Otentikasi dan Manajemen Pengguna Hotspot Router Mikrotik Menggunakan RADIUS dan PHP-MySQL

David Cesar Pramudita[(1)]
Aryo Pinandito S.T, M.MT [(2)], Eko Sakti Pramukantoro, S.Kom, M.Kom[(2)]
[(1)]Mahasiswa, [(2)]Dosen Pembimbing I, [(2)]Dosen Pembimbing II
Program Studi Informatika/Ilmu Komputer
Program Teknologi Informasi dan Ilmu Komputer
Jl. Veteran No.8, Malang 65145, Indonesia
Email : david.csar4@gmail.com

ABSTRAK

Router Mikrotik telah menyediakan sistem manajemen terhadap user hotspot melalui paket program yang terpisah bernama User Manager. Permasalahan utama adalah integrasi aplikasi user manager kedalam perangkat keras router mikrotik dinilai kurang efektif dan fleksibel, karena untuk melakukan proses manajemen terhadap user hotspot harus dilakukan pada tiap-tiap router yang berada pada area hotspot yang tentunya akan membutuhkan waktu yang relatif lama. Dari permasalahan tersebut maka dibuatlah sistem baru dengan memanfaatkan eksternal RADIUS server sebagai pusat dari proses otentikasi maupun manajemen terhadap user hotspot mikrotik. Dari hasil pengujian sistem yang telah dilakukan, proses otentikasi pada sistem internal RADIUS terbukti 13 % lebih cepat dibandingkan dengan sisten dengan eksternal RADIUS. Sedangkan dari sisi proses manajemen sistem manajemen terpusat melalui eksternal RADIUS terbukti dapat meminimalkan waktu ¾ lebih cepat dibanding sistem internal RADIUS.

ABSTRACT

Mikrotik Router provides management system of hotspot user through separated program package named User Manager. The main problem is user manager application on the router mikrotik hardware is considered less effective and flexible. It is because of the management process of hotspot user has to be done to each router on the hotspot area which takes much time. Due to that problem, the new system was made by using RADIUS external server as the center of the authentication process and the management of mikrotik hotspot user. Based on the result of the testing system, authentication prosess in internal RADIUS system prove that 13% more faster than eksternal RADIUS system. Whereas from management prosess centralize management using eksternal RADIUS can minimalize time ¾ more faster than internal RADIUS server.

Keyword : Mikrotik hotspot, RADIUS, freeradius, Management users

I. Pendahuluan

Komunikasi tanpa kabel/nirkable *(wireless)* telah menjadi kebutuhan dasar gaya hidup baru masyarakat informasi. LAN nirkable yang lebih dikenal dengan jaringan Wi-Fi menjadi teknologi alternative dan relative lebih mudah diimplementasikan di lingkungan kerja *(SOHO/Small Office Home Office)*, seperti di perkantoran, laboratorium komputer, dan sebagainya. Installasi perangkat jaringan Wi-fi lebih fleksibel karena tidak membutuhkan penghubung kabel antar komputer [TRI-05]. Kemudahan-kemudahan yang ditawarkan wireless LAN menjadi daya tarik tersendiri bagi para pengguna komputer menggunakan teknologi ini untuk mengakses suatu jaringan komputer atau internet [AGU-05].

Mikrotik merupakan salah satu produk dari sekian banyak merek hardware yang sering digunakan sebagai perangkat keras yang digunakan untuk membangun sebuah jaringan berbasis *wireless.* Mikrotik juga menyediakan sistem manajemen jaringan melalui packet program yang terpisah bernama user manager. Namun hal yang menjadi suatu permasalahan adalah integrasi aplikasi user manager kedalam perangkat keras router mikrotik dinilai kurang efektif dan fleksibel jika diimplementasikan kedalam jaringan hotspot yang luas dimana titik

layanan tersebar pada suatu wilayah. Karena untuk melakukan proses manajemen terhadap user hotspot harus dilakukan pada tiap-tiap router yang berada pada area hotspot yang tentunya akan membutuhkan waktu yang relatif lama.

