

PfSense HOTSPOT Installation

Hello Fellas ;

Hotspot kurulumunun nasıl yapılacağını inceliyor olacağız. In this section we'll talk about hotspot installation on our PfSense's Firewall.

This article and workshop example based on Mr. **SAMET YILMAZ's** works. You can find the original text and application examples by visiting <http://sametyilmaz.com.tr/pfsense-ghost-hot-spot-kurulumu-ve-ilk-ayarlar.html>

Alright ,of course you can ask yourself if there is an existing text why do i need to spend my time for this article. The reason is lots of links under the URL 's expired and installation take lots of time and for newbies who new in command screen video lesson make things easily understandable

With this short briefing lets have a look at what we need ;

- MySQL Server Installation
- MySQL database and user establishing
- Php Components Installation
- Database Configuration and copying Ghost to PfSense Public folder
- Squid,FreeRadius 2 Installation and settings
- Captive Portal installaiton and establishing a connecting with Freeradius2
- Handshaking FreeRadius2 and MYSQL Server
- Ghost first settings

Installation Requirements ;

1-) PfSense version must be "**2.1.3-RELEASE-i386-FreeBSD8.3**" to grt new version you can check <http://files.uk.pfsense.org/mirror/downloads/old/>

2-) Putty application for consol connection to our PfSense machine

3-) Wincap application to monitorising files on PfSense machine

Proper PfSense and connection with Puty done

Lets get started ;

1-) Mysql installation

```
pkg_add -r http://ftp-archive.freebsd.org/pub/FreeBSD-Archive/old-releases/i386/8.3-RELEASE/packages/databases/mysql-server-5.5.21.tbz
```

```
# /usr/local/bin/mysql_install_db --basedir=/usr/local
```

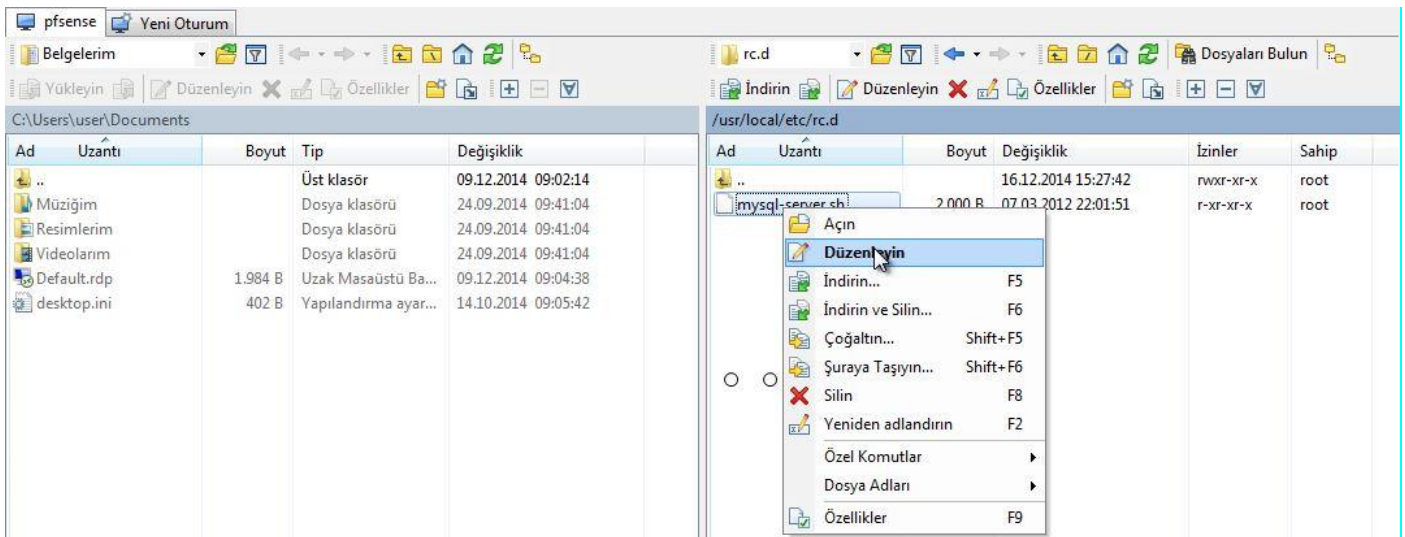
2-) With this command line we'll give proper writing permission to MySQL indexes

```
# chmod 777 /var/db/mysql
```

3-) **Changing** Mysql-server file name for executing startup

```
# mv /usr/local/etc/rc.d/mysql-server /usr/local/etc/rc.d/mysql-server.sh
```

4-) Executing WinSCP application and initialising a connection to our PfSense machine. On WinSCP click on Find Files and searching [mysql-server.sh](#) when it's done right click on it then edit

