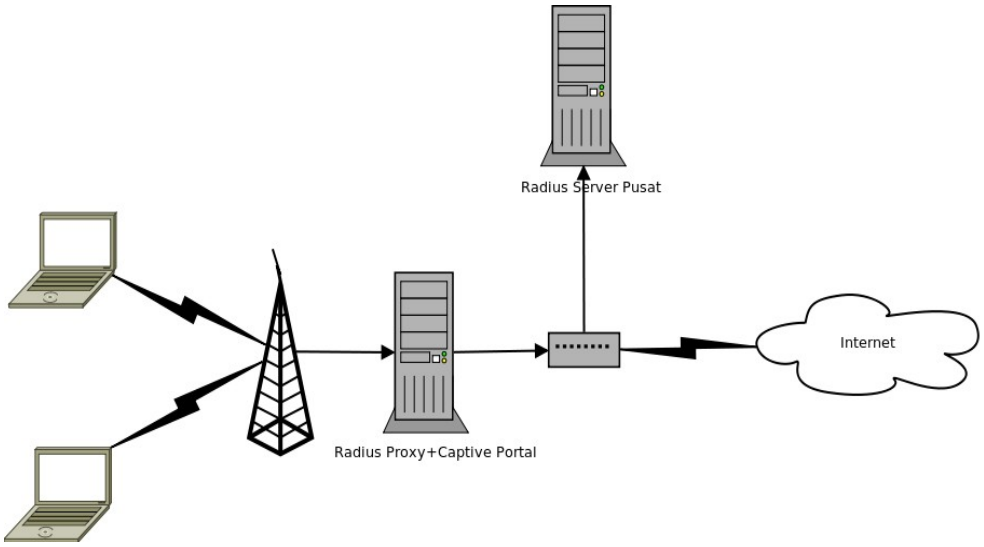
Konfigurasi Router UGM Hotspot

1. Skema Jaringan dan Kebutuhan Sistem

1. Skema Jaringan UGM-Hotspot

Cara kerja dari UGM-Hotspot adalah apabila ada user yang akan terkoneksi ke jaringan internet UGM menggunakan jaringan wireless harus terautentikasi terlebih dahulu menggunakan e-mail UGM, sehingga nantinya user dapat terkoneksi ke semua jaringan wireless di UGM yang telah mengimplementasikan UGM-Hotspot hanya dengan mengguankan satu account. Berikut adalah gambaran skema jaringan dari UGM-Hotspot.



Dengan menggunakan skema jaringan UGM-Hotspot di atas, apabila sewaktu-waktu kita membutuhkan user lokal untuk login ke jaringan menggunakan UGM-Hotspot maka kita juga dapat membuat user lokal di mesin radius proxy tanpa harus membuat mail UGM.

2. Kebutuhan Sistem

Untuk membangun UGM-Hotspot minimal kita harus menyiapkan satu unit PC yang nantinya akan kita fungsikan sebagai router UGM-Hotspot dan satu buah wireless akses point. Kebutuhan hardware minimal dari router UGM-Hotspot adalah minimal Pentium III atau yang setara, memori minimal 256MB, hardisk 5GB (instalasi minimal) dan 2 buah Ethernet Card. Distro yang digunakan menggunakan CentOS Linux 5.5, walaupun sebenarnya konfigurasinya relatif sama dengan distro-distro linux lainya, dengan sedikit penyesuaian.

2. Menyiapkan Domain

Untuk bisa menggunakan sertifikat SSL UGM, router yang digunakan untuk UGM-Hotspot harus sudah mempunyai domain sendiri, berikut tahapan instalasi dan konfigurasi named pada distribusi CentOS Linux di router UGM-Hotspot. Pertama install terlebih dahulu paket named dengan perintah yum

```
yum -y install named
```

Selanjutnya buat konfigurasi utama dari named di /etc/named.conf dan isikan dengan baris berikut

```
zone "hotspot.ugm.ac.id" {
        type master;
        file "/var/named/db.domain";
};
zone "2.168.192.in-addr.arpa" {
        type master;
        notify no;
        file "/var/named/db.ip";
};
options {
  directory "/var/named";
forward first;
  forwarders {
    172.16.30.7;
  };
};
```

buat file untuk pemetaaan dari IP ke domain

```
;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     hotspot.ugm.ac.id. hotspot.ugm.ac.id. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
1       IN      PTR     hotspot
```

kemudian sebaliknya, buat file untuk memetakan alamat domain ke IP

```
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     hotspot.ugm.ac.id. hotspot.ugm.ac.id. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
@       IN      A       192.168.2.1
hotspot IN      A       192.168.2.1
```

kemudian jalankan ulang service named dan lakukan percobaan ping ke alamat hotspot.ugm.ac.id, apabila tidak terjadi kesalahan maka domain hotspot.ugm.ac.id telah berjalan dengan benar.

