DOI: http://dx.doi.org/10.22441/fifo.2020.v12i1.005

Implementasi System Captive Portal Dengan Otentikasi RADIUS

Fandi Ali Mustika[1], Febryo Ponco Sulistyo[2], Chairul Anhar Tanof [3]

[1.2.3] *Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana*
Jl. Raya Meruya Selatan, Kembangan, Jakarta, 11650
[1.]fandi.ali@mercubuana.ac.id, [2]febryo.ponco@mercubuana.ac.id, [3]chaerul.at@gmail.com[3]

Abstract

The rapid development of Internet networks in offices, industries, homes, and universities, transforming the conventional system into modern, especially with the Internet. Therefore, it is very important to use a good authentication method to avoid unauthorized user access. Wireless network without authentication can harm users in their activities using Internet access. One of the most effective ways for secure wireless network authentication with Captive portals with Radius authentication method. Captive portals are web pages that control Hyper Text Transfer Protocol (HTTP) browser access to the Internet. The user who is in authentication is their MAC address. Radius is a service that authenticates and authorizes users to network and network infrastructure. This paper will discuss how to use RADIUS authentication with captive portals to manage user authentication on wireless networks. Built-in security mechanism in Wifi 802.11.x equipment to control who can associate to an Access Point (AP). The use of captive portal so that the AP works without configuration settings, so it does not burden the work of the AP itself.

Keywords: *Captive Portal, Radius, Authentication, Wireless Network*

Abstrak

Perkembangan jaringan internet yang semakin pesat di kantor, industri, rumah, dan universitas, mengubah sistem konvensional menjadi modern, terutama dengan adanya internet. Oleh karena itu, sangat penting untuk menggunakan metode otentikasi yang baik untuk menghindari akses pengguna yang tidak sah. Wireless network tanpa otentikasi dapat membahayakan pengguna dalam aktivitas mereka dalam menggunakan akses internet. Salah satu cara yang paling efektif untuk otentikasi wireless network yang aman dengan Captive Portal dengan metode otentikasi Radius. Captive portal adalah halaman web yang mengkontrol Hyper Text Transfer Protocol (HTTP) akses browser ke internet. Pengguna yang di otentikasi adalah MAC address mereka. Radius adalah layanan yang mengotentikasi dan mengotorisasi pengguna ke jaringan dan infrastruktur jaringan. Mekanisme keamanan built-in di peralatan Wifi 802.11.x untuk mengontrol siapa saja yang dapat berasosiasi ke Access Point (AP). Penggunaan captive portal agar AP bekerja tanpa seting konfigurasi, sehingga tidak membebani kerja dari AP itu sendiri.

Kata Kunci: Captive Portal, Radius, Otentikasi, Wireless Network

I. PENDAHULUAN

Pada abad ke 21 ini, internet sudah menjadi alat yang tidak bisa dipisahkan oleh semua orang tanpa memandang usia. Tujuannya bervariasi salah satunya sebagai sumber terpercaya untuk mendapatkan informasi dan transaksi bisnis dan lainnya sebagai media untuk terhubung ke orang yang berbeda di seluruh dunia, memainkan game online.

Salah satu masalah terbesar bagi infrastruktur Wifi, terutama yang membuka akses untuk umum seperti hotspot adalah authentikasi dari pengguna. Captive portal menjadi mekanisme populer bagi infrastruktur wifi dan operator hotspot yang memberikan authentikasi bagi pengguna infrastruktur maupun manajemen flow IP, seperti traffic shaping dan kontrol bandwidth, tanpa perlu menginstalasi aplikasi khusu di komputer pengguna. Proses authentikasi secara aman dapat dilakukan melalui sebuah web browser biasa di sisi pengguna[1].

Beberapa peneliti telah mengungkapkan kerentanan dalam WPA2, yang merupakan terkuat dalam enkripsi dan otentikasi wifi saat ini. Oleh karena itu, untuk meningkatkan keamanan wireless network, mekanisme captive portal telah diperkenalkan yang menggunakan halaman web untuk mengauthentikasi pengguna. Jika pengguna mencoba mengakses internet, web browser akan mengarahkan permintaan ke halaman login[2].

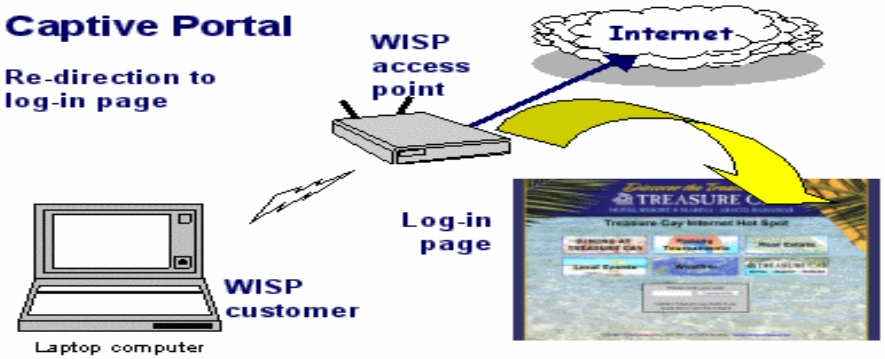
Jadi ide dasar captive portal sangat sederhana. Daripada kita tergantung pada mekanisme keamanan built-in di peralatan wifi 802.11b untuk mengkontrol siapa saja yang dapat berasosiasi ke Access Point (AP), menggunakan captive portal kita mengkonfigurasi agar AP bekerja tanpa WEP dan merupakan network terbuka.