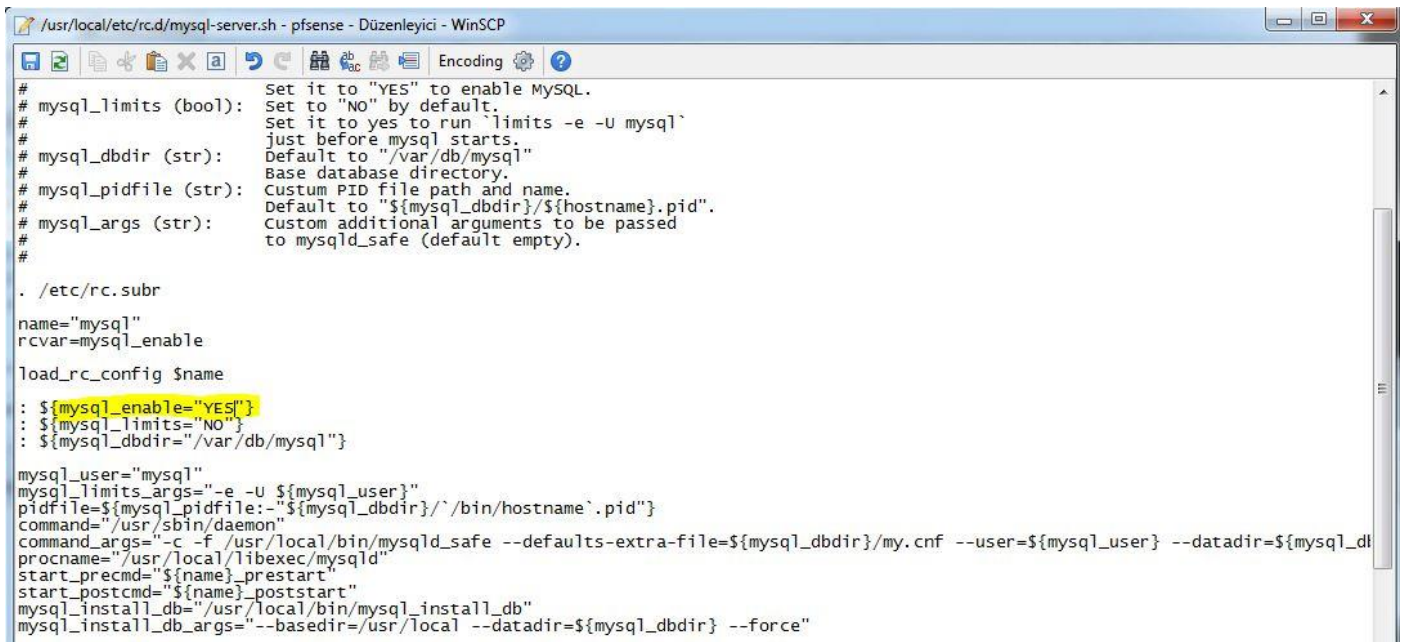


Find this line.

```
# : ${mysql_enable="NO"}
```

Change like this

```
#: ${mysql_enable="YES"}
```



Click on Save and uploaded.

5-) Enter the command line which is below and starting msqj

```
# /usr/local/etc/rc.d/mysql-server.sh start
```

6-) After this step restarting PfSense Machine

7-)Specify a password for MySQL Server root user.This part is important because we'll use this password for further installations.As you can see i choose "admin" as password i

```
# /usr/local/bin/mysqladmin -u root password 'admin'
```

Restarting PfSense machine after this step

8-) Now we'll establish database and user that using by Ghost on MySQL server.Connecting to MySQL console use your password

```
# mysql -u root -p
```

9-) Create a database with name Radius for host and Freeradius

```
# CREATE DATABASE radius;
```

10-) Create a MySQL user for Ghost and Freeradius

```
# CREATE USER 'radius'@'localhost';
```

11-) Specify a password for our user. In this example i'll set password as "admin" you can give another password than "admin"

```
# SET PASSWORD FOR 'radius'@'localhost' = PASSWORD('admin');
```

12-) Give permission to user to reach Radius Database on MySQL server

```
# GRANT ALL ON radius.* TO 'radius'@'localhost';
```

Restarting PfSense Machine

To connect MySQL database externally you have to set your 3306 port as PfSense LAN leg

13-) Entering MySQL with this command line and using our password "admin"

```
# mysql -u root -p
```

14-)

```
# GRANT ALL ON radius.* TO 'radius'@'%' IDENTIFIED BY 'admin';
```

MySQL Server and its Database installation which include below information are done

Database Name : Radius

Database User : Radius

User Password : admin

To reach command Line press Ctrl + C

15-) To TR ID confirmation and MySQL execute these commands respectively. The Important point is these scripts working successfully for every PfSense server however the main point is we'll make a SOAP installation to TR ID confirmation if your PHP version that existing on PfSense different than SOAP some problem may occur in a situation like this check your php version with `php -v` command and install proper SOAP version from FreeBSD repo . Now on PfSense 2.1 working without any problem If you face any problem use `pkg_info` command to list package list then use `pkg_delete -f` command to remove SOAP.

Start with this package installation ;

```
pkg_add -rfi http://ftp-archive.freebsd.org/pub/FreeBSD-Archive/ports/i386/packages-8.3-release/All/php5-soap-5.3.10_1.tbz
```

16-) Using this commands

```
# touch /etc/php_dynamodules/mysql
```

```
# touch /etc/php_dynamodules/php-soap
```

Restarting PfSense Machine after this step.

17-) If you have a server that include MySQL Apache, IIS or MYSQL you can install Ghost and Radius' databases on them. (To Captive Portal files SOAP and MySQL extension steps must be done)

```
# mkdir /usr/local/www/ghost
```

```
# cd /usr/local/www/ghost
```

```
# fetch http://sametyilmaz.com.tr/ghost.tar
```

Alternatively+

```
# fetch http://www.serdarbayram.net/download/ghost.tar
```

```
# tar xvzf ghost.tar
```

18-) DataBase table that using by Freeradius and Ghost execute these commands. First ; import SQL file to database that we've created before use your specific password in this example i'll use "admin" as password

