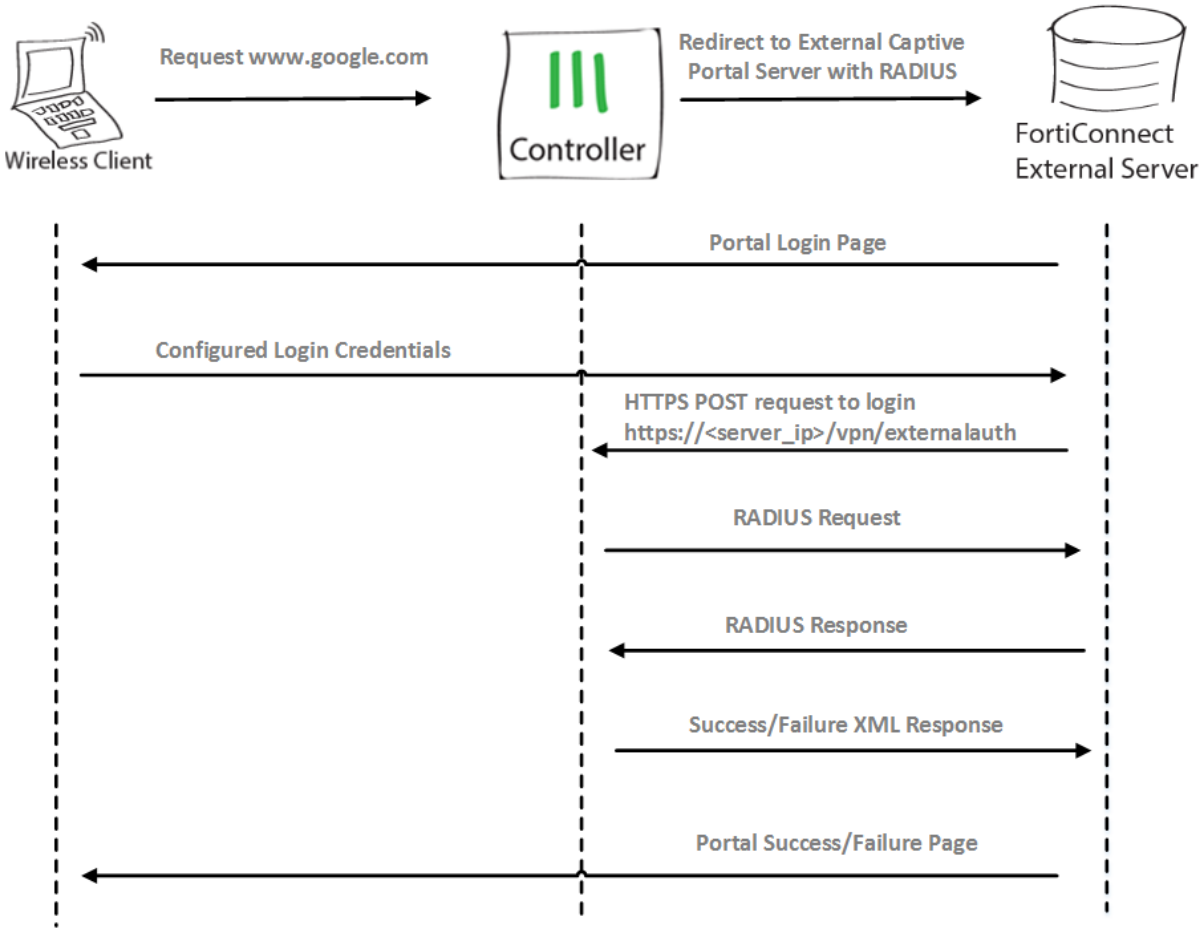
THE FORTINET COOKBOOK

FortiWLC External Captive Portal

FORTINET

Contents

The FortiWLC integrates with several external captive portal solutions like FortiConnect , FortiAuthenticator, and Aruba Clear Pass. The underlying HTTP/HTTPS client redirection mechanism to send unauthenticated traffic to receive the captive portal login page differs with each solution.
This document describes an example to configure the FortiWLC external captive portal solution using FortiConnect as the external server. Any third party captive portal solution can be integrated with FortiWLC following this example.
For more information on integrating Aruba Clear Pass with FortiWLC, see the *FortiWLC-ClearPass Integration* cookbook.



The controller redirects with GET/POST requests to the configured URL along with following parameters.

POST Variable	Description
Server_IP	The controller's IP address.
Login_url	The login URL format is **https://<server_ip>/vpn/externalauth** OR **https://<server_ip>/vpn/externalapauth** in the bridge mode.
Original_url	The original URL requested by the controller.
ssid	The SSID to which the wireless station is connected.
station_mac	The MAC address of the wireless client.
station_ip	The IP address of the wireless client.