Sistematikanya adalah saat seseorang pengguna berusaha untuk melakukan browsing ke internet, captive portal akan memaksa pengguna yang belum terauthentikasi untuk menuju ke authentikasi web dan akan di beri form login termasuk informasi tentang hotspot yang sedang dia gunakan[3].

Captive portal merupakan suatu teknik authentikasi dan pengamanan data yang lewat dari network internal ke network eksternal. Captive portal sebenarnya merupakan mesin router atau geteway yang memproteksi atau tidak mengizinkan adanya trafik, sampai user melakukan register terlebih dahulu kedalam sistem. Biasanya captive portal ini digunakan pada infrastruktur wireless seperti hotspot area, tapi tidak menutup kemungkinan diterapkan pada jaringan nirkabel.

Berikut adalah perancangan dan pembuatan perangkat lunak (*software*) dari sistem yang akan dibuat. Langkah-langkah pertama dalam pembuatan sistem mulai dari instalasi paket-paket yang dibutuhkan, konfigurasi dan pengujian sistem.

Captive portal merupakan suatu teknik authentikasi dan pengamanan data yang lewat dari network internal ke network eksternal. Cara kerjanya adalah user dengan wireless client diizinkan untuk terhubung wireless untuk medapatkan IP address (DHCP)[4]. Pada saat seorang pengguna berusaha untuk melakukan browsing ke internet, captive portal akan memaksa pengguna yang belum terauthentikasi untuk menuju ke authentikasi web dan akan di beri form login termasuk informasi tentang hotspot yang sedang digunakan.

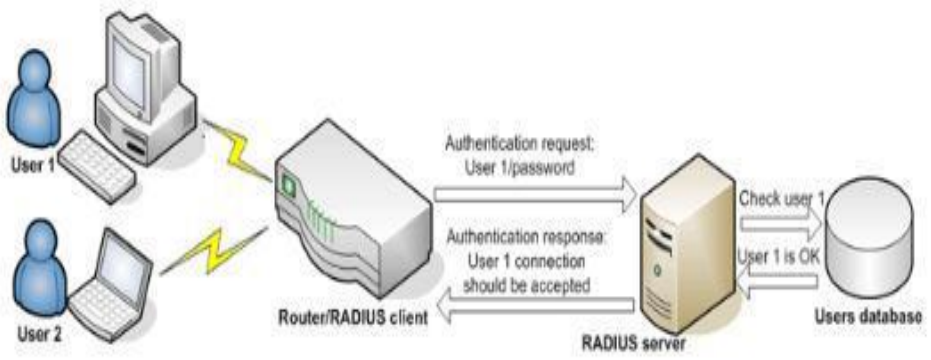


Gambar 1. Captive Portal

Remote Authentication Dial-In User Service (RADIUS) adalah untuk menyediakan mekanisme keamanan dan manajemen user pada jaringan model client-server. Radius merupakan protokol yang dikembangkan untuk proses AAA (Authentication, Authorization, and Accounting)[5]. Berikut ini adalah RFC (Request For Comment) yang berhubungan dengan radius:

- RFC 2865 : Remote Authentication Dial-In User Service (Radius)
- RFC 2866 : Radius Accounting
- RFC 2867 : Radius Accounting for Tunneling
- RFC 2868 : Radius Authentication for Tunneling
- RFC 2869 : Radius Extention
- RFC 3162 : Radius Over IPv6
- RFC 2548 : Microsoft Vendor-Specific RADIUS Attributes

DOI: http://dx.doi.org/10.22441/fifo.2020.v12i1.005



Gambar 2. Infrastruktur RADIUS

Server radius menyediakan mekanisme keamanan dengan mengenai otentikasi dan otorisasi koneksi yang dilakukan oleh user. Pada saat komputer client akan menghubungkan diri dengan jaringan maka server radius akan meminta identitas user (username dan password) yang kemudian akan dicocokkan dengan data yang ada dalam database server radius yang kemudian user diijinkan untuk menggunakan layanan dalam jaringan internet[6].

II. METODOLOGI PENELITIAN

Metodologi penelitian yang digunakan pada sistem captive portal dengan otentikasi radius dapat digambarkan pada gambar 3 dibawah ini.

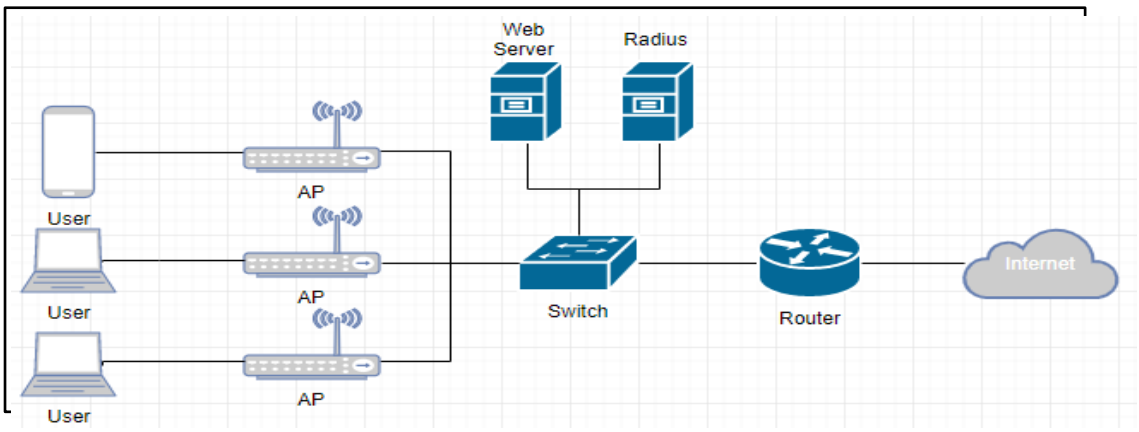
Gambar 3. Metode Penelitian

Model ini melingkupi aktifitas-aktifitas sebagai berikut:

