

## Article history

Received July 12, 2018

Accepted Nov 15, 2018

# PERANCANGAN DAN IMPLEMENTASI HOTSPOT CERDAS BERBASIS MIKROTIK OS DAN WEB SERVER MINI PC RASPBERRY PI

Tria Aprilianto<sup>1</sup>, Samsul Arifin<sup>2</sup>

<sup>1 2</sup> STMIK Asia Malang,

Email : <sup>1</sup> [raptorapril@gmail.com](mailto:raptorapril@gmail.com) <sup>2</sup> [samsul@asia.ac.id](mailto:samsul@asia.ac.id)

## Abstrak

Dalam penelitian ini dikembangkan sebuah sistem jaringan komputer berbasis router os dan web server autentifikasi yang ditanamkan dalam sebuah mini PC, proses autentifikasi login user diterapkan pada sebuah sistem hotspot router yang dikombinasikan dengan mini PC sehingga dapat menghasilkan sebuah sistem manajemen yang bagus atau yang dapat disebut sebagai hotspot cerdas. Hotspot cerdas yang dibangun memiliki kemampuan untuk melakukan manajemen dan otentifikasi user.

Manajemen user yang dibangun dalam sistem hotspot cerdas ini memiliki kemampuan untuk menentukan otoritas user, hirarki limitasi bandwidth, serta limitasi terhadap situs serta konten yang dapat diakses oleh user, sistem ini mampu mendeteksi konten-konten atau situs yang mengandung malware, phishing, atau pornografi. Kemampuan ini dibuat dengan mengimplementasikan serta memodifikasi fitur firewall dalam mikrotik OS.

Otentifikasi user dibangun dengan menggabungkan fitur hotspot dalam router OS serta web server yang ditanamkan dalam sebuah mini PC Raspberry PI. Otentifikasi user diterapkan dengan dua kali proses login yaitu proses login pertama dengan memasukkan username dan password dengan tujuan untuk penentuan hak akses user, kemudian proses login kedua berupa pertanyaan yang sesuai dengan kelas user yang diberikan. Pertanyaan yang diberikan berupa soal yang berhubungan dengan mata kuliah prodi Sistem Komputer. Hasil yang diperoleh dari dibangunnya sistem hotspot cerdas ini adalah sistem hotspot yang dapat memberikan edukasi bagi user dan memberi pelayanan kenyamanan lebih bagi user serta media pembelajaran mata kuliah Administrasi Jaringan Komputer di STMIK Asia Malang. Berdasarkan pengujian sistem yang telah dilakukan didapatkan beberapa kelemahan terhadap otentifikasi dan limitasi yang telah dibuat, akan tetapi dari kelemahan tersebut secara garis besar bisa disimpulkan bahwa sistem bisa berjalan cukup baik.

Kata Kunci: Router OS, Mikrotik, Firewall, Otentifikasi User, Manajemen user, Web server, Raspberry Pi.

## 1. PENDAHULUAN

### Latar Belakang

Perkembangan teknologi khususnya internet sangat berperan dalam kehidupan sehari-hari. Dengan adanya internet, informasi dapat dengan mudah disebarluaskan dan diakses oleh banyak orang. Di era modern ini kebutuhan akan internet sudah menjadi hal utama bagi sebagian besar orang. Penyalahgunaan serta pemberian informasi tidak bertanggung jawab dan negatif banyak terjadi di internet, banyak sekali situs dan informasi yang mengandung malware, phishing, pornografi atau hal-hal lain yang mengandung unsur negatif dan bahkan kriminal.

Laboratorium Prodi Sistem Komputer di STMIK Asia Malang adalah tempat bagi

mahaMahasiswa prodi Sistem Komputer untuk melakukan praktikum dan juga melakukan kegiatan perkuliahan. Salah satu layanan yang diberikan laboratorium ini adalah penggunaan internet hotspot gratis di luar jam perkuliahan, tidak adanya manajemen yang baik dalam pemberian layanan tersebut sering kali menimbulkan beberapa masalah. Masalah yang timbul diantaranya adalah tidak adanya otoritas dan hak akses user yang mengakibatkan pengguna saling berebut dalam penggunaan bandwidth serta dapat mengakses situs dan informasi yang mengandung malware, phishing, pornografi atau hal-hal lain yang mengandung unsur negatif.

Router OS Mikrotik adalah sebuah alat yang memiliki kemampuan melakukan

manajemen dalam jaringan. Sehingga sangat dimungkinkan dilakukan pengaturan jalur perjalanan data, user, bandwidth, web filtering dan penanganan apabila terjadi kesalahan pada jaringan komputer. Sedangkan Raspberry Pi merupakan mini PC yang dapat digunakan untuk jaringan komputer dan aplikasi web server. Web server yang di tanam pada Raspberry Pi sebagai penyedia manajemen layanan dan sistem informasi yang dapat diakses oleh user.

Berdasarkan hal tersebut maka dalam penelitian ini akan dibangun sebuah sistem hotspot cerdas dengan mengimplementasikan Router OS Mikrotik dan Raspberry PI. Otentifikasi user dibangun dengan menggabungkan fitur hotspot dalam router OS serta web server yang ditanamkan dalam sebuah mini PC Raspberry PI. Otentifikasi user diterapkan dengan dua kali proses login yaitu proses login pertama dengan memasukkan username dan password dengan tujuan untuk penentuan hak akses user, kemudian proses login kedua berupa pertanyaan yang sesuai dengan kelas user yang diberikan. Pertanyaan yang diberikan berupa soal yang berhubungan dengan mata kuliah prodi Sistem Komputer, proses ini diharapkan dapat mengedukasi user sehingga dapat menambah efektifitas atau manfaat dari web login tersebut. Hasil yang diharapkan dari dibangunnya sistem hotspot cerdas ini adalah sistem hotspot yang dapat memberikan edukasi bagi user dan memberi pelayanan kenyamanan lebih bagi user serta media pembelajaran mata kuliah Administrasi Jaringan Komputer di STMIK Asia Malang.

### Rumusan Masalah

Berdasarkan latar belakang di atas, maka peneliti merumuskan masalah dalam penelitian ini adalah bagaimana merancang serta mengimplementasikan Hotspot Cerdas Berbasis Mikrotik OS dan web server Mini PC Raspberry PI

### Batasan Masalah

Berdasarkan dalam latar belakang di atas peneliti dalam penelitian ini memberikan batasan-batasan sebagai berikut :

1. Pengujian dan Implementasi jaringan dilakukan pada laboratorium prodi Sistem Komputer STMIK Asia Malang.

2. User dalam pengujian meliputi Mahasiswa dan Dosen
3. Testing system dilakukan pada semester genap 2018 pada laboratorium prodi Sistem Komputer dan sebagai media pembelajaran kelas mata kuliah Administrasi Jaringan Komputer di Prodi Sistem Komputer STMIK Asia Malang
4. Management user yang dibangun meliputi hak akses user, limitasi bandwidth, serta filter situs dan konten.
5. Otentifikasi yang dibuat berupa username dan password serta soal pertanyaan yang harus dijawab oleh user.

## 2 TINJAUAN PUSTAKA

### 2.2.1 Konsep Dasar Hotspot

Hotspot adalah area dimana seorang client dapat terhubung dengan jaringan internet secara wireless (nirkabel/tanpa kabel) dari PC, note book atau gadget seperti Handphone dalam jangkauan radius kurang lebih beberapa ratus meteran atau tergantung dari kekuatan frekuensi/signal. Hotspot gateway merupakan salah satu fitur yang ada di Mikrotik RouterOs. Hotspot gateway digunakan untuk mengkonfigurasi jaringan wireless yang hanya bisa digunakan dengan username dan password tertentu.

### 2.2.2 Mikrotik Router

Mikrotik dikenal luas sebagai Router. Router merupakan perangkat jaringan yang digunakan untuk menghubungkan beberapa jaringan (Network). Dalam jaringan yang lebih kompleks, Router digunakan untuk memilahkan bagi paket data untuk mencapai komputer tujuan. Beberapa implementasi router yang paling sering digunakan adalah pembagian bandwidth, pengaturan IP dan jalur, security berbasis firewall dll.

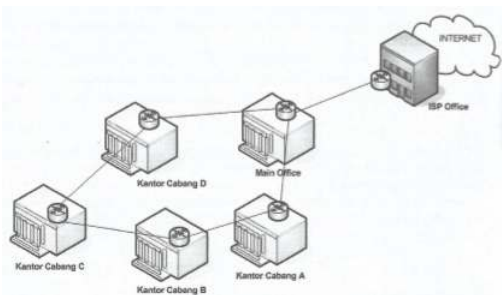


**Gambar 2.1**  
**Mikrotik Router**

### 2.2.3 Intermediary Device (routing)

Sebagai intermediary device (routing) merupakan fungsi utama Router, menghubungkan beberapa Network dan berusaha untuk menentukan jalur terbaik untuk menuju komputer tujuan. Dari gambar 2.10 dapat dilihat ada beberapa Network yang terpisah pada beberapa kantor cabang, dan Router Mikrotik menghubungkan network-network tersebut.

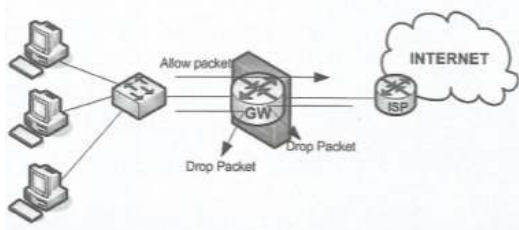
Router Mikrotik juga akan memilih jalur terbaik untuk menuju internet yang ada di kantor pusat. Misalnya, jika berada di kantor cabang B, maka untuk menuju internet, Router Mikrotik akan memilih jalur melalui kantor cabang A. Karena jalur melalui kantor cabang A lebih pendek daripada melalui kantor cabang C.



**Gambar 2.2**  
**Router Sebagai Intermediary Device (Routing)**

### 2.2.4 Firewall

Firewall merupakan perangkat yang berfungsi untuk memeriksa dan menentukan paket data yang dapat keluar atau masuk dari sebuah jaringan. Dengan kemampuan menentukan apakah sebuah paket data bisa masuk dan keluar dari suatu jaringan maka firewall berperan untuk melindungi jaringan dari serangan yang berasal dari jaringan luar (outside Network). Selain ditunjukkan untuk melindungi jaringan, firewall juga dapat difungsikan untuk melindungi sebuah komputer user atau Host (single Host). Firewall jenis ini disebut Host firewall.



