IMPLEMENTASI KONSEP MULTI-NAS DENGAN MENGINTEGRASIKAN VPN SERVER DAN FREERADIUS SERVER DALAM MEMBANGUN SISTEM OTENTIKASI JARINGAN WIFI

Muh. Ibnu Habil Hanafi¹, Suwanto Raharjo², Suraya³

^{1,2,3} Teknik Informatika, institut Sains & Teknologi AKPRIND Yogyakarta ¹ <u>ibnu.habil.h@gmail.com</u>, ² <u>wa2n@akprind.ac.id</u>, ³ <u>suraya_pandev@yahoo.com</u>

ABSTRACT

Some of WiFi networks is only provided the security with default security system, and some have not any security, and also the users management system for people who use the WiFi is not available. It can be occurred because a lack of oversight on development and maintenance the resources of WiFi network services. By analyzing the problems, it will be possible to get the best solution to generates a secure WiFi network services. Steps done in process of designing a network infrastructure on solution to generates a secure WiFi network services, Multi-NAS concept with FreeRADIUS server as authentication method and integration methods of VPN with FreeRADIUS server is can be used to support the purpose of designed network infrastructure. By implementing of those methods will be able to increase the security of WiFi network and user internet access. In the implementation process, data analysis is required to applying those methods in as an analysis infrastructure requirements by referring to the system that runs in infrastructure as basic knowledge of Linux, Mikrotik and Computer Networks. Thereby, implementation the method of authentication system on infrastructure will be provide a good security in the WiFi network and provide a secure users internet access of WiFi network.

Keywords: WiFi, Server, FreeRADIUS, Network.

INTISARI

Beberapa jaringan *WiFi* yang tersedia di lingkungan publik hanya menggunakan sistem keamanan yang sudah tersedia yaitu keamanan dasar, dan bahkan ada yang tidak menggunakan sistem keamanan apapun, dan juga untuk pengelolaan pengguna yang menggunakan jaringan *WiFi* tidak disediakan. Hal tersebut dapat terjadi karena kurangnya pengawasan terhadap pengembangan dan pemeliharaan sumber daya layanan jaringan *WiFi*. Dengan melakukan analisa terhadap permasalahan tersebut, maka akan dimungkinkan untuk mendapatkan solusi terbaik dalam menghasilkan sebuah layanan jaringan *WiFi* yang aman.

Tahap yang dilakukan dalam proses perancangan infrastruktur jaringan dalam menghasilkan solusi membuat layanan jaringan *WiFi* yang aman, penggunaan konsep *Multi-NAS* dengan metode sistem otentikasi *FreeRADIUS server* dan metode integrasi *VPN* dengan *FreeRADIUS server* dapat digunakan untuk mendukung tujuan perancangan infrastruktur jaringan. Dengan implementasi dari metode-metode tersebut akan dapat meningkatkan keamanan pada sisi jaringan *WiFi* dan pengguna. Dalam proses implementasinya, analisa data diperlukan untuk dapat menerapkan metode tersebut yang berupa analisa terhadap kebutuhan infrastruktur dengan mengacu pada sistem yang berjalan dalam infrastruktur yaitu berupa pengetahuan dasar mengenai *Linux, Mikrotik* dan Jaringan Komputer.

Dengan demikian, penerapan infrastruktur dengan metode sistem otentikasi akan memberikan keamanan yang baik pada jaringan *WiFi* dan akses internet pengguna jaringan *WiFi*.

Kata kunci: WiFi, Server, FreeRADIUS, Jaringan.

PENDAHULUAN

Menghadapi perkembangan jaman yang penuh dengan kegiatan akses data untuk memenuhi kebutuhan informasi pada lingkungan global seperti sekarang ini yang hampir semua aktivitas dilakukan secara *mobile* dengan mengandalkan jaringan nirkabel yang dianggap sangat fleksibel, sudah sewajarnya harus melakukan analisa terhadap kebutuhan dan keamanan pada jaringan yang disediakan untuk mengurangi dampak akibat dari kurangnya keamanan pada jaringan *Wireless Fidelity (WiFi)* yang tersedia. Beberapa jaringan *WiFi* yang

tersedia di lingkungan publik hanya menggunakan sistem keamanan yang sudah tersedia (keamanan dasar), seperti *Wired Equivalent Privacy (WEP), WiFi Protected Access (WPA)* serta *WiFi Protected Access II (WPA2)* dan bahkan ada yang tidak menggunakan sistem keamanan apapun, dan juga untuk pengelolaan pengguna yang menggunakan jaringan *WiFi* tersebut juga hampir tidak disediakan. Hal ini banyak diabaikan oleh pengguna dan juga mayoritas tidak diketahui oleh pengguna, kemungkinan yang tidak diingikan mungkin bisa terjadi, seperti gangguan pada jaringan *WiFi* tersebut karena kurangnya keamanan yang diterapkan, ataupun dikarenakan banyaknya pengguna yang menggunakan sebuah titik akses *WiFi* yang menyebabkan jaringan tidak dapat berjalan dengan baik, karena tidak adanya pengelolaan pengguna yang tertata.

Dalam proses penyediaan layanan jaringan *WiFi* yang bermutu, dari beberapa metode yang sering digunakan yaitu metode otentikasi *server* berupa *RADIUS server*. Penggunaan otentikasi *server* ditujukan untuk mendukung keamanan proses otentikasi jaringan untuk dapat menjadi lebih baik karena *server* yang akan bertindak langsung untuk mengotentikasi *dial-in* pengguna dan mengotorisasi *request* ke layanan yang disediakan. Disamping itu, *RADIUS* juga memiliki sistem *user management* yang memberikan kemudahan dalam pengelolaan profil pengguna dengan menggunakan *database* serta dapat mengatur kebijakan tertentu terhadap data dari profil pengguna. Selain dari metode otentikasi *server*, penggunaan perangkat-perangkat *NAS* (*Network Access Server*) berupa Mikrotik sebagai *hotspot server* dan *VPN* (*Virtual Private Network*) untuk mengenkapsulasi lalu lintas koneksi internet pengguna juga diperlukan dengan mengintegrasikan ke dalam infrastruktur sistem otentikasi sebagai *Multi-NAS* yang dapat memberikan keamanan akses internet yang lebih baik untuk pengguna.

Dengan demikian, untuk menghasilkan solusi jaringan *WiFi* yang bermutu dibutuhkan penerapan sistem keamanan pendukung untuk menyediakan jaringan *WiFi* yang aman serta pengelolaan pengguna yang tertata melalui sistem otentikasi *FreeRADIUS server* dan integrasi konsep *Multi-NAS* dengan tujuan untuk memudahkan pengelolaan pengguna, pemeliharan sumber daya jaringan, meningkatkan keamanan akses internet dan jaringan *WiFi*.

Dalam penelitian ini, rumusan masalah yang tercakup dalam penelitian yang dilakukan diantaranya yaitu bagaimana meningkatkan keamanan jaringan *WiFi* dengan implementasi sistem otentikasi *FreeRADIUS Server*, Bagaimana mengintegrasikan konsep *Multi-NAS* dengan menggunakan *VPN Server* terhadap sistem otentikasi *FreeRADIUS Server*, Bagaimana cara implementasi sistem otentikasi *FreeRADIUS* terhadap jaringan *hotspot server* pada Mikrotik dan Bagaimana implementasi *low cost* (biaya rendah) pada sektor *IT (Information Technology)* dengan memanfaatkan aplikasi berlisensi *opensource* untuk menunjang infrastruktur jaringan *WiFi*.

Untuk Tujuan dari penelitian ini adalah membangun infrastruktur jaringan dengan sistem terintegrasi dalam proses otentikasi jaringan *WiFi* dan keamanan lalu lintas jaringan untuk meningkatkan keamanan pengguna dalam mengakses internet menggunakan jaringan *WiFi*

TINJAUAN PUSTAKA

Dalam melaksanakan penelitian ini digunakan beberapa referensi yang berhubungan dengan objek penelitian terutama dari penelitian-penelitian sebelumnya, ditantaranya yaitu penelitian tentang bagaimana membangun *captive portal* sebagai otentikasi *user*, dan memanajemen *client* pada jaringan *WiFi Hotspot* (Rofiq, 2009). Penelitian tentang sistem AAA (*Authentication, Authorization, Accounting*) dalam proses memilih dan menentukan *software* yang berfungsi untuk otentikasi *user*, menganalisa dan membandingkan *software* yang berfungsi sebagai *captive portal* (Lubis, 2010). Kemudian penelitian mengenai pemanfaatan teknologi Mikrotik dalam membangun jaringan *WiFi Hotspot* (Prabowo, 2012). Penelitian dalam memanfaatkan dan menggunakan *Linux* sebagai teknologi *Opensource* untuk membangun *RADIUS Server* (Hadi, 2012).