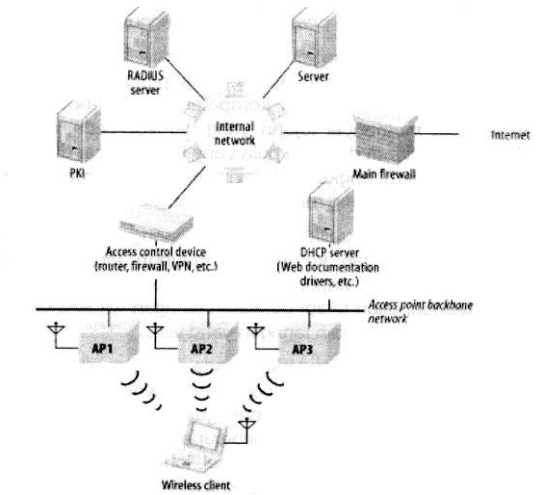
RADIUS merupakan suatu protokol yang dikembangkan untuk proses AAA (*authentication, authorization, and accounting.). Remote Access Dial-in User Service (RADIUS)*, merupakan suatu mekanisme akses kontrol yang mengecek dan mengautentifikasi *(authentication)* user atau pengguna berdasarkan pada mekanisme authentikasi yang sudah banyak digunakan sebelumnya, yaitu menggunakan metode *challenge/response.* RADIUS menjalankan sistem administrasi pengguna yang terpusat. Sistem ini tentunya akan mempermudah tugas seorang administrator. Dengan sistem ini pengguna dapat menggunakan hotspot di tempat yang berbeda-beda dengan melakukan autentikasi ke server RADIUS[PIT-11].

2. Tinjauan Pustaka

2.1 Hotspot

Secara fungsional, *hotspot public* merupakan jaringan wireless yang menyediakan koneksi jaringan ke internet maupun jarungan intranet perusahaan. Peralatan yang dapat melakukan koneksi tidak terbatas hanya berupa notebook akan tetapi peralatan jaringan wireless yang lain seperti PDA, ponsel atau peralatan jaringan lain. Beberapa fungsionalitas yang ditawarkan pada jaringan wireless public adalah e-mail, chatting, shopping , upload dan download file, bermain game online, hingga surfing web. Para pengguna mobile dapat dengan mudah melakukan aktivitasnya melalui beberapa tempat tanpa dibebeani dengan keruwetan kabel, sepert di kamar hotel, lobi hotel mall atau café. Beberapa unsur dasar pengembangan serta installasi peralatan jaringan yang dibutuhkan adalah [MUL-08]:

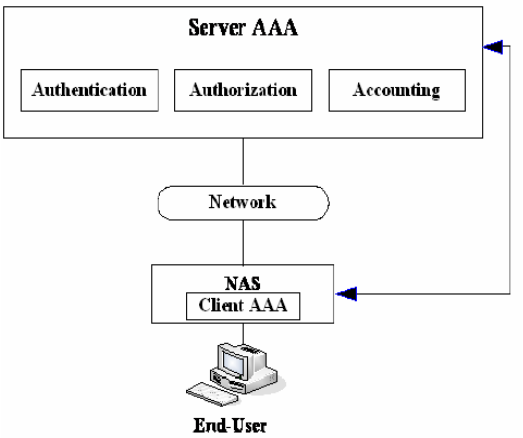
- Mobile station *Access Point*,
- peralatan pengatur akses (Router, Switch, VPN, firewall dan lain-lain)
- Server (server web,
- Server AAA/RADIUS, DHCP) ,
- ISP dan Wireless ISP



Gambar 2.1 Topologi Wlan standar
Sumber: [MUL-08]

2.2 Protokol AAA

Protokol AAA (Authentication, Authorization, Accounting) mengatur mekanisme bagaimana tata cara berkomunikasi, baik antara client ke domain domain jaringan maupun antar client dengan domain yang berbeda dengan tetap menjaga keamanan pertukaran data [WAR-04].



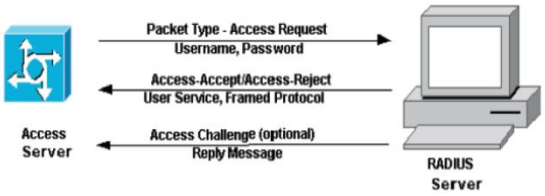
Gambar 2.2 Model arsitektur jaringan AAA
Sumber: [VEN-02]

Pada gambar menununjukkan mekanisme jaringan AAA dimana prosesnya dijeleskan sebagai berikut [VEN-02] :

1. User melakukan koneksi keperalatan NAS point to point sebagai langkah awal koneksi ke jaringan;
2. Network Access Server (NAS) sebagai client AAA kemudian melakukan pengumpulan informasi pengguna dan melanjutkan data pengguna ke server;
3. Server AAA menerima dan memproses data pengguna, kemudian memberikan balasan ke NAS berupa pesan penerima atau penolakan pendaftaran dari pengguna;
4. NAS sebagai client AAA kemudian menyampaikan pesan server AAA tersebut kepada pengguna, bahwa pendaftaran ditolak atau diterima beserta layanan yang diperkenankan untuk akses.