1. Definisi Sistem
   Mendefinisikan sistem yang akan dibuat dengan penjabaran awal sistem, identifikasi kebutuhan sistem, tujuan dan manfaat sistem, cara kerja sistem dan topologi jaringan sistem.
2. Spesifikasi Kebutuhan
   Proses spesifikasi kebutuhan akan menjabarkan tentang awal perancangan sistem dengan menentukan spesifikasi kebutuhan yang sesuai definisi sistem. Spesifikasi kebutuhan terdiri dari atas spesifikasi perangkat keras dan perangkat lunak.
3. Konfigurasi Sistem
   Pada tahap ini, spesifikasi kebutuhan yang telah ditentukan akan di rancang sesuai dengan topologi jaringan dan direalisasikan sebagai serangkaian program atau unit program yang memungkinkan untuk menjalankan tujuan sistem pada cara kerja sistem.
4. Pengujian Sistem
   Unit program diintegrasikan dan diuji sebagai sistem lengkap untuk menjamin bahwa persyaratan sistem telah dipenuhi. Setelah pengujian sistem, sistem siap digunakan dan dianalisis.
5. Analisa Sistem
   Unit yang teah diuji akan dilakukan analisa untuk mendapatkan hasil yang diinginkan.

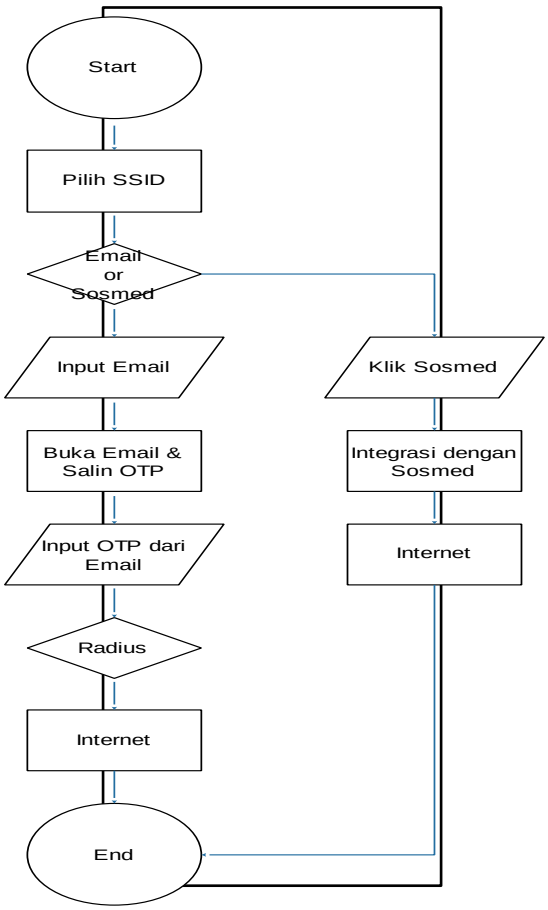
Pada tahap ini sistem dibuat sesuai dengan kebutuhan layanan jaringan wireless yang ada. Sistem yang digunakan dalam penelitian ini menggunakan radius yang saling terintegrasi dalam pencocokan akun dilengkapi

dengan captive portal sebagai antarmuka dalam proses login jaringan hotspot. Sistem ini di desain terlebih dahulu menggunakan topologi jaringan. Topologi jaringan dapat dilihat pada gambar 4 dibawah ini.



Gambar 4. Topologi Jaringan System Captive Portal

Sistem authentikasi jaringan hotspot menggunakan radius yang dimana radius server authentikasi dan captive portal sebagai antarmuka langsung ke jaringan lokal hotspot yang akan diakses oleh klien melalui jaringan lokal. User akan memilih SSID yang sudah dibuat, user akan memilih untuk metode loginnya yaitu dari email atau sosial media, dimana ketika user memilih email maka user akan mendapatkan angka OTP yang dikirimkan ke email user untuk authentikasi ke radius apakah OTP yang diterima user sama dengan OTP yang disimpan oleh radius. Ketika authentikasi OTP email user dengan radius sesuai maka user bisa menggunakan internet yang telah disediakan. Jika user memilih sosial media, user akan menemukan form integrasi ke sosial media user sebagai authentikasi masuk ke jaringan internet wifi. Cara kerja sistem authentikasi hotspot menggunakan radius ini akan dijelaskan pada gambar 5.



Gambar 5. Flowchart Cara Kerja Sistem

III. HASIL DAN PEMBAHASAN

Pada tahap ini, akan ada pengujian dan hasil analisa perangkat lunak captive portal yang akan dibagi menjadi beberapa bagian yang meliputi:

1. Pengujian authentikasi user pada radius server
2. Setting pada *controller* WLC
3. Pengujian authentikasi user pada Captive Portal