Pada penelitian sebelumnya mengenai sistem otentikasi *FreeRADIUS server* pada jaringan *WiFi* (Hanafi, 2014), dalam otentikasi jaringan tanpa kabel (*Wireless*) masih belum menggunakan metode pendukung terhadap teknologi Mikrotik sebagai *Hotspot Server* dengan *FreeRADIUS* sebagai *RADIUS Server* dan hanya sebatas implementasi sistem otentikasi dari teknologi tersebut.

WiFi merupakan singkatan dari *Wireless Fidelity*, yang memiliki pengertian yaitu sekumpulan standar yang digunakan untuk jaringan lokal nirkabel (*Wireless Local Area Networks – WLAN*) yang didasari pada spesifikasi IEEE 802.11 (Arifin, 2006). Standar terbaru dari spesifikasi 802.11a atau b, seperti 802.11g saat ini sedang dalam penyusunan, spesifikasi terbaru tersebut menawarkan banyak peningkatan mulai dari luas cakupan yang lebih jauh hingga kecepatan transfernya.

Mikrotik adalah sistem operasi dan perangkat lunak yang digunakan untuk memfungsikan komputer sebagai *router* (Herlambang, dkk, 2008). *PC router* tersebut dilengkapi dengan berbagai fasilitas dan alat, baik untuk jaringan kabel maupun nirkabel. Pada standar perangkat keras berbasiskan *Personal Computer (PC)* mikrotik dikenal dengan kestabilan, kualitas kontrol dan fleksibilitas untuk berbagai jenis paket data dan penanganan proses rute atau lebih dikenal dengan istilah *routing*. Sedangkan aplikasi yang dapat diterapkan dengan Mikrotil selain *routing* adalah aplikasi kapasitas akses (*bandwidth*), manajemen, *firewall*, *wireless access point (WiFi), backhaul link*, sistem *hotspot*, *Virtual Private Network (VPN) server* dan masih banyak lainnya.

RADIUS adalah singkatan dari (Remote Access Dial In User Service). RADIUS menjadi bagian dari solusi AAA (Authentication, Authorization, Accounting) yang berikan oleh Livingston Enterprises ke Merit Network pada tahun 1991 (Walt, 2011). Merit Network adalah sebuah perusahaan penyedia jasa internet non-profit, yang membutuhkan suatu cara kreatif untuk mengelola akses dial-in ke berbagai Points-Of-Presence (POP) di dalam jaringan. Solusi yang disediakan oleh Livingston Enterprises adalah pusat penyimpanan data user pada berbagai macam RAS (dial-in) server yang digunakan untuk otentikasi, otorisasi dan akuntasi. Pengguna mendapatkan akses data ke suatu jaringan dan sumber dayanya melalui berbagai jenis perangkat seperti Ethernet switches, WiFi dan VPN server yang semua itu menawarkan akses jaringan. Semua perangkat tersebut perlu menggunakan beberapa bentuk kontrol untuk memastikan keamanan dan penggunaan yang tepat. Persyaratan ini biasanya dideskripsikan sebagai authentication, authorization dan accounting (AAA) atau terkadang juga disebut dengan Triple A Framework. Network Access Server (NAS) adalah sebuah perangkat yang mengontrol akses ke suatu jaringan, seperti VPN server yang bertindak sebagai klien RADIUS (Schmid, dkk, 1999). Di dalam FreeRADIUS, NAS bertindak sebagai broker untuk meneruskan request pengguna ke FreeRADIUS server. Perangkat-perangkat NAS yang digunakan di dalam sebuah infrastruktur jaringan yang memiliki radius server dalam menyediakan akses untuk komunikasi data radius server disebut sebagai Multi-NAS.

FreeRADIUS merupakan sebuah proyek *opensource* yang menyediakan implementasi kaya fitur dari protokol *RADIUS* dengan berbagai sitem tambahan (Walt, 2011). Pengembangan *FreeRADIUS* dimulai pada tahun 1999 setelah masa depan *RADIUS Server Livingston* menjadi tidak menentu. Hal ini memungkinkan untuk menciptakan *RADIUS Server* baru yang *opensource* dan dapat mencakup keterlibatan masyarakat secara aktif.

DaloRADIUS merupakan RADIUS web platform. Pada dasarnya platform ini digunakan untuk mengelola RADIUS server sehingga secara teoritis dapat mengelola semua RADIUS server namun secara khusus adalah untuk mengelola FreeRADIUS dan struktur databasenya (Tal, 2012). Sebagai aplikasi berbasis web, DaloRADIUS berperan sebagai konsol manajemen untuk mengontrol semua aspek dari RADIUS server sekaligus menyediakan fitur komersial dan professional seperti manajemen user, informasi akuntansi, laporan dalam bentuk grafis, sistem penagihan, serta integrasi dengan layanan GoogleMaps untuk geo-lokasi NAS server dan Hotspot center.

Virtual Private Network (VPN) adalah sebuah teknologi jaringan komputer yang dikembangkan oleh perusahaan skala besar yang menghubungkan antar jaringan diatas jaringan lain menggunakan internet yang membutuhkan jalur *privacy* dalam komunikasinya (Forouzan, 2007). Sifat pribadi VPN berarti bahwa trafik data VPN pada umumnya tidak terlihat atau dienkapsulasi lalu lintas jaringan yang mendasarinya. Dalam istilah lainnya, VPN merupakan cara untuk mensimulasikan jaringan pribadi melalui jaringan publik, seperti internet (Scott, dkk, 1999). Hal ini dikenal sebagai "*virtual*" karena bergantung pada koneksi virtual yaitu koneksi sementara yang tidak memiliki *physical presence*, tetapi terdiri dari paket yang dikirimkan melewati berbagai mesin di internet. Didalam teknologi yang digunakan VPN untuk melindungi komunikasi data di dalam jaringan *internet*, terdapat diantaranya konsep penting yang dapat digunakan seperti *firewall*, otentikasi, enskripsi dan *tunneling*.

METODOLOGI PENELITIAN

Metodologi penelitian yang dilakukan berupa analisa data. Tahap analisis ini merupakan tahap yang sangat penting karena kesalahan pada tahap ini dapat mengakibatkan kesalahan pada tahap selanjutnya sehingga dibutuhkan suatu metode yang dapat digunakan sebagai pedoman dalam pengerjaan proses berikutnya. Data-data yang diperlukan untuk melakukan penelitan ini antara lain:

- 1. Pengetahuan tentang sistem operasi *Linux*
- 2. Mengetahui tentang tata kelola *Linux Server*
- 3. Mengetahui dasar penggunaan Mikrotik
- 4. Mengetahui konsep dasar jaringan *Wireless*
- 5. Pemahaman tentang dasar-dasar jaringan computer

Pada penelitian ini, terdapat beberapa bahan dan alat penelitian atas kebutuhan infrastruktur yang akan diterapkan, diantaranya yaitu:

- 1. Bahan Penelitian
 - Simulasi admin sebagai pengelola infrastruktur
 - Data klien sementara sebagai pengguna untuk uji coba infrastruktur
- 2. Alat Penelitian Berupa Hardware
 - Komputer Server
 - VPS
 - Access Point
 - Modem USB
 - Kabel UTP
 - Mikrotik
 - Perangkat Klien
- 3. Alat Penelitian Berupa Software
 - FreeRADIUS Server
 - DaloRADIUS
 - OpenVPN Server

Perancangan infrastruktur pada penelitian ini dengan berupa sistem otentikasi jaringan dapat digambarkan seperti yang tampak pada gambar 1 berikut ini:



Gambar 1. Rancangan insfrastruktur jaringan

Keterangan gambar rancangan infrastruktur jaringan di atas adalah sebagai berikut:

	: Jalur proses kerja Mikrotik <i>Hotspot</i>
\longrightarrow	: Proses otentikasi FreeRADIUS server terhadap login user
	: Proses otentikasi FreeRADIUS server terhadap OpenVPN server
	: Hasil dari proses otentikasi Login User
	: Hasil dari proses otentikasi VPN User
	: Jalur akses internet modem USB sebagai Gateway