The external captive portal server provides the login page to the client after receiving the redirect. After the client enters the login credentials, the external captive portal server sends an HTTPS POST to the controller and passes the following credentials.

POST Variable	Description
POST url	The login URL format is **https://<server_ip>/vpn/externalauth** OR **https://<server_ip>/vpn/externalapauth** in the bridge mode.
userid	The user name provided by the client.
password	The password provided by the client.
station_mac	The MAC address of the wireless client.
station_ip	The IP address of the wireless client.

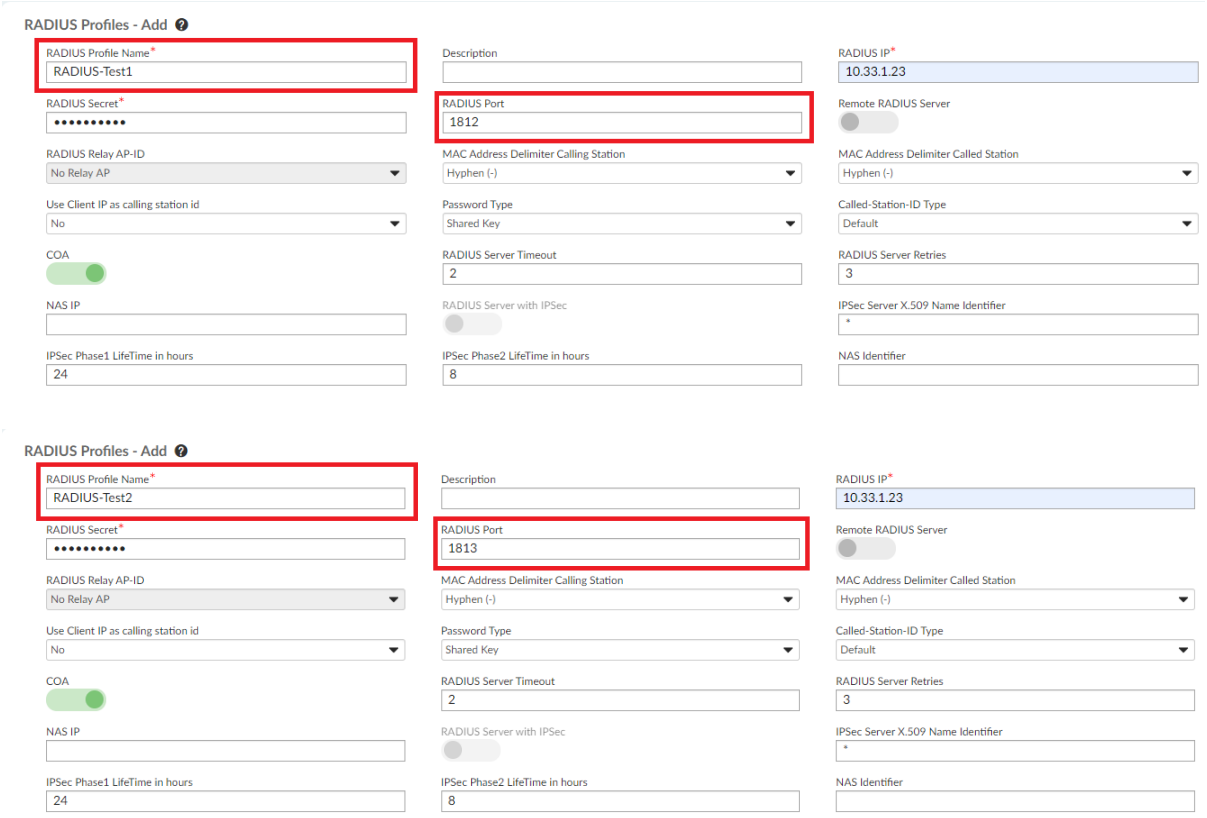
The controller then sends a RADIUS authentication request to the external captive portal server (if it handles RADIUS) or any other configured RADIUS server. The RADIUS authentication result is sent to the external captive portal server as an XML response. The following is an example.

#<HTTParty::Response:0x7fb96ee07660 @parsed_response={"external_web_auth"=>{"status"=>"success"}}, @response=#<Net::HTTPOK 200 OK readbody=true>, @headers={"content-type"=>["application/xml; charset=\"UTF-8\""], "connection"=>["close"], "server"=>["Apache"], "date"=>["Thu, 19 Jun 2014 19:32:41 GMT"], "content-length"=>["101"]}>

Based on the response, the external captive portal server provides the login success/failure page to the client. If the client authentication is successful, the external captive portal server optionally redirects the client to the original URL or a pre-defined URL, and the controller allows all traffic from that client.

