pfSense Version 2.4.5 Open VPN Configuration Guide

Contents

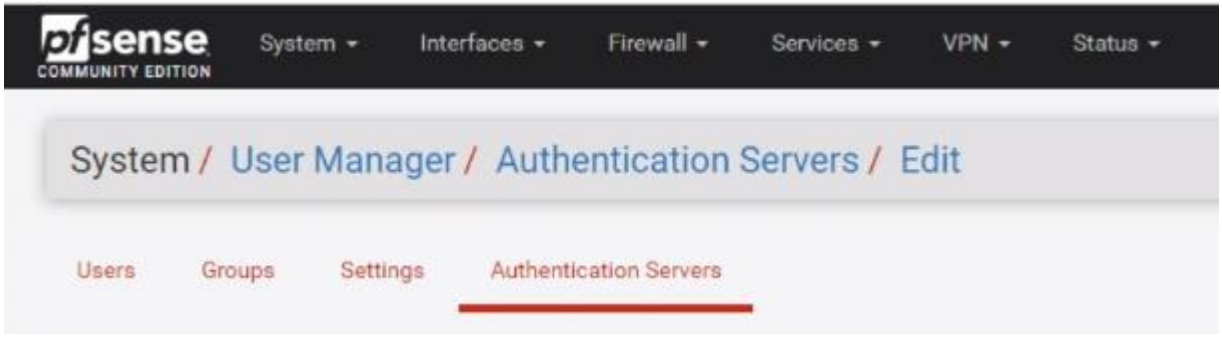
Configuring a pfSense running version 2.4.5 for SSL VPN.

This document outlines how to configure a pfSense for MFA protection with Censornet MFA.

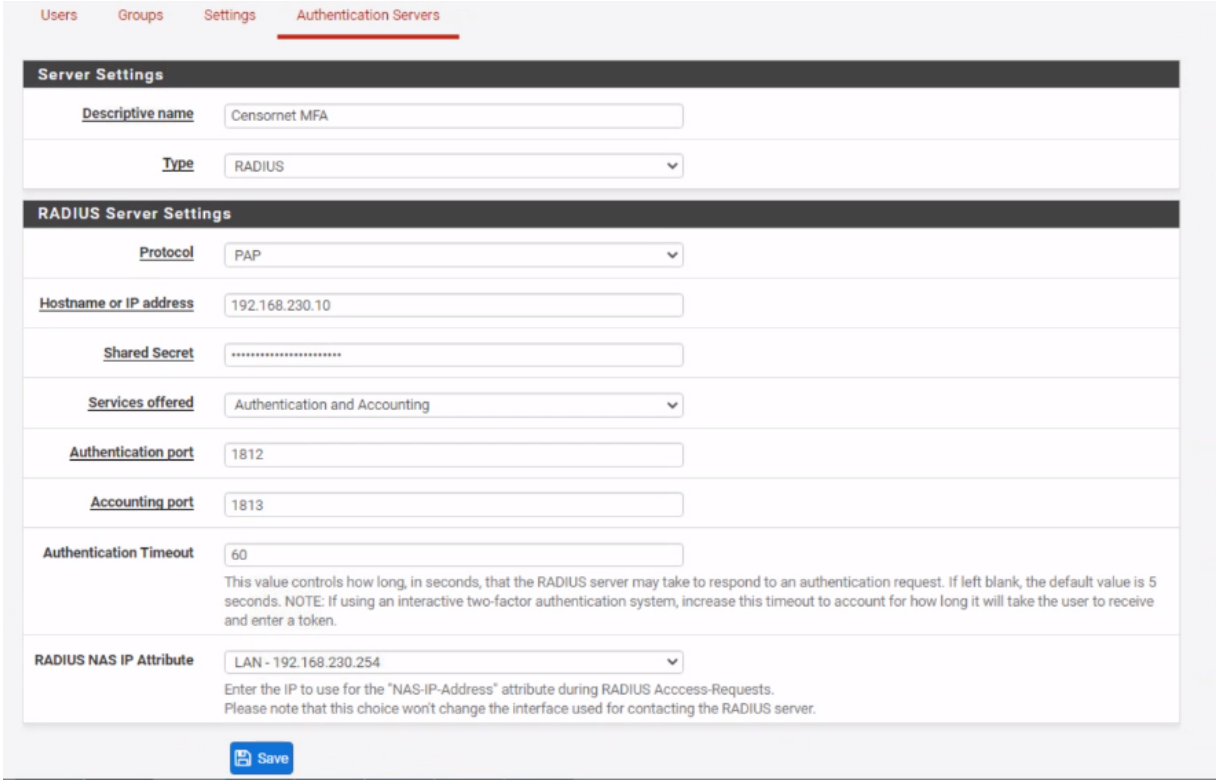
To complete the setup, it is required that you have a pfSense VPN product, a Microsoft radius server (NPS), and an installation of the Censornet MFA Authentication Client Software powered by SMS PASSCODE. Please refer to the Censornet support site for further guidance to install the Censornet MFA Authentication Client Software.

The Radius Server.

To configure the pfSense with the Censornet MFA protected radius server, navigate to System, User manager, Authentication Servers.



On the screen select the Add button



Descriptive name: Choose a friendly name.

Type: RADIUS

Protocol: PAP

Hostname or IP address: the name or IP address of the Censornet MFA protected radius server

Server Secret: The same shared secret that you have entered in the radius server's radius client.