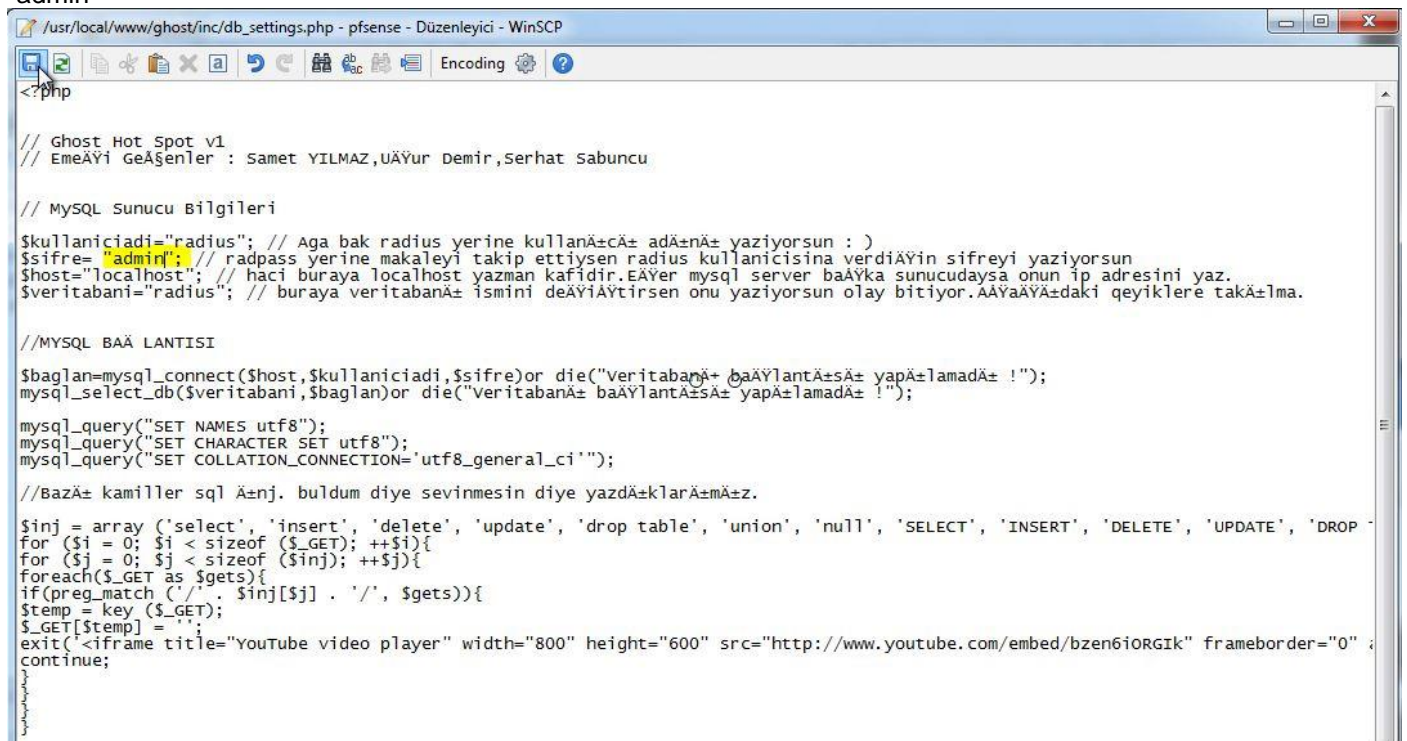
```
# mysql -p -u radius radius < /usr/local/www/ghost/ghost.sql
```

19-) To connect Ghost Managing Console to database ; Information in MySQL connection file must be change according to SQL database and user

To do this we'll use Winscp and connect to pfSense machine

```
/usr/local/www/ghost/inc/db_settings.php
```

To search bar section write "db_settings.php" and open it in "Edit Mode" in this section we'll change user name as Radius (in my example i've choose Radius as a user name you can give a different name) and it's password as "admin"



```
#!/usr/bin/php

// Ghost Hot Spot v1
// EmeÄYi GeÄŞenler : Samet YILMAZ,UÄYur Demir,Serhat Sabuncu

// MySQL Sunucu Bilgileri
$kullaniciadi="radius"; // Aga bak radius yerine kullanÄ±cÄ± adÄ±nÄ± yaziyorsun : )
$sifre="admin"; // radpass yerine makaleyi takip ettiysen radius kullanicisina verdiÄYin sifreyi yaziyorsun
$host="localhost"; // haci buraya localhost yazman kafidir.EÄYer mysql server baÄYka sunucudaysa onun ip adresini yaz.
$veritabani="radius"; // buraya veritabanÄ± ismini deÄYiyÄYtirsen onu yaziyorsun olay bitiyor.AÄYaÄYÄ±daki qeyiklere takÄ±lma.

//MYSQL BAÄ LANTISI
$baglan=mysql_connect($host,$kullaniciadi,$sifre)or die("veritabanÄ± baÄYlantÄ±sÄ± yapÄ±lamadÄ± !");
mysql_select_db($veritabani,$baglan)or die("veritabanÄ± baÄYlantÄ±sÄ± yapÄ±lamadÄ± !");

mysql_query("SET NAMES utf8");
mysql_query("SET CHARACTER SET utf8");
mysql_query("SET COLLATION_CONNECTION='utf8_general_ci'");

//BazÄ± kamiller sql Ä±nj. buldum diye sevinmesin diye yazdÄ±klarÄ±mÄ±z.
$inj = array ('select', 'insert', 'delete', 'update', 'drop table', 'union', 'null', 'SELECT', 'INSERT', 'DELETE', 'UPDATE', 'DROP');
for ($i = 0; $i < sizeof ($_GET); ++$i){
    for ($j = 0; $j < sizeof ($inj); ++$j){
        foreach($_GET as $gets){
            if(preg_match ("/". $inj[$j] . '/', $gets)){
                $temp = key ($_GET);
                $_GET[$temp] = '';
                exit(<iframe title="YouTube video player" width="800" height="600" src="http://www.youtube.com/embed/bzen6iORGIk" frameborder="0" ;
            }
        }
    }
}
continue;
```

Alright Fellas SSH part is done.

Enter the PfSense Interface then **System**→**Packages** and install these packages respectively

1.Freeradius2

2.Squid

System: Package Manager



Name	Category	Version	Description
freeradius2	System	2.1.12_1/2.2.5_3 pkg v1.6.10	A free implementation of the RADIUS protocol. Support: MySQL, PostgreSQL, LDAP, Kerberos FreeRADIUS and FreeRADIUS2 settings are not compatible so don't use them together or try to update On pfSense docs there is a how-to which could help you on porting users. Package info
squid	Network	2.7.9 pkg v.4.3.4	High performance web proxy cache. No package info, check the forum

20-) When the installation is done we'll configure Captive Portal settings
click on Services→ Captiveportal then click on + sign

Captiveportal: Zones

Zone	Interfaces	Number of users	Description
captiveportal	LAN	0	

Zone Identification editing

Services: Captive portal: Edit Zones

Edit Captiveportal Zones

Zone name	<input type="text" value="captiveportal"/> <small>Zone name. Can only contain letters, digits, and underscores (_).</small>
Description	<input type="text" value="hotspot test"/> <small>You may enter a description here for your reference (not parsed).</small>

We'll enable Captive Portal as below

[After Authentication Redirection URL](#) : In this section you can add a site to redirecting our clients .Save the settings.