3.1 Pengujian Authentikasi User pada Radius Server

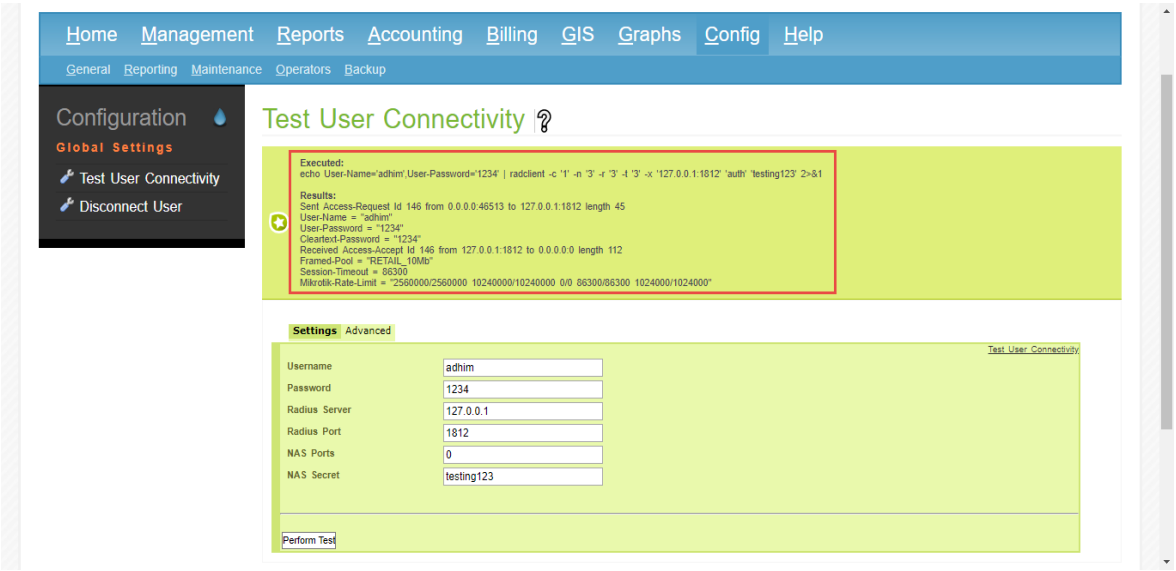
Pada pengujian ini dilakukan untuk menguji proses authentikasi pada sistem apakah user telah ada pada radius server. Dimana prosesnya untuk memasukkan username dan password user. Untuk mengecek apakah username dan password tersebut sudah sinkron dengan cara berikut:

```
root@freeradius:/home/freeradius# radtest adhim 1234 localhost 1812 testing123
```

apabila user tersebut telah terauthentikasi maka keterangannya adalah *access-accept*. Hal ini menunjukan bahwa username dan password serta secret yang dimasukkan telah terekam di radius server, dapat dilihat pada gambar 6 dan 7 dibawah ini.

```
root@freeradius:/home/freeradius# radtest adhim 1234 localhost 1812 testing123
Sent Access-Request Id 159 from 0.0.0.0:50988 to 127.0.0.1:1812 length 75
        User-Name = "adhim"
        User-Password = "1234"
        NAS-IP-Address = 192.168.168.18
        NAS-Port = 1812
        Message-Authenticator = 0x00
        Cleartext-Password = "1234"
Received Access-Accept Id 159 from 127.0.0.1:1812 to 0.0.0.0:0 length 112
        Framed-Pool = "RETAIL_10Mb"
        Session-Timeout = 86300
        Mikrotik-Rate-Limit = "2560000/2560000 10240000/10240000 0/0 86300/86300 1024000/1024000"
```

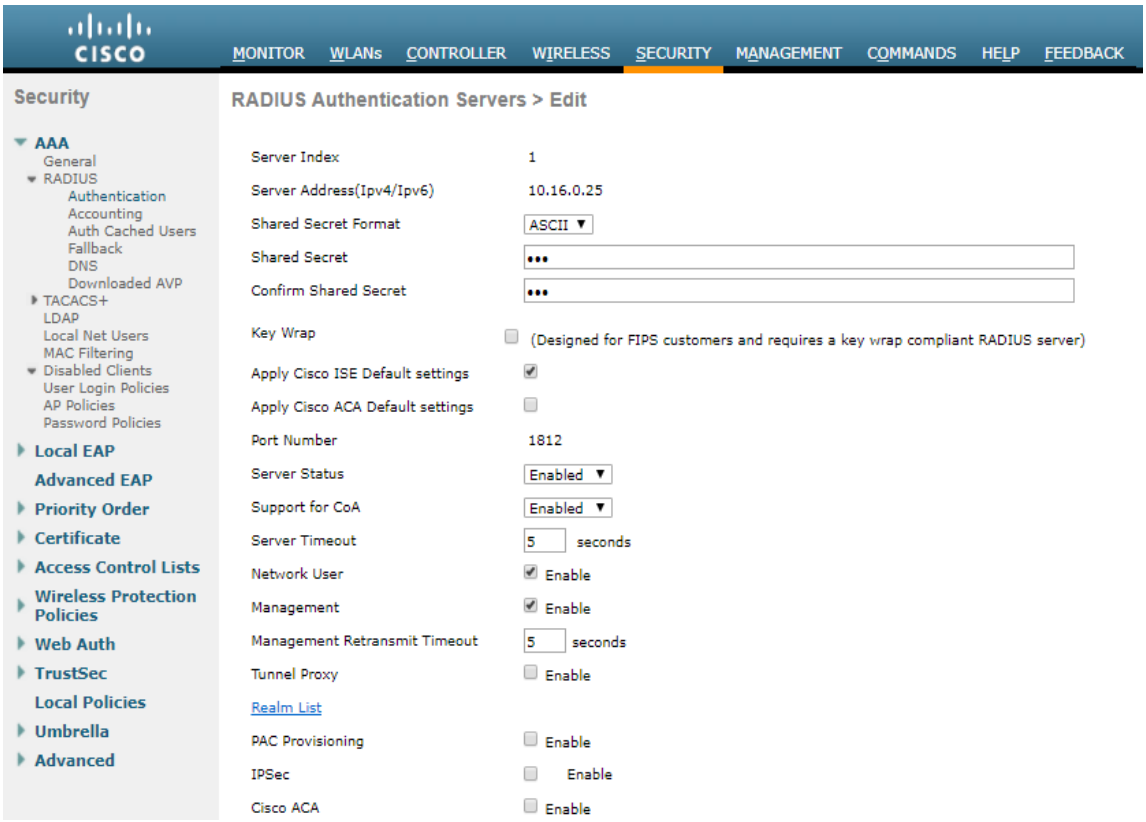
Gambar 6. Authentikasi Radius Server Via CLI