**Gambar 2.3**  
**Router Mikrotik sebagai Firewall**

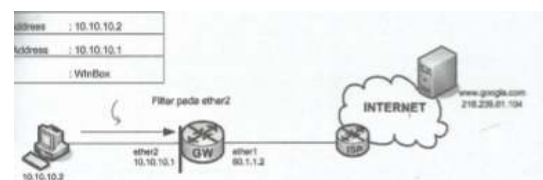
### 2.2.5 Filter

Fitur Filter pada firewall digunakan untuk menentukan apakah suatu paket data masuk atau tidak ke dalam sebuah sistem Router itu sendiri. Paket data yang akan ditangani fitur Filter ini adalah paket yang ditunjukkan pada salah satu interface Router. Fitur filter pada Router Mikrotik memiliki 3 chain, yaitu input, output dan forward. Chain output yang berfungsi menangani paket data yang berasal dari Router.

#### 1. Chain input

Chain input berperan untuk melakukan filter terhadap paket-paket yang ditujukan bagi interface-interface Router. Hal tersebut berguna untuk membatasi akses terhadap Router Mikrotik, misalnya dilakukan pembatasan pada akses konfigurasi. Dalam dunia Network security sering diistilahkan dengan teknik membatasi akses terhadap port-port Router yang dapat menimbulkan celah keamanan.

Chain input pada firewall akan menangani paket data yang ditunjukkan pada interface Router Mikrotik. Paket data ini biasanya adalah paket data pada saat akan melakukan konfigurasi, misalnya pada saat memasukkan IP Address 10.10.10.1 pada WinBox. Chain input ini berguna untuk membatasi akses konfigurasi terhadap Router Mikrotik. Penggunaan chain input dapat anda lihat pada ilustrasi gambar 2.8 dimana ada sebuah paket data yang ditunjukkan kepada interface ether2. Karena melakukan perlindungan pada interface – interface Router, maka chain input ini dapat diterapkan pada dua interface Router Mikrotik anda (pada ether1 dan ether2).



**Gambar 2.4**  
**Penerapan Chain Input**

Penerapan chain input pada interface ether1 berfungsi memberikan perlindungan terhadap akses yang mungkin terjadi dari internet. Sedangkan penerapannya pada ether2 memberikan perlindungan terhadap kemungkinan akses dari dalam jaringan.

Konfigurasi *chain input* pada ether1 dan ether2

```
1: [admin@Mikrotik] > ip firewall filter add chain=input in-interface=ether1 protocol=tcp dst-port=20,21,22,23,80,8291 action=drop
2: [admin@Mikrotik] > ip firewall filter add chain=input in-interface=ether1 protocol=tcp dst-port=8291 src-Address=64.110.100.2 action=accept
```

Adapun penjelasan dari konfigurasi tersebut adalah sebagai berikut :

- 1: Penerapan filter dengan menggunakan *chain input* pada ether1, ditunjukkan untuk membatasi akses terhadap port -port yang terbuka. Ini akan membatasi percobaan konfigurasi yang mungkin dilakukan dari internet oleh orang – orang yang tidak bertanggung jawab. Port yang terbuka secara default untuk keperluan konfigurasi pada Router Mikrotik adalah 22 (ssh), 23 (telnet), 20 dan 21 (ftp), 80 (WebPig) 8291 (WinBox). Sehingga perintah yang dapat anda gunakan untuk menerapkan filter pada ether1.
- 2: komputer dengan IP Address 64.110.10.2 diijinkan untuk melakukan konfigurasi menggunakan winbox (dst 8291).

Sedangkan untuk sisi *interface* ether2 yang dihubungkan dengan jaringan lokal, juga dapat menerapkan *filtering* dengan *chain input*. Misalkan dalam satu *Network* hanya akan mengaktifkan satu IP Address yaitu IP Address *administrator* jaringan.

Konfigurasi *filtering* dengan *chain input* :

```
[admin@Mikrotik] > ip firewall filter add chain=input in-interface=ether2 src-Address=10.10.10.4 action=accept
```

```
[admin@Mikrotik] > ip firewall filter add chain=input in-interface=ether2 protocol=icmp connection-state=established action=accept
```

```
[admin@Mikrotik] > ip firewall filter add chain=input in-interface=ether2 protocol=icmp action=drop
```

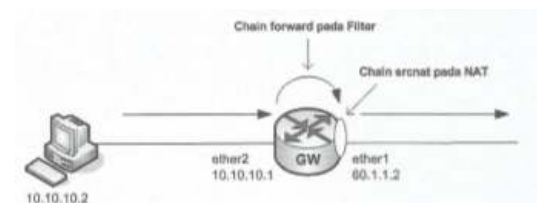
```
[admin@Mikrotik] > ip firewall filter add chain=input in-interface=ether1 protocol=tcp dst-port=20,21,22,23,80,8291 action=drop
```

Adapun penjelasan dari konfigurasi tersebut adalah sebagai berikut :

Perintah konfigurasi membatasi akses konfigurasi dari keseluruhan komputer yang ada dalam jaringan 10.10.10.0/24, namun memberikan akses konfigurasi (baik SSH, telnet, Winbox maupun ping) dari komputer 10.10.10.4 yang diskenarioikan sebagai komputer yang sering di gunakan oleh *administrator* jaringan.

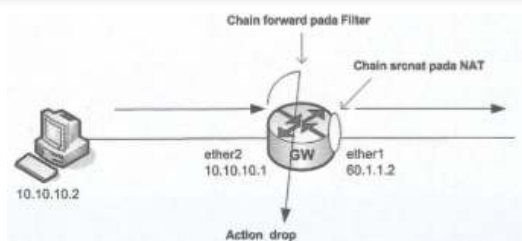
### 1. *Chain forward*

*Chain forward* pada filter Router Mikrotik digunakan untuk menangani paket data yang akan melintas Router. *Chain forward* akan menangani paket data yang melintas Router, baik paket data jaringan lokal yang ingin ke internet maupun sebaliknya, sama dengan yang dilakukan oleh NAT, namun perbedaan keduanya adalah jika *chain srcnat* pada NAT menangani paket data dengan melakukan perubahan IP Address pengirim maka *chain forward* pada Filter hanya akan menangani paket data tanpa melakukan perubahan apapun pada IP Address pengirim.



**Gambar 2.5**  
**Penerapan Filter dan NAT**

Pada gambar diatas terlihat akses internet dari komputer 10.10.10.2 akan diterima di ether2. Router Mikrotik akan menggunakan filter dengan *chain forward* terlebih dahulu untuk memeriksa paket data tersebut. Kemudian paket data diserahkan ke NAT yang akan mengubah IP Address pengirim dari paket tersebut. Sehingga, akan terlihat bahwa *chain forward* pada filter memegang kendali terlebih dahulu sebelum *chain srcnat* pada NAT. ini mengakibatkan konfigurasi *action=masquerade* pada NAT tidak akan berfungsi jika *action=drop* telah dijalankan di *chain forward* pada filter, seperti terlihat pada gambar berikut:



**Gambar 2.6**  
**Action Drop Pada Filter**

Konfigurasi *chain forward*:

```
[admin@gateway] > ip firewall filter add
chain=forward src-Address=10.10.10.2-
10.10.10.5 in-interface=ether2 action=accept
[admin@gateway] > ip firewall filter add
chain=forward src-Address=10.10.10.0/24 in-
interface=ether2 action=drop
```

Konfigurasi filter dengan *chain forward* hanya mengizinkan komputer 10.10.10.2-10.10.10.5 untuk mengakses internet.

*Chain forward* dapat digunakan untuk memblokir akses internet terhadap situs tertentu maupun aktifitas user yang ingin men-download jenis – jenis file tertentu.

Adapun konfigurasi yang akan memblokir akses internet ke situs [www.playboy.com](http://www.playboy.com) dan aktifitas download file.mp3 sebagai berikut:

Konfigurasi blokir situs:

```
[admin@gateway] > ip firewall filter add
chain=forward src-Address=10.10.10.0/24
content=www.playboy.com action=drop
[admin@gateway] > ip firewall filter add
chain=forward src-Address=10.10.10.0/24
content=.mp3 action=drop
```

Adapun penjelasan dari konfigurasi sebagai berikut :

Dengan menggunakan opsi *content=www.plaboy.com* , bila ada komputer *user* yang memasukkan kata [www.playboy.com](http://www.playboy.com) pada mesin pencari (*Search Engine*), maka *Search Engine* tidak akan memberikan hasil apapun.

### 2.2.1 Raspberry PI

Raspberry Pi merupakan komputer mini yang memiliki ukuran kecil yaitu sebesar kartu ATM tetapi mampu menjalankan tugas yang sama dengan komputer PC. Raspberry Pi dirilis dengan lisensi *Open-Source Hardware* yang berarti rancangan perangkat kerasnya dirilis ke publik agar dapat bebas dipelajari, dimodifikasi, didistribusi, dirakit, dan dijual sesuai rancangan aslinya. Karena dirilis dengan lisensi *Open-*

*Source Hardware*, Raspberry pi telah dipergunakan untuk berbagai keperluan, diantaranya untuk hardware yang menjalankan: media center, *Networked* komputer, dan web server. Salah satu sistem operasi yang digunakan oleh raspberry pi adalah raspbian. Raspbian adalah sistem operasi bebas berbasis Debian GNU/ Linux dan dioptimalkan untuk perangkat keras Raspberry Pi



**Gambar 2.7**  
**Raspberry Pi 3**

### 2.2.2 Web Server

Web server merupakan suatu perangkat lunak yang berjalan di sisi server dan bertugas untuk menerima permintaan dari web browser, menerjemahkan permintaan tersebut, dan mengembalikan ke web browser hasil dari permintaan. Fungsi utama Server atau Web server adalah untuk melakukan atau akan mentransfer berkas permintaan pengguna melalui protokol komunikasi yang telah ditentukan sedemikian rupa. halaman web yang diminta terdiri dari berkas teks, video, gambar, file dan banyak lagi.

Salah satu contoh dari Web Server adalah Apache. Apache (Apache Web Server – The HTTP Web Server) merupakan web server yang paling banyak dipergunakan di Internet. Program ini pertama kali didesain untuk sistem operasi lingkungan UNIX. Apache mempunyai program pendukung yang cukup banyak. Hal ini memberikan layanan yang cukup lengkap bagi penggunaanya..