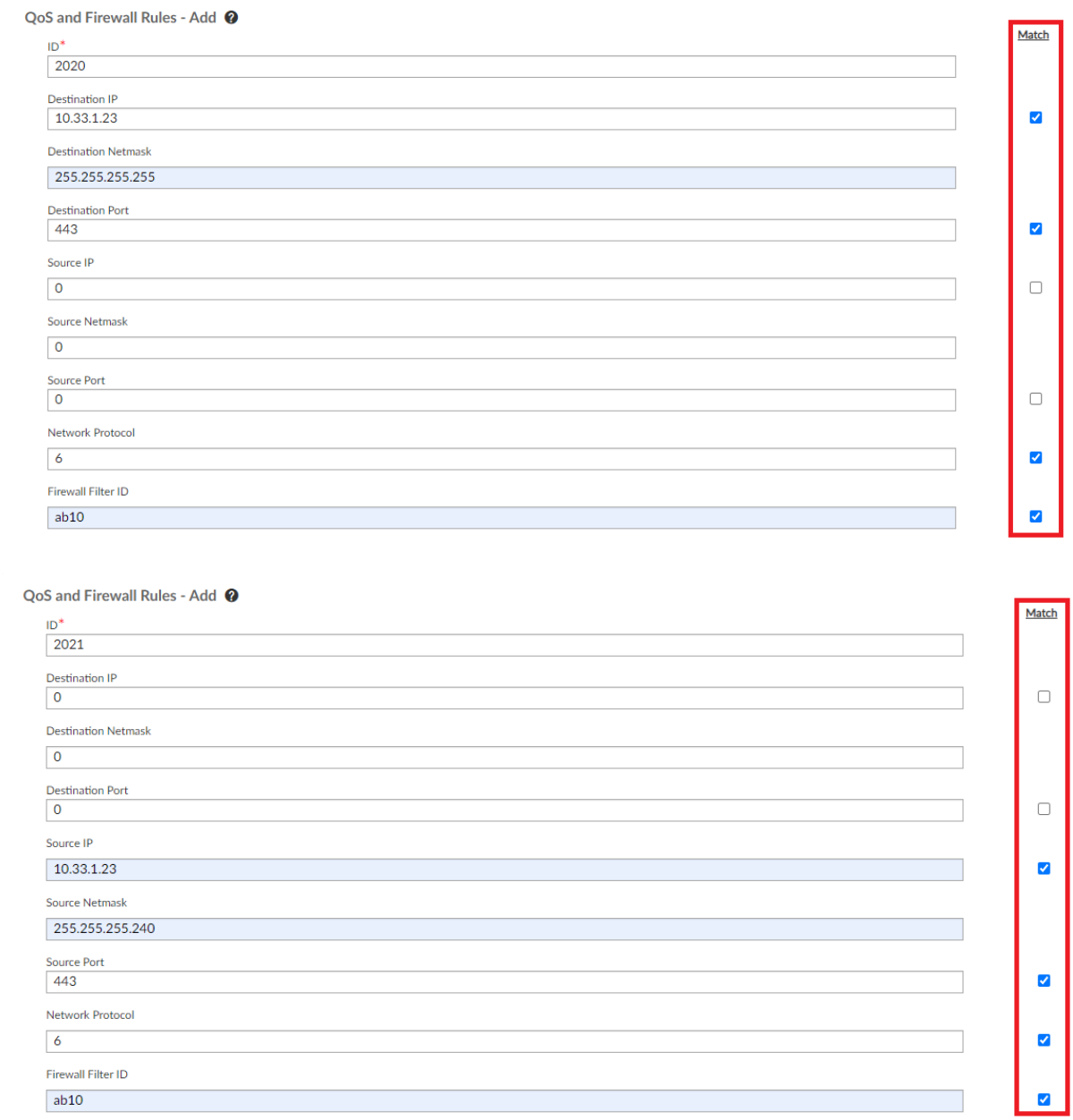
Configuring a RADIUS Profile

Navigate to **Configuration > Security > RADIUS** and create a RADIUS profile each for authentication and accounting.