Services: Captive portal: captiveportal



Captive portal(s)	Pass-through MAC	Allowed IP addresses	Allowed Hostnames	Vouchers	File Manager
<input checked="" type="checkbox"/> Enable captive portal					
Interfaces	WAN LAN Select the interface(s) to enable for captive portal.				
Maximum concurrent connections	<input type="text"/> per client IP address (0 = no limit) This setting limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many users can load the portal page or authenticate at the same time! Possible setting allowed is: minimum 4 connections per client IP address, with a total maximum of 100 connections.				
Idle timeout	<input type="text"/> minutes Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.				
Hard timeout	<input type="text"/> minutes Clients will be disconnected after this amount of time, regardless of activity. They may log in again immediately, though. Leave this field blank for no hard timeout (not recommended unless an idle timeout is set).				
Pass-through credits allowed per MAC address	<input type="text"/> per client MAC address (0 or blank = none) This setting allows passing through the captive portal without authentication a limited number of times per MAC address. Once used up, the client can only log in with valid credentials until the waiting period specified below has expired. Recommended to set a hard timeout and/or idle timeout when using this for it to be effective.				
Waiting period to restore pass-through credits	<input type="text"/> hours Clients will have their available pass-through credits restored to the original count after this amount of time since using the first one. This must be above 0 hours if pass-through credits are enabled.				
Reset waiting period on attempted access	<input type="checkbox"/> Enable waiting period reset on attempted access If enabled, the waiting period is reset to the original duration if access is attempted when all pass-through credits have already been exhausted.				
Logout popup window	<input type="checkbox"/> Enable logout popup window If enabled, a popup window will appear when clients are allowed through the captive portal. This allows clients to explicitly disconnect themselves before the idle or hard timeout occurs.				
Pre-authentication redirect URL	<input type="text"/> Use this field to set \$PORTAL_REDIRURL\$ variable which can be accessed using your custom captive portal index.php page or error pages.				
After authentication Redirection URL	<input type="text"/> http://www.serdarbayram.net If you provide a URL here, clients will be redirected to that URL instead of the one they initially tried to access after they've authenticated.				

21-) Now let's configure our Prox Server. Click on **Servers**→**Proxy** Server change settings as below.

General Upstream Proxy Cache Mgmt Access Control Traffic Mgmt Auth Settings Local Users

Proxy interface LAN
WAN
loopback
The interface(s) the proxy server will bind to.

Allow users on interface
If this field is checked, the users connected to the interface selected in the 'Proxy interface' field will be allowed to use the proxy, i.e., there will be no need to add the interface's subnet to the list of allowed subnets. This is just a shortcut.

Transparent proxy
If transparent mode is enabled, all requests for destination port 80 will be forwarded to the proxy server without any additional configuration necessary.

Bypass proxy for Private Address Space (RFC 1918) destination
Do not forward traffic to Private Address Space (RFC 1918) **destination** through the proxy server but directly through the firewall.

Bypass proxy for these source IPs
Do not forward traffic from these **source** IPs, CIDR nets, hostnames, or aliases through the proxy server but directly through the firewall. Separate by semi-colons (;). [Applies only to transparent mode]

Bypass proxy for these destination IPs
Do not proxy traffic going to these **destination** IPs, CIDR nets, hostnames, or aliases, but let it pass directly through the firewall. Separate by semi-colons (;). [Applies only to transparent mode]

Enable logging
This will enable the access log. Don't switch this on if you don't have much disk space left.

Log store directory
The directory where the log will be stored (note: do not end with a / mark)

Log rotate
Defines how many days of logfiles will be kept. Rotation is disabled if left empty.

Proxy port
This is the port the proxy server will listen on.

ICP port
This is the port the Proxy Server will send and receive ICP queries to and from neighbor caches. Leave this blank if you don't want the proxy server to communicate with neighbor caches through ICP.

Visible hostname
This is the URL to be displayed in proxy server error messages.

Administrator email
This is the email address displayed in error messages to the users.

Language
Select the language in which the proxy server will display error messages to users.

Disable X-Forward
If not set, Squid will include your system's IP address or name in the HTTP requests it forwards.

Disable VIA

22-) So far so good Proxy settings is done so let's get Free Radius 2 and Captive Portal integration done. Click on **Services** → **Freeradius** and click on **NAS/Clients** then click on + button to add a client

FreeRADIUS: Clients



Users MACs **NAS / Clients** Interfaces Settings EAP SQL Certificates LDAP View config XMLRPC Sync

Client IP Address	Client IP Version	Client Shortname	Client Protocol	Client Type	Require Message Authenticator	Max Connections	Description
+							

Save

Client ip address: Enter a LAN ip address

Client shortname : Give a name

Client share Secret: Give a password. In this example i've choose admin as password

FreeRADIUS: Clients: Edit



Users | MACs | **NAS / Clients** | Interfaces | Settings | EAP | SQL | Certificates | LDAP | View config | XMLRPC Sync

General Configuration

Client IP Address
Enter the IP address of the RADIUS client. This is the IP of the NAS (switch, access point, firewall, router, etc.).

Client IP Version

Client Shortname
Enter a short name for the client. This is generally the hostname of the NAS.

Client Shared Secret
Enter the shared secret of the RADIUS client here. This is the shared secret (password) which the NAS (switch or accesspoint) needs to communicate with the RADIUS server.