Gambar 7. Authentikasi Radius Server Via Web

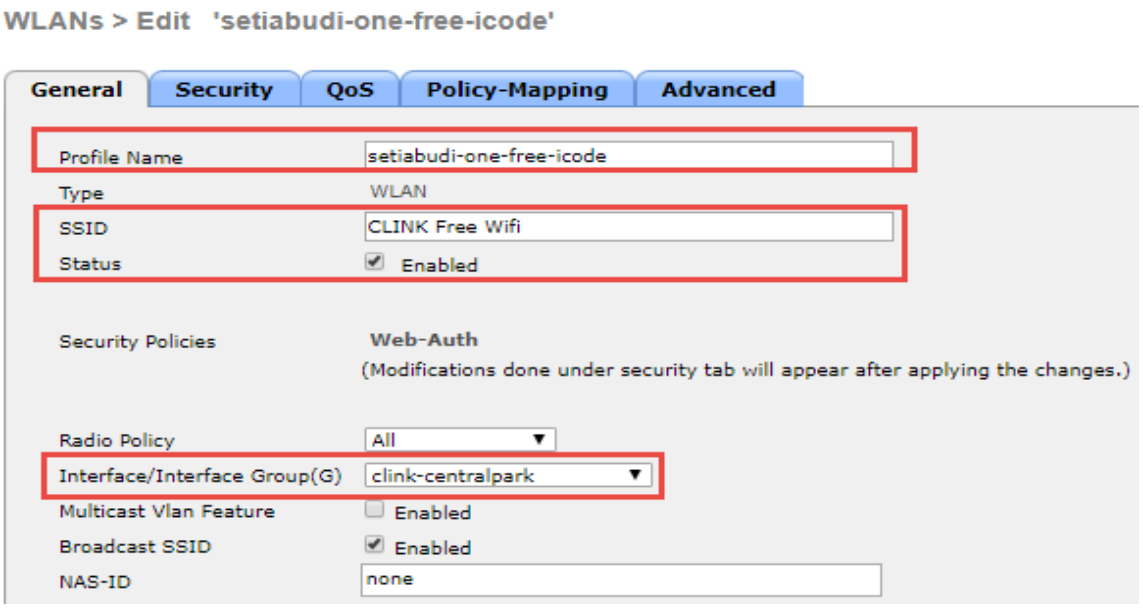
3.2 Setting pada *Controller* WLC

Seting radius dari wlc ini merupakan penghubung antara WLC dengan radius berisikan IP radius dan secret yang akan digunakan berserta default portnya yaitu 1812.



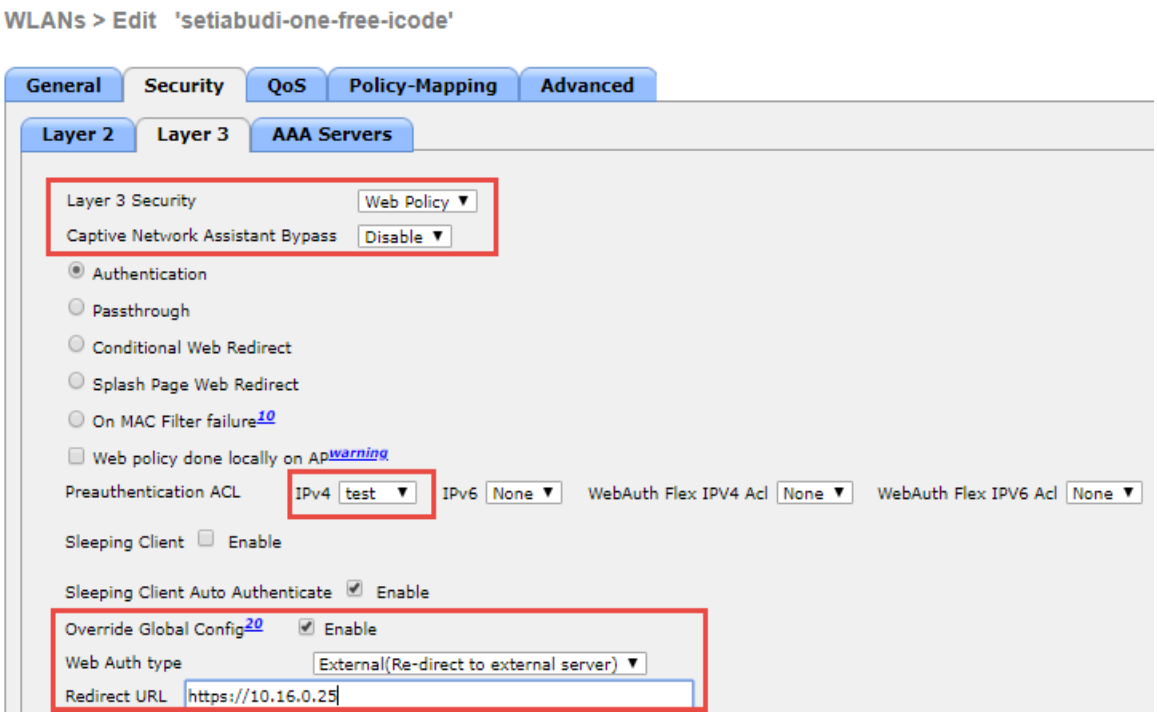
Gambar 8. Setting Radius Authentikasi di WLC

Selanjutkan baru dibuatkan WLAN dengan profile name, SSID dan interface yang akan digunakan.



