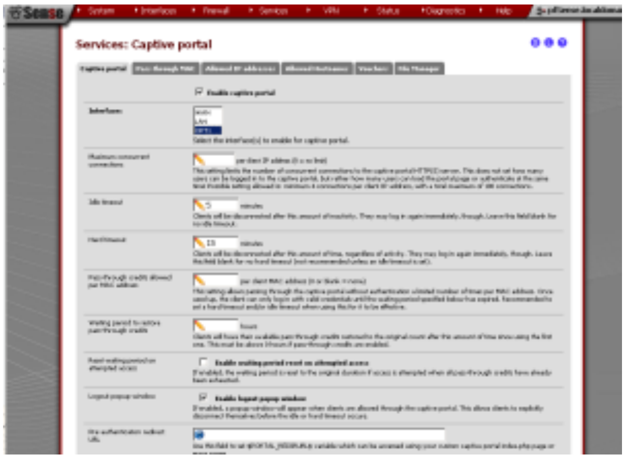
pfSense Captive Portal: Part One

Captive portal forces an HTTP client to see a special web page, usually for authentication purposes, before using the Internet normally. A captive portal turns a web browser into an authentication device. This is done by intercepting all packets, regardless of address or port, until the user opens a browser and tries to access the Internet. At that time, the browser is redirected to a web page which may require authentication and/or payment, or simply display an acceptable use policy and require the user to agree. Setting up a pfSense captive portal is fairly simple, yet pfSense 2.0 provides a number of different options which allow admins a high level of control over their networks.

Configuring a pfSense Captive Portal



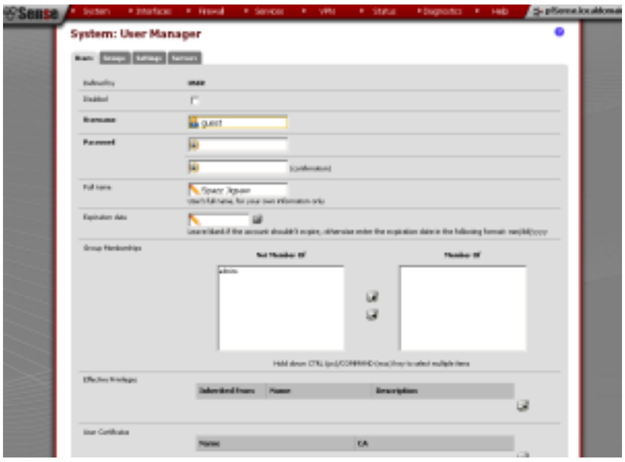
Captive portal settings page in pfSense 2.0.

In order to configure captive portal in pfSense, first navigate to **Services** -> **Captive Portal**. From the "**Captive portal**" tab click the "**Enable captive portal**" check box. At "**Interfaces**", choose one or more interfaces (for this example, we will select OPT1). At "**Idle timeout**", specify a timeout (for this example, we will specify 10 minutes). At "**Hard timeout**", specify a timeout (for this example, we will specify 90 minutes).

Next, click the "**Enable logout popup window**" so users may log themselves out when they are finished. At "**Redirection URL**", specify a URL (for this example, we will specify http://pfsensesetup.com). At "**Authentication**", select "**Local User Manager**". Then press "**Save**" to save the changes.

Next, navigate to **System** -> **User Manager**. Click on the "**Users**" tab, and click on the "**plus**" button to add a new user. At "**Username**", enter a user name, and at "**Password**", enter a password. At "**Full name**", type the full name of the user. Then press the "**Save**" button to save the changes.

Now, any user from the OPT1 network who attempts to browse the web will first have to authenticate. Once authenticated, they will be directed to pfSense Setup HQ, where they may then surf the web before they encounter a timeout which we defined, at which point they will have to authenticate again.