Dalam penelitian ini dibuat perencanaan untuk menguji infrastruktur jaringan. Perencanaan dalam proses pengujian terhadap infrastruktur jaringan yang telah dibuat adalah untuk mendapatkan hasil dari proses implementasi yang akan dikerjakan. Adapun rencana yang akan dilakukan guna mendapatkan hasil pengujian terhadap infrastruktur jaringan yang telah dibuat adalah sebagai berikut:

- 1. Melakukan pengujian sistem otentikasi FreeRADIUS terhadap jaringan WiFi.
- 2. Melakukan pengujian sistem otentikasi *FreeRADIUS* terhadap penggunaan *VPN.*
- 3. Melakukan pengujian menggunakan 2 macam *provider* internet dalam hal membandingkan koneksi internet saat menggunakan dan tanpa *VPN* dengan memakai *tool traceroute.*

PEMBAHASAN

Pengujian sistem otentikasi terhadap implementasi otentikasi data *user FreeRADIUS server*, akan dilakukan dengan menggunakan perangkat komputer yaitu komputer *laptop*. Untuk memastikan *user* yang digunakan berhasil terotentikasi dan masuk ke dalam jaringan *WiFi*, dapat melakukan pemeriksaan pada *log* Mikrotik dengan menggunakan *software winbox* seperti yang ditunjukkan pada gambar 2.

			all	₹
Jan/02/1970 00:00:08	system info	router rebooted		
Jan/02/1970 00:00:12	interface info	ether1 link up (speed 100M, full duplex)		
Jan/02/1970 00:00:12	interface info	ether2 link up (speed 100M, full duplex)		
Jan/02/1970 00:01:19	system info account	user admin logged in from 100.2.50.1 via winbox		
Jan/02/1970 00:03:51	dhcp info	dhcp1 deassigned 10.18.0.7 from 2C:D0:5A:40:F8:FF		
Jan/02/1970 00:03:51	dhcp info	dhcp1 assigned 10.18.0.7 to 2C:D0:5A:40:F8:FF		
Jan/02/1970 00:04:56	hotspot info debug	localU1 (10.18.0.7): trying to log in by http-chap		
Jan/02/1970 00:04:56	hotspot account i	localU1 (10.18.0.7): logged in		

Gambar 2. Isi log dari Mikrotik

Pada gambar 2, di bagian akhir dari *log* terlihat data *login* yang digunakan oleh pengguna berhasil terhubung ke dalam jaringan *WiFi*. Dari *log* tersebut terbukti bahwa data *user* berhasil terotentikasi oleh *FreeRADIUS* server dengan terhubungnya *user* tersebut ke dalam jaringan. Bila data *user* yang digunakan tidak benar maka proses otentikasi tidak akan berhasil dan otomatis *user* juga tidak akan berhasil masuk ke dalam jaringan *WiFi* terlebih lagi untuk mengakses internet.

Kemudian pengujian selanjutnya yaitu pengujian otentikasi terhadap data user *OpenVPN*. Pengujian yang dilakukan terhadap salah satu *VPN server*. *User* yang sebelumnya telah terhubung ke dalam jaringan *WiFi* dan telah dapat mengakses internet maka dengan demikian *user* tersebut dapat langsung mencoba menggunakan *VPN*. Perlu untuk diperhatikan, syarat utama untuk dapat menggunakan dan terhubung ke jaringan *VPN* harus terlebih dahulu memiliki akses internet, jika tidak ada akses internet maka akan tidak mungkin dapat menggunakan *VPN*.

Penggunaan VPN dari sisi user memerlukan software openvpn client, dan dalam pengujian yang dilakukan menggunakan *linux* yang sudah terinstall openvpn client. Untuk dapat menggunakan VPN, user terlebih dahulu memerlukan file-file certificate yang sudah dibuat dari server yang terdiri dari ca.crt, ta.key, radmin.ovpn. Proses koneksi jaringan VPN memerlukan data user untuk dapat masuk ke jaringan VPN. Data user diperlukan karena sistem dibuat dengan mengintegrasikan VPN terhadap FreeRADIUS sehingga dengan demikian user FreeRADIUS yang akan digunakan oleh VPN.

pplications Places	9	1	122	423.	D	(38%)	45	7:48 PM	0
0 0 freedom@404: -/VPN/uclaud2									
lle Edit View Search Terminal Help									
B. DBA Vers Sanch Termand Imp engements-1-6 youryUndary and particular the provide state of the provide state of the provide and particular for freedom: and particular for freedom: and particular for freedom: the provide state of the provide state of the provide state for the particular for freedom in the provide state of the provide state for the provide state of the provide state of the provide state of the provide state of the provide state of the provide state of the provide state of the provide state state of the provide state of the provide state of the provide state of the provide state of the provide state of the provide state of the provide state of the provide state state of the provide state of the provide state of the provide state of the provide state state of the provide state of the provide state of the provide state of the provide state of the provide state of the provide state of the provide state of the provide state state of the provide state of the provide state of the provide state state of the provide state state of the provide state of the provide state of the provide state state of the provide state state of the provide state of the provide state of the provide state of the provide state of the provide state state of the provide state state of the provide state of] [Per C aut C aut Optic	H] [then then	1Pv6 tica] but tion tion	lt on	ı Feb	4 201	•]	

Gambar 3. Proses otentikasi user VPN

Seperti yang tampak pada gambar 3, saat perintah untuk menjalankan openvpn client dieksekusi maka akan muncul proses yang meminta *user* untuk memasukkan data *username & password* yang telah dimiliki, disaat itulah proses otentikasi dari *FreeRADIUS* akan berlangsung dan apabila data *user* yang dimasukkan valid maka proses ekseskusi akan diteruskan dan jika data *user* tidak valid maka proses akan dihentikan.

Proses otentikasi telah berhasil ditandai dengan status *initialization sequence completed.* Dengan mendapatkan status tersebut maka hal itu menandakan *VPN* telah berhasil terhubung, seperti yang ditunjukkan pada gambar 4.