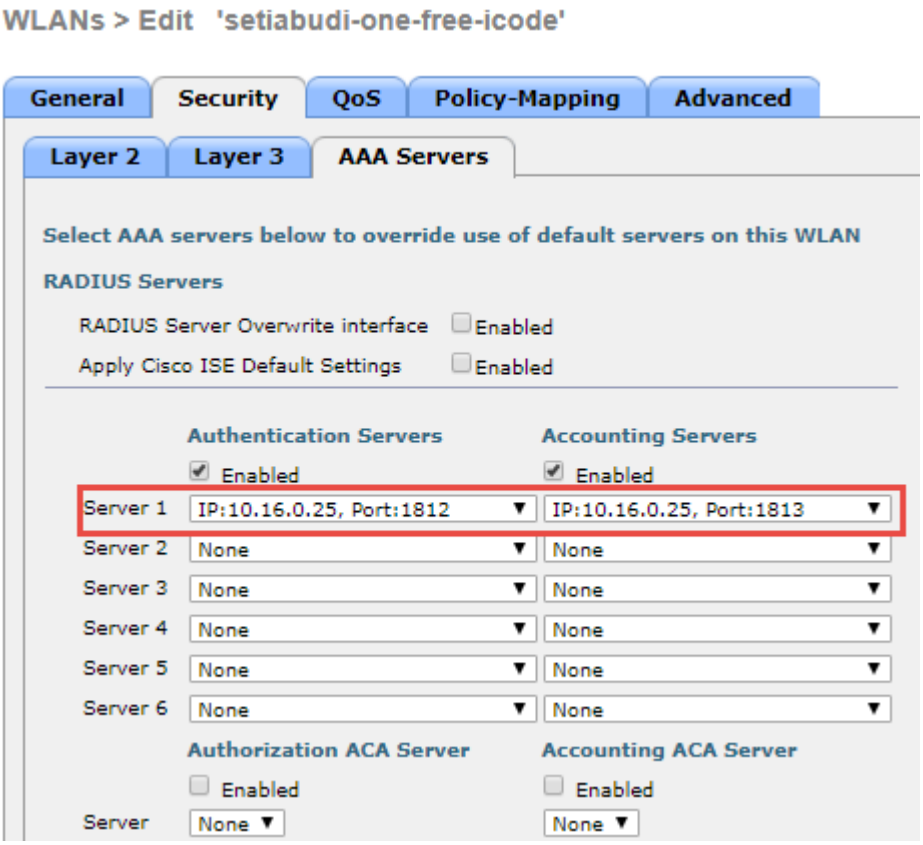
Gambar 9. Create Profile Name dan SSID

Setelah itu baru setting *security* yang akan dipakai dan dihubungkan dengan captive portal. Pada tab layer 3 diharuskan untuk memilih Web Policy, preauthentication ACL IPv4 diisikan hasil yang telah dibuat pada gambar 12 untuk mengallow semua sosmed yang dibutuhkan dengan menggunakan *Access Control List* (ACL).



Gambar 10. Setting *Security* Layer 3 di WLC

Setelah Layer 3 disetting silahkan ke tab AAA Servers yaitu dimana tab ini berisikan tentang *authentication server* dan *accounting server* yang berada di radius.



Gambar 11. Setting AAA Server di WLC

Setelah *security* telah disetting semua, selanjutkan dibuatkan *access control list* yang dimana ACL ini akan mengallow semua IP yang dibutuhkan untuk bisa koneksi ke sosmed tanpa internet.

Access Control Lists > Edit

< Back

General

Access List Name test

Deny Counters 5832591

Seq	Action	Source IP/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	207.148.75.205	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any	Any	Outbound	604075
2	Permit	0.0.0.0	/ 0.0.0.0	207.148.75.205	/ 255.255.255.255	Any	Any	Any	Any	Inbound	517955
3	Permit	10.16.0.25	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	TCP	Any	Any	Any	Any	466579
4	Permit	0.0.0.0	/ 0.0.0.0	10.16.0.25	/ 255.255.255.255	TCP	Any	Any	Any	Any	412861
5	Permit	10.16.0.25	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	UDP	Any	Any	Any	Any	0
6	Permit	0.0.0.0	/ 0.0.0.0	10.16.0.25	/ 255.255.255.255	UDP	Any	Any	Any	Any	3
7	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	TCP	Any	110	Any	Inbound	13570
8	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	TCP	110	Any	Any	Outbound	15243
9	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	TCP	Any	995	Any	Inbound	773
10	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	TCP	Any	143	Any	Inbound	22
11	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	TCP	143	Any	Any	Outbound	8
12	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	TCP	Any	993	Any	Inbound	9471
13	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	TCP	993	Any	Any	Outbound	10089
14	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	TCP	995	Any	Any	Outbound	1080
15	Permit	0.0.0.0	/ 0.0.0.0	157.240.24.35	/ 255.255.255.255	TCP	Any	HTTPS	Any	Inbound	19868
16	Permit	0.0.0.0	/ 0.0.0.0	157.240.24.35	/ 255.255.255.255	TCP	HTTPS	Any	Any	Outbound	0
17	Permit	0.0.0.0	/ 0.0.0.0	157.240.13.35	/ 255.255.255.255	Any	Any	Any	Any	Any	9127
18	Permit	0.0.0.0	/ 0.0.0.0	157.240.24.174	/ 255.255.255.255	TCP	Any	HTTPS	Any	Any	2423
19	Permit	157.240.24.174	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	TCP	HTTPS	Any	Any	Any	3147
20	Permit	157.240.13.35	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any	Any	Any	6564
21	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	UDP	DNS	Any	Any	Any	164955
22	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	UDP	Any	DNS	Any	Any	170414