2.3 RADIUS

RADIUS (Remote Access Dial-In User Service) adalah protocol AAA yang sebagian besar digunakan di dunia, kompetitor pesainngnya adalah *TICACS+* dan *Kerberos*. Salah satu yang membuat RADIUS lebih baik dibandingkan dengan protocol AAA yang telah ada yaitu vendor dari RADIUS bersifat independen. RADIUS tidak dikontrol oleh vendor tunggal hal ini berlawanan dengan TACACS+ (Cisco) dan Kerberos (Merit) [VEN-02]. RADIUS dikembangkan di pertengahan tahun 90 an oleh Lilingston Entetprise (kemudian dibeli oleh Lucent Technology) untuk menyediakan perlatan NAS dengan didukung layanan authentikasi dan accounting. RADIUS melakukan autentikasi user melalui serangkain komunikasi antara client dan server. Bila user berhasil melakukan autentikasi, maka user tersebut dapat menggunakan layanan yang disediakan oleh jaringan [ANO-06].



Gambar 2.4 Mekanisme authentikasi mengunakan RADIUS server
Sumber: [ANO-06]

Keterangan:

a) User melakukan dial-in menggunakan modem pada Network Access Server (NAS). NAS akan meminta user memasukan nama dan password jika koneksi modem berhasil dibangun.
b) NAS akan membangun paket data berupa informasi, yang dinamakan access-request. Informasi ini diberikan NAS pada server RADIUS berisi informasi spesifik dari NAS itu sendiri yang meminta access-request, port yang digunakan untuk koneksi modem serta nama dan password. Untuk proteksi dari hackers, NAS yang bertindak sebagai RADIUS client, melakukan enkripsi password sebelum dikirimkan pada RADIUS server. Access-request ini dikirimkan pada jaringan dari

RADIUS client ke RADIUS server. Jika RADIUS server tidak dapat dijangkau, RADIUS client dapat melakukan pemindahan rute pada server alternatif pada konfigurasi NAS.

c) Ketika access-request diterima, server autentikasi akan memvalidasi permintaan tersebut dan melakukan dekripsi paket data untuk memperoleh informasi nama dan password. Jika nama dan password sesuai dengan basis data pada server, server akan mengirimkan access-accept yang berisi informasi kebutuhan sistem network yang harus disediakan oleh user, missal RADIUS server akan menyampaikan pada NAS bahwa user memerlukan TCP/IP dan/atau Netware menggunakan PPP *(Point-to-Point Protocol)* atau user memerlukan SLIP (Serial Line Internet Protocol) untuk dapat terhubung pada jaringan. Selain itu access-accept ini dapat berisi informasi untuk membatasi akses user pada jaringan. Jika proses login tidak menemui kesesuaian, maka RADIUS server akan mengirimkan accessreject pada NAS dan user tidak dapat mengakses jaringan.

d) Untuk menjamin permintaan user benar-benar diberikan pada pihak yang benar, RADIUS server mengirimkan authentication key atau signature, yang menandakan keberadaannya pada RADIUS client.

III. Metodologi Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah :

1. Studi literatur dilakukan dari segi teori maupun implementasi sistem, dimana semua sumber bacaan diperoleh dari internet, textbook, jurnal ilmiah maupun tugas ahir.
2. Analisa kebutuhan, dalam tahap analisa kebutuhan dilakukan analisa terhadap aspek yang harus dipenuhi oleh sistem baik secara fungsional maupun non fungsional
3. Perancangan sistem, dalam tahap ini akan menjelaskan rancangan dari sistem yang akan dibuat.
4. Implementasi Sistem, merupakan tahap pembuatan sistem berdasarkan dari rrancangan yang telah dibuat.
5. Pengujian, Proses pengujian dilakukan untuk menguji apakah fungsionalitas dari sistem dapat berjalan dengan baik.
6. Analisa Hasil pengujian, menjelaskan hasil analisa terhadap sistem yang telah dibuat beserta perbandingannya dengan sistem yang telah ada.
7. Penganmbilan kesimpulan dan saran, berisikan inti dari hasil penelitian yang telah dilakukan dimana memuat hasil analisis yang telah dibuat berdasarkan hasil pengujian yang dilakukan pada penelitian dan juga berisi masukan untuk pengembangan penelitian.