System: User Manager

Defined by	USER
Disabled	□
Username	guest
Password	
	(confirmation)
Full name	
Expiration date	
Group Memberships	Not Member Of: admin Member Of
Effective Privileges	Inherited From | Name | Description
User Certificates	Name | CA

Adding a user with the pfSense User Manager.

pfSense Captive Portal: Additional Options

Although the above example will enable us to set up a functioning captive portal, there are some additional settings on the captive portal configuration page that are worth mentioning. “**Maximum concurrent connections**” allows you to limit the number of concurrent connections to the captive portal. It does not limit how many users can be logged into the captive portal, but rather how many users can load the portal page to authenticate at the same time. The default is no limit (0). Otherwise, the minimum setting is 4 connections per client IP address, with a maximum of 100.

“**Pass-through credits allowed per MAC address**” allows passing through the captive portal without authentication a limited number of times per MAC address. Once this number is used up, the client can only log in with valid credentials until a waiting period specified has expired (this parameter is “**Waiting period to restore pass-through credits**“). Finally, the “**Enable waiting period reset on attempted access**” check box resets the waiting period to the original duration if access is attempted when all pass-through credits have already been exhausted.

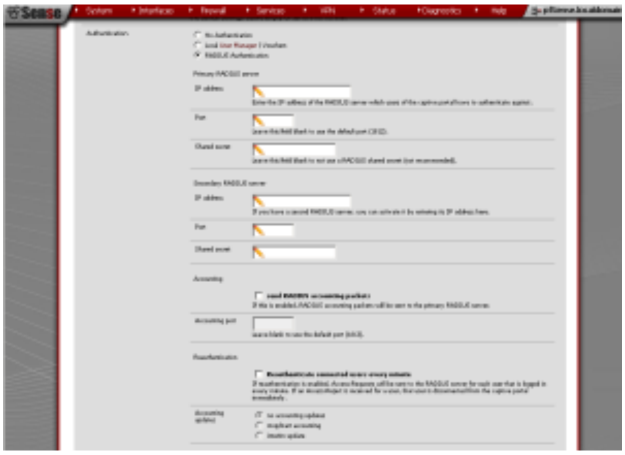
In part two, I will cover some of the other pfSense captive portal options available in pfSense 2.0. (Dans la deuxième partie, je vais aborder certaines des autres pfSense captive portal options disponibles dans pfSense 2.0.)

External Links:

Captive Portal on Wikipedia

Captive Portal on doc.pfsense.org

pfSense Captive Portal: Part Two (RADIUS Server, etc.)



Authentication
○ No Authentication
○ Local User Manager / Vouchers
● RADIUS Authentication

Primary RADIUS server
IP address
Port
Shared secret

Secondary RADIUS server
IP address
Port
Shared secret

Accounting
□ send RADIUS accounting packets

Accounting port

Reauthentication
□ Reauthenticate connected users every minute

Accounting updates
● no accounting updates
○ stop/start accounting
○ interim update

Configuring RADIUS settings in pfSense 2.0.

In part one, I covered configuration of a simple captive portal in pfSense. In this part, I continue explaining some of the more esoteric captive portals settings, including a look at what RADIUS is and configuring RADIUS settings.

At "**Pre-authentication redirect URL**", you can set the value of the $PORTAL_REDIRURL$ variable. This variable can be accessed using your custom captive portal index.php page or error pages. At "**After authentication Redirection URL**", you can provide a URL that clients will be redirected to instead of the one they initially tried to access after they authenticated.

The next option is the "**Disable concurrent logins**" check box. If this option is set, only the most recent login per username will be active. Subsequent logins will cause machines previously logged in with the same username to be disconnected. Next is the "**Disable MAC filtering**" check box; if checked, pfSense will make no attempt to ensure that the MAC address of the client stays the same when they are logged in. The "**Enable Pass-through MAC automatic additions**" check box will ensure that users of that MAC address will never have to authenticate again if this option is checked. Any authenticated users who access the Internet while this is enabled will have a MAC passthrough entry added. To remove an entry, you either have to log in and remove it manually from the "**Pass-through MAC tab**" or send a POST from another system to remove it. The "**Enable Pass-through MAC automatic addition with username**" check box will cause pfSense to save the user name used during authentication. Again, to remove the passthrough MAC entry, you either have to log in and remove it manually from the "**Pass-through MAC**" tab or send a POST from another system to remove it.