Miscellaneous Configuration

Client Protocol
Enter the protocol the client uses. (Default: UDP)

Client Type
Enter the NAS type of the client. This is used by checkrad.pl for simultaneous use checks. (Default: other)

Require Message Authenticator
RFC5080 requires Message-Authenticator in Access-Request. But older NAS (switches or accesspoints) do not include that. (Default: no)

Max Connections
Takes only effect if you use TCP as protocol. This is the mirror of "Max Requests Server" from "Settings" tab. (Default 16)

NAS Login
If your NAS supports it you can use SNMP or finger for simultaneous-use checks instead of (s)radutmp file and accounting. Leave empty to choose (s)radutmp. (Default: empty)

NAS Password
If your NAS supports it you can use SNMP or finger for simultaneous-use checks instead of (s)radutmp file and accounting. Leave empty to choose (s)radutmp. (Default: empty)

Description
Enter any description you like for this client.

Click on Save button to save

23-)Accounting and Authentication packages detection that sending by Captive Portal,click on Interface and create 2 interfaces like below

FreeRADIUS: Interfaces



Users | MACs | NAS / Clients | **Interfaces** | Settings | EAP | SQL | Certificates | LDAP | View config | XMLRPC Sync

Interface IP Address	Port	Interface Type	IP Version	Description
----------------------	------	----------------	------------	-------------

As an Interface Ip enter * .Set Port 1812 interface type as Authentication

FreeRADIUS: Interfaces: Edit



Users MACs NAS / Clients **Interfaces** Settings EAP SQL Certificates LDAP View config XMLRPC Sync

General Configuration

Interface IP Address
Enter the IP address (e.g. 192.168.100.1) of the listening interface. If you choose * then it means all interfaces. (Default: *)

Port
Enter the port number of the listening interface. Different interface types need different ports.
You could use this as an example:
Authentication = 1812
Accounting = 1813
Status = 1816
IMPORTANT: For every interface type listening on the same IP address you need different ports.

Interface Type
Enter the type of the listening interface. (Default: auth)

IP Version
Enter the IP version of the listening interface. (Default: IPv4)

Description
Optionally enter a description here for your reference.

As Interface IP enter * 1813 as port Interface type Accounting then click on Save

FreeRADIUS: Interfaces: Edit



Users MACs NAS / Clients **Interfaces** Settings EAP SQL Certificates LDAP View config XMLRPC Sync

General Configuration

Interface IP Address
Enter the IP address (e.g. 192.168.100.1) of the listening interface. If you choose * then it means all interfaces. (Default: *)

Port
Enter the port number of the listening interface. Different interface types need different ports.
You could use this as an example:
Authentication = 1812
Accounting = 1813
Status = 1816
IMPORTANT: For every interface type listening on the same IP address you need different ports.

Interface Type
Enter the type of the listening interface. (Default: auth)

IP Version
Enter the IP version of the listening interface. (Default: IPv4)

Description
Optionally enter a description here for your reference.

FreeRADIUS: Interfaces



Users MACs NAS / Clients **Interfaces** Settings EAP SQL Certificates LDAP View config XMLRPC Sync

Interface IP Address	Port	Interface Type	IP Version	Description
*	1812	auth	ipaddr	
*	1813	acct	ipaddr	

Click on Save button.

24-) To complete Captive Portal and FreeRadius 2 integration click on Services →Captive Portal and configure as below

The screenshot shows the configuration page for Captive Portal authentication. It is divided into several sections:

- Authentication:** Includes radio buttons for 'No Authentication', 'Local User Manager / Vouchers', and 'RADIUS Authentication' (which is selected). A checkbox 'Allow only users/groups with 'Captive portal login' privilege set' is checked.
- Radius Protocol:** Includes radio buttons for 'PAP' (selected), 'CHAP_MD5', 'MSCHAPv1', and 'MSCHAPv2'.
- Primary Authentication Source:** A red header section containing:
 - Primary RADIUS server:** Fields for IP address (192.168.1.1), Port (1812), and Shared secret (admin).
- Secondary RADIUS server:** Fields for IP address, Port, and Shared secret, all currently empty.

As Authentication Type choose Radius Authentication seçin and set Radius Protocol as PAP.Set Radius server infos like above.Choose IP address as PFSense server LAN interface ip address.Set as Authentication use 1812 or leave blank as default it connects 1812 automatically

Shared Secret :When we added NAS Client on Freeradius section we'll use "admin" as password.

Accounting Partition ;

Set details as below and choose 1813 as Accounting Portal.To send Account updates to Radius click on Start-Stop accounting.Click on Save then exit

Accounting

send RADIUS accounting packets
If this is enabled, RADIUS accounting packets will be sent to the primary RADIUS server.

Accounting port
Leave blank to use the default port (1813).

Accounting updates
 no accounting updates
 stop/start accounting
 interim update

RADIUS options

Reauthentication **Reauthenticate connected users every minute**
If reauthentication is enabled, Access-Requests will be sent to the RADIUS server for each user that is logged in every minute. If an Access-Reject is received for a user, that user is disconnected from the captive portal immediately.

RADIUS MAC authentication **Enable RADIUS MAC authentication**
If this option is enabled, the captive portal will try to authenticate users by sending their MAC address as the username and the password entered below to the RADIUS server.

MAC authentication secret

RADIUS NAS IP attribute
Choose the IP to use for calling station attribute.

Session-Timeout **Use RADIUS Session-Timeout attributes**
When this is enabled, clients will be disconnected after the amount of time retrieved from the RADIUS Session-Timeout attribute.

Type
If RADIUS type is set to Cisco, in Access-Requests the value of Calling-Station-Id will be set to the client's IP address and the Called-Station-Id to the client's MAC address. Default behavior is Calling-Station-Id = client's MAC address and Called-Station-Id = pfSense's WAN IP address.

Accounting Style **Invert Acct-Input-Octets and Acct-Output-Octets**
When this is enabled, data counts for RADIUS accounting packets will be taken from the client perspective, not the NAS. Acct-Input-Octets will represent download, and Acct-Output-Octets will represent upload.