IV. Perancangan Sistem

4.1 Analisa Kebutuhan

Berikut kebutuhan-kebutuhan fungsional yang dibutuhkan sistem:

a. Sistem manajemen user hotspot harus menyediakan fitur otentikasi bagi admin hotspot yang ingin malakukan manajemen terhadap user hotspot.
b. Sistem manajemen hotspot harus menyediakan fitur create, read, update dan delete untuk menambahkan data key yang akan digunakan untuk hak akses terhadap jaringan hotspot.

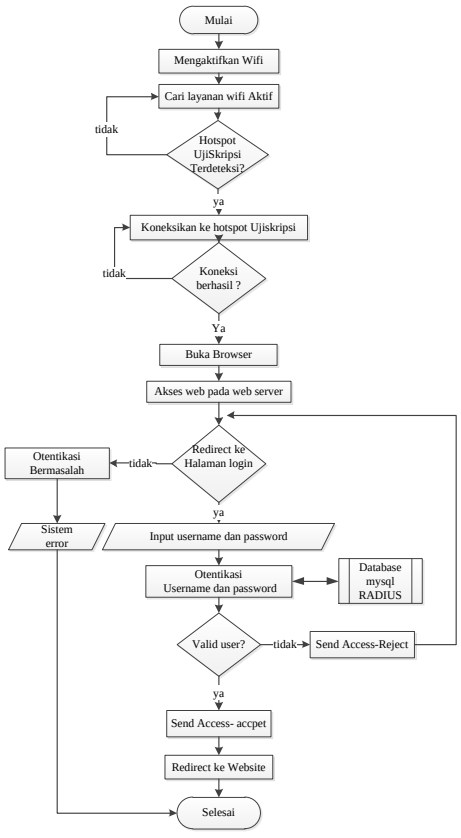
Sedangkan kebutuhan non fungsional yang harus dipenuhi oleh sistem anatara lain:

a. *Avalibility* data yang tersimpan dalam database server harus terjamin keberadaannya
b. *Security*, data user yang tersimpan harus dijamin keamanannya.
c. Basis data harus memiliki performa yang baik dalam hal proses *query* yang cepat
d. Sistem yang mampu menangani *login request* dalam jumlah banyak dalam setiap waktu
e. Sistem yang mampu memberikan kemudahan dalam hal proses manajemen terhadap user hotspot mikrotik.

4.2 Perancangan Proses

4.2.1 Perancangan Proses Otentikasi

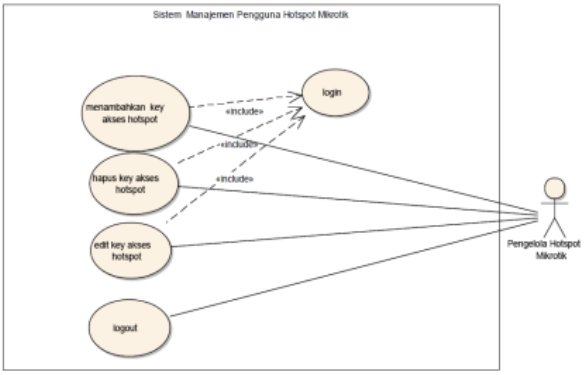
Perancangan sistem otentikasi user bertujuan untuk menjelaskan bagaimana proses otentikasi pengguna hotspot mikrotik dilakukan oleh sistem. Adapun tahapan-tahapan dalam proses otentikasi dijelaskan melalui diagram alur pada gambar 4.2



Gambar 4.1 Diagram alur sistem Otentikasi pengguna Hotspot

4.2.1 Perancangan Proses Manajemen Pengguna Hotspot Mikrotik

Proses manajemen pengguna hotspot mikrotik akan disumulasikan melalui program yang telah dibuat sendiri oleh peneliti dimana seluruh kebutuhan fungsionalitas yang dimiliki oleh program simulasi manajemen pengguna hotspot mikrotik akan dimodelkan menggunakan UML *(Unified Modeling Language).* Dalam proses pengembangan aplikasi web peneliti menggunakan metode pemrograman berbasis MVC *(Model View Controller)* dengan menggunakan *framework PHP.*



Gambar 4.2 Diagram *use cas* manajemen pengguna hotspot mikrotik

4.3 Perancangan Database Sistem

Dalam membangun sistem dibutuhkan database pendukung yang terdiri dari 8 buah table dimana semua tabel merupakan tabel bawaan dari program freeradius. Sehingga peneliti tidak perlu untuk melakukan pembuatan ulang table database namun hanya perlu melakukan proses import dua buah file bernama schema.sql dan nas.sql dimana hasil *dump* file database tersebut, Dari delapan tabel hanya dua buah table yang digunakan oleh program untuk melakukan proses manajemen terhadap user. Table radcheck merupakan tabel yang digunakan untuk proses otentikasi user dimana nantinya ketika admin hotspot ingin menambahkan, menghapus, dan

mengedit key yang digunakan untuk hak akses client pada jaringan hotspot semua operasi dilakukan melalui tabel ini. Berikut merupakan struktur dari table radcheck.

