The **captive portal** technique forces an [HTTP](http://en.wikipedia.org/wiki/HTTP) client on a network to see a special web page (usually for [authentication](http://en.wikipedia.org/wiki/Authentication) purposes) before using the [Internet](http://en.wikipedia.org/wiki/Internet) normally. A captive portal turns a [Web browser](http://en.wikipedia.org/wiki/Web_browser) into an authentication device. This is done by intercepting all [packets](http://en.wikipedia.org/wiki/Packet_(information_technology)), 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](http://en.wikipedia.org/wiki/Payment_gateway), or simply display an [acceptable use policy](http://en.wikipedia.org/wiki/Acceptable_use_policy) and require the user to agree. Captive portals are used at many [Wi-Fi](http://en.wikipedia.org/wiki/Wi-Fi) [hotspots](http://en.wikipedia.org/wiki/Hotspot_(Wi-Fi)), and can be used to control wired access (e.g. apartment houses, hotel rooms, business centers, "open" [Ethernet](http://en.wikipedia.org/wiki/Ethernet) jacks) as well.

Since the [login page](http://en.wikipedia.org/wiki/Logging_(computer_security)) itself must be presented to the client, either that login page is locally stored in the [gateway](http://en.wikipedia.org/wiki/Gateway_(computer_networking)), or the [web server](http://en.wikipedia.org/wiki/Web_server) hosting that page must be "[whitelisted](http://en.wikipedia.org/wiki/Whitelist)" via a [walled garden](http://en.wikipedia.org/wiki/Walled_garden_(media)) to bypass the authentication process. Depending on the feature set of the gateway, multiple web servers can be whitelisted (say for [iframes](http://en.wikipedia.org/wiki/Iframe) or [links](http://en.wikipedia.org/wiki/HTML_element#Links_and_anchors) within the login page). In addition to whitelisting the [URLs](http://en.wikipedia.org/wiki/Uniform_Resource_Locator) of web hosts, some gateways can whitelist [TCP ports](http://en.wikipedia.org/wiki/TCP_ports). The [MAC address](http://en.wikipedia.org/wiki/MAC_address) of attached clients can also be set to bypass the login process.

## Implementation

There is more than one way to implement a captive portal.

1. Redirection by HTTP: If an unauthenticated client requests a website, [DNS](http://en.wikipedia.org/wiki/Domain_name_system) is queried by the browser and the appropriate IP resolved as usual. The browser then sends an [HTTP](http://en.wikipedia.org/wiki/HTTP) request to that [IP address](http://en.wikipedia.org/wiki/IP_address). This request, however, is intercepted by a [firewall](http://en.wikipedia.org/wiki/Firewall_(computing)) (configured as a [transparent proxy](http://en.wikipedia.org/wiki/Proxy_server)) and forwarded to a redirect server. This redirect server responds with a regular HTTP response which contains [HTTP status code 302](http://en.wikipedia.org/wiki/List_of_HTTP_status_codes#3xx_Redirection) to redirect the client to the Captive Portal. To the client, this process is totally transparent. The client assumes that the website actually responded to the initial request and sent the redirect.
2. IP Redirect: Client traffic can also be redirected using IP redirect on the layer 3 level. This has the disadvantage that content served to the client does not match the URL.
3. Redirection by DNS: When a client requests a website, [DNS](http://en.wikipedia.org/wiki/Domain_name_system) is queried by the browser. The firewall will make sure that only the DNS server(s) provided by DHCP can be used by unauthenticated clients (or, alternatively, it will forward all DNS requests by unauthenticated clients to that DNS server). This DNS server will return the IP address of the Captive Portal page as a result of all DNS lookups.

In order to perform redirection by DNS the captive portal is using [DNS poisoning](http://en.wikipedia.org/wiki/DNS_poisoning) to perform a

## Limitations

Some of these implementations merely require users to pass an [SSL](http://en.wikipedia.org/wiki/Secure_Sockets_Layer) encrypted login page, after which their [IP](http://en.wikipedia.org/wiki/Internet_Protocol) and [MAC address](http://en.wikipedia.org/wiki/MAC_address) are allowed to pass through the [gateway](http://en.wikipedia.org/wiki/Gateway_(computer_networking)). This has been shown to be exploitable with a simple [packet sniffer](http://en.wikipedia.org/wiki/Packet_sniffer). Once the IP and MAC addresses of other connecting computers are found to be authenticated, any machine can spoof the MAC address and IP of the authenticated target, and be allowed a route through the gateway. For this reason some captive portal solutions created extended authentication mechanisms to limit the risk for usurpation.

Captive portals require the use of a browser; this is usually the first application that users start, but users who first use an email client or other will find the connection not working without explanation, and will need to open a browser to validate. A similar problem can occur if the client joins the network with pages already loaded into its browser, causing undefined behavior when such a page tries HTTP requests to its origin server.