3. Instalasi httpd dan Konfigurasi SSL UGM

Service httpd digunakan untuk menangani autentikasi melalui captive portal dan juga untuk meletakan file html kita (uam hompage) yang nantinya dapat digunakan untuk meletakan informasi-informasi penting dan juga aturan yang harus di patuhi oleh pengguna UGM-Hotspot. Untuk menginstall httpd dengan dukungan ssl gunakan perintah yum berikut

```
yum -y install httpd mod_ssl
```

Dengan menggunakan perintah di atas berarti httpd telah terinstall dan telah mendukung koneksi ssl, selanjutnya lakukan penyesuaian konfigurasi httpd agar menggunakan sertifikat SSL UGM. Pada file konfigurasi httpd /etc/httpd/conf.d/ssl.conf, ubah pada bagian sertifikat SSL sehingga menjadi seperti berikut.

```
SSLCertificateFile /etc/pki/tls/certs/star_ugm_ac_id.crt
SSLCertificateKeyFile /etc/pki/tls/private/ca.key
SSLCertificateChainFile /etc/pki/tls/certs/DigiCertCA.crt
```

Untuk mendapatkan sertifikat SSL UGM, silahkan menghubungi bagian jaringan PPTiK UGM. Terakhir, jalankan ulang service httpd dan lakukan percobaan koneksi https ke server.

4. Instalasi dan Konfigurasi Radius

Remote Authentication Dial In User Service(RADIUS) merupakan protokol yang menyediakan layanan otentifikasi, otorisasi dan akunting secara terpusat, di centos service ini disediakan secara gratis oleh freeradius, untuk menginstall freeradius di CentOS Linux gunakan perintah berikut

```
yum -y install freeradius2
```

radius yang kita install hanya akan menjadi radius proxy dari radius pusat, konfigurasi radius proxy akan lebih sederhana, sehingga kita hanya perlu menambahkan sedikit konfigurasi pada file /etc/raddb/proxy.conf dan tambahkan baris berikut

```
realm ugm.ac.id {
        authhost = 10.13.253.3:1812
        secret  = radius-secret
        nostrip
}

realm mail.ugm.ac.id {
        authhost = 10.13.253.3:1812
        secret  = radius-secret
        nostrip
}
```

pada bagian radius-secret sesuaikan dengan radius secret di tempat anda, untuk mendapatkan radius-secret silahkan menghubungi bidang jaringan di PPTiK atau menghubungi tim Integrasi, karena untuk bisa berkomunikasi dengan radius pusat, radius proxy kita harus mempunyai radius secret yang sama dengan radius-secret yang ada pada radius pusat, dan juga radius proxy kita harus terdaftar terlebih dahulu pada radius pusat sebagai client.

Setelah proses instalasi selesai, selanjutnya lakukan uji coba radius dengan perintah radclient berikut

```
radtest masrifqi@mail.ugm.ac.id password_email localhost 0 testing123
Sending Access-Request of id 201 to 127.0.0.1 port 1812
     User-Name = "masrifqi@mail.ugm.ac.id"
     User-Password = "password_email"
     NAS-IP-Address = 127.0.0.1
     NAS-Port = 0
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=201,
length=20
```

Dari output hasil tes diatas terlihat koneksi ke radius sudah *Access-Accept* yang berarti percobaan koneksi berhasil.