NAS Identifier
Specify a NAS identifier to override the default value (hotspot.localdomain)

MAC address format
This option changes the MAC address format used in the whole RADIUS system. Change this if you also

Restarting Captive Portal and Freeradius services by click on **Status → Services**

Status: Services



Service	Description	Status	
apinger	Gateway Monitoring Daemon	Running	
captiveportal	Captive Portal: captiveportal	Running	
dnsmasq	DNS Forwarder	Running	
ntpd	NTP clock sync	Running	
radiusd	FreeRADIUS Server	Running	
squid	Proxy server Service	Running	

Restart Service

25-) As you can see services have been started successfully .To testing this click on **Services** → **Freeradius** → **Users** section create a standard user and start a process from a client that on Captive Portal

FreeRADIUS: Users: Edit



Users | MACs | NAS / Clients | Interfaces | Settings | EAP | SQL | Certificates | LDAP | View config | XMLRPC Sync

General Configuration

Username:
Enter the username. Whitespace is possible. If you do not want to use username/password but custom options then leave this field empty.

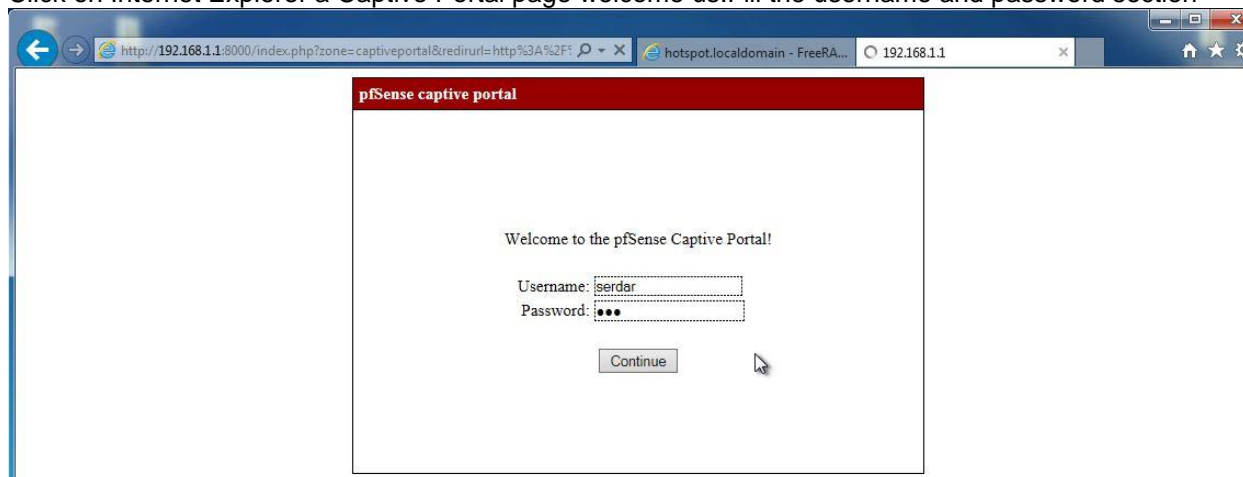
Password:
Enter the password for this username. If you do not want to use username/password but custom options then leave this field empty.

Password encryption:
Select the password encryption for this user. Default: Cleartext-Password

Enable One-Time-Password for this user:
This enables the possibility to authenticate against an username and an one-time-password. The client to generate OTP can be installed on various mobile device platforms like Android and more.

IMPORTANT: You need to enabled mOTP first in FreeRADIUS => Settings (Default: unchecked)

Click on Internet Explorer a Captive Portal page welcome us.Fill the username and password section



26-) Lets get Freeradius and MySQL server integration done. Click on **Services**→**FreeRadius**→**SQL** section and set as below

FreeRADIUS: SQL



Users | MACs | NAS / Clients | Interfaces | Settings | EAP | SQL | Certificates | LDAP | View config | XMLRPC Sync

Enable SQL Database- Server 1

Enable SQL Support:
Enable this if you like to connect freeRADIUS to a SQL database. (Default: unchecked)
You **must enable at least** one of the following options: Authorization, Accounting, Session, Post-Auth.

Enable SQL Authorization:
Enable this if usernames and passwords are stored on a SQL database.
SQL support must be enabled for this to work. (Default: Disable)

Enable SQL Accounting:
Enable this if accounting packets should be logged to a SQL database.
SQL support must be enabled for this to work. (Default: Disable)

Enable SQL Session:
Enable this to use the "rlm_sql" module (fast) to check for simultaneous connections instead of "radutmp" (slow).
SQL support must be enabled for this to work. (Default: Disable)

Enable SQL Post-Auth:
Enable this if you like to store post-authentication data on a SQL database.
SQL support must be enabled for this to work. (Default: Disable)

SQL Database Configuration - Server 1

Database Type:
Choose the database type. (Default: mysql)

Server IP Address:
Enter the IP address of the database server (Default: localhost)

Server Port Address:
Enter the port address of the database server (Default: 3306)

Database Username:
Enter the username of the database server (Default: radius)

Database Password:
Enter the password of the database server (Default: radpass)

Database Table Configuration:
Choose database table configuration: (Default: radius)
 For all **except** Oracle choose: **radius**
 For Oracle change and paste the following line according your environment:
(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=localhost)(PORT=1521))(CONNECT_DATA=(SID=your_sid)))

On the below side of page MySQL server infos and databases infos required. In this example i've configured as below and you can change it as you wish.

