

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

Muh. Ibnu Habil Hanafi<sup>1</sup>, Suwanto Raharjo<sup>2</sup>, Suraya<sup>3</sup>

<sup>1,2,3</sup> Teknik Informatika, institut Sains & Teknologi AKPRIND Yogyakarta

<sup>1</sup> [ibnu.habil.h@gmail.com](mailto:ibnu.habil.h@gmail.com), <sup>2</sup> [wa2n@akprind.ac.id](mailto:wa2n@akprind.ac.id), <sup>3</sup> [suraya\\_pandev@yahoo.com](mailto:suraya_pandev@yahoo.com)

### 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 diinginkan 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, pemeliharaan 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, diantaranya yaitu penelitian tentang bagaimana membangun *captive portal* sebagai otentikasi *user*, dan manajemen *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 berbasis *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 Mikrotik 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 akuntansi. 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 profesional 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, enkripsi dan *tunneling*.

**METODOLOGI PENELITIAN**

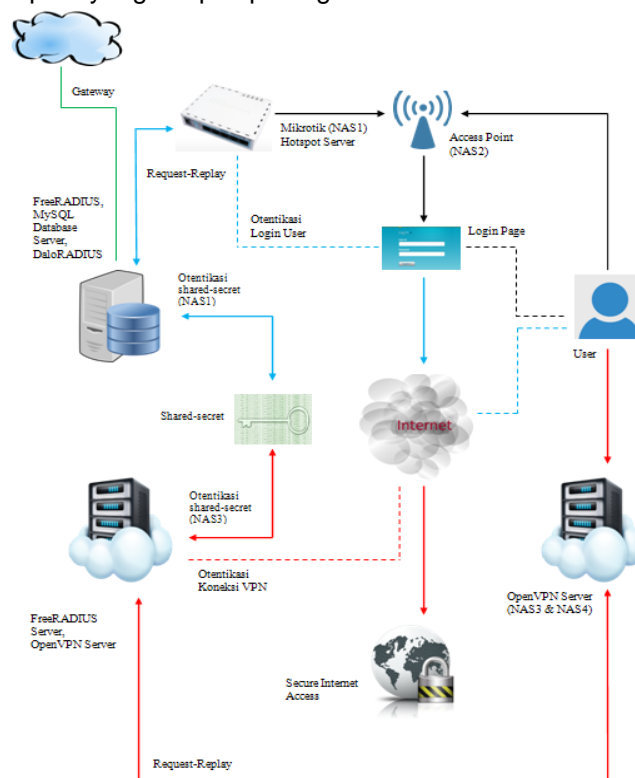
Metodologi penelitian yang dilakukan berupa analisa data. Tahap analisis ini merupakan tahap yang sangat penting karena kesalahan pada tahap ini dapat mengakibatkan kesalahan pada tahap selanjutnya sehingga dibutuhkan suatu metode yang dapat digunakan sebagai pedoman dalam pengerjaan proses berikutnya.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

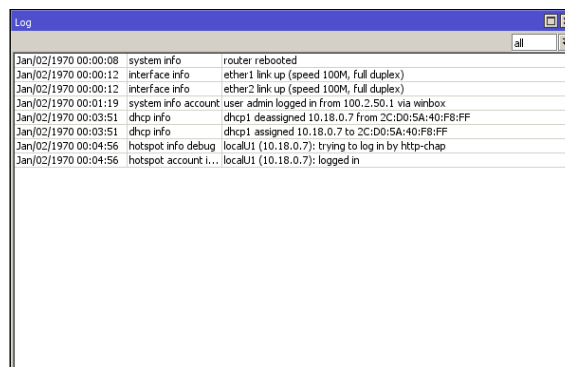
	: Jalur proses kerja Mikrotik <i>Hotspot</i>
	: Proses otentikasi <i>FreeRADIUS</i> server terhadap <i>login user</i>
	: Proses otentikasi <i>FreeRADIUS</i> server terhadap <i>OpenVPN</i> server
	: Hasil dari proses otentikasi <i>Login User</i>
	: Hasil dari proses otentikasi <i>VPN User</i>
	: Jalur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

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.