Nama Attribute	Type	Null
Id	Int(11)	No
username	Varchar(64)	No
Attribute	Varchar(64)	No
Op	Char(2)	No
Value	Varchar(253)	No

Table 4.1 Struktur table radcheck

Untuk meningkatkan sisi keamanan sistem data agar data yang disimpan pada table radcheck tidak mudah dibaca oleh orang lain yang tidak berkepentingan maka dari itu sistem menerapkan enskripsi terhadap password. pengaturan enskripsi dilakukan melalui table radgroupcheck.

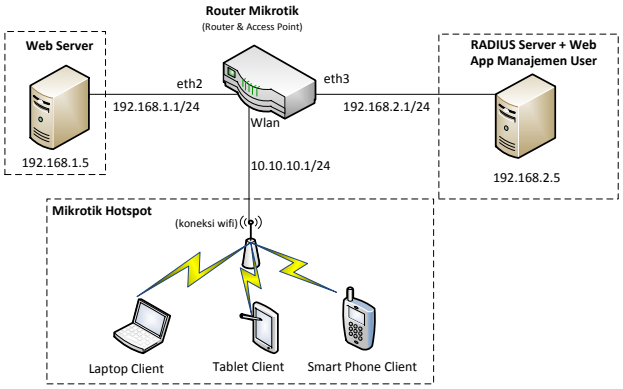
Nama Attribute	Type	Null
Id	Int(11)	No
groupname	Varchar(64)	No
attribute	Varchar(64)	No
Op	Char(2)	No
Value	Varchar(64)	No

Table 4.2 Struktur table radgroupcheck

4.4 Perancangan Topologi Jaringan

perancangan topologi jaringan yang digunakan pada penelitian dijelaskan seperti pada gambar 4.13 berikut Berikut merupakan penjelasan bagaimana sistem bekerja :

1. Client hotspot yang telah terkoneksi pada layanan wifi maka secara otomatis akan mendapatkan alamat IP DHCP dari router, adapun alamat network yang dari client hotspot 10.10.10.1/24
2. Ketika client hotspot mengakses sebuah halaman website pada alamat IP 192.168.1.2 secara otomatis router akan melakukan proses routing dari network 10.10.10.1/24 ke alamat network dari web server yaitu 192.168.1.1/24
3. Seketika itu pula maka router akan menampilkan halaman portal otentikasi dimana user dituntut untuk memasukkan username dan password untuk proses otentikasi user hotspot.
4. Proses authentikasi sendiri akan mengirim paket data inputan user yang berisi username dan password ke sebuah server otentikasi yang berada pada server radius yang berada pada alamat network 192.168.2.1/24 dengan alamat ip address static 192.168.2.5,
5. *RADIUS* akan melakukan pengecekan melalui proses query database pada table radcheck, jika RADIUS status otentikasi bernialai Access-accept maka secara otomatis akan dapat mengakses sebuah halaman website yang berada pada *web server*. Namun jika hasil proses otentikasi bernilai *access-reject* maka akses layanan hotspot tidak akan diberikan dan user akan secara otomatis diarahkan kembali ke halaman web portal otentikasi.



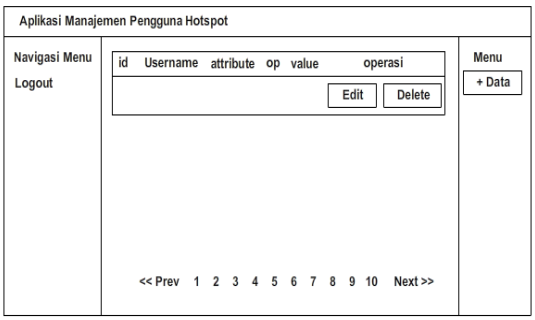
Gambar 4.13 Perancangan Topologi Jaringan

4.5 Perancangan Antarmuka Aplikasi

Berikut merupakan perancangan antarmuka program manajemen pengguna hotspot mikrotik.

1. Dashboard utama

Gambar 4.15 adalah rancangan halaman utama dari program dimana berisikan data beserta menu operasi yang dapat dijalan untuk melakukan pengelolaan data pada sistem.