- Server IP Address: localhost
- Server Port Address (MySQL Default Port): 3306
- Database Username : Radius
- Database Password : **admin**
- Database Table Congiuration : Radius

SQL Socket Maximum Queries:
If you have issues with SQL sockets lasting too long, you can limit the number of queries performed over one socket. After X queries, the socket will be closed. Use 0 for no limit. (Default: 0)

Read Clients from Database:
Set to **yes** to read RADIUS clients from the database ('nas' table). Clients will only be read on server startup. (Default: yes)

RADIUS Client Table:
Choose the table to keep RADIUS client info. (Default: nas)

Enable Redundant SQL Database Support

Read Client from Database default as Yes change it as No
 Save settings and click on **Status → System Logs** menu and monitorise SQL connection. Log records must be like this

Dec 16 14:58:18	radiusd[79147]: rlm_sql (sql): Driver rlm_sql_mysql (module rlm_sql_mysql) loaded and linked
Dec 16 14:58:18	radiusd[79147]: rlm_sql (sql): Attempting to connect to radius@localhost:3306/radius
Dec 16 14:58:18	radiusd[79147]: rlm_sql (sql): Attempting to connect rlm_sql_mysql #0
Dec 16 14:58:18	radiusd[79147]: rlm_sql_mysql: Starting connect to MySQL server for #0
Dec 16 14:58:18	radiusd[79147]: rlm_sql (sql): Connected new DB handle, #0
Dec 16 14:58:18	radiusd[79147]: rlm_sql (sql): Attempting to connect rlm_sql_mysql #1
Dec 16 14:58:18	radiusd[79147]: rlm_sql_mysql: Starting connect to MySQL server for #1
Dec 16 14:58:18	radiusd[79147]: rlm_sql (sql): Connected new DB handle, #1
Dec 16 14:58:18	radiusd[79147]: rlm_sql (sql): Attempting to connect rlm_sql_mysql #2
Dec 16 14:58:18	radiusd[79147]: rlm_sql_mysql: Starting connect to MySQL server for #2
Dec 16 14:58:18	radiusd[79147]: rlm_sql (sql): Connected new DB handle, #2
Dec 16 14:58:18	radiusd[79147]: rlm_sql (sql): Attempting to connect rlm_sql_mysql #3
Dec 16 14:58:18	radiusd[79147]: rlm_sql_mysql: Starting connect to MySQL server for #3
Dec 16 14:58:18	radiusd[79147]: rlm_sql (sql): Connected new DB handle, #3
Dec 16 14:58:18	radiusd[79147]: rlm_sql (sql): Attempting to connect rlm_sql_mysql #4
Dec 16 14:58:18	radiusd[79147]: rlm_sql_mysql: Starting connect to MySQL server for #4
Dec 16 14:58:18	radiusd[79147]: rlm_sql (sql): Connected new DB handle, #4
Dec 16 14:58:18	radiusd[79147]: Loaded virtual server <default>
Dec 16 14:58:18	radiusd[79198]: Ready to process requests.

Click on **Status**→ **Services** and be sure services running successfully.

Status: Services



Service	Description	Status	
apinger	Gateway Monitoring Daemon	Running	
captiveportal	Captive Portal: captiveportal	Running	
dnsmasq	DNS Forwarder	Running	
ntpd	NTP clock sync	Running	
radiusd	FreeRADIUS Server	Running	
squid	Proxy server Service	Running	

27-) All services running successfully. Now let's install Ghost Portal file for Captive Portal welcome screen

Ghost Welcome Screen : <http://www.sametyilmaz.com.tr/portal.rar>

Alternative link : <http://www.serdarbayram.net/download/portal.rar>

From Services → Captive Portal editing it .

SSL Certificate: webConfigurator default

Portal page contents: C:\Users\user\Desktop\ Gözet...

Upload an HTML/PHP file for the portal page here (leave blank to keep the current one). Make sure to include a form (POST to "") with a submit button (name="accept") and a hidden field with name="redirurl" and value="". Include the "auth_user" and "auth_pass" and/or "auth_voucher" input fields if authentication is enabled, otherwise it will always fail. Example code for the form:

```
<form method="post" action="$PORTAL_ACTIONS$">
  <input name="auth_user" type="text">
  <input name="auth_pass" type="password">
  <input name="auth_voucher" type="text">
  <input name="redirurl" type="hidden" value="$PORTAL_REDIRURL$">
  <input name="accept" type="submit" value="Continue">
</form>
```

Authentication error page contents: C:\Users\user\Desktop\ Gözet...

The contents of the HTML/PHP file that you upload here are displayed when an authentication error occurs. You may include "\$PORTAL_MESSAGES", which will be replaced by the error or reply messages from the RADIUS server, if any.

Logout page contents: Gözet...

The contents of the HTML/PHP file that you upload here are displayed on authentication success when the logout popup is enabled.

Save **Cancel**

Note: Changing any settings on this page will disconnect all clients! Don't forget to enable the DHCP server on your captive portal interface! Make sure that the default/maximum DHCP lease time is higher than the timeout entered on this page. Also, the DNS forwarder needs to be enabled for DNS lookups by unauthenticated clients to work.

Portal page contents : Upload HTML file for the portal page here

Authentication Error page contents : Upload error.html. Click on Save and done.

In portal.rar file that you have downloaded before find **captiveportal-config.php** and editing as you wish

```
captveportal-config - Not Defteri
Dosya Düzen Biçim Görünüm Yardım
<?php
// Ghost Hot Spot v1
// Emeği Geçenler : Samet YILMAZ,Uğur Demir,Serhat Sabuncu

// MySQL Sunucu Bilgileri
$kullaniciadi="radius"; // Aga bak radius yerine kullanıcı adını yazıyorsun : )
$sifre= "admin"; // radpass yerine makaleyi takip ettiysen radius kullanıcısına verdiğin şifreyi yazıyorsun
$host="localhost"; // hacı buraya localhost yazman kafidir. Eğer mysql server başka sunucudaysa onun ip adresini yaz.
$veritabani="radius"; // buraya veri tabanı ismini değiştiren onu yazıyorsun olay bitiyor. Aşağıdaki qeyiklere takılma.

//MYSQL BAĞLANTISI
$dbaglan=mysql_connect($host,$kullaniciadi,$sifre)or die("Veritabani bağlantısı yapılamadı !");
mysql_select_db($veritabani,$dbaglan)or die("Veritabani bağlantısı yapılamadı !");
mysql_query("SET NAMES 'utf8'");
```