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*.



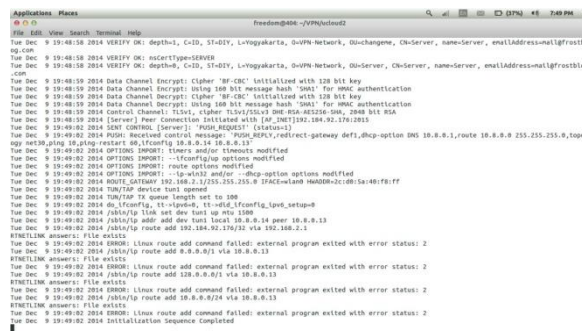
Penggunaan *VPN* dari sisi *user* memerlukan *software openvpn client*, dan dalam pengujian yang dilakukan menggunakan *linux* yang sudah terinstall *openvpn client*. Untuk dapat menggunakan *VPN*, *user* terlebih dahulu memerlukan *file-file certificate* yang sudah dibuat dari *server* yang terdiri 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*.



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 eksekusi akan diteruskan dan jika data *user* tidak valid maka proses akan dihentikan.

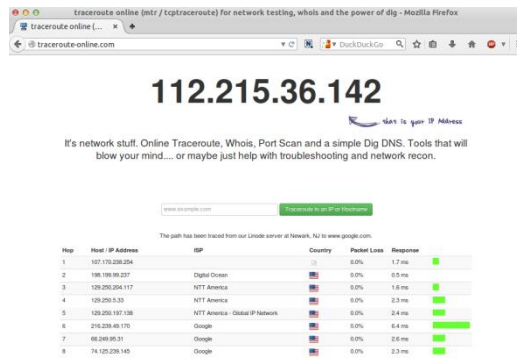
Proses otentikasi telah berhasil ditandai dengan status *initialization sequence completed*. Dengan mendapatkan status tersebut maka hal itu menandakan *VPN* telah berhasil terhubung, seperti yang ditunjukkan pada gambar 4.



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.

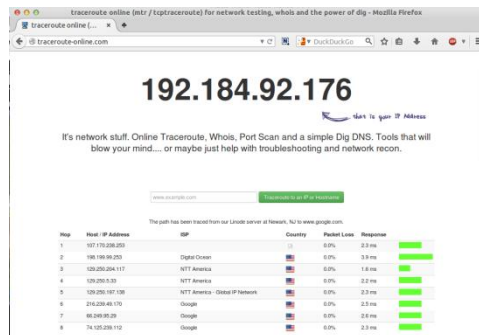
Pengujian terakhir yang dilakukan yaitu pengujian dalam membandingkan koneksi internet. Dalam pengujian yang dilakukan setelah menggunakan jaringan *WiFi* adalah melakukan *traceroute* terhadap [www.google.com](http://www.google.com). *Provider* yang pertama digunakan yaitu *XL Axiata*, dengan jumlah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



Gambar 5. Halaman hasil proses *traceroute provider XL*

Pada gambar 5 terlihat halaman dari hasil proses *traceroute* muncul saat melakukan akses ke *website www.google.com*. 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.

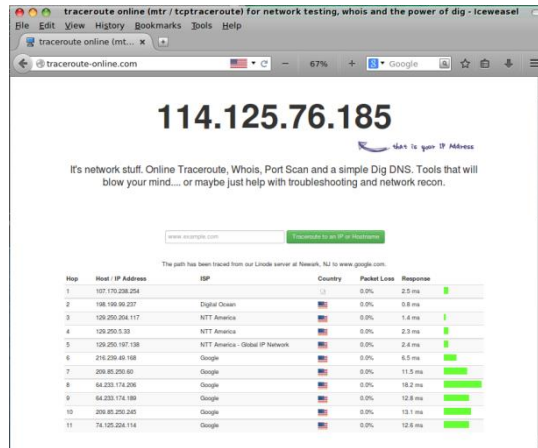


Gambar 6. Halaman hasil proses *traceroute* menggunakan *VPN network 1*

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*.