Application	ns Places																				2 .	4	22.0	12	DO	7%)	45	7:49 PM
000										free	edom(p404	1:-/1	PN/u	cloud	12												
rile tdit	View Se	rch Te	minal	rielp																								
ue Dec 9	9 19:48:	8.2014	VERIF	OK:	Septh=1	. C=ID.	. ST=D	DIY.	LeY	'ogya	karti	a. 0	-VPP	N-Net	work	. 0	Uncha	ngem	. CN-	Serv	er, s	ane-	Serv	ver.	enall	Addr	ess-r	all@frost
g.con																												
ue Dec 1	9 19:48:	8 2014	VERIF	OK: 1	scertT	ype=SER	RVER																					
ue Dec 1	9 19:48:	8 2014	VERIF	OKI	Septh=8	, C=ID,	, ST=D	δIΥ,	L=Y	ogya	ikarta	a, 0	I=VPf	N-Net	work	, 0	U+Ser	ver,	CN=Se	rver	, nar	e+Se	rver	r, er	satlAd	dres	s-nat	løfrostbi
con																												
ue Dec 1	9 19:48:	9 2014	Data	hanne	1 Encry	pt: Cip	pher '	'BF-0	C8C1	ful	tial	ized	I WL	th 12	s bt	t h	ey											
ue Dec 1	9 19:48:	9 2614	Data	hanne'	L Encry	pt: Usi	ing 16	58 b1	it m	10558	ige hi	ash	'SH/	41' f	or H	MAC	auth	entle	ation									
ue Dec 1	9 19:48:	9 2014	Data	hanne'	i Decry	pt: Clj	pher '	'8F+0	C8C,	1.81	tlalf	lzed	1.9413	th 12	8 pt.	th	ey											
ue Dec 1	9 19:48:	9 2014	Data	hanne'	L Decry	pt: Usi	ing 16	50 b1	dt #	10554	ige hi	ash	'SHI	A1' f	or H	MAC	auth	entle	attor									
ue Dec 1	9 19:48:	9 2014	Contr	/l Cha	snel: T	LSV1, 0	clpher	t TLS	SV1/	SSLV	(3 DH	C+RS	A-A	15256	- 5HA	, 2	048 b	it R	A									
ue Dec 1	9 19:48:	9 2014	[Serv	r] Pe	rr Conn	ection	Initi	Lated	d wi	.th [AF_17	NET]	192.	.184.	92.1	761	2015											
Ue Dec 1	9 19:49:1	2 2014	SENT	ONTRO.	. [Serv	er]: 'f	PUSH_R	YEONI	EST!	(st	atus-	-1)																
ue Dec. 1	9 19:49:1	2 2014	PUSH:	Recel	red con	trol m	essage	81.13	PUSH	LREP	24,14	edtr	ect	gate	наў і	def	1,dhc	p-opt	ton I	N5 1	0.8.0	-1,1	oute	8 10.	.8.0.0	255	.255.	255.0,top
gy net30.	,ping 18	ping-r	start	68,15	config	10.8.0.	.14 16	3.8.8	8,13	r.																		
ue dec 1	9 19:49:1	2 2814	OPTIO	IS IMP	RT: tt	ners at	nd/or	tim	root	s no	difle	ed.																
ue Dec 9	9 19:49:1	2 2014	OPTIC	IS IMP	/RT1	tfconfi	lg/up	opti	lons	mod	stries	5																
ue dec s	9 19:49:1	2 2014	OP110	12 TWD	AT: ro	ute opi	tions	nodi	itte	10																		
ue dec 1	9 19:49:1	2 2014	Ob110	12 TMM	ALT	(p-win)	32 and	J/or	0	incp-	optic	08.0	ip tu	ons n	00(1	led			100									
ue uec y	9 19:49:0	2 2014	HOUTE	GATEM	er 192.	168.2.1	1/255.	.255.	.255	1.0 1	PACES	-wia	100 1	HEADD	R+2C	108	15814	0118	TT -									
ue Dec 1	9 19:49:1	2 2014	TUN/T	iP dev	ice tun	1 opens	ed	202	100																			
ue Dec 1	9 19:49:1	2 2014	TUN/T	PTX	foene f	ength r	set to	> 100	۰																			
ue dec 1	9 19:49:1	2 2014	00_11	20119	, 11-31	pv0+0,	££->0	110_1	tree	inflg	L'the	b_se	tup	-0														
ue pec 1	9 191491	2 2014	/5018	tp tt	A set	Dev tur	n1 up	ntu	150	10																		
ue uec 1	9 19:49:	2 2014	ISDLO	1p ao	1. 900	DEV TUI	n1 LOC	281.7	10.0	1.0.3	14 per	er 1	0.0.	.0.13														
ue Dec 1	9 19:49:1	2 2014	/sbtn	tp ro	ite add	192.11	64.92.	.176)	/32	via	192.3	168.	2.3															
INETLINK	answers	File	XLSES																									
ue pec	9 191492	2.2014	EXHOR	LUng	route	- 200 CI	ormand	1 101	tteo	i ex	terna	er b	rogi	ran e	xite	10 W	LUN e	rror	state	151 Z								
Ue Dec 1	9 19:49:1	2.2014	75010	th Lo	/te add	0.0.0.	.0/1 V	ne :	10.8	1.0.3	1.3																	
INCILINA	4054675	Pile .	CODOD	1.0.00												11	100											
or oec	9 19:49:1	2 2014	(able	Linu	1 route	400 0	ormano o o / s	a rar	i teo		ccer na	ac p	rogi	can e	Arre	N W	un e	1101	statt	A: 8								
TREAT THE	9 191491	2 2014	/soun	sh to	Jue aug	120.0	.0.0/1	1 144	# 10																			
in Dec. 7	0.00.00.0	7 2014	EBBOR	11000		add or		1 5.1	61 md							4 -												
ue Dec 1	0 10:45:	2 2014	Zehin.	Line co	ite add	10 0 0	0.0/74	e (8) 4 - 1 -	. 10		1.13	· · P	- 981	and 4	~ · Ce	~ W			*****	- A								
TRUTT THE	A	F114	1.010	sp 10	#00	44.0.1	***124	1.46	- 10																			
the first of	10.0015	3 3014	EREOR	1.1		and the			11.00							4.14	in the second											
ue Dec 1	1 10-45-	2 2014	Tolti	linet	ion fee	and co	comple		i see	1. 10.4		ar 9	n ogi	Carry M				1.1.41	*****	8 A 4								
00.000 1	- A#1921	014	*******	122200	Act 266	Manage 1	compre	12.00																				

Gambar 4. Hasil akhir proses otentikasi VPN

Pada gambar 4, hasil eksekusi diteruskan setelah proses otentikasi *user* berhasil. Dari proses eksekusi yang berjalan tampak isi dari konfigurasi variabel *easy-rsa* yang telah dilakukan sebelumnya di dalam *server*. Data tersebut berisikan informasi berupa lokasi dan alamat *email* yang bisa digunakan oleh *user* bila ingin menghubungi pihak penyedia *VPN* tersebut.

Pengujian terakhir yang dilakukan yaitu pengujian dalam membandingkan koneksi internet. Dalam pengujian yang dilakukan setelah menggunakan jaringan *WiFi* adalah melakukan *traceroute* terhadap <u>www.google.com</u>. *Provider* yang pertama digunakan yaitu XL Axiata, dengan jumlah *user* yang terhubung ke jaringan *WiFi* berjumlah 1 (satu) klien dan untuk pengujiannya dilakukan melalui *traceroute online*.

🗲 🛞 tracerouti	e-online.com	Ψ.C		DuckDuckGo	٩, ١	合 向	+	Ĥ	•	Ŧ	
		112.215.3	6.1	42							
				R	has is y	our IP	Midness	s			
10	e network etuff O	nline Traceroute Whole Port Sc	an and a e	imple Dia D	INIS T	onle	hatw	all			
	blow your m	ind or maybe just help with tro	hleshooti	ng and net	work re	con	a nare in				
		wess example com	cercule to an IP o	e Rostrame							
		Anan sa tudoja Yosa Sa	cercule to an P o	r Hodrame							
		www.example.com	cercule to pr 12 c	e Ploginame							
Нер	p Host / IP Address	weak example com The path has been inced from our Linder server al 7 159	lewark, NJ to war Country	e Pooltome e poogle com. Packet Loss 0.0%	Respons						
Hop 1	 Host / IP Address 107.170.230.254 198.190.19.237 	www.example.com 11 The path has been traced from our Linois server at 1 150* Datable Coven	consulte to an EP of lewark, NJ 15 smit Country D	e pogle com. Packet Loss 0.0%	Respons 1.7 mil	10					
Hep 1 2 3	 Host / IP Address 107.170.228.254 198.199.59.237 128.259.204.117 	www.example.com 20 The path has been fraced from our Linder solver at h 10 Dight Doesn NTT Among a	Invariant to an E of Country	e pogle com. Packet Loss 0.0% 0.0%	Respons 1.7 mil 0.5 mil 1.6 mil	50					
Hop 1 2 3 4	 Host / JP Address 197, 170, 208, 254 198, 109, 592, 257 128, 258, 254, 117 128, 256, 254 	terms an ample score from our Lande server at the path has been faced from our Lande server at the score Output Ocean. NTT America. NTT America.	control to an IP o lewark, NJ to see Country	e Doctorne e google com. Packet Loss 8.0% 8.0% 8.0% 8.0%	Respons 1.7 mi 0.5 mi 1.6 mi 2.3 mi						
Hop 1 2 3 4 5	 Host / IP Address 107.170.228.254 198.198.90.237 129.258.254.117 129.256.5.37 129.250.5.73 129.250.137.158 	The path has been faced from our Linder server at 7 10 Digital Costs. Digital Costs. NIT America. NIT America. NIT America. NIT America.	corrule to an ED lowark, NJ to see Country Di ED ED ED ED ED ED	e pogle com. Packet Loss 8.0% 8.0% 8.0% 8.0% 8.0%	Respons 1.7 mia 0.5 mia 1.6 mia 2.3 mia 2.4 mia						
Hop 1 2 3 4 5 0	 Host / IP Address 107.170.208.254 108.109.69.237 129.250.204.117 129.250.53 129.250.137.138 216.234.81.70 	Interscenations of the second second at the second at the second second at the second	consults to an EP of lowark, NJ to see Country Di Country	P Bostome s google.com. Packet Loss 0.0% 0.0% 0.0% 0.0% 0.0% 0.0%	Respon 1.7 mk 0.5 ms 1.6 ms 2.3 ms 2.4 ms 6.4 ms						
Hop 1 2 3 4 5 6 7	 Host / IP Address 107, 178 208,254 198, 198, 89, 237 129, 258, 254, 117 129, 256, 533 129, 256, 137, 158 216, 239, 45, 176 02, 298, 53, 1 	where examples care The path has been fraced from our Davids server all gen Uptat Deesn NTT Avence NTT Avence NTT Avence Oxyge	levark. NJ 15 sear	e google.com. Packet Loss 8.0% 8.0% 8.0% 8.0% 8.0% 8.0% 8.0% 8.0%	Respons 1.7 mi 0.5 mi 1.6 mi 2.3 mi 2.4 mi 6.4 mi 2.6 mi						

Gambar 5. Halaman hasil proses traceroute provider XL

Pada gambar 5 terlihat halaman dari hasil proses *traceroute* muncul saat melakukan akses ke *website* <u>www.google.com</u>. Jelas tertampil alamat *IP* dari *provider* internet yang digunakan, dan untuk proses *traceroute* yang berjalan tidak tampak adanya *packet loss* namun teradapat grafik respon yang cukup tinggi pada *hop* ke 6 (enam). Hal tersebut menandakan bahwa pada titik tersebut *traceroute* mendapatkan respon yang cukup lambat yang dimungkinkan padatnya lalu lintas pada titik jalur tersebut ataupun karena jauhnya jarak dari titik tersebut dan titik sebelumnya.