Configuring QoS Settings

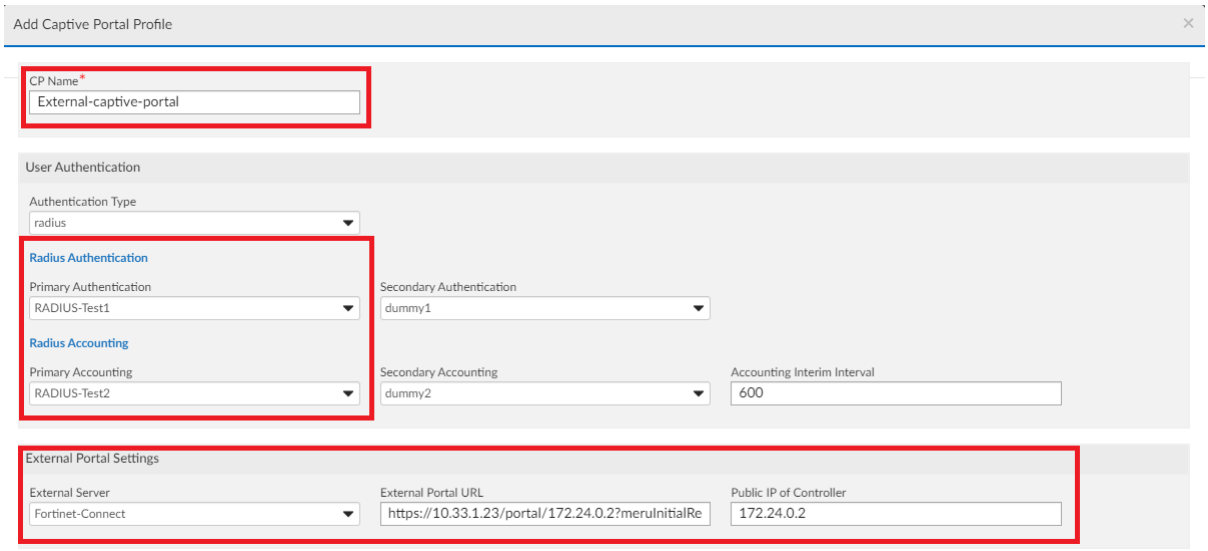
Navigate to **Configuration > Policies > QoS > QoS and Firewall Rules** and configure the QoS and Firewall rules to allow pre-authentication traffic to the external captive portal server.
Ensure that the **Match** option is enabled for the configured fields.


QoS and Firewall Rules - Add
ID*
2020
Destination IP
10.33.1.23
Destination Netmask
255.255.255.255
Destination Port
443
Source IP
0
Source Netmask
0
Source Port
0
Network Protocol
6
Firewall Filter ID
ab10
Match
QoS and Firewall Rules - Add
ID*
2021
Destination IP
0
Destination Netmask
0
Destination Port
0
Source IP
10.33.1.23
Source Netmask
255.255.255.240
Source Port
443
Network Protocol
6
Firewall Filter ID
ab10
Match

Configuring Captive Portal Profile

Navigate to **Configuration > Security > Captive Portal** to specify the captive portal profile settings.

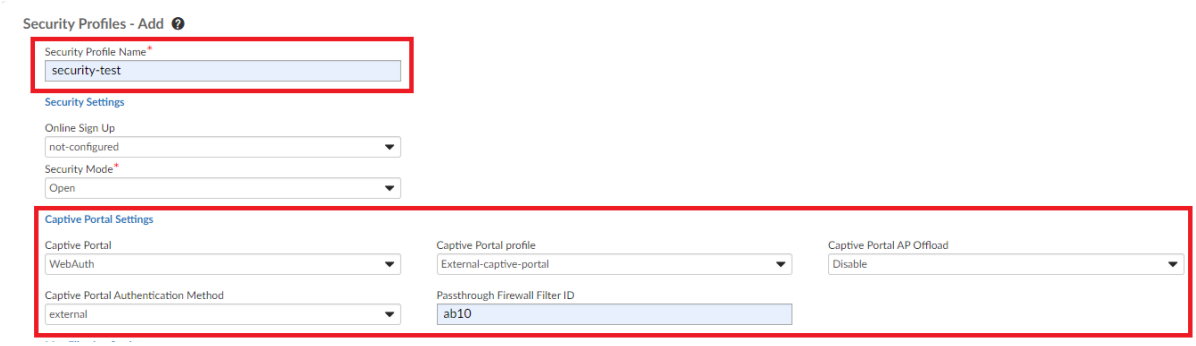
The following screen-shots illustrate the process to create and assign a captive profile with FortiConnect as the external server.



Note:
The format of the external portal URL for FortiConnect is *https://<External-CP domain name>/portal/<controllerPublicIPaddress>?meruInitialRedirect*
Configure the portal URL accordingly when using a third-party external server.

Enabling Captive Portal in the Security Profile

The captive portal profile must be enabled in the security profile.



Note: In the **Passthrough Firewall Filter ID**, enter a firewall filter ID that was created using **Configuration > Qos > System Settings > QoS and Firewall Rules**.

Configuring ESS Profile

Navigate to **Configure > Wireless > ESS** to create an ESS profile and add the captive portal enabled security profile.