The next check box, "**Enable per-use bandwidth restriction**", allows you to restrict each user who logs in to a specified default bandwidth. RADIUS can override the default settings. The default download/upload speeds (in Kbit/s) is specified in the next two edit boxes.

RADIUS Explained

The next section is “**Authentication**“. Here you have three broad options: “**No Authentication**“, “**Local User Manager/Vouchers**” (which was the method user in the configuration example in part one), and “**RADIUS Authentication**“. Remote Access Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for computers that connect and use a network service. It is often used by ISPs and enterprises to manage access to the Internet or internal networks, wireless networks, and integrated e-mail services. If RADIUS is enabled, the user or machine sends a request to a Remote Access Server (RAS) to gain access to a particular network resource using access credentials. The credentials are passed to the RAS device via the link-layer protocol. In turn, the RAS sends a RADIUS Access Request message to the RADIUS server, requesting authorization to grant access via the RADIUS protocol. The requests includes access credentials, typically in the form of username and password or security certificate provided by the user. The RADIUS server checks that the information is correct using authentication schemes such as PAP, CHAP, or EAP. The RADIUS server returns one of three responses: Access Reject (the user is unconditionally denied access), Access Challenge (the server requests more information), or Access Accept (the user is granted access). If the user is granted network access, the Network Access Server (NAS) will send a packet to the RADIUS server indicating it should begin accounting, which will continue until the user’s network access is closed.

Specifying a RADIUS Server

pfSense gives us a variety of options for RADIUS configuration. Under “**Primary RADIUS server**“, you can enter the IP address, port, and shared secret (a shared secret is a piece of data known only to the parties involved used either for authentication or to feed a key derivation function to produce keys to use for encryption and/or MACing of messages). There is an identical series of edit boxes under “**Secondary RADIUS server**“. Under “**Accounting**“, click the “**send RADIUS accounting packets**” check box to send accounting packets to the primary RADIUS server. At “**Accounting port**“, you can specify a port (leaving it blank causes the default port, 1813, to be used). At “**Accounting updates**“, there are three options: [1] no accounting updates; [2] stop/start accounting, and [3] interim update.

Check “**Enable RADIUS MAC authentication**” to make the captive portal try to authenticate users by sending their MAC address in the username and the password entered in the “Shared secret” edit box to the RADIUS server. “RADIUS NAS IP attribute” allows you to choose the IP of the Network Access Server. Checking “**Use**

RADIUS Session Timeout attributes" will cause clients to be disconnected after the amount of time retrieved from the RADIUS Session-Timeout attribute is reached. "**Type**" can be set to "**default**" or "**cisco**"; if it is set to Cisco, the value of Calling Station-ID will be set to the client's IP address and the Called station-ID to the clients MAC address, instead of to the MAC address and WAN UP address respectively.

At "**MAC address format**", you can change the MAC address format used for the whole RADIUS system. The default is to have the 48-bit address in hexadecimal separated by colons into octets. Checking "**Enable HTTPS login**" will cause the username and password to be transmitted over an HTTPS connection to protect against eavesdroppers. The next few fields, "**HTTPS server name**", "**HTTPS certificate**", "**HTTPS private key**", "**HTTPS intermediate certificate**" are parameters related to configuring your HTTPS server.

Changing Default Portal/Error/Logout Pages

"**Portal page contents**" allows you to upload an HTML/PHP file for the portal page. You must include a form with a submit button (name="accept"), a hidden field with name "rediurl" and value="", and "auth_user", "auth_pass" and "auth_voucher" if authentication is enabled. "**Authentication error page contents**" allows you to upload an error page to display when an authentication error occurs. Finally, "**Logout page contents**" allows you to upload an HTML/PHP file to display when the logout popup is enabled.

External Links:

RADIUS at wikipedia.org

How to Set Up a Radius Server on pfSense Using the FreeRadius Package on hubpages.com