Pengujian selanjutnya yaitu saat *user* telah terhubung ke jaringan *VPN*. Saat *user* menggunakan *VPN* sudah dipastikan *user* tersebut akan dikenali sebagai *user* dari luar yang artinya bukan dikenali sebagai *provider* XL Axiata saat mengakses internet. Hal ini dapat dipastikan dengan mengakses situs yang menyediakan layanan cek *IP*. Dalam hal ini proses yang sama masih dilakukan yaitu menggunakan *traceroute* guna mendapatkan perbandingan dalam mengakses internet.

d traceroute-	online.com	* (:) MA [DuckDuckGo 	٩	\$	ė	+	ŧ	•	*
		192.184.9	2.	176							
				K.	han Te	9000	17 N	64+855			
It's	network stuff. O	nline Traceroute, Whois, Port Sc	an and a	simple Dia D	NS.	Тоо	ls th	at wil	11		
	blow your m	ind or maybe just help with tro	ubleshoe	oting and net	work	reco	on.				
		Anna accargia com	nd en culto So an 1	P is Hustiane							
		www.assample.com	activite to an	P or Hostiane							
Нар	Host / IP Address	reven accargin com	icencente for an licencente, NJ to r Counter	IP is Hussiame www.google.com. Y Packet Loos	Respo	0.64					
Hop 1	Host / IP Address 107.170.208.253	www.ccample.com	Komoulis da un Komoulis da un Counter Di	17 or Hussiame www.google.com. y Packet Loss 0.0%	Respo 2.3 m	nae					
Hop 1 2	Host / IP Address 9/7:170.228.253 193.199.99.253	www.acample.com The path has been faced from our Linoit server at SSP Optial Ocean	iewark, NJ to m Countr	17 or Hossivane every people core. y People Core. 0.0% 0.0%	Respo 2.3 mi 3.9 mi	nse					
Mog. 1 2 3	Host / IP Address 107 176 208 255 198 199 59 253 129 256 256 117	Intern scarryth com	iowark, NJ to t Countr	P or Hostname www.google.com. y Packet Loss 0.0% 0.0% 0.0%	Respo 2.3 m 3.9 m 1.6 m	-	-				
Mop 1 2 3 4	Host / IP Address 197 170 208 250 198 199 99 250 128 250 204 117 129 250 5.33	www.scample.com The path has been faced from set Jacob server at set Optic Ocion NTT America NTT America	County	Por Hassourie www.google.com. y Pecket Loss 0.0% 0.0% 0.0% 0.0%	Respo 23 m 39 m 1.6 m 22 m						
Nop 1 2 3 4 5	Host / IP Address 197 176 298 255 198 199 99 255 129 256 354 117 129 250 5.35 129 256 197 139	www.example.com	Romound So and Romark, NJ So County 20 10 10 10 10 10 10 10 10 10 10 10 10 10	1 ¹⁷ is Housewall www.google.com. y Packet Loss 0.0% 0.0% 0.0% 0.0%	Respo 2.3 m 3.8 m 1.8 m 2.2 m 2.3 m	nse					
Mog 1 2 3 4 5 5	Host / IP Address 107 170 208-850 198 199 59 253 128 260 264 117 129 250 133 129 250 157 139	www.example.com	iovesni, NJ to an Country P	17 is Hostoweg www.google.com. y Packet Loos 0.0% 0.0% 0.0% 0.0% 0.0% 0.0%	Respo 23 mi 39 mi 18 mi 22 mi 23 mi 25 mi						
Nop 1 2 3 4 5 6 7	Host / IP Address 97,773284,850 986,99,925 924,850,841,17 929,250,3,33 929,255,197,138 216,229,48,170 94,249,352	ener scarget care The path-taskeen tracked from our Lindon saver at get Optic Overs NTT Avenus NTT Avenus NTT Avenus NTT Avenus NTT Avenus Overs	Result, NJ 10 Countr P	Part Factories while google.com. Y Packet Loss 0.0% 0.0% 0.0% 0.0% 0.0% 0.0% 0.0% 0.0%	Respo 23 mi 38 mi 18 mi 22 mi 23 mi 25 mi 26 mi						

Gambar 6. Halaman hasil proses traceroute menggunakan VPN network 1

Pada gambar 6 menunjukkan perubahan alamat *IP* yang tertampil, alamat *IP* tersebut adalah merupakan alamat *IP* dari *VPN server*. Dari sisi tersebut keuntungan didapatkan oleh *user* yaitu *user* hanya akan dikenali sebagai orang yang mengakses menggunakan jaringan *provider* tersebut yaitu berupa jaringan *VPN*. Dengan demikian alamat *IP user* yang sebelumnya akan dipalsukan atau digantikan oleh alamat *IP* jaringan *VPN*.

Pada saat berada pada jaringan VPN, proses akses internet masih berjalan sedikit lebih lambat ketika pengujian dilakukan. Hal ini memang akan terjadi karena dari awal jaringan provider XL sedang tidak berjalan baik, akan tetapi akses internet jauh lebih stabil saat menggunakan VPN.

Pengujian selanjutnya yaitu dengan mengganti *provider* untuk *modem USB* yang digunakan yaitu Telkomsel. Proses yang akan dilakukan sama seperti proses saat menggunakan *provider* sebelumnya yaitu dengan menggunakan *traceroute.*