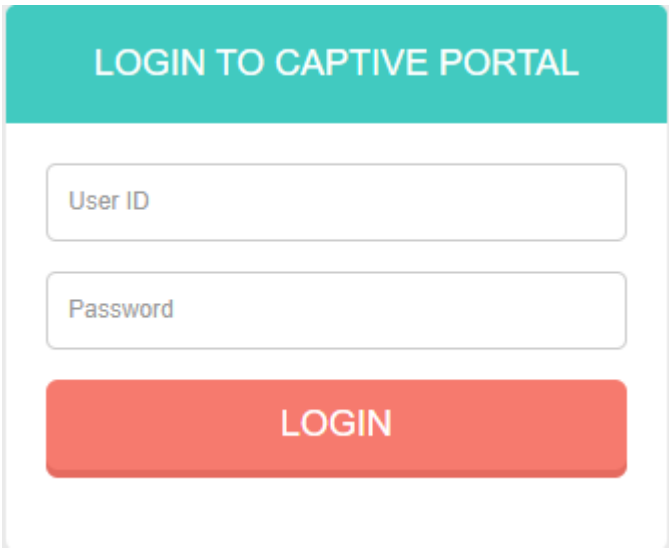
Gambar 12. *Create Access Control List* di WLC

3.3 Pengujian authentikasi user pada Captive Portal

Setelah setting semua dilakukan maka akan dicoba untuk pengujian authentikasi user pada captive portal yang dimana user bisa menggunakan device apa saja baik laptop maupun menggunakan HP. Berikut ketika user sudah memilih SSID yang telah ditetapkan pada gambar 13 dibawah ini.

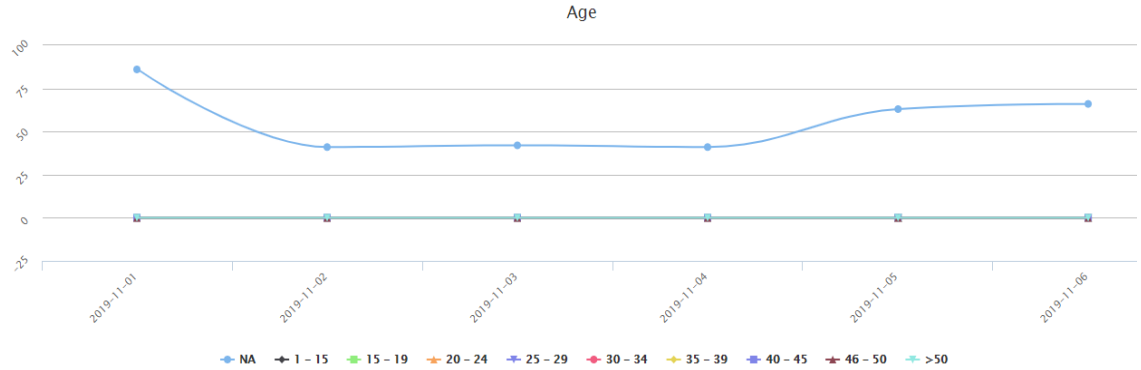
Gambar 13. Halam Login Captive Portal

Untuk memonitoring semua yang ada di captive portal baik yang menggunakan SSID, maka dibuatlah aplikasi untuk memonitoring itu semua. Berikut adalah form login untuk masuk ke monitoring captive portal pada gambar 14 dibawah ini.



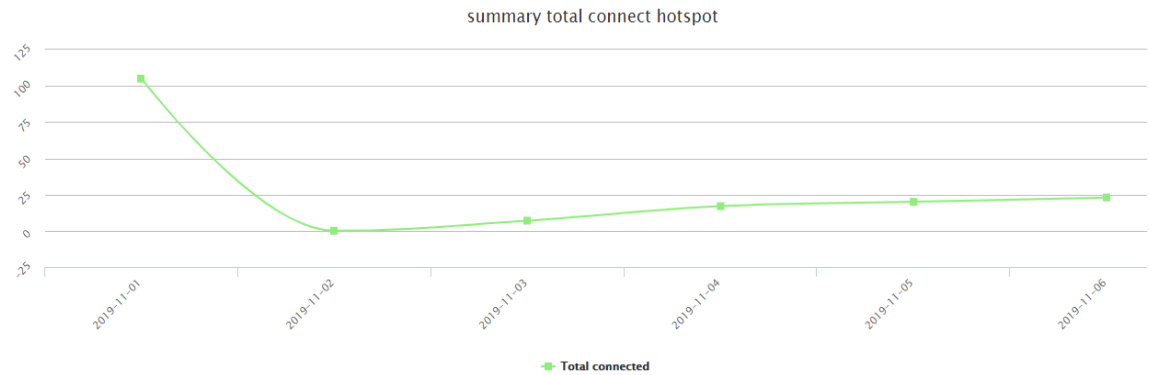
Gambar 14. Form Login Dashboard Captive Portal

Peneliti melakukan percobaan selama seminggu untuk mengetahui pengguna yang menggunakan SSID yang disediakan oleh peneliti dengan beberapa parameter yang telah disediakan seperti *device* yang digunakan user, login menggunakan apa, umur pengguna dan jumlah yang koneksi ke SSID.