### 2.2.3 Web Login

Web login adalah halaman login yang ditampilkan pertama kali ketika ada pengguna mengakses internet atau web server. Kegunaan dari halaman web ini adalah sebagai keamanan sehingga hanya pengguna yang mengetahui *Username* dan *Password* yang benar yang dapat mengakses internet

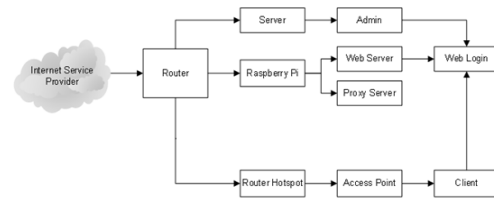
### 3 METODOLOGI PENELITIAN

#### 3.1 Jenis Penelitian

Jenis penelitian yang dilakukan adalah dengan metode eksperimen. Dimana dalam penelitian ini difokuskan pada penerapan Router OS Mikrotik dan Raspberry PI dalam merancang dan mengimplementasikan sebuah hotspot sistem yang dapat memberikan sebuah nilai edukasi atau cerdas.

#### 3.2 Desain Arsitektur Jaringan

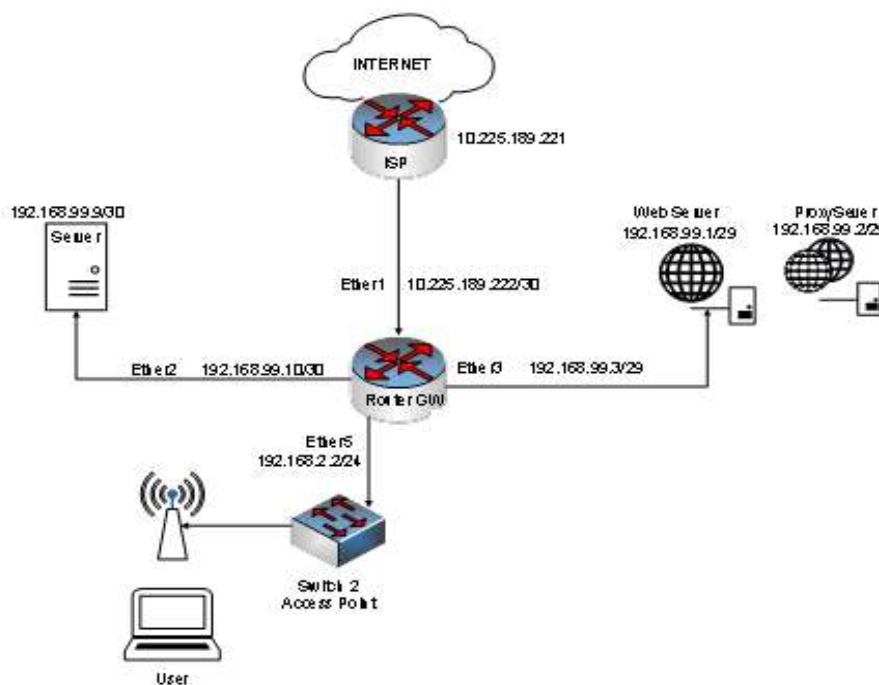
Desain Arsitektur Jaringan bertujuan untuk merancang kerangka penelitian bagaimana mengembangkan sistem hotspot dengan mengimplementasikan router dan mini pc raspberry PI. Perancangan dibuat dengan mengimplementasikan web server yang ditanamkan pada raspberry PI dan juga memaksimalkan fungsi firewall yang ada di dalam router. Secara umum arsitektur jaringan yang dibangun dapat dilihat pada gambar di bawah ini.



**Gambar 3.1**  
**Arsitektur Jaringan**

#### 3.3 Manajemen Jaringan dan desain Routing

Manajemen Jaringan Hotspot cerdas diimplementasikan dengan mengoptimalkan fungsi dan peranan dari sebuah Router Mikrotik yang digabungkan dengan sebuah server yang dibuat menggunakan sebuah mini PC raspberry. Router mikrotik berperan sebagai pengatur lalu lintas yang ada dalam jaringan serta security dalam penentuan akses yang diperoleh client, situs yang tidak dapat diakses oleh client dimasukkan dalam filter yang ada di firewall mikrotik. List situs atau konten tersebut dibuat dalam address list dan layer7 serta memanfaatkan mangle rule. Secara umum desain manajemen dan routing yang akan dibuat dapat dilihat pada gambar berikut

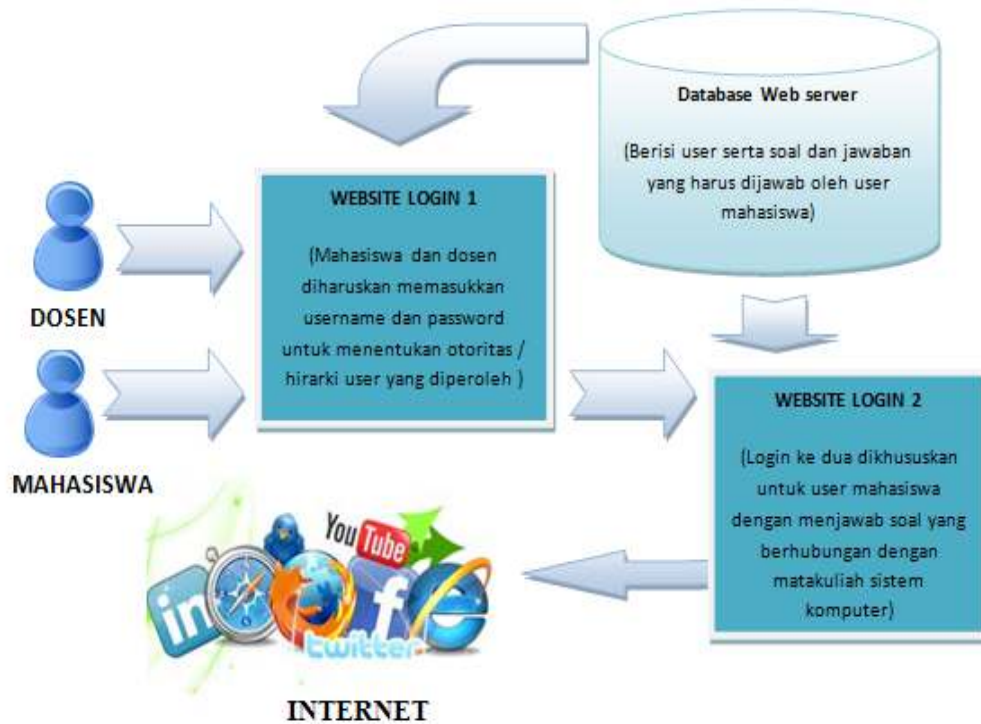


**Gambar 3.2**  
**Desain Routing Jaringan**

### 3.4 Login Sistem

Secara umum login sistem yang akan dirancang dapat digambarkan pada gambar di bawah ini. Otentifikasi login sistem yang dibuat

ditanamkan pada mini PC raspberry PI dalam sebuah database my sql dan web server php. Hirarki user dikelompokkan menjadi dua yaitu dosen dan mahasiswa.



**Gambar 3.3**  
**Arsitektur Login Sistem**

### 3.5 User (client)

Dalam system yang dibangun User dikelompokkan menjadi 2 yaitu Dosen dan Mahasiswa. Setiap user memiliki otoritas akses dan manajemen bandwidth masing-masing.

#### 1. Dosen

Secara umum dosen mendapatkan bandwidth yang lebih besar serta proses otentifikasi login hanya dilakukan sekali yaitu dengan memasukkan username dan password saja.



**Gambar 3.4**  
**Alur User (dosen)**

#### 2. Mahasiswa

User Mahasiswa diharuskan melakukan otentifikasi login sebanyak 2 kali yaitu dengan memasukkan username dan password serta diharuskan menjawab pertanyaan yang diberikan oleh sistem.

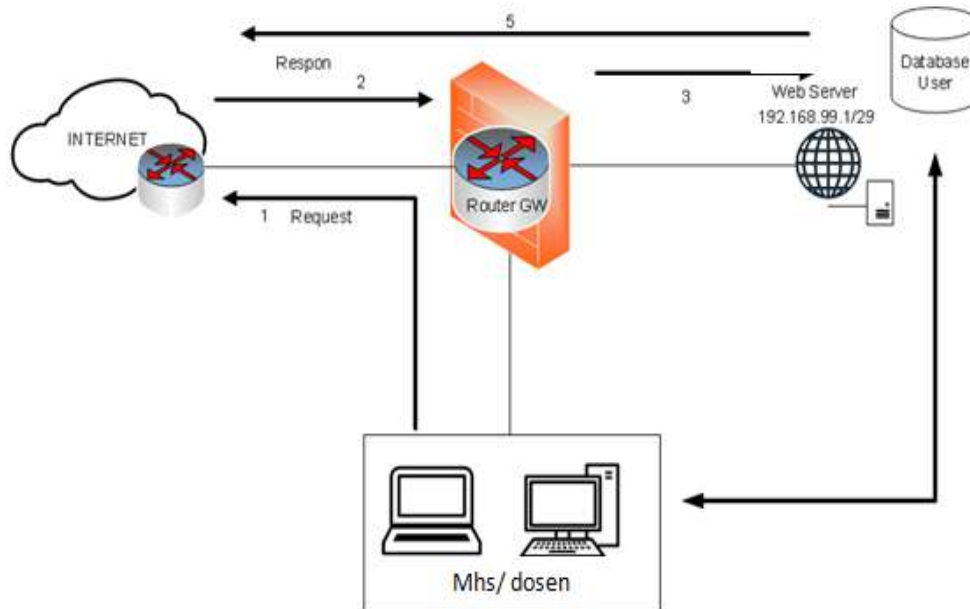


**Gambar 3.5**  
**Alur User (Mahasiswa)**

### 3.6 Web Server

Pada perancangan implementasi Raspberry Pi web Server difungsikan

sebagai tempat penyimpanan database *user Login*, kalender akademik, dan web *Login*. Adapun implementasi web *Server* ditunjukkan pada gambar berikut



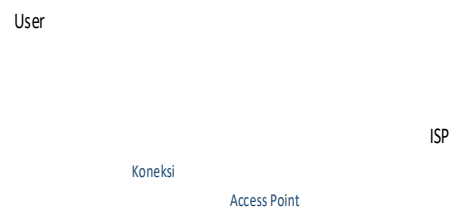
**Gambar 3.6**  
**Web Server**

## 4 PEMBAHASAN

### 4.1 Analisis Masalah

Dalam kegiatan sehari-hari Lab Prodi Sistem Komputer telah ditunjang dengan fasilitas Internet (Hotspot). Belum adanya tenaga administrator jaringan yang bekerja pada Lab menyebabkan terjadinya beberapa permasalahan muncul dalam jaringan hotspot tersebut.