racerout								
() tracero	ute-online.com	- D•	67%	+ 😫• G	oogle	9 2		+
				~ -				
		114.125.7	6.1	85				
				R	At 16 9007	IP Man	166	
	5 10 10 10 10 10 10 10 10 10 10 10 10 10			20125 51	100000			
It	's network stuff. Or	nline Traceroute, Whois, Port Sca	an and a sir	mple Dig D	NS. Tool	is that w	will	
	blow your m	ind or maybe just help with tro	ubleshootir	ng and net	vork reco	on.		
		www.esample.com	cercule to an 1P o	e Heatrame				
		www.esample.com	carote to an IP o	e Houtrame				
		www.example.com	Consulta to an IP of Neurania, NJ to war	v Hoatrame w google com.				
Но	Bost / IP Address	www.exumple.com	Central to you 12 of Newsials, NJ to war Country	v Hattram w google com. Packet Loss	Response			
Ho 1	Bost / IP Address 107.170.238.254	www.example.com	Country Country	r Hadfræme w.google.com. Packet Loss 0.0%	Response 2.5 ma			
Hoj 1 2	 Host / IP Address 107, 170, 238, 254 198, 190, 99, 227 	www.exempts.com	Constitution and Pro- Newsian, NJJ to war Country	v Acatteries w google.com. Packet Loss 0.0% 0.0%	Response 2.5 ma 0.8 ma			
Ho 1 2 3	 Host / IP Address 107.170.208.254 108.199.99.227 129.250.204.117 	www.example.com	Newality to an 10 or Newality, NJ to war Country	e Noofreener w google com. Packet Loos 0.0% 0.0% 0.0%	Response 2.5 ma 0.8 ma 1.4 ma	1		
Ho 1 2 3 4	 Host / IP Address 107, 170, 208, 254 108, 190, 90, 207 108, 250, 204, 177 109, 250, 1, 30 	www.example.com	Newality to an IP of Newality, NJ to war Country	e Mostraamer w google.com. Packet Loos 0.0% 0.0% 0.0%	Response 2.5 ma 0.8 ma 1.4 ma 2.3 ma	1		
Ho 1 2 3 4 5	 Hoot / IP Address. 107.170.208.254 108.190.00.227 129.250.204.117 129.250.533 128.250.197.138 	www.example.com	Newark, NJ to war Country	r HCatramer W google.com. Packet Loss 0.0% 0.0% 0.0% 0.0%	Response 2.5 ms 0.8 ms 1.4 ms 2.3 ms 2.4 ms	1		
Hoo 1 2 3 4 5 6	 Host / IP Address 107.170.208.254 108.190.80.207 129.250.201.117 129.250.153 129.250.157.138 129.250.197.138 214.254.40.168 	www.excepts.com 200 The path has been toose it on a Linete server at 7 BP Digital Oneon NTT Awardon NTT Awardon NTT Awardon NTT Awardon	Country Country	Picciframe w.google.com. Packet Loss 0.0% 0.0% 0.0% 0.0% 0.0%	Response 2.5 ma 0.8 ma 1.4 ma 2.3 ma 2.4 ma 8.5 ma	-		
Hoo 1 1 2 3 4 5 6 7	 Host / IP Address. 107, 170, 234, 254 108, 190, 802, 237 129, 250, 204, 117 129, 250, 133 129, 250, 133 129, 250, 107, 138 216, 239, 40, 108 208, 852, 60 	www.exempts.com 20 The path has been traced here not Jacob server of gift Digital Ocean NTT Analosa NTT Analosa NTT Analosa NTT Analosa NTT Analosa NTT Analosa	Newsistic, NJ to over Country	P Mostramm w google.com. Packet Loss 0.0% 0.0% 0.0% 0.0% 0.0% 0.0%	Response 2.5 ma 0.8 ma 1.4 ma 2.3 ma 2.4 ma 6.5 ma 11.5 ma	-		
Hoo 1 2 3 4 5 6 7 8	 Host / IP Address, 107:10:202.054 108:10:0:0:227 109:200:204.17 109:200:3:04 109:200:3:04	www.energence.com	Newsite to put to even Country	Kooframm w geogle.com. Packet Loos 0.0% 0.0% 0.0% 0.0% 0.0% 0.0% 0.0% 0.0%	Response 2.5 ma 0.8 ma 1.4 ma 2.3 ma 2.4 ma 1.5 ma 11.5 ma 18.2 ma	-		
Hote 1 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	 Host / IP Address 107.170.201.054 108.109.0627 109.200.054 109.200.0117 109.200.0117 109.200.107.138 109.200.8107 109.200.8107 109.200.8117 209.85.200.60 44.203.174.108 	www.exercities.com The path has been tracked here not Jacob server of gen Digital Docen NTT Anance. NTT Anance. NTT Anance. Statistics. Sta	Needad to us the Country	* Rottrom w. google.com. Packet Loss 0.0% 0.0% 0.0% 0.0% 0.0% 0.0% 0.0% 0.	Response 2.5 ma 0.8 ma 1.4 ma 2.3 ma 4.5 ma 1.5 ma 11.5 ma 11.5 ma 12.8 ma			
Hop 1 1 2 3 4 5 5 6 6 7 7 8 8 8 9 10	 Nost / IP Address, 107: 170 208.054 108: 109.8027 109.200.8027 109.200.8017 109.200.8027 109.200.8017 109.200.8027 109.200.8027 109.200.802 	www.strappits.com	Needs by a 10 of 1	Plethormo w google.com. Packet Loss 0.0% 0.0% 0.0% 0.0% 0.0% 0.0% 0.0% 0.	Response 2.5 ma 0.8 ma 1.4 ma 2.3 ma 2.4 ma 4.5 ma 11.5 ma 11.5 ma 11.2 ma 12.8 ma			

Gambar 7. Hasil proses traceroute provider Telkomsel

Pada gambar 7 menunjukkan perubahan mencolok dari proses sebelumnya yaitu perubahan alamat *IP*. Hal tersebut terjadi karena internet yang digunakan pada *modem USB* telah diganti dari yang sebelumnya menggunakan XL diganti dengan menggunakan Telkomsel. Proses *traceroute* yang berjalan menghasilkan jumlah *hops* yang berbeda yaitu berjumlah 11 (sebelas) dengan beberapa diantaranya memiliki grafik respon yang cukup tinggi.

Proses akses internet berjalan jauh lebih cepat dengan menggunakan provider Telkomsel ketika pengujian dilakukan. Tidak seperti sebelumnya, akses internet berjalan lancar dimungkinkan karena memang pada area tempat pengujian dilakukan provider Telkomsel memiliki kualitas jaringan yang baik sehingga bila mengakses internet pada area tersebut akan mendapatkan akses internet yang cepat. Dengan provider Telkomsel sebagai layanan internet yang digunakan pada modem USB, selanjutnya user yang telah terhubung ke jaringan WiFi akan dihubungkan ke jaringan VPN server yang memiliki lokasi server yang sama. VPN yang digunakan kali ini ialah VPN ke 2 (dua), karena pada penelitian ini memiliki 2 (dua) VPN server dengan lokasi server yang sama.

		The second se		100 100		CONTRACTOR OF THE OWNER
racerout	e-online.com	• C =	67%	+ 📴• G	oogle	
		00 040 0	0 4	00		
	1	92.249.6	50.1	96		
				-		
				~	han is your	IF Mdress
It's i	network stuff. Online	Traceroute, Whois, Port Sca	n and a sir	mple Dia D	NS. Tool	is that will
	blow your mind	or maybe just help with trop	ublachootic	and and not	Hork race	NO NO
	biow your minu.	of maybe just neip with to	ubieariootii	ig and nea	NOIR IOUG	211.
		ex acampla con	centre to an Pro	Notrana -		
		ev acample com	constata an Pra	Maltune -		
	The	en arangia son 10 path has bein traced from our Linode server at 9	constants as Pos	Madhaine w.google.com		
Нар	The Heat / IP Address	en arangia can path has been Inced hon our Linole server at 5 159	Centrate to an IP o Generath, NJ to even Country	v google.com. Packet Loss	Пацьская	
Hap 1		ns a conglis con 10 path has been tacad hon our Lineals server at 7 159	Centrate to an 12 o Generath, NJ to serve Country 2	Hadisate v google.com. Packet Loss 0.0%	Response 0.6 ms	
Hop 1 2		en accepto con 20 alth has been tacad hon our Linceto server at 9 1589 Digital Ocean	Generality, NJ to over Country	Plathane w google.com. Packet Loss 0.0%	Response 0.6 mil	
Hap 1 2 3	The Heat / JP Address 107,179,282,255 108,199,95,253 129,250,254,117	ex atomptic com. The server of 5 gas. gash has been forced from our Lineods server of 5 gas. Digital Occess. NTT America.	Secure to an R of Security 2 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	v google.com Packet Loss 0.0% 0.0% 0.0%	Beepcoar 0.6 m 1.1 m 1.8 m	;
Hap 1 2 3 4	The Near / IP Address 107, 170 238, 255 198, 199, 253 198, 299, 253 192, 209, 254, 177 129, 200, 1, 30	en ananja sen. To gath ha ben faced from or Lindo serve at 9 189 Digita Ocean NTT Annata NTT Annata NTT Annata	Country	Platinum v google.com 0.0% 0.0% 0.0% 0.0%	Response 0.6 mi 1.1 mi 1.8 mi 2.3 mi	1
Hep 1 2 3 4 5	The Next / P Addees 107.170.238.255 108.109.0255 108.200.024.117 108.200.103 108.200.103	ne ananyle son. Teo alfh ha baer hacid fors ou Enole arear af y sof Digital Ocean NTT Anexica NTT Anexica NTT Anexica	Country	Postuate e große com. Postet Loss 6 0% 6 0% 6 0% 6 0% 6 0%	Response 0.6 ms 1.1 ms 1.8 ms 2.3 ms 2.4 ms	-
Hop 1 2 3 4 5 6	The Hotal / IP Addoms 107.75.28(225) 198.195.92.233 192.200.294.117 122.200.294.117 122.200.137 122.200.107.138	en anampin com gast has been fraced from de Chode server al 9 1897 Digital Oceans NTT Anenica NTT Anenica NTT Anenica NTT Anenica Oceans	Country Country	Pacteriore Pacter Loss 8 0% 8 0%	Response 0.6 ma 1.1 ma 1.8 ma 2.3 ma 2.4 ma 2.4 ma	
Hop 1 2 3 4 5 6 7	The Pleast / IP Addresses 107, 170 238 255 108, 196 98 253 108, 209 49, 177 128 200, 1.07 128 200, 1.07 128 200, 107, 108 274 209 48 168 274 209 48 265	ere example som. To park has been head Horn av Enode somer ef 3 Big Digital Coses: NTT Among NTT Among NTT Among NTT Among Orogie Orogie	Country 2 3 3 3 3 3 3 3 4 3 4 3 4 5 4 5 4 5 4 5 4	Pacteriore Pacter Loss 0.0% 0.0% 0.0% 0.0% 0.0% 0.0% 0.0%	Respicae 0.6 mi 1.1 mi 1.6 mi 2.3 mi 2.4 mi 2.4 mi 2.4 mi 11.0 mi	
Hop 1 2 3 4 5 6 7 8	The Head / B Addease 107.179 238-255 108.199 253 108.299 253 108.299 254.177 108.299 254.177 108.299 254.173 108.299 254.185 275.299 45 48 2016 M 242.255	en exemple com gell has been head horn aut Carda aver al 3 gell has been head horn aut Carda aver al 4 gell de Coere Stiff Annola WTT Annola WTT Annola WTT Annola WTT Annola Oragin Oragin	Country	Possesere w google cors. Packet Loss 0.0% 0.0% 0.0% 0.0% 0.0% 0.0%	Bespione 0.6 mi 1.3 mi 1.8 mi 2.3 mi 2.4 mi 2.4 mi 11.0 mi 12.9 mi	
Hap 1 2 3 4 5 6 7 8 0	The Next / P Address 100, 700 208, 205 100, 100 208, 417 100, 200, 204, 417 100, 200, 307 100, 200, 307, 308 274, 220, 40, 50 274, 220, 40, 50 40, 203, 174, 206 44, 223, 175, 505	en somplexen. 10 park he her hon av Ende some at 3 park Paper Overs 417 Anna 417 Anna 417 Anna 417 Anna 417 Anna Gogin Gogin Gogin Gogin	Second State Second	Policipum w google.com. Poliet.Loss 0.0% 0.0% 0.0% 0.0% 0.0% 0.0%	Response 0.6 mi 1.1 mi 1.8 mi 2.3 mi 2.4 mi 2.4 mi 11.0 mi 12.9 mi 15.2 mi	
Hep 1 2 3 4 5 6 7 8 8 8 9 9 9 9	The Transmission of the term of term o	en ranges om att hat been hen an Londa over at h ser Også Over Att Anexas Att Anexas Att Anexas Over Orge Orge Orge Orge Orge Orge Orge Or	Security 2 Security	NUCLEAR AND A CON- M google.com. Packet Loss 0.0% 0.0% 0.0% 0.0% 0.0% 0.0% 0.0% 0.0% 0.0%	Варролан 0.6 m 1.1 m 1.8 m 2.3 m 2.4 m 2.4 m 2.4 m 11.0 m 12.9 m 15.2 m	