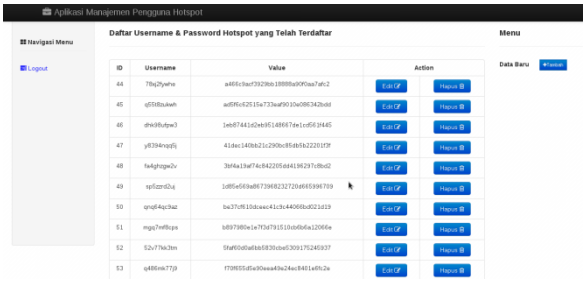


Gambar 4. 14Form inputan data key baru

V. Implementasi

5.1 Implementasi Antarmuka Program

menambahkan data baru, menghapus data dan mengedit data yang telah ada. Selain menyediakan opersi terkait pengelolaan terhadap data pada halaman dashboard juga disediakan menu logout yang berfungsi untuk keluar dari program.



Gambar 5.1 Dashboard menu utama program
Sumber: Perancangan

VI. Pengujian dan Analisis

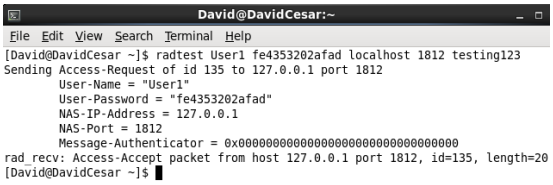
6.1 Pengujian Fungsional

Pada tahap pengujian sistem secara fungsional dilakukan dengan dua buah skenario. Skenario pertama dilakukan dengan melakukan proses pengujian otentikasi pada sisi server RADIUS sedangkan skenario kedua dilakukan pengujian otentikasi pada client hotspot mikrotik melalui captive portal.

6.1.1 Pengujian Otentikasi pada RADIUS Server

Pengujian ini dilakukan untuk memastikan RADIUS server dapat berjalan dengan baik dalam melakukan proses otentikasi terhadap data user yang terekam dalam database MySQL. Berikut perintah untuk melakukan pengujian otentikasi

```
# radtest user1 adminuser localhost
  1812 testing123
```



Gambar 6.1 Keterangan *reply-message* dari pengujian otentikasi

Dari hasil pengujian proses otentikasi pada RADIUS server secara umum server dapat berjalan dengan baik dalam hal menangani permintaan *authentication request* hal ini dapat diketaui melalui status dari proses otentikasi yang bernilai *access-accept.*

6.1.2 Pengujian Otentikasi Melalui *Captive Portal*

Pengujian otentikasi captive portal dilakukan untuk untuk menguji apakah proses otentikasi di sisi client hotspot dapat berjalan dengan baik. Berikut merupakan hasil pengujian otentikasi yang dilakukan pada client hotspot malalui captive portal.

Kondisi	Username	Password	Proses Login	
			S	G
Database kosong	-	-		√
Data Baru	User1	fe4353202afad	√	
Ubah password	User1	fe4353202afad		√
Passsword baru	User1	Fag4re245halog4	√	
Case Sensitif	User1	Fe4353202afad		√
Case Sensitif	User1	FE4353202AFAD		√
Case Sensitif	user1	fe4353202afad	√	
Data dihapus	-	-		√

Tabel 6.1 Hasil pengujian otentikasi melalui captive portal'

Berdasarkan pada tabel hasil pengujian didapat bahwa ketika username dan password tidak ada pada database server RADIUS maka proses otentikasi gagal dilakukan. Demikian juga ketika username benar (sesuai) namun password yang dimasukkan tidak sesuai huruf besar-kecilnya, maka akses untuk masuk ke halaman login akan gagal. Begitu pula ketika data yang telah ada dalam database server otentikasi dihapus maka proses login tidak dapat dilakukan. Secara umum sistem otentikasi dan manajemen user telah berjalan dengan baik, namun sistem sedikit memiliki kekuraan dalam hal tidak dapat membedakan besar kecilnya huruf pada bagian username

6.2 Pengujian Non fungsional

. Pengujian performa dilakukan dengan menghitung nilai *response time*, *trougput* dan *resource system* yang meliputi *CPU usage*, RAM, dan *disk usage* yang digunakan oleh router mikrotik. Pengujian dilakukan dengan melakukan *stress load* dengan mengirimkan proses otentikasi dalam jumlah besar pada server server default internal RADIUS maupun eksternal RADIUS dimana untuk melakukan proses ini digunakan aplikasi Apache Jmeter. Pengujian dilakukan dengan jumlah thread sebesar 100, waktu ramp-up 1 detik dan jumlah perulangan sebesar 1 kali. Berikut hasil *benchmarking* berdasarkan pengujian yang telah dilakukan dengan menggunakan aplikasi Apache Jmeter