Permasalahan yang sering terjadi dikarenakan tidak adanya security yang dipasang pada jaringan hotspot, tidak adanya pembagian bandwidth, tidak adanya otoritas pengguna, dan tidak adanya batasan akses pada situs internet. Dimana sistem akses hotspot Lab Prodi Sistem Komputer yang berjalan saat ini ditunjukkan pada gambar 4.1.



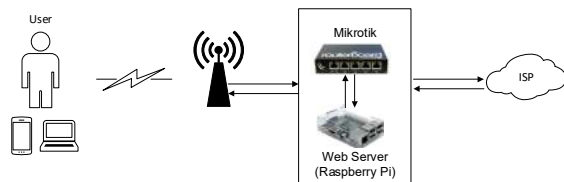
**Gambar 4.1**  
**Sistem Akses Hotspot Lab Sistem Komputer**  
**(Sedang Berjalan)**

Gambar 4.1 menunjukkan sistem akses hotspot yang ada di Lab Sistem Komputer. Akses hotspot dari user ke internet tidak menggunakan sistem keamanan seperti username dan password. Hal tersebut menyebabkan tidak adanya hak akses user, sehingga semua user yang masuk ke dalam jaringan hotspot tidak terkontrol



## 4.2 Sistem Ideal Manajemen Hotspot

Sistem ideal manajemen hotspot dirancang untuk melihat alur dari sistem yang dibangun pada penelitian ini. Selain itu sistem ideal manajemen hotspot juga dapat digunakan untuk perbandingan antara manajemen yang lama, dengan manajemen baru yang dibahas pada penelitian ini. Adapun sistem ideal manajemen hotspot ditunjukkan pada gambar 4.2



**Gambar 4.2**  
**Sistem Ideal Manajemen Hotspot**

Pada sistem sebelumnya dalam manajemen hotspot yang lama hanya ada tiga perangkat yaitu user, wifi, dan isp. Gambar 4.2 menunjukkan adanya penambahan perangkat

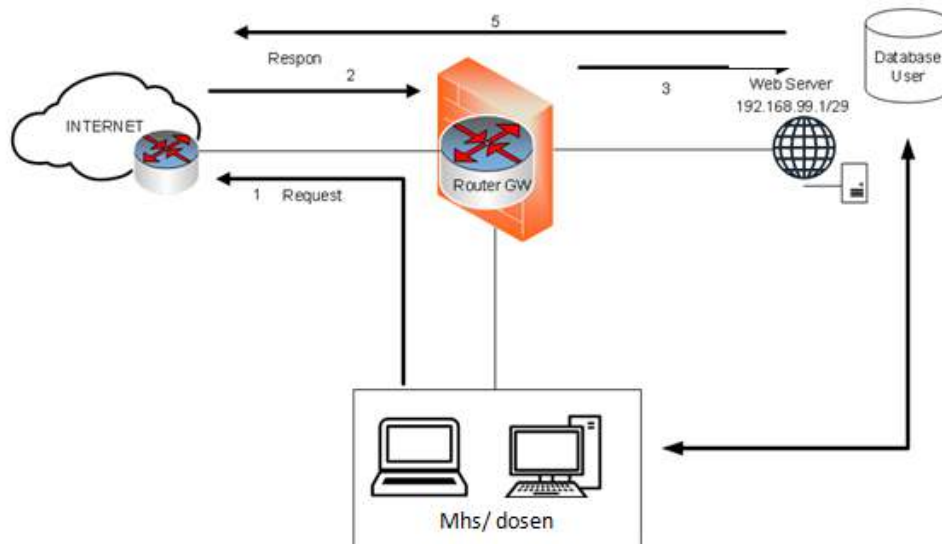
pada hotspot. Penambahan perangkat yaitu mikrotik router dan web server raspberry pi. Penambahan dua perangkat terletak diantara access point dan isp, hal tersebut dikarenakan proses manajemen hotspot berada di mikrotik dan web server raspberry pi.

## 4.3 Perancangan Implementasi Raspberry Pi

Penggunaan Raspberry Pi dalam penelitian ini bertujuan untuk memanfaatkan teknologi dan fitur yang ada di dalam Raspberry Pi. Raspberry Pi akan diimplementasikan sebagai web *Server* dan *Proxy Server*.

### 4.3.1 Web Server

Pada perancangan implementasi Raspberry Pi web *Server* difungsikan sebagai tempat penyimpanan database *user Login* dan web *Login*. Adapun implementasi web *Server* ditunjukkan pada gambar 4.3.



**Gambar 4.3**  
**Web Server Raspberry Pi**

*User* (hotspot) dan admin yang terhubung dengan jaringan tidak dapat melakukan akses internet tanpa melakukan *Login* terlebih dahulu. Pada gambar 4.3 ditunjukkan bahwa pada saat *user* melakukan request ke internet dan tanpa melakukan *Login* sebelumnya, maka firewall yang ada di mikrotik router akan me-redirect request *user* ke web *Server*. Web *Server* akan menampilkan halaman

web *Login* dan melakukan autentikasi *user Login*. Jika *user* telah berhasil melakukan autentikasi, maka request *user* akan di-accept oleh mikrotik.

### 4.3.2 Database

Pada Raspberry Pi dibangun pula database sebagai tempat penyimpanan data dari

web server. Pada database yang akan dirancang memiliki beberapa tabel diantaranya, tabel user, tabel jadwal, dan tabel autentikasi Mahasiswa.

#### 1. Tabel user

Pada perancangan web server raspberry pi database user dibangun untuk melakukan penyimpanan data autentikasi user. Database yang dibangun yaitu database *logiskasia* yang terdiri dari tiga table yaitu table user\_table, table autentikasi\_mahasiswa dan table jadwalku.

Tabel user\_table merupakan tabel database *logiskasia* yang menyimpan data username dan password user hotspot Lab Sistem Komputer. Adapun perancangan tabel user\_tabel ditunjukkan pada tabel 4.1

**Tabel 4.1**  
**Perancangan Tabel User\_Table Database**  
***logiskasia***

Nama	username	password	Angkatan	tipe
Samsul Arifin	Dosen1	Samsul	-	Dosen
Ahmad Gazali	Ahmad	15202193	2015	Mahasiswa
Admin	admin	adminhotspot	-	admin

Pada tabel 4.1 tabel terediri dari field nama, username, password, angkatan, dan tipe. Field nama digunakan untuk mengetahui pemilik username dan password dari user. Field kelas dan jurusan hanya dapat diisi dengan tipe user Mahasiswa. Field tipe yang terdiri dari Dosen, Mahasiswa, dan admin digunakan untuk membedakan user hotspot Lab Sistem Komputer serta digunakan sebagai user profile di mikrotik.

#### 2. Tabel Autentikasi Mahasiswa

Pada perancangan web login, user dengan tipe Mahasiswa harus melakukan autentikasi dengan menjawab pertanyaan yang muncul pada halaman autentikasi. Halaman autentikasi yang

akan dibangun memiliki perancangan tabel database seperti pada tabel 4.2.

**Tabel 4.2**  
**Perancangan Tabel Autentikasi Mahasiswa**  
**Database *logiskasia***

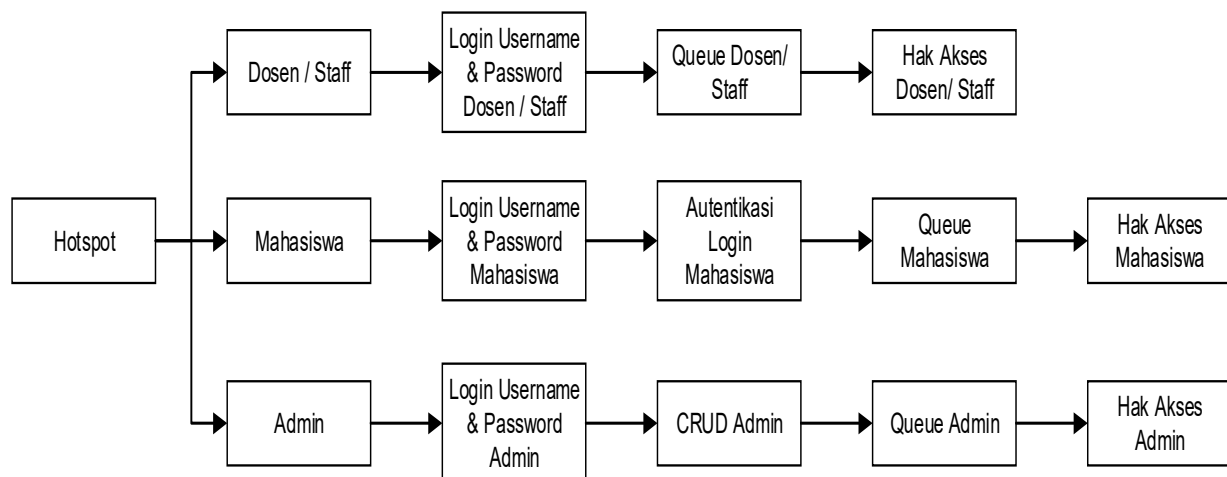
Pertanyaan	Jawaban	Tipe	Gambar

Pada perancangan tabel autentikasi Mahasiswa seperti yang ditunjukkan pada tabel 4.2. Terdapat field pertanyaan yang akan difungsikan sebagai penyimpan data pertanyaan. Field jawaban akan berisi jawaban dari pertanyaan yang dibuat. Field tipe difungsikan untuk menyimpan data tipe user sesuai dengan bertanya dan jawaban yang dibuat. Field gambar digunakan untuk menyimpan nama gambar yang di upload untuk mendukung pertanyaan yang dibuat.

#### 4.4 Manajemen Jaringan

Pada pembahasan ini manajemen jaringan dirancang untuk jaringan hotspot dan jaringan LAN yang ada di Lab Sistem Komputer. Manajemen jaringan dirancang untuk mengontrol dan memantau jaringan yang ada di Lab Sistem Komputer. Pengontrolan dapat dilakukan dengan pengecekan perangkat keras yang terhubung pada topologi jaringan. Topologi jaringan yang dibangun dapat dijadikan acuan, sehingga pada saat terjadi kerusakan pada perangkat keras, konfigurasi dapat dilakukan ulang dengan melihat topologi yang dibangun. Sedangkan pemantauan dapat dilihat melalui konfigurasi yang diatur dalam *router*.