Gambar 8. Halaman hasil proses traceroute menggunakan VPN network 2

Pada gambar 8 hasil yang didapatkan masih sama seperti pengujian sebelumnya yaitu alamat *IP user* akan digantikan oleh alamat *IP VPN server* yang dalam hal ini *VPN* yang digunakan *user* adalah *VPN network* 2 sehingga *IP VPN server* yang didapatkan akan berbeda dengan *VPN network* 1. Sedangkan dalam hal proses *traceroute* yang berjalan juga tampak stabil dengan beberapa *hops* memiliki respon yang kecil dan beberapa memiliki *hops* yang cukup tinggi. *Hops* dengan respon kecil menandakan proses paket dijalankan dengan waktu yang singkat karena pada titik tersebut mungkin tidak banyak lalu lintas paket yang berjalan, sedangkan pada *hops* dengan respon yang cukup tinggi dimungkinkan masing-masing titik tersebut berada dengan jarak yang jauh satu sama lain atau mungkin dikarenakan jumlah lalu lintas paket yang terlalu besar pada titik-titik tersebut.

Proses akses internet saat menggunakan VPN yang dilakukan dalam pengujian terhadap jaringan *provider* Telkomsel berjalan sesuai dengan yang diharapkan, akses internet berjalan lancar dan stabil.

Pengujian yang selanjutnya dilakukan yaitu pengujian terhadap penggunaan VPN terhadap free WiFi publik. Penggunaan VPN dalam jaringan free WiFi publik dapat berjalan sebagaimana saat penggunaan dengan jaringan WiFi yang telah dibuat, hal ini bisa dilakukan sebab jaringan VPN berasal dari jaringan publik milik VPS dengan berupa IP public. Dengan melalui IP public tersebut menjadikan VPN dapat berjalan pada jenis jaringan apapun dengan syarat pengguna harus terlebih dahulu memiliki koneksi internet. Pengujian terhadap jaringan free WiFi publik dilakukan pada layanan jaringan free WiFi dari ISP Telkom yaitu Speedy Instan@wifi.id.

Setelah mendapatkan akses internet, langkah selanjutnya melakukan pengujian terhadap penggunaan VPN. Pengujian ini dilakukan untuk mengetahui apakah VPN dapat digunakan pada jaringan WiFi tersebut. Pada beberapa jaringan WiFi, ada yang memiliki sistem blok terhadap penggunaan jaringan *private* seperti VPN, SSH dan lain sebagainya, hal inilah yang mendasari dilakukannya pengujian ini. Dan dari pengujian yang dilakukan telah didapatkan hasil yang menunjukkan bahwa VPN tetap dapat digunakan pada jaringan WiFi Speedy Instan@wifi.id seperti yang ditunjukkan pada gambar 9.



Gambar 9. Hasil otentikasi VPN terhadap jaringan Free WiFi public

Dari hasil yang ditunjukkan pada gambar 9, proses otentikasi dengan menggunakan data *login userP1;userP1* dapat dieksekusi hingga mendapatkan hasil *Initialization Sequence Completed* yang menandakan bahwa *laptop* telah berhasil terhubung ke jaringan *VPN.*

Berdasarkan pengujian dari infrastruktur jaringan sistem otentikasi jaringan WiFi dengan menggunakan FreeRADIUS server dan integrasi OpenVPN server dengan FreeRADIUS server dengan lingkup Multi-NAS di dalam infrastruktur yang telah diimplementasikan, dapat dilihat bahwa implementasi infrastruktur berhasil berfungsi dengan baik.

Dalam proses otentikasi yang berjalan, *FreeRADIUS* dapat merespon data *user* dari *database* yang digunakan oleh pengguna *WiFi*. Hal tersebut dapat dilihat melalui fitur *report* yang ada pada aplikasi *DaloRADIUS* seperti yang ditunjukkan pada gambar 10.

Reports 🍐	Last (Connection Attempts	+	
🥃 Online Users	CSV Expor	t		
	1			
	Username	Password	Start Time	RADIUS Reply
Last Connection Attempts	localU1	0x69e4446d877236b9f021ec35886ebb5016	2014-12-01 13:00:52	Access-Accept
%	userP1	0xeff6162827b15f0d585ec3f232ad71137a	2014-12-01 12:00:46	Access-Accept
Any 👻	userP1	0xa42da05b0c3a49e0393b5d8c44f5f07b05	2014-12-01 11:16:06	Access-Accept
Start Date	PAGE 1 OF	1		
2014-01-01				
End Date				

Gambar 10. Hasil otentikasi data user jaringan WiFi

Pada gambar 10 terlihat bahwa proses otentikasi telah berhasil diproses dan otentikasi tersebut telah mengeksripsi *password* dari tiap *user* yang menggunakan *WiFi*. Dengan proses

enkripsi maka data *user* akan tetap aman terlebih lagi untuk jaringan *WiFi* yang telah dibuat akan mendapatkan keamanan yang lebih baik karena sistem yang bekerja adalah dengan proses otentikasi untuk setiap *user* yang menggunakan *WiFi*, sehingga dengan demikian *user* yang tidak memiliki data *login* maka tidak akan bisa masuk ke jaringan *WiFi*.

Selain melihat hasil dari proses otentikasi, di dalam aplikasi *DaloRADIUS* juga terdapat fitur untuk melihat *user* yang sedang menggunakan *WiFi*, hal ini dapat dilihat pada gambar 11.



Gambar 11. Daftar online users pada jaringan WiFi

Dengan hasil yang ditunjukkan pada gambar 11, tampak bahwa *user* yang sedang menggunakan *WiFi* berjumlah 1 (satu). Status *online users* seperti gambar di atas hanya akan berhasil ditampilkan apabila proses otentikasi berhasil dilakukan, jika proses otentikasi tidak berhasil dilakukan maka tidak akan tertampil daftar *online users* pada halaman tersebut.

Dari hasil yang ditunjukkan pada gambar di atas, menandakan *user* telah berhasil mengakses internet. Kemudian pengujian berlanjut dengan penggunaan *VPN*. Pengujian ini akan tampak berbeda yaitu dari sisi proses otentikasi, seperti hasil pengujian pada gambar 12.