Ket.	Internal RADIUS		Eksternal RADIUS	
	Response time	*Troughtput*	*Response time*	*Trought put*
Uji 1	364	24,7	576	18,1
Uji 2	431	25,1	730	17,3
Uji 3	407	24,9	436	49,1
Uji 4	326	32,6	384	47,9
Rata-rata	400	26,8	531.5	33.1

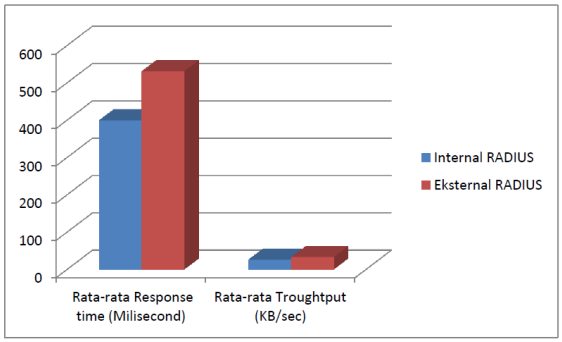
Tabel 6.2 Hasil *benchmarking* sistem internal dan eksternal RADIUS

Sedangkan pengujian *resource system* pada router mikrotik melalui proses *stress load* dilakukan dengan konfigurasi kontrol group dengan jumlah *thread* = 100, periode *ramp-up* = 1 (dalam detik), jumlah perulangan = 10. Pengujian *stress load* dilakukan dengan menggunakan dua buah komputer dengan dimana proses *stress load* dilakukan dalam waktu yang bersamaan. Berikut hasil berdasarkan proses pengujian yang telah dilakukan

Sistem	Resource System		
	Rata-rata CPU Usage (%)	Rata-rata RAM (%)	Rata-rata Disk Usage (%)
Internal RADIUS	5	51,7	33,5
Eksternal RADIUS	6	53	33,4

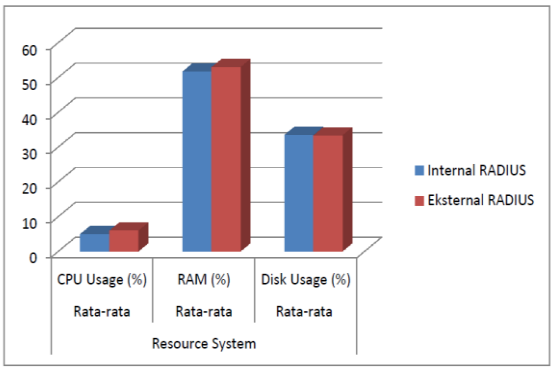
Table 6.3 Hasil pengujian *resource system* pada router mikrotik RB-751

Berdasarkan hasil pengujian yang didapatkan secara umum router yang menggunakan sistem internal RADIUS sebagai proses otentikasi dan manajemen user memiliki performa yang lebih baik dibandingakan sistem eksternal RADIUS hal ini dibuktikan dari nilai resource system dari router mikrotik yang lebih kecil, meskipun selisih nilai performa dari kedua sistem hanya terpaut relatif kecil. Adapun perbandingan resource system eksternal radius dan internal radius dalam hal *CPU usage* sebesar 6 % : 5%, RAM sebesar 53 % : 51,7% (dalam MiB) dan *disk usage* sebesar 33,4 % : 33,5 % (dalam MiB).



Gambar 6.2 Grafik perbandingan rata-rata *response time*, dan *throughput*

Berdasarkan hasil pengujian yang didapatkan secara umum router yang menggunakan sistem internal RADIUS sebagai proses otentikasi dan manajemen user memiliki performa yang lebih baik dibandingakan sistem eksternal RADIUS hal ini dibuktikan dari nilai resource system dari router mikrotik yang lebih kecil, meskipun selisih nilai performa dari kedua sistem hanya terpaut relatif kecil. Adapun perbandingan resource system eksternal radius dan internal radius dalam hal *CPU usage* sebesar 6 % : 5%, RAM sebesar 53 % : 51,7% (dalam MiB) dan *disk usage* sebesar 33,4 % : 33,5 % (dalam MiB).