Platforms that have [Wi-Fi](http://en.wikipedia.org/wiki/Wi-Fi) and a [TCP/IP stack](http://en.wikipedia.org/wiki/TCP/IP_stack) but do not have a web browser that supports [HTTPS](http://en.wikipedia.org/wiki/HTTPS) cannot use many captive portals. Such platforms include the [Nintendo DS](http://en.wikipedia.org/wiki/Nintendo_DS) running a game that uses [Nintendo Wi-Fi Connection](http://en.wikipedia.org/wiki/Nintendo_Wi-Fi_Connection). Non browser authentication is possible using [WISPr](http://en.wikipedia.org/wiki/WISPr), an [XML](http://en.wikipedia.org/wiki/XML)-based authentication protocol for this purpose, or MAC-based authentication or authentications based on other protocols.

There also exists the option of the platform vendor entering into a service contract with the operator of a large number of captive portal hotspots to allow free or discounted access to the platform vendor's servers via the hotspot's [walled garden](http://en.wikipedia.org/wiki/Walled_garden_(media)), such as the deal between Nintendo and [Wayport](http://en.wikipedia.org/wiki/Wayport,_Inc.)[[*citation needed*](http://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]. For example, [VoIP](http://en.wikipedia.org/wiki/Voice_over_IP) [SIP](http://en.wikipedia.org/wiki/Session_Initiation_Protocol) ports could be allowed to bypass the gateway to allow phones to work.

# Captive Portal Troubleshooting

### From PFSenseDocs

Jump to: [navigation](http://doc.pfsense.org/index.php/Captive_Portal_Troubleshooting#column-one), [search](http://doc.pfsense.org/index.php/Captive_Portal_Troubleshooting#searchInput)

The best source of captive portal troubleshooting information can be found in the [pfSense book](http://pfsense.org/book).

|  |
| --- |
| Contents  * [1 Captive portal not redirecting](http://doc.pfsense.org/index.php/Captive_Portal_Troubleshooting#Captive_portal_not_redirecting) * [2 500 Server Errors with Captive Portal + RADIUS](http://doc.pfsense.org/index.php/Captive_Portal_Troubleshooting#500_Server_Errors_with_Captive_Portal_.2B_RADIUS) * [3 Captive Portal Rule Generation](http://doc.pfsense.org/index.php/Captive_Portal_Troubleshooting#Captive_Portal_Rule_Generation) * [4 IPFW tables](http://doc.pfsense.org/index.php/Captive_Portal_Troubleshooting#IPFW_tables) * [5 Sysctl's](http://doc.pfsense.org/index.php/Captive_Portal_Troubleshooting#Sysctl.27s)   + [5.1 net.inet.ip.fastforwarding](http://doc.pfsense.org/index.php/Captive_Portal_Troubleshooting#net.inet.ip.fastforwarding) |

### Captive portal not redirecting

If your clients are not being redirected to the portal page when attempting to browse on an interface with captive portal enabled, it's most always one of the following causes.

1. DNS resolution not functioning - the clients on the captive portal interface must either be using the DNS forwarder on pfSense, on the IP of the interface where the client resides (which is the default configuration), or if using some other IP for DNS, it must be an allowed IP entry. If DNS fails, the browser never issues the HTTP request, hence it cannot be intercepted and redirected.
2. Firewall rules on the captive portal interface do not allow the initial HTTP request - if the user is trying to browse to google.com, but you're not allowing HTTP to google.com, the HTTP request will be blocked and hence cannot be redirected. Under Firewall>Rules, on the interface where captive portal is enabled, you must be allowing the traffic that you want to be redirected (most commonly HTTP to any destination).

### 500 Server Errors with Captive Portal + RADIUS

As suggested in [this forum thread](http://forum.pfsense.org/index.php/topic,14417.0.html), this is likely due to the RADIUS server not responding. It may not be running, or it may be overloaded.

You might also check the contents of /var/log/lighttpd.error.log just after receiving the error for more clues.

### Captive Portal Rule Generation

Examine the captiveportal\_init\_rules function in [/etc/inc/captiveportal.inc](https://github.com/bsdperimeter/pfsense/blob/master/etc/inc/captiveportal.inc) to see how the initial rules are generated using ipfw.

### IPFW tables

Show all tables

ipfw table all list

Table 1 holds authenticated/allowed clients. Allows traffic from clients to enter the interface.

ipfw table 1 list

Table 2 holds authenticated/allowed clients. Allows traffic to clients to leave the interface.

ipfw table 2 list

See captiveportal.inc for a look at what the other tables are used for.

### Sysctl's

Some Sysctl options can cause problems with the Captive Portal. Sysctl options can be set via the System -> Advanced -> System Tunables tab.

#### net.inet.ip.fastforwarding

If fastforwarding is enabled ( set to 1) it can cause problems with the initial redirection to the captive portal login page. Set it to "0" to disable this option.

Retrieved from "<http://doc.pfsense.org/index.php?title=Captive_Portal_Troubleshooting&oldid=4110>"

[Categories](http://doc.pfsense.org/index.php/Special:Categories):

* [Captive Portal](http://doc.pfsense.org/index.php/Category:Captive_Portal)
* [Troubleshooting](http://doc.pfsense.org/index.php/Category:Troubleshooting)