Manajemen jaringan yang akan dirancang memiliki fungsi untuk memanajemen konfigurasi, memanajemen *accounting* dan memanajemen keamanan. Adapun diagram manajemen jaringan seperti pada gambar 4.4.



**Gambar 4.4**  
**Manajemen Jaringan Lab Sistem Komputer**

Pada gambar 4.4 menunjukkan pembagian otoritas, autentikasi, dan accounting pada manajemen hotspot. Dimana otoritas merupakan pembagian user, autentikasi dari proses otoritas, dan accounting yang merupakan pembagian bandwidth setiap user.

#### 4.4.1 Pembagian User dan Autentikasi

Dalam perancangan jaringan hotspot *user* dibagi menjadi tiga yaitu Dosen / staff, admin dan Mahasiswa. Pembagian *user* bertujuan untuk pengaplikasian QoS yang dirancang sehingga tepat sasaran. Untuk dapat mengakses internet yang ada di area hotspot Lab Sistem Komputer *user* harus melakukan *Login* terlebih dahulu dengan autentikasi *username* dan *password* yang ada di web *Server Raspberry Pi*.

#### 4.4.2 Alokasi Pembagian Bandwidth

Alokasi pembagian bandwidth pada jaringan hotspot yang akan dirancang menggunakan queue tree. Pembagian bandwidth akan dilakukan secara dinamis. Dimana, alokasi bandwidth yang didapat oleh seorang *user* akan bergantung yang sedang menggunakan bandwidth di jaringan. Queue tree dialokasikan untuk jaringan hotspot dengan pembagian user Mahasiswa, Dosen, dan admin. Adapun perancangan alokasi bandwidth user ditunjukkan pada tabel 4.3.

**Tabel 4.3**  
**Alokasi Bandwidth Queue Tree**

No.	Target User	Limit At (bit/s) Upload/ Download	Max Limit (bit/s) Upload/ Download
1.	Mahasiswa	256K/384K	1M/10M
2.	Dosen	256K/384K	1M/ 4M
3.	Admin	256K/384K	1M/1M

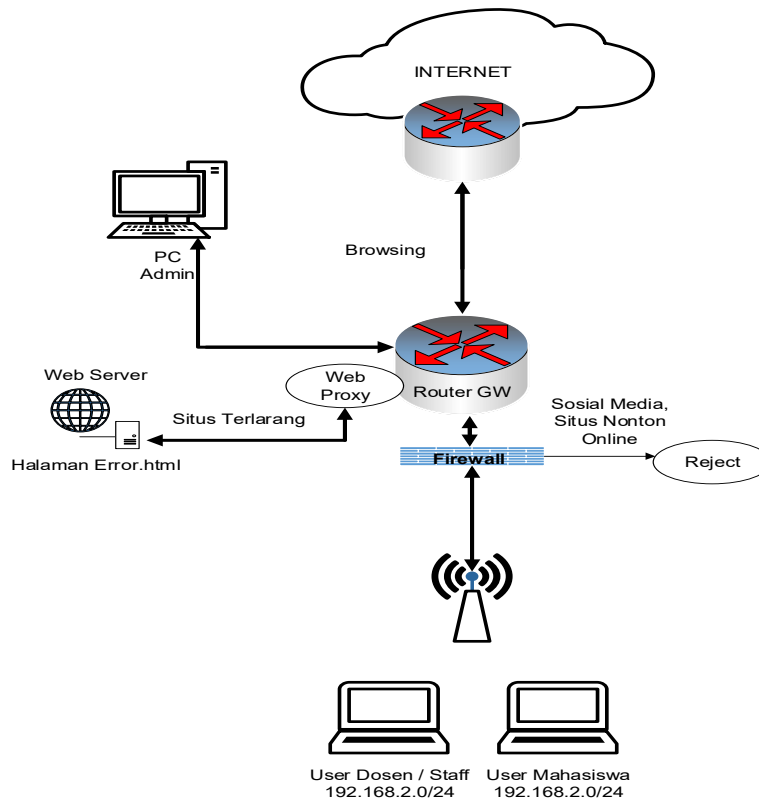
Masing-masing upload dan download memiliki parent packet sebesar 15M.

#### 4.4.3 Hak Akses Situs

Hak akses situs dirancang untuk memberikan batasan-batasan akses situs otoritas *user* tertentu. Hak akses *user* yang dirancang yaitu pembatasan akses situs.

Pembatasan akses situs menjadi salah satu otoritas dan *accounting* dalam perancangan manajemen jaringan. Dengan melakukan pembatasan akses situs bandwidth yang digunakan dapat berjalan dengan maksimal pada saat melakukan browsing. Selain itu Lab Sistem Komputer sebagai tempat penelitian, wajib memberikan batasan akses situs. Hal tersebut dilakukan agar fasilitas hotspot yang disediakan dapat dimanfaatkan sebagai mana mestinya dalam menunjang kegiatan belajar mengajar. Dalam perancangan pembatasan akses situs, beberapa situs yang akan dibatasi penggunaannya yaitu sosial media untuk otoritas Mahasiswa serta situs yang

mengandung konten terlarang untuk seluruh *user*. Adapun perancangan pembatasan akses situs digambarkan pada gambar 4.5.



**Gambar 4.5**  
**Pembatasan Akses Situs**

Pada gambar 4.5 menunjukkan proses pengiriman dan penerimaan paket data yang ditandai dengan tanda panah. Pada saat user dengan address Mahasiswa mengakses sosial pada jam tertentu, maka router akan melakukan proses reject yang dijalankan pada firewall mikrotik. Sedangkan pada saat user mengakses situs terlarang yang terdaftar pada web proxy mikrotik, maka router akan mengarahkan permintaan user ke halaman error yang ada di web server. Adapun halaman error webserver ditunjukkan pada gambar 4.6.



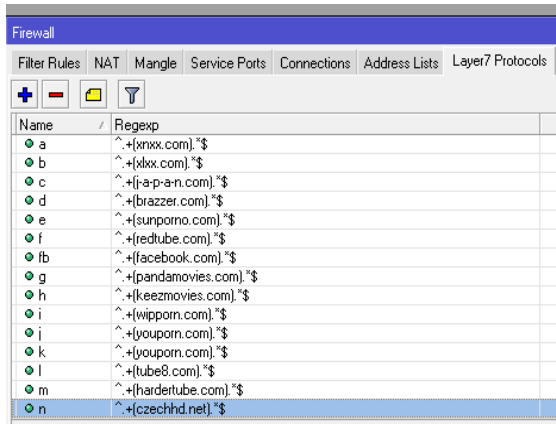
**Gambar 4.6**  
**Tampilan Website Redirect**

Situs youtube dan facebook dapat diakses seluruh *user* pada pukul 15.00-06.00 WIB. Sedangkan untuk situs pornografi akan di-reject selamanya. Pada perancangan ini pembatasan situs akan memanfaatkan fitur *Address list* dan filter rules yang ada pada firewall mikrotik. Adapun perancangan pada *Address list* diunjukkan pada gambar 4.7.

Name	/ Address	Timeout
F		
facebook	31.13.24.0/21	
facebook	31.13.64.0/24	
facebook	31.13.64.0/19	
facebook	31.13.64.0/18	
facebook	31.13.65.0/24	
facebook	31.13.66.0/24	
facebook	31.13.67.0/24	
facebook	31.13.68.0/24	
facebook	31.13.69.0/24	
facebook	31.13.70.0/24	
facebook	31.13.71.0/24	
facebook	31.13.72.0/24	
facebook	31.13.73.0/24	
facebook	31.13.74.0/24	
facebook	31.13.75.0/24	

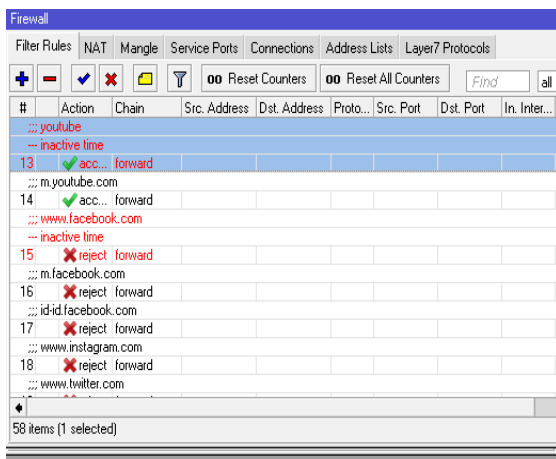
**Gambar 4.7**  
**Address List Situs Facebook**

Pada gambar 4.7 situs yang ada pada *Address list* di inputkan secara otomatis melalui pengaturan yang ada di *firewall rules*. Sedangkan untuk pembatasan akses situs menggunakan *layer 7 protocols* ditunjukkan pada gambar 4.8.



**Gambar 4.8**  
**Pembatasan Situs Layer 7 Protocols**

Gambar 4.8 menunjukkan contoh list situs yang ada pada layer 7. Untuk pembatasan akses situs menggunakan *filter rules firewall* ditunjukkan pada gambar 4.9.



**Gambar 4.9**  
**Filter Rules Situs**

Gambar 4.9 merupakan screenshot dari perancangan pembatasan situs menggunakan filter rules firewall.

## 5. IMPLEMENTASI & PENGUJIAN

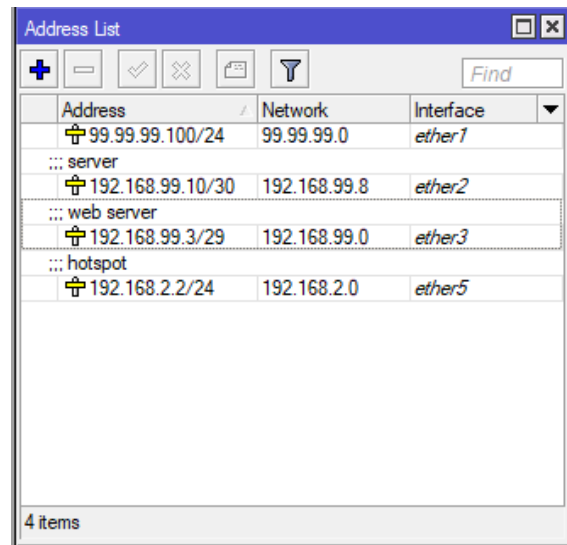
### 5.1 Mikrotik Router

Mikrotik Router secara hardware telah ditunjukkan pada implementasi pada topologi, sedangkan pada sistem meliputi, ip address,

route gateway, hotspot, *firewall*, dns server, web proxy, dan *queue*.