Apabila suatu saat kita ingin menambahkan user lokal di radius untuk keperluan mendesak tanpa perlu membuat email UGM, maka kita dapat menambahkannya pada file /etc/raddb/users dengan baris berikut

```
rifqi  Cleartext-Password := "testing"
```

Apabila terjadi kegagalan autentikasi atau untuk mengecek kesalahan konfigurasi pada file konfigurasi radius kita dapat menjalankan radius dengan mode debug menggunakan perintah berikut

```
/usr/sbin/radius -X
```

5. Instalasi dan Konfigurasi Chillispot

Chillispot merupakan captive portal yang nantinya akan digunakan oleh user untuk melakukan autentikasi sebelum dapat terkoneksi ke jaringan wireless. Paket chillispot untuk CentOS Linux tidak disediakan secara default oleh distro CentOS, sehingga untuk menginstallnya kita harus mengunduhnya terlebih dahulu, paket chillispot untuk distro berbasis Redhat dapat di download pada url berikut : http://www.chillispot.info/download/chillispot-1.1.0.i386.rpm, setelah proses download selesai, install paket chiilispot dengan perintah rpm berikut

```
rpm -ivh  chillispot-1.1.0.i386.rpm
```

Ubah konfgurasi utama dari chillispot terletak pada file /etc/chilli.conf hingga menjadi seperti berikut

```
net 192.168.2.0/24
dynip 192.168.2.0/24
statip 192.168.2.0/24
dns1 192.168.2.1
dns2 172.16.30.7
radiusserver1 127.0.0.1
radiusserver2 10.55.1.22
radiussecret testing123
dhcpif eth1
uamserver https://hotspot.ugm.ac.id/cgi-bin/hotspotlogin.cgi
uamhomepage https://hotspot.ugm.ac.id/welcome.html
uamsecret ht2eb8ej6s4et3rg1ulp
uamlisten 192.168.2.1
```

```
uamallowed ugm.ac.id
```

Seteleh melakukan penyesuaian konfigurasi pada chillispot, selanjutnya buat halaman UAM hompages sederhana bernama welcome.html yang kita letakan di /var/www/htdocs/ yang dapat di isi dengan informasi-informasi prosedur ataupun aturan yang harus di patuhi oleh para pengguna Hotspot-UGM.
Aktifkan fitur ip_forwarding dengan mengedit file /etc/sysctl menjadi seperti berikut

```
# Controls IP packet forwarding
net.ipv4.ip_forward = 1
```

Kopikan file hotspotlogin.cgi ke direktori cgi-bin

```
cp /usr/share/doc/chillispot-1.1.0/hotspotlogin.cgi /var/www/cgi-bin
```

edit file hotspotlogin.cgi pada bagian berikut

```
$uamsecret = ht2eb8ej6s4et3rg1ulp;
$userpassword=1;
```

Kopikan file rules iptables ke direktori sbin

```
cp /usr/share/doc/chillispot-1.1.0/firewall.iptables /sbin
```

kemudian tabahkan baris berikut pada file /etc/rc.local sebelum baris exit agar file rules iptables akan dijalankan secara otomatis ketika komputer di hidupkan.