Gambar 6.3 Grafik perbandingan rata-rata *resource system* pada router mikrotik

VII. Kesimpulan dan Saran

7.1 Kesimpulan

Dari hasil penelitian dan analisa yang sudah dilakukan, dapat diambil kesimpulan sebagai berikut:

1. Sistem otentikasi dan manajemen user hotspot router mikrotik yang bersifat internal terbukti dapat dilakuakan secara terpisah dengan cara mengeluarkan fungsionalitas yang dimiliknya kedalam sebuah eksternal radius server yang berada di luar router mikrotik.
2. Sistem otentikasi dan manajemen user hotspot router mikrotik terbukti dapat dilakukan menggunakan eksternal RADIUS server dengan memanfaatkan program PHP sebagai *tools* untuk melakukan proses manajemen terhadap data yang digunakan user untuk proses otentikasi pada layanan hotspot, dimana data-data tersebut disimpan dalam database MySQL server RADIUS.
3. Dalam melakukan proses otentikasi sistem internal RADIUS terbukti 13 % lebih cepat jika dibandingkan dengan sistem ekternal RADIUS hal ini merujuk pada hasil pengujian rata-rata nilai *response time* sistem internal dan ekstenral *RADIUS* yang

menunjukan perbandingan sebesar 400 : 532 *milisecond.*

4. Sistem manajemen terpusat yang dilakukan melalui eksternal RADIUS server terbukti dapat meminimalkan waktu ¾ lebih cepat dengan asumsi proses manajemen 4 buah router dengan jumlah user 40 melalui eksternal RADIUS dibutuhkan waktu 6 menit, sedangkan jika dilakukan melalui setiap router membutuhkan waktu rata-rata 2 menit untuk menambahkan 10 user.

7.2 Saran

Saran yang diberikan untuk perkembangan penelitian antara lain:

1. Perlunya perancangan topologi jaringan yang lebih kompleks yang menggunakan banyak router, agar tingkat efisensi proses manajemen user hotspot menggunakan eksternal RADIUS dapat terlihat.
2. Jumlah user yang digunakan dalam pengujian otentikasi sebaiknya ditambah agar performa sistem dapat benar-benar terlihat.

Daftar pustaka

[ANO-06] Anonymous. 2006. "How Does RADIUS Work" [terhubung berkala]. http://www.cisco.com/image/gif/paws/12433/32.pdf[1 Nov 2013].

[ANO-06] Anonymous. 2006. "Hotspot Gateway" [terhubung berkala]. http://www.mikrotik.com/testdocs/ros/2.9/ip/hotspot.php [4 Maret 2014].

[TRI-05] Priyambodo, T.K dan Heriadi,D.2005, Jaringan Wi-Fi Teori dan Implementasi, Andi, Yogyakarta.

[AGU-05] Setiawan, A.W.2005. Remote Authentication Dial In User Service (RADIUS) untuk Autentikasi Pengguna Wireless LAN, Tugas Mata Kuliah EC-5010 Keamanan Sistem Informasi, Institut Teknologi Bandung (ITB), Bandung.

[PIT-11] Pitikasari, A.R.2011. "Ambisi Telkom 2012, Hadirkan 100 Ribu Titik Wifi di Indonesia", Republika (Jakarta), 7 Desember.

[KUN-11] Kunang, Y.N. dan Yadi, I.Z. 2008. Autentikasi Pengguna Wireless LAN Berbasis Radius Server (Studi Kasus WLAN Universitas Bina Darma, Jurnal Ilmiah Matrik, Vol. 10 No. 2.

[ENA-10] Enaceanu, Alexandru. 2010. "Cost Effective RADIUS Authentication for Wireless Client". Database System Journal, Vol. 1, No. 2, hal 27-32

[SAL-13] Saliau, A.M., and Kolo,M.1., Muhammad,M.K.,Nafiu,L.A. 2013. "Internet Authentication and Billing (Hotspot) System Using Mikrotik Router Operating System". International Journal of Wireless Communication and Mobile Computing, Vol 1, No. 1, hal. 51-57

[CHA-07] Charter, Denny.2007. Konsep Dasar Wireless LAN. [terhubung berkala].http://ilmukomputer.org/wp content/uploads/2008/02/charter-konsepwlan.pdf [1 Nov 2013].

[MUL-08] Mulyanta, Edi. 2008, Pengenalan Protokol Jaringan Wireless Komputer, Andi, Yogyakarta.

[VEN-02] Ventura,Hakan.2002. "DIAMETERNext Generation's AAA Protocol",[terhubung berkala].http://www.diva-portal.org/smash/get/diva2:18347/FULLTEXT01.pdf [4 Nov 2013].

[WAR-04] Warsito.2004."Sistem Kemanan Jaringan Multi Domain Menggunakan Protokol DIAMETER", Laporan Akhir EC7010 InstitutTeknologi Bandung (ITB),Bandung.

[HAS-02] Hassell, Jonathan. 2002. Radius, O'Reilly & Associates, Inc, New York