#### 5.1.1 IP Address

IP address address diimplementasikan pada masing-masing port interface yang tersedia pada router mikrotik rb 450. Adapun IP Address yang digunakan yaitu di bagi menjadi 4 (empat) IP Address seperti yang ditunjukkan pada gambar 5.1.



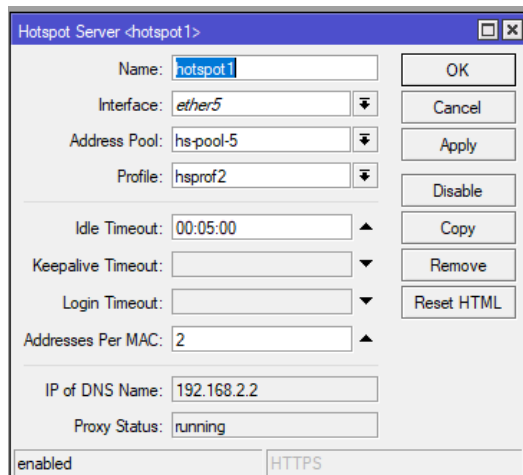
**Gambar 5.1**  
**IP Address Mikrotik**

Pada interface ether 1 IP Address 99.99.99.100/24 digunakan sebagai alamat ip yang terhubung dengan ISP. Ether 2 diimplementasikan IP Address 192.168.99.10/30, IP tersebut terhubung dengan server yang dimiliki Lab Sistem Komputer. IP Address 192.168.99.3/29 merupakan ip address yang ada pada ether 3. IP tersebut difungsikan untuk menghubungkan router mikrotik dengan Web Server Raspberry Pi.

Pada implementasi IP Address port Interface yang tersedia pada router mikrotik telah digunakan secara keseluruhan.

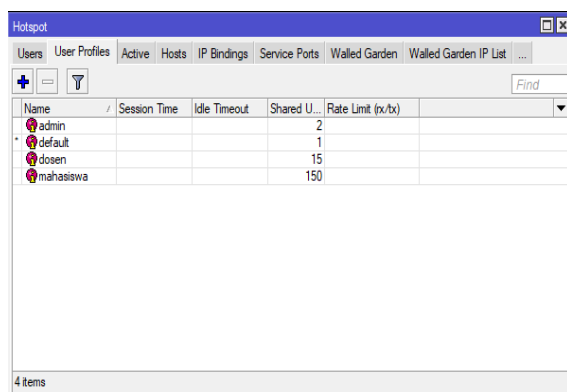
#### 5.1.2 Hotspot

Implementasi hotspot pada mikrotik router ditujukan untuk user dapat menggunakan akses internet dengan perantara wifi (*access point*). Hotspot pada mikrotik router memiliki fitur web login, fitur tersebut yang dimanfaatkan dan dimodifikasi pada penelitian ini.



**Gambar 5.2**  
**Server Hotspot**

Pada gambar 5.2 hotspot diimplementasikan pada interface ether5 dan mengaktifkan DHCP server. IP DNS untuk hotspot yaitu 192.168.2.2 seperti pada gambar 5.3, hotspot memiliki 3 user profile yaitu, Mahasiswa, Dosen, dan admin.



**Gambar 5.3**  
**User Profile Hotspot**

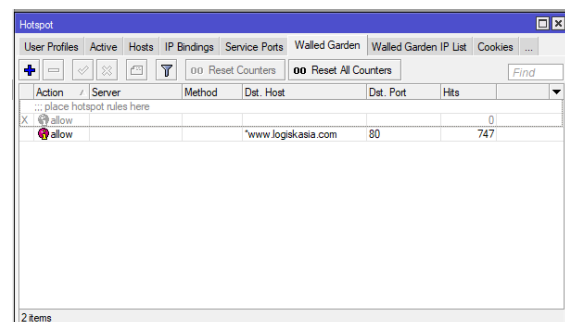
Pada gambar 5.3 masing-masing user profile memiliki jumlah maksimal pengguna, dimana user profile Mahasiswa memiliki 150 pengguna, user profil Dosen dengan 15 pengguna, dan user profile admin dengan 3 pengguna.

Setiap user profile memiliki perlakuan yang berbeda khususnya pada Mahasiswa, sehingga untuk membedakan ip address yang didapatkan oleh user profile ditambahkan pengaturan *incoming-filter*. Untuk Mahasiswa *incoming-filter* = Mahasiswa-in, untuk Dosen *incoming-filter* = Dosen-in dimaksudkan, dan untuk admin *incoming-filter* = admin-in.

*Incoming-filter* dimaksudkan untuk menyaring ip address yang masuk, yang selanjutnya ip address akan dikirim ke *Address List* yang ada pada *firewall*. Dari IP Address yang telah terdaftar di *Address List* mikrotik akan memberikan perlakuan yang berbeda pada setiap user profile yang masuk.

Pada gambar 5.3 terdapat implementasi *incoming-packet-mark* dan *outgoing-packet-mark*, implementasi tersebut akan digunakan pada saat *queue tree* dijalankan, dengan masing-masing tanda yang sudah diberikan pada setiap user profile.

Dalam implementasinya hotspot login akan diarahkan pada web server raspberry pi. Sehingga, untuk dapat mengakses hotspot login yang ada pada web server raspberry pi, diperlukan implementasi walled garden seperti pada gambar 5.4.

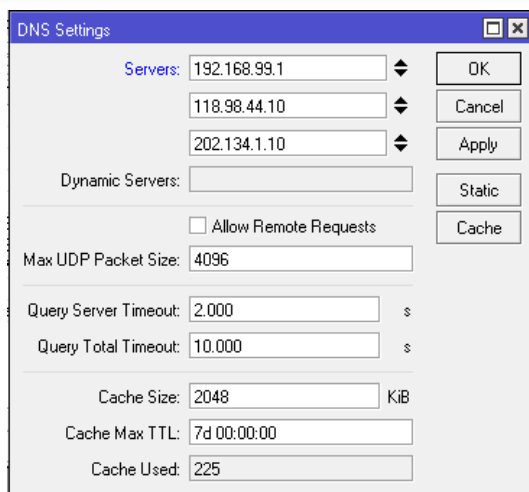


**Gambar 5.4**  
**Walled-garden Hotspot**

Pada gambar 5.4 implementasi *walled-garden* dilakukan dengan cara mendaftarkan DNS [www.logiskasia.com](http://www.logiskasia.com), yang merupakan DNS dari web server raspberry pi.

### 5.1.2.1 DNS Server

Domain Name Server (DNS) diimplementasikan dengan tujuan seluruh ip address dapat mengakses web server dan jaringan internet. DNS yang pertama di *list* adalah DNS web server, hal tersebut bertujuan agar user hotspot saat pertama login dapat mengakses server lokal terlebih dahulu. DNS yang kedua yaitu DNS yang terintegrasi dengan jaringan internet. Implementasi DNS server ditunjukkan pada gambar 5.5



**Gambar 5.5**  
**DNS Server**

DNS Server dengan IP Address 192.168.99.1 merupakan DNS yang dimiliki oleh web server raspberry pi. Jika DNS web server tidak didaftarkan pada kolom DNS pertama besar kemungkinan pada saat login router tidak dapat menemukan web server lokal. IP Address 202.134.1.10 dan IP Address 118.98.44.10 merupakan ip address yang terintegrasi dengan internet. Jika DNS server tidak diisi dengan IP address DNS Server internet ada kemungkinan seluruh jaringan lokal tidak dapat mengakses internet.

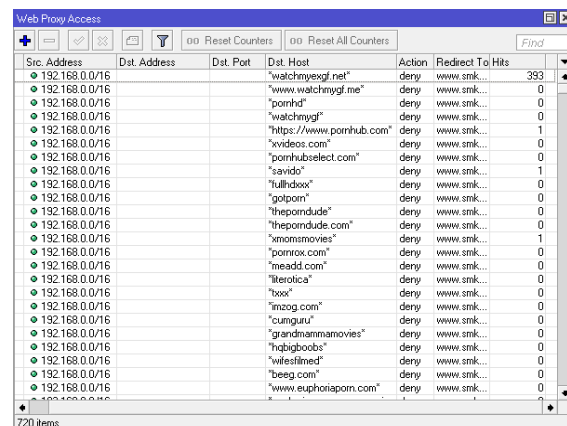
### 5.1.3 Web Proxy

Web Proxy mikrotik router pada penelitian ini, diimplementasikan sebagai penyimpanan cache web server dan blokir situs. Untuk dapat melakukan cache dan blokir situs web proxy perlu dilakukan pengaktifan seperti pada gambar 5.6.

```
[admin@MikroTik] > ip proxy print
enabled: yes
src-address: ::
port: 3128
anonymous: no
parent-proxy: ::
parent-proxy-port: 0
cache-administrator: admin@logiskasia.com
max-cache-size: unlimited
max-cache-object-size: 2048KiB
cache-on-disk: yes
max-client-connections: 600
max-server-connections: 600
max-fresh-time: 3d
serialize-connections: no
always-from-cache: yes
cache-hit-dscp: 4
cache-path: hotspot/error.html
```

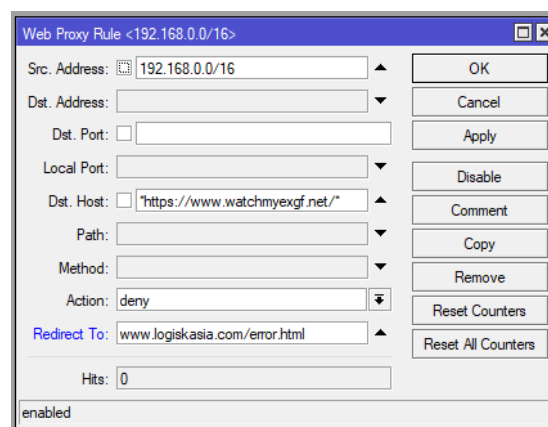
**Gambar 5.6**  
**Web Proxy**

Web proxy diaktifkan kondisi enabled:yes, port 3128 merupakan port web proxy yang diimplementasikan untuk forward situs yang di blokir. Adapun situs yang diblokir menggunakan web proxy berjumlah 718, ditunjukkan pada gambar 5.7.