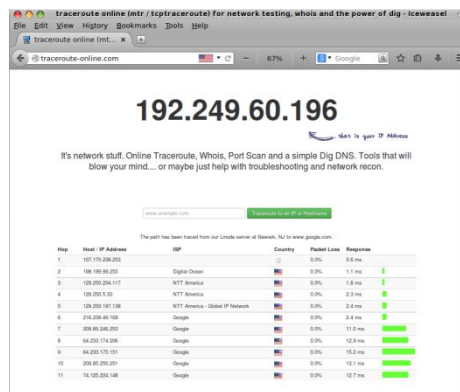
Pengujian selanjutnya yaitu dengan mengganti *provider* untuk *modem USB* yang digunakan yaitu *Telkomsel*. Proses yang akan dilakukan sama seperti proses saat menggunakan *provider* sebelumnya yaitu dengan menggunakan *traceroute*.



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.



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.

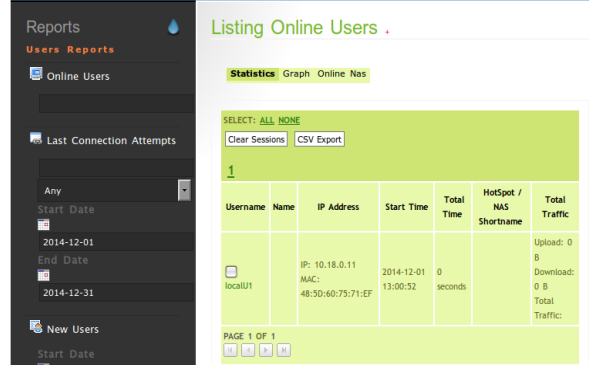
Dalam proses otentikasi yang berjalan, FreeRADIUS dapat merespon data user dari database yang digunakan oleh pengguna WiFi. Hal tersebut dapat dilihat melalui fitur report yang ada pada aplikasi DaloRADIUS seperti yang ditunjukkan pada gambar 10.

Gambar 10. Hasil otentikasi data user jaringan WiFi

Pada gambar 10 terlihat bahwa proses otentikasi telah berhasil diproses dan otentikasi tersebut telah mengekstriksi 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*.

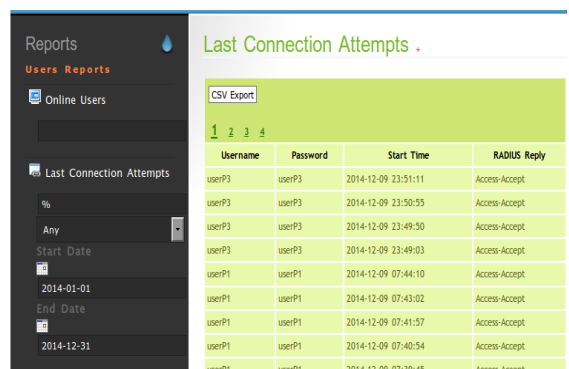
Selain melihat hasil dari proses otentikasi, di dalam aplikasi *DaloRADIUS* juga terdapat fitur untuk melihat *user* yang sedang menggunakan *WiFi*, hal ini dapat dilihat pada gambar 11.



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.



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 kewanaman 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.

Username	Name	IP Address	Start Time	Total Time	HotSpot / NAS Shortname	Total Traffic
user3		IP: 10.8.0.6 MAC: 112.215.44.128	2014-12-09 23:53:57	0 seconds	WiFi-Network-2	Upload: 0 B Download: 0 B Total Traffic:
user1		IP: 10.8.0.6 MAC: 114.125.77.140	2014-12-09 23:58:06	0 seconds	WiFi-Network	Upload: 0 B Download: 0 B Total Traffic:

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 mengurangi resiko penyalahgunaan layanan *WiFi*, karena untuk setiap *user* yang ingin 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, Dedy., 2012, *Penerapan Teknologi Mikrotik 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