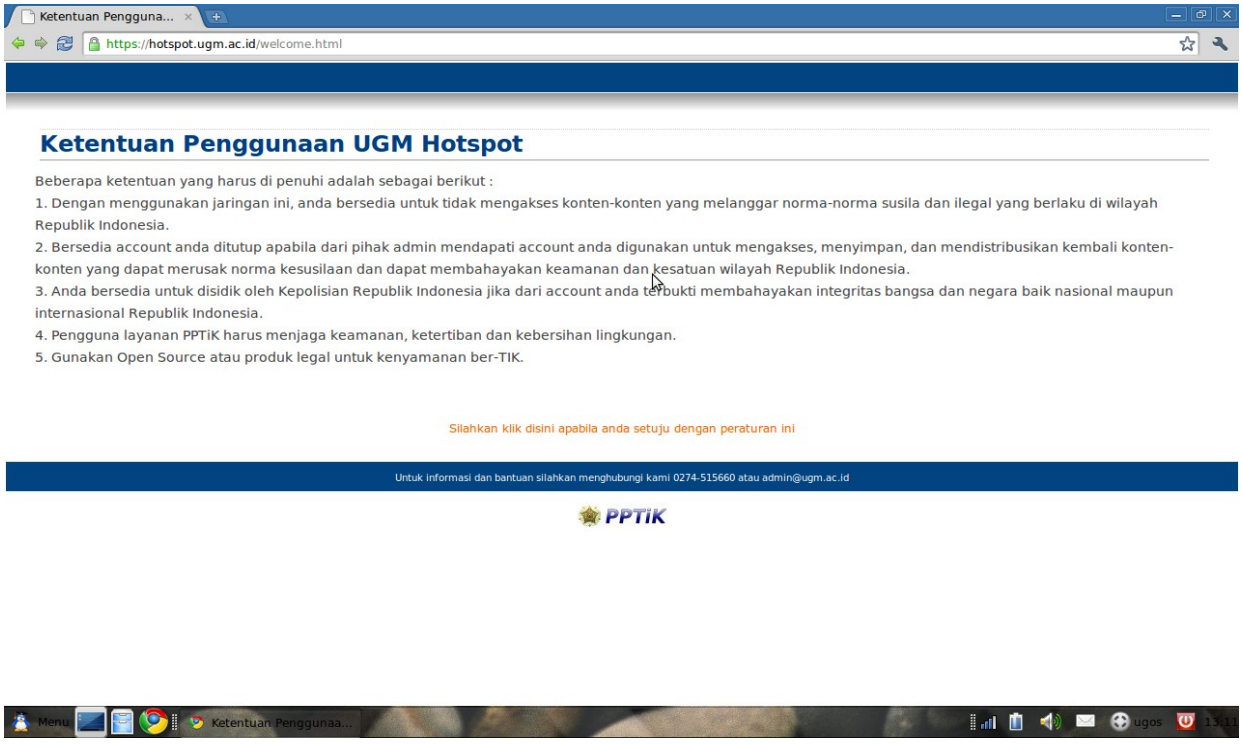
```
bash /sbin/firewall.iptables
```

Untuk menalankan service chillispot gunakan perintah berikut

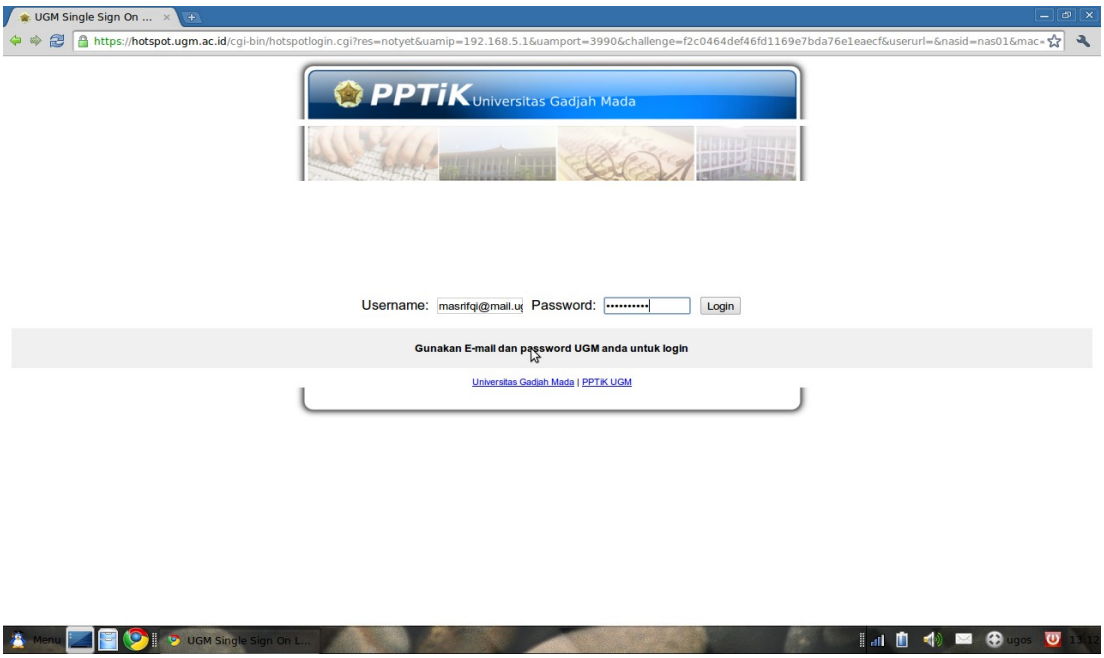
```
/etc/init.d/chillispot start
```

6. Uji Coba

Ketika user akan melakukan browsing ke internet, client akan di redirect ke halaman uam hompages



Halaman login



Setelah login berhasil akan muncul jendela pup-up yang menginformasikan berapa lama user tersebut telah login dan juga link untuk Logout apabila user tersebut t akan mengakhiri session loginya.