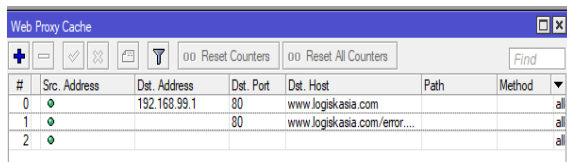
**Gambar 5.7**  
**Daftar Situs Terlarang**

Situs yang diblokir melalui web proxy merupakan situs yang mengandung konten porno sehingga diperlukan pemblokiran situs. Implementasi blokir situs dengan web proxy bertujuan untuk me-redirect situs porno ke halaman web server raspberry pi, implementasinya ditunjukkan pada gambar 5.8.



**Gambar 5.8**  
**Redirect Web Proxy**

Pada gambar 5.8 terdapat Src. Address 192.168.0.0/16, pada saat ada ip address yang berasal dari blok ip mengakses situs yang terdaftar dalam list access dengan action deny, maka mikrotik router akan me-redirect request user ke www.logiskasia.com/error.html . Aktifasi cache web server raspberry pi ditunjukkan pada gambar 5.9.



#	Src. Address	Dst. Address	Dst. Port	Dst. Host	Path	Method
0		192.168.99.1	80	www.logiskasia.com		all
1			80	www.logiskasia.com/error...		all
2						all

**Gambar 5.9**  
**Cache Web Proxy**

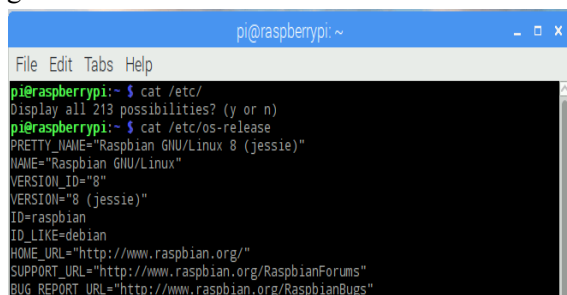
Cache web server diimplementasikan pada dst-host www.logiskasia.com dengan port 80 dan *action* allow.

## 5.2 Raspberry pi

Raspberry pi pada penelitian ini, diimplementasikan sebagai web server. Dalam implementasinya web server, dan *database*.

### 5.2.1 Sistem Operasi Raspberry Pi

Sistem operasi yang diimplementasikan pada raspberry pi yaitu sistem operasi raspbian. Sistem operasi yang diimplementasikan dapat dilihat pada gambar 5.10.



```

pi@raspberrypi: ~
File Edit Tabs Help
pi@raspberrypi:~$ cat /etc/
Display all 213 possibilities? (y or n)
pi@raspberrypi:~$ cat /etc/os-release
PRETTY_NAME="Raspbian GNU/Linux 8 (jessie)"
NAME="Raspbian GNU/Linux"
VERSION_ID="8"
VERSION="8 (jessie)"
ID=raspbian
ID_LIKE=debian
HOME_URL="http://www.raspbian.org/"
SUPPORT_URL="http://www.raspbian.org/RaspbianForums"
BUG_REPORT_URL="http://www.raspbian.org/RaspbianBugs"
    
```

**Gambar 5.10**  
**Sistem Operasi Raspbian**

Pada gambar 5.10 terdapat keterangan os yang digunakan pada raspberry pi yaitu OS raspbian versi 8 (jessie). Raspberry dengan os tersebut memiliki tampilan dekstop dan menu seperti pada gambar 5.11.

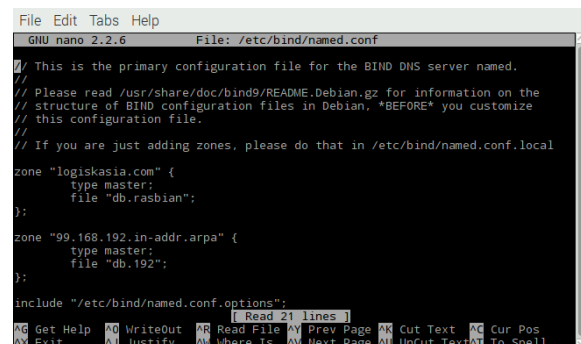


**Gambar 5.11**  
**Tampilan Dekstop Raspbian**

Pada tampilan dekstop terdapat simbol buah raspberry, dimana simbol tersebut merupakan icon / tombol menu yang ada pada sistem operasi raspbian.

### 5.2.2 Web Server

Web Server sebagai salah satu sistem utama yang telah dirancang pada tugas akhir ini, diimplementasikan sebagai penyedia *web login* hotspot Lab Sistem Komputer. Pada implementasinya web server dibangun menggunakan aplikasi bind9, agar web server dapat diakses dari jaringan luar diperlukan dns server dan ip address. Sebelum mengimplementasikan dns server dan ip address diperlukan konfigurasi bind seperti pada gambar 5.12, untuk membangun file yang menyimpan dns dan ip address.

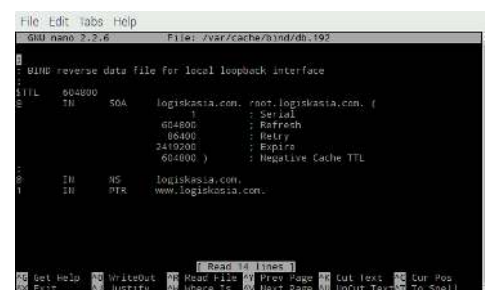


```

File Edit Tabs Help
GNU nano 2.2.6 File: /etc/bind/named.conf
// This is the primary configuration file for the BIND DNS server named.
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
// If you are just adding zones, please do that in /etc/bind/named.conf.local
zone "logiskasia.com" {
    type master;
    file "db.rasbian";
};
zone "99.168.192.in-addr.arpa" {
    type master;
    file "db.192";
};
include "/etc/bind/named.conf.options";
    
```

**Gambar 5.12**  
**Directory Bind web server**

Pada gambar 5.12, file yang dibuat yaitu file db.rasbian yang digunakan untuk menyimpan konfigurasi dns server dan db.192 untuk menyimpan ip address server raspberry pi. Untuk implementasi dns server raspberry pi ditunjukkan pada gambar 5.13.



```

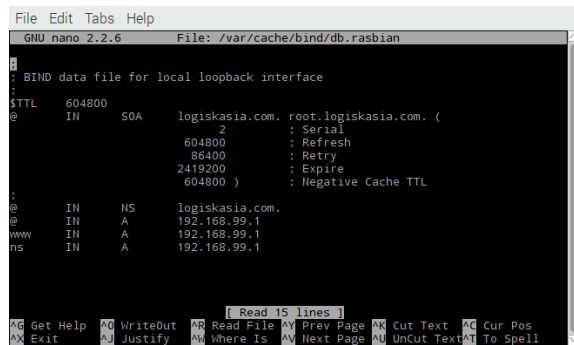
File Edit Tabs Help
GNU nano 2.2.6 File: /var/cache/bind/db.192
BIND reverse data file for local loopback interface
$TTL 604800
IN SOA logiskasia.com. root.logiskasia.com. (
    : Serial
    604800 : Refresh
    86400 : Retry
    2419200 : Expire
    604800 ) : Negative Cache TTL
;
IN NS logiskasia.com.
IN PTR www.logiskasia.com.
    
```

**Gambar 5.13**  
**DNS Web Server**

Gambar 5.13 menunjukkan file db.192 dengan dns server yang diimplementasikan pada bind raspberry pi dengan name server

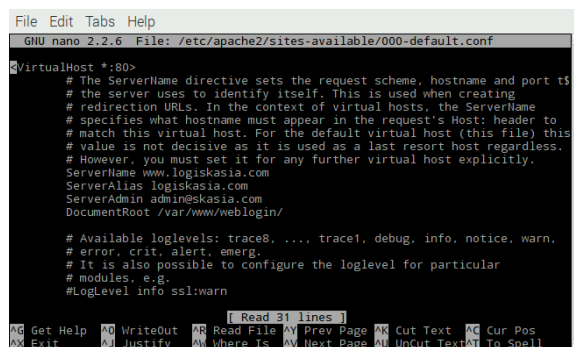


logiskasia.com. Sedangkan untuk konfigurasi file db.rasbian ditunjukkan pada gambar 5.14.



**Gambar 5.14**  
**IP Address Web Server**

Pada Gambar 5.14 terdapat *list* ip address yang diimplementasikan untuk web server. Sedangkan untuk penyimpanan file *web login* disimpan pada site-available apache2, seperti yang ditunjukkan pada gambar 5.15.

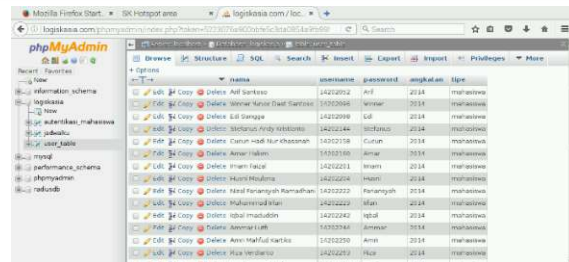


**Gambar 5.15**  
**Site-Available Web Server**

Situs dari web Server yang dapat diakses yaitu halaman *web login*, dengan servername www.logiskasia.com, dimana directory *web login* disimpan pada DocumentRoot /var/www/weblogin/.

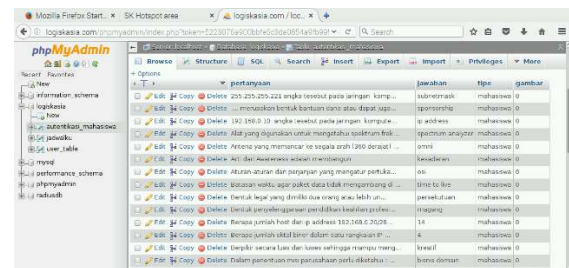
### 5.2.3 Database

Database dibangun dengan tujuan untuk menyimpan data *web login* yang diimplementasikan pada web server. Adapun database logiskasia yang dibangun sesuai perancangan yang memiliki tabel user, tabel autentikasi Mahasiswa. Adapun tabel yang diimplementasikan ditunjukkan pada gambar 5.16 dan gambar 5.17.



**Gambar 5.16**  
**Tabel User**

Gambar 5.16 menunjukkan tabel user yang telah tersimpan pada database logiskasia. Tabel user berisi nama, tipe user, kelas, jurusan, username, dan password. Untuk tabel autentikasi Mahasiswa ditunjukkan pada gambar 5.17.



**Gambar 5.17**  
**Tabel Soal Autentikasi**

Gambar 5.17 merupakan implementasi tabel autentikasi pada database Mahasiswa. Pada tabel soal autentikasi berisi field pertanyaan, jawaban, kelas, jurusan, dan gambar.