Reports 🌢	Last Cor	nection	Attempts .	
🧧 Online Users	CSV Export			
	Username	Password	Start Time	RADIUS Reply
Last Connection Attempts	userP3	userP3	2014-12-09 23:51:11	Access-Accept
	userP3	userP3	2014-12-09 23:50:55	Access-Accept
Any 🔽	userP3	userP3	2014-12-09 23:49:50	Access-Accept
Start Date	userP3	userP3	2014-12-09 23:49:03	Access-Accept
	userP1	userP1	2014-12-09 07:44:10	Access-Accept
2014-01-01	userP1	userP1	2014-12-09 07:43:02	Access-Accept
End Date	userP1	userP1	2014-12-09 07:41:57	Access-Accept
2014-12-31	userP1	userP1	2014-12-09 07:40:54	Access-Accept

Gambar 12. Hasil otentikasi data user VPN

Pada gambar 12, terlihat hasil dari proses otentikasi pada penggunaan data *user* terhadap jaringan *VPN*. Dari hasil tersebut terdapat perbedaan dari hasil proses otentikasi pada *user* jaringan *WiFi* yaitu data *login* yang berupa *password* tidak dienkripsi, meskipun demikian *user* tetap berhasil terotentikasi oleh *FreeRADIUS server*.

Perbedaan yang terdapat dari proses otentikasi pada jaringan VPN bukan merupakan kegagalan sistem, akan tetapi memang telah dikonfigurasi seperti itu untuk setiap proses otentikasi user VPN tidak akan dilakukan enkripsi, hal ini dilakukan karena aspek dari penggunaan VPN yang telah memiliki proses keamanan yang cukup baik seperti yang telah dijelaskan sebelumnya. Untuk mengingat kembali bahwa setiap user yang ingin menggunakan VPN terlebih dahulu harus memiliki *file certificate* yang telah dibuat dari *server*, dengan melalui *certificate* tersebut proses *handshake* pada jaringan VPN akan diproses. Hal tersebutlah yang menjadikan alasan tidak digunakan proses enkripsi untuk setiap proses otentikasi user VPN karena proses *handshake* pada jaringan VPN memiliki kemanan yang baik.

Seperti halnya daftar *online users* pada jaringan *WiFi*, pengguna yang menggunakan *VPN* juga akan dapat tertampil dalam daftar *online users* seperti yang ditunjukkan pada gambar 13.



Gambar 13. Daftar online users pengguna VPN

Pada gambar 13 terlihat 2 (dua) pengguna yang sedang menggunakan *VPN*. Namun terlihat seperti keganjilan pada gambar tersebut yaitu kedua pengguna tersebut memiliki alamat *IP* yang sama, *MAC* yang berbeda dan *NAS shortname* yang berbeda.

Hal yang terjadi pada gambar di atas bukanlah sebuah kesalahan, perlu diingat kembali bahwa pada infrastruktur yang dibuat memiliki 2 (dua) *VPN server*, dan *subnet* pada masing-masing *server* dibuat sama sehingga menghasilkan alamat *IP* yang sama ketika hanya terdapat 1 (satu) pengguna pada masing-masing *VPN server*, hal tersebut terjadi karena merupakan *default DHCP* yang berada pada konfigurasi *VPN server*. Pada pengujian saat menggunakan *VPN*, kedua *VPN server* digunakan sehingga bila diteliti lebih lanjut pada gambar di atas akan dapat dibedakan yaitu melalui *NAS shortname*. Dengan melalui *NAS shortname* tersebut akan memudahkan untuk melihat pengguna yang sedang menggunakan *VPN* dari salah satu *server*.

Dan kemudian dari pengujian penggunaan VPN terhadap jaringan free WiFi publik, didapatkan hasil yang menunjukkan bahwa tidak terjadi proses blokir terhadap jaringan VPN saat digunakan. Proses pemblokiran VPN ketika menggunakan jaringan free WiFi memang akan sulit ditemukan, karena tidak banyak layanan WiFi yang memiliki sistem pemblokiran terlebih pada layanan free WiFi publik yang memang ditujukan untuk penggunaan secara gratis oleh publik dengan kebijakan tertentu. Meskipun bila sistem pemblokiran pada jaringan WiFi itu ditemukan mungkin hanya akan terdapat pada tempat tertentu seperti misalnya di perusahaan, hal ini dikarenakan sistem pemblokiran semacam itu sulit untuk diterapkan karena untuk sistem WiFi yang berjalan harus dapat membedakan jenis jaringan misalnya seperti bagaimana cara jaringan WiFi tersebut dapat mendeteksi bahwa user sedang menggunakan VPN, dan bagaimana jaringan WiFi tersebut dapat mengenali bahwa itu adalah protokol UDP atau TCP. Sistem semacam inilah yang perlu diterapkan terlebih dahulu untuk membuat sistem pemblokiran, dan dengan begitu akan mungkin terjadi pemblokiran akses internet saat menggunakan VPN pada jaringan WiFi yang memiliki sistem tersebut.

KESIMPULAN

Berdasarkan hasil dari serangkaian kegiatan penelitian dengan pengujian yang telah dilakukan, maka dapat diambil beberapa kesimpulan bahwa Penerapan sistem otentikasi dengan menggunakan *FreeRADIUS server* dapat memberikan tingkat keamanan jaringan *WiFi* menjadi lebih baik karena dengan sistem otentikasi yang terenkripsi, pada sisi *server* akan menjadi lebih aman dalam menjaga data *user* yang terhubung ke dalam jaringan *WiFi*. Dan juga infrastruktur dengan sistem otentikasi dapat menggunakan *WiFi* harus terlebih dahulu memiliki data *user* dalam *database FreeRADIUS server*, serta dengan penggunaan *VPN* dapat memberikan peranan dalam menyediakan kualitas keamanan akses internet untuk pengguna yang menggunakan jaringan *WiFi*.

DAFTAR PUSTAKA

Arifin, Zaenal., 2006, *Mengenal Wireless LAN (WLAN)*. Yogyakarta: ANDI Publisher Forouzan, B. A., 2007, *Data Communications and Networking*. New York: McGraw-Hill

- Hadi, Sofian., 2012, Desain dan Implementasi Otentikasi Jaringan Hotspot Menggunakan Coovachilli dan FreeRADIUS pada Linux Ubuntu 10.04 LTS, PKPI, Jurusan Teknik Informatika, FTI, IST AKPRIND, Yogyakarta
- Hanafi, Muh. Ibnu Habil., 2014, Implementasi Sistem Otentikasi Jaringan Wifi Dengan FreeRADIUS Server PT. Medianusa Permana Batam. PKPI, Jurusan Teknik Informatika, FTI, IST AKPRIND, Yogyakarta
- Herlambang, Moch. Linto, Catur L, Azis., 2008, Panduan Lengkap Menguasai Router Masa Depan Menggunakan MikroTik RouterOS[™]. Yogyakarta:ANDI Publisher
- Lubis. F., 2010, Analisa Perbandingan Easyhotspot dan Mikrotik dalam Penerapan Hotspot Area dengan Sistem AAA, Skripsi, Jurusan Teknik Informatika, FTI, IST AKPRIND, Yogyakarta
- Prabowo, Deddy., 2012, Penerapan Teknologi Mlkrotik Router Untuk Manajemen Bandwidth dan Pemasangan Hotspot Broadband Access (Speedy) PT. Telkom Boyolali, PKPI, Jurusan Teknik Informatika, FTI, IST AKPRIND, Yogyakarta
- Rofiq, M., 2009, *Pemanfaatan Captive Portal sebagai Otentikasi Client untuk Keamanan Jaringan Hotspot,* Skripsi, Jurusan Teknik Informatika, FTI, IST AKPRIND, Yogyakarta
- Schmid, Martin W. Murhammer, Orcun Atakan, Zikrun Badri, Beonjun Cho, Hyun Jeong Lee, Alexander., 1999, A Comprehensive Guide to Virtual Private Networks, Volume III: Cross-Platform Key and Policy Management. USA:ITSO-IBM Corp
- Scott, Paul Wolfe, Mike Erwin, Charlie., 1999, Virtual Private Networks, Second Edition. California:O'Reilly
- Tal, Liran., 2011, *DaloRADIUS User Guide (Volume 1)*. England:CreateSpace Independent Publishing Platform.
- Walt, Dirk Van Der., 2011, FreeRADIUS Beginner's Guide. Birmingham: Pack Publisher