32	time<1ms	TTL=64
ply	from	bytes=32	time<1ms	TTL=64
ply	from	bytes=32	time<1ms	TTL=64
ply	from	bytes=32	time<1ms	TTL=64
ply	from	bytes=32	time<1ms	TTL=64
ply	from	bytes=32	time<1ms	TTL=64
ply	from	bytes=32	time<1ms	TTL=64
ply	from	bytes=32	time<1ms	TTL=64
ply	from	bytes=32	time<1ms	TTL=64
ply	from	bytes=32	time<1ms	TTL=64
ply	from	bytes=32	time<1ms	TTL=64

Dari hasil pengujian dengan menggunakan VPN, komputer pusat dan komputer cabang sudah terhubung dan lancar, dan tidak terganggu.