#### 5.2.3.1 Web Login (web Server) dengan Mikrotik

Pada dasarnya hotspot mikrotik memiliki halaman login. Pada penelitian ini web login yang ada pada mikrotik dialihkan pada halaman web login yang ada pada web server raspberry pi. Implementasi yang dilakukan pada halaman web login mikrotik, ditunjukkan pada segmen program 4.1.

#### Segmen Program 4.1 Dns Web Server Pada Login.Html Mikrotik

```
0 <script type="text/javascript">
1:
0 window.location.replace("http://www.lo
2: giskasia.com/");
```

Segmen program 4.1 dns web server pada login.html mikrotik menunjukkan, script 01-02: pada javascript login.html mikrotik, terdapat

script  
window.location.replace("http://www.logiskasi  
a.com");. Script yang ada pada javascript  
login.html ditujukan pada saat user mengakses  
halaman login.html mikrotik, akan diarahkan ke  
halaman login web server dengan dns  
www.logiskasia.com. Pada saat user berhasil  
melakukan proses login mikrotik akan  
meredirect ke halaman status login. Untuk  
melakukan proses login web server berhasil  
masuk ke mikrotik diimplementasikan script  
seperti pada segmen program 4.2.

#### Segmen Program 4.2 Iframe Status Login Hotspot Pada Status Login Web Server

```
0 <iframe class="iframe-login-hidden"  
1 src="http://192.168.2.2/login?dst=&popu  
: p=true&username=admin  
&password=admin"></iframe>  
0 <iframe class="iframe-login-hidden"  
2 src="http://192.168.2.2/login?dst=&popu  
: p=true&username=dosen  
&password=dosen"></iframe>  
0 <iframe class="iframe-login-hidden"  
3 src="http://192.168.2.2/login?dst=&popu  
: p=true&username=mahasiswa  
&password=mahasiswa"></iframe>
```

Segmen program 4.2 merupakan segmen  
program yang digunakan untuk mengaktifkan  
user hotspot yang berhasil melakukan login pada  
web login. Apadun pejelasan dari masing-  
masing segmen yaitu, 01: iframe status login  
yang digunakan untuk user admin yang berhasil  
melakukan login. 02: merupakan pop up iframe  
dari status login berhasil, dengan username  
Dosen. 03: merupakan pop up iframe dari status  
login berhasil, dengan username Mahasiswa.  
Masing-masing dari segmen program  
diimplementasikan pada halaman status login  
berhasil yang ditunjukkan pada gambar 5.18,  
gambar 5.19, dan gambar 5.20.



**Gambar 5.18**  
Halaman Status Admin Berhasil Login

Pada gambar 5.18 diimplementasikan  
iframe script 01 dari segmen program 4.2.  
Gambar 5.18 merupakan halaman create read  
update delete admin. Halaman CRUD  
diimplementasikan untuk mempermudah saat  
mengakses CRUD database.



**Gambar 5.19**  
Halaman Status Dosen Berhasil Login

Gambar 5.19 merupakan halaman status  
user dosen berhasil login. Pada gambar 5.19  
terdapat iframe script 02 segmen program 4.2



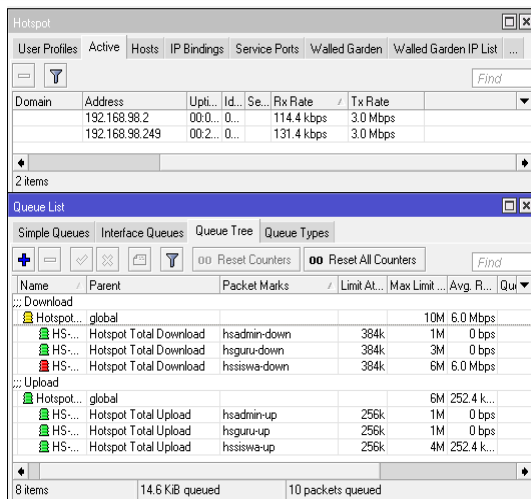
**Gambar 5.20**  
Halaman Status User Mahasiswa Berhasil  
Login

Gambar 5.20 merupakan halaman status  
user dosen berhasil login. Pada gambar 5.20  
terdapat iframe script 03 segmen program 4.2

### 5.3 Pengujian

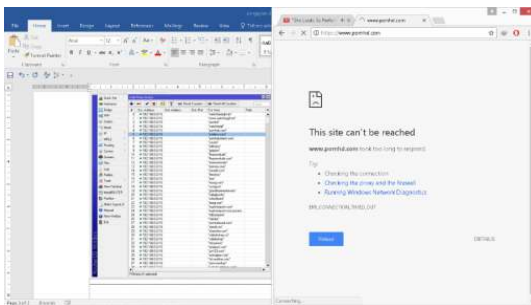
Pengujian yang dilakukan meliputi  
limitasi bandwidth, proses login, firewall dan  
proxy, serta penilaian terhadap pertanyaan yang  
diberikan oleh sistem kepada user.

Berikut adalah hasil screenshot hasil  
pengujian bandwidth yang dilakukan terhadap 2  
orang user



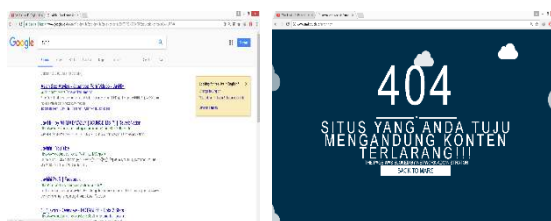
**Gambar 5.21**  
**Pengujian bandwidth**

Selanjutnya berikut adalah hasil screenshot hasil pengujian terhadap situs yang telah dimasukkan dalam layer 7 dan address list mikrotik



**Gambar 5.22**  
**Blok Situs**

Sedangkan untuk situs yang telah terdaftar dalam web proxy yang telah dibuat maka berhasil di redirect ke halaman berikut



**Gambar 5.23**  
**Redirect Situs**

Dari 20 user dalam pengujian proses Autentifikasi redirect login Web Server dapat berjalan cukup baik. Sedangkan dari penilaian quisoner terhadap pertanyaan yang dibuat sekitar 90 % penilaian mengatakan bahwa pertanyaan

yang dibuat sangat sesuai dengan pembelajaran di prodi sistem komputer, tim penilai yang digunakan adalah 3 orang dosen pengampu mata kuliah Jaringan di STMIK Asia Malang.

Dari semua proses pengujian yang telah dilakukan bisa disimpulkan bahwa sistem yang dibuat sudah bisa berjalan cukup baik dengan nilai akurasi dan keberhasilan yang cukup memuaskan.

## 6 PENUTUP

### 6.1 Kesimpulan

Dari hasil pengujian yang telah dilakukan didapatkan kesimpulan, sebagai berikut:

1. Manajemen hotspot yang telah dibangun dinilai lebih baik dari sebelumnya. Dimana mikrotik router dapat bekerja sesuai dengan perancangan dan implementasi yang telah dilakukan.
2. Manajemen bandwidth dapat berjalan sesuai dengan perancangan dengan nilai max-limit download satu user siswa aktif sebesar 6 Mbps, sedangkan dua user mahasiswa aktif masing-masing mendapatkan max-limit 3 Mbps .
3. Dari 718 situs yang mengandung konten terlarang yang masuk list web proxy access deny, diambil sample sejumlah 40 situs. Didapatkan presentase hasil yaitu sebesar 5% gagal block redirect, dan 95% berhasil melakukan block situs. Situs yang gagal di block dan redirect merupakan situs berbasis https.
4. Halaman login hotspot yang ada pada web server dapat diakses oleh user, dengan pengujian dilakukan oleh 20 user dan presentase hasil pengujian user login username password yaitu 90%, sedangkan presentase autentikasi mahasiswa secara sistem berjalan 80%.
5. Proses Autentifikasi Web Server dengan pertanyaan kepada user dapat berjalan cukup baik, dan dari quisoner terhadap pertanyaan yang dibuat sekitar 90 % penilaian mengatakan bahwa pertanyaan yang dibuat sangat sesuai dengan pembelajaran di prodi sistem komputer.

## 6.2 Saran

Dari Penelitian yang telah dibuat maka didapatkan beberapa saran untuk penelitian selanjutnya sebagai berikut :

1. Penambahan Sistem e-learning dalam jaringan lokal.
2. Penambahan sistem remote untuk pengontrolan jaringan dari jarak jauh.
3. Penambahan situs pornografi yang belum ada dalam list web proxy dan pemblokiran pada gambar yang mengandung content pornografi.
4. Memperbaiki sistem firewall yang digunakan sehingga dapat melakukan update situs dengan otomatis.
5. Penambahan sistem hidden soal yang telah berhasil dijawab atau telah digunakan.

## DAFTAR PUSTAKA

- Rudito, A. R., Sularsa, A., & Rosmiati, M. (2015). Pembuatan Server Portable Berbasis Raspberry Pi Untuk Mendukung Pelaksanaan Assessment. *eProceedings of Applied Science*, 1(3).
- Dawood, R., Qiana, S. F., & Muchallil, S. (2014). Kelayakan Raspberry Pi sebagai Web Server: Perbandingan Kinerja Nginx, Apache, dan Lighttpd pada Platform Raspberry Pi. *Jurnal Rekayasa Elekrika*, 11(1), 25-29.
- Richardson, M., & Wallace, S. (2012). *Getting started with raspberry PI*. " O'Reilly Media, Inc."
- Jogiyanto, H. M. (2007). *Desain & Analisa Sistem Informasi : Pendekatan Terstruktur Teori dan Praktek Aplikasi Bisnis*. Penerbit Andi.
- Sofana, I. (2013). *Membangun Jaringan Komputer Mudah Membuat Jaringan Komputer (Wire & Wireless) Untuk Pengguna Windows dan Linux*. *Bandung: Informatika*.
- Iwan, S. (2011). *Teori & Modul Praktikum Jaringan Komputer*. *Bandung: Penerbit Modula*.
- Towidjojo, R. (2016). *Mikrotik Kungfu: Kitab 1*. Jakarta: Jasakom.
- Towidjojo, R. (2016). *Mikrotik Kungfu: Kitab 2*. Jakarta: Jasakom.
- Towidjojo, R. (2016). *Mikrotik Kungfu: Kitab 3*. Jakarta: Jasakom.
- Towidjojo, R. (2016). *Mikrotik Kungfu: Kitab 4*. Jakarta: Jasakom.