28-) Captive-Portal → Filemanager section Services: Captive portal: captiveportal



Captive portal Pass-through MAC Allowed IP addresses Allowed Hostnames Vouchers File Manager

Name	Size
captiveportal-config.php	1 KB
captiveportal-jquery-1.11.0.min.js	94 KB
captiveportal-logo.png	60 KB
captiveportal-sms.php	4 KB
captiveportal-tc.php	3 KB
TOTAL	163 KB

Note:
Any files that you upload here with the filename prefix of captiveportal- will be made available in the root directory of the captive portal HTTP(S) server. You may reference them directly from your portal page HTML code using relative paths. Example: you've uploaded an image with the name 'captiveportal-test.jpg' using the file manager. Then you can include it in your portal page like this:

```

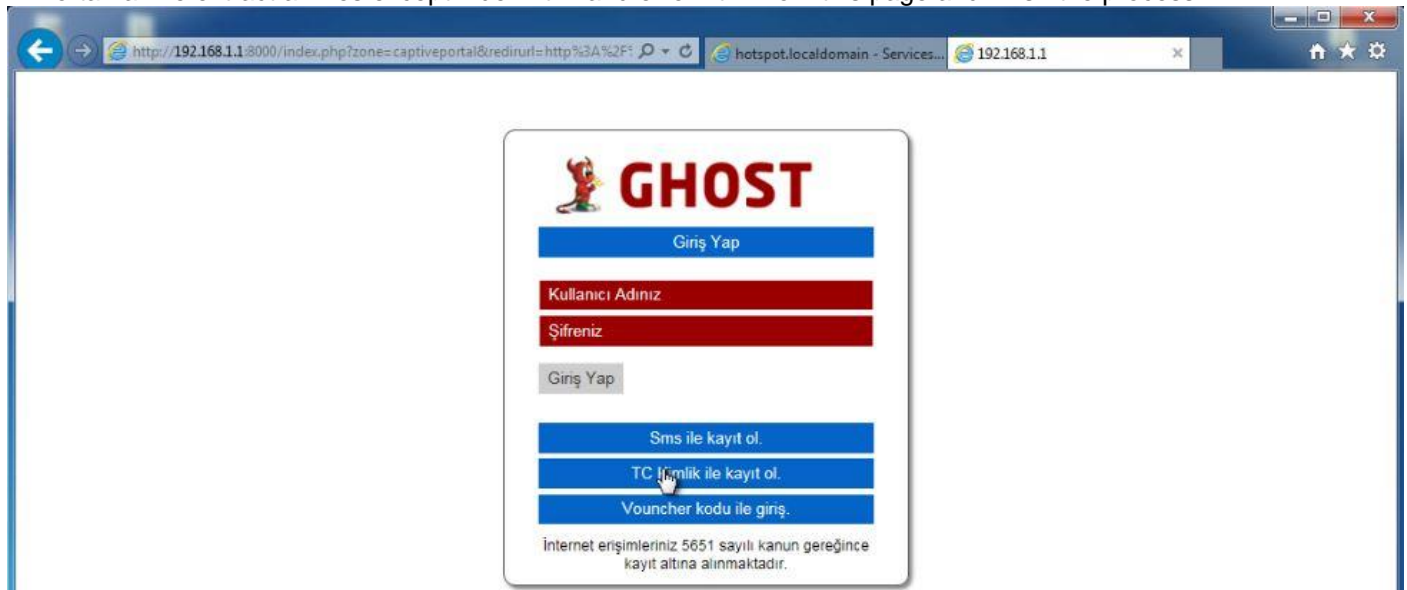
```

In addition, you can also upload .php files for execution. You can pass the filename to your custom page from the initial page by using text similar to:

```
<a href="/captiveportal-aup.php?zone=$PORTAL_ZONE&redirurl=$PORTAL_REDIRURL$">Acceptable usage policy</a>
```

The total size limit for all files is 1.00 MB.

In Portal.rar file extract all files except index.html and error.html from this page and finish the process



As you can see in this picture Ghost page welcome us succesfully.If you want to change logo enter the Captive Portal Managing Screen and upload your own logo with .png extension.To removing Sms or TR ID sections open the index.html file and remove related fields.

How to Reach Ghost Managing Panel

From <http://pfsenseipadres/ghost> you can reach the panel.If you've changed PFSense port you can reach the panel from [http://pfsenseipadres:\[port\]/ghost](http://pfsenseipadres:[port]/ghost)

adresinden Ghost paneline ulaşabilirsiniz. Eğer PFSense'nin portunu değiştirdiyseiz [http://pfsenseipadres:\[port\]/ghost](http://pfsenseipadres:[port]/ghost) şeklinde erişebilirsiniz.

Ghost Default User Name and Password

User Name: admin

Password : ghost



Kullanıcı

Şifre

Hakkında

Welcome screen will be like this and you can see the login user from "Online Users" section

Dashboard **Yeni** Loglar Kullanıcılar Attribute My Account Logout

Yeni Kullanıcı Yeni Attribute

Yeni Kullanıcı oluştur

Yeni Attribute oluştur

Ghost Kullanıcı Listesi

TC Kimlik Kullanıcıları

SMS Kullanıcıları

Kullanıcı Erişim Logları

Detaylı Kullanıcı Logları

SMS Gönderim Logları

Rad Check Attribute Listesi

Rad Reply Attribute Listesi

Sms ve Limit Ayarları

Ghost Hesap Bilgileri

Online Kullanıcılar

KULLANICI ADI -	- BAŞLANGIÇ TARİHİ -	IP ADRESİ -	MAC ADRESİ -
sbayram64	2014-12-16 15:04:55	192.168.1.55	00:0c:29:d5:2b:e4

Sayfalar

Installation have been done suuccessfully.Hope its helpful

Author

Serdar BAYRAM