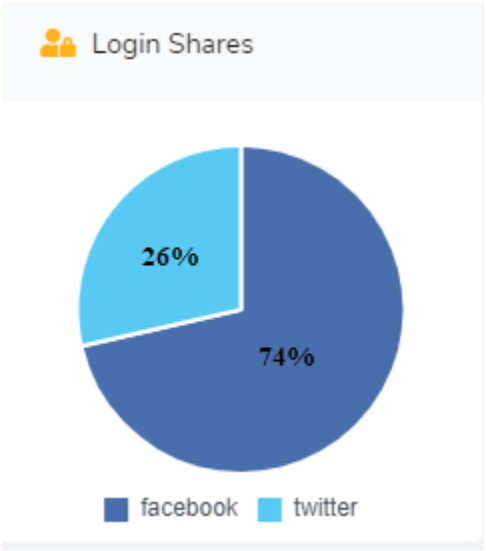
Gambar 15. Perbandingan Usia Pengguna Terhubung

Dilihat pada gambar 15, perbandingan usia pengguna yang terhubung di SSID yaitu paling banyak yang menggunakan adalah dari umur 40 – 45 tahun sebesar 78 orang yang terhubung di SSID pada tanggal 01-11-2019.

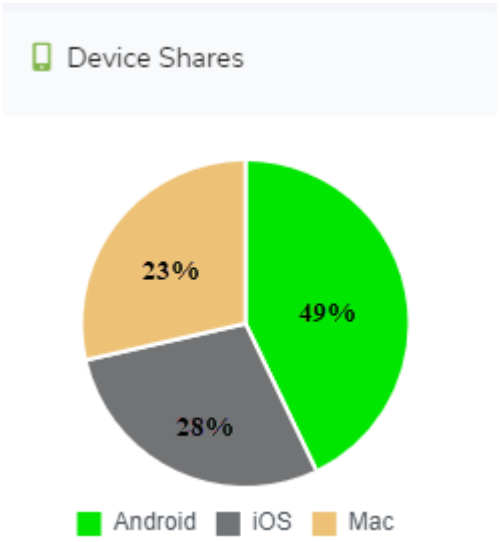


Gambar 16. Total yang Terhubung

Dilihat pada gambar 16, total pengunjung SSID yang disediakan sebesar 110 orang pada tanggal 01-11-2019. Dari jumlah pengunjung SSID kebanyakan login menggunakan sosmed yaitu Facebook sebesar 74% dan twitter sebesar 26% untuk login ke jaringan internet, bisa dilihat pada gambar 17. Pada gambar 18, jumlah pengunjung SSID kebanyakan menggunakan *device* Android sebesar 495, IOS sebesar 28% dan Mac sebesar 23%.



Gambar 17. Perbandingan Login Sosmed



Gambar 18. Perbandingan Pengguna *Device*

IV. KESIMPULAN

Percobaan yang dilakukan menunjukkan bagaimana caranya mencapai konfigurasi captive portal dan radius server untuk authentikasi pengguna pada jaringan internet. Hanya pengguna yang sah dengan data yang benar dapat masuk untuk bisa internetan. Dari metode authentikasi radius yang digunakan bersama captive portal dapat memberikan keamanan dalam mengakses data di jaringan internet dengan aman.. Dengan pengguna yang dapat masuk melalui OTP email maupun sosial media dapat kita bandingkan penggunanya. Tidak hanya itu, kita juga bisa melihat *device* yang digunakan oleh user. Semoga makalah ini dapat bermanfaat bagi masyarakat yang ingin menerapkan teknologi pengamanan jaringan internet menggunakan radius.

V. DAFTAR PUSTAKA

[1] F. Mustika and S. Ramadhani, "Optimization Performance Protocol Leach Sensor Network With Multi Sink," in *Proceedings of the The 1st International Conference on Computer Science and Engineering Technology Universitas Muria Kudus*, 2018.

[2] R. dos R. Fontes and C. E. Rothenberg, "Mininet-WiFi," in *Proceedings of the 2016 conference on ACM SIGCOMM 2016 Conference - SIGCOMM '16*, 2016, pp. 607–608.

[3] F. L. Aryeh, M. Asante, and A. E. Y. Danso, "Securing Wireless Network Using pfSense Captive Portal with RADIUS Authentication – A Case Study at UMaT *," *Ghana J. Technol.*, vol. 1, no. 1, pp. 40–45, 2016.

[4] A. Hindle, "Swarmed: Captive portals, mobile devices, and audience participation in multi-user music performance," *Proc. Int. Conf. New Interfaces Music. Expr.*, pp. 174–179, 2013.

[5] A. H. Muttaqin, A. F. Rochim, and E. D. Widianto, "Sistem Autentikasi Hotspot Menggunakan LDAP dan Radius pada Jaringan Internet Wireless Prodi Teknik Sistem Komputer," *J. Teknol. dan Sist. Komput.*, vol. 4, no. 2, p. 282, 2016.

[6] D. K. Hermawan, A. Sudarsono, I. Winarno, S. St, and M. Kom, "Implementasi Bandwith Management Captive Portal Pada Jaringan Wireless Di Pens-Its," pp. 1–6, 2012.