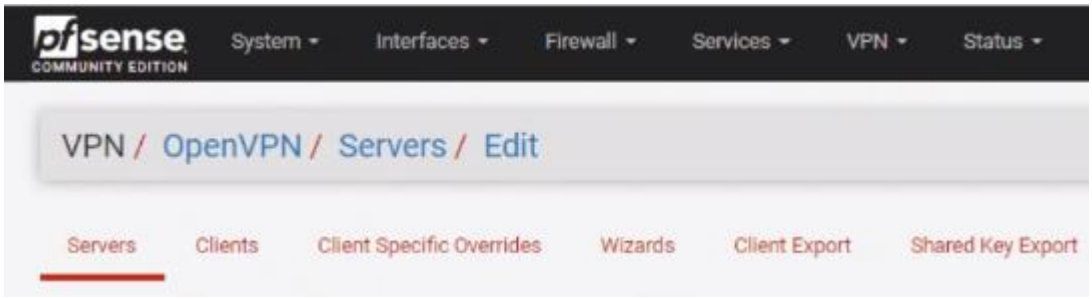
Authentication port: 1812

Authentication Timeout: 60

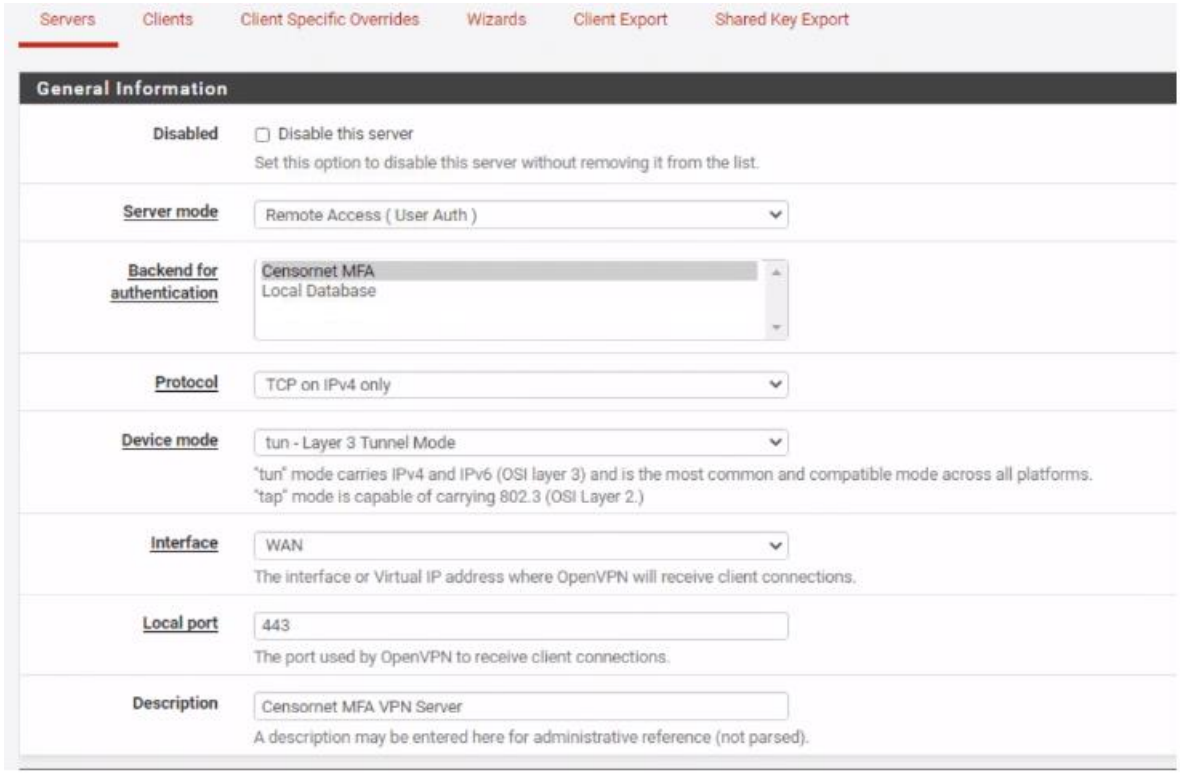
RADIUS NAS IP Attribute: Select the LAN interface.

OpenVPN Setup

Navigate to VPN, OpenVPN, Servers add a new VPN server or edit an existing one.



Change the Server mode to "Remote Access (User Auth), Under the section Backend for authentication, Select the newly created Censornet MFA radius server.



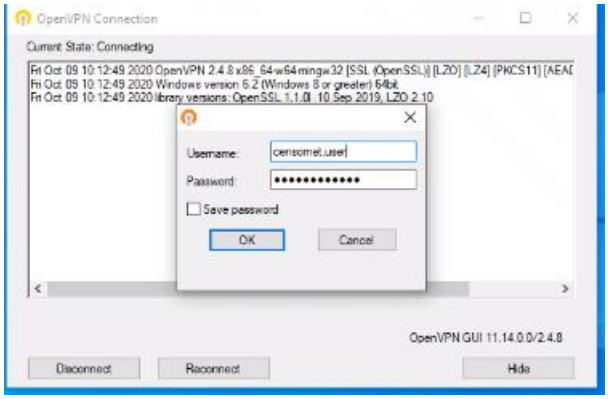
By default, pfSense renegotiates the VPN connection every 3600 (1 hour) which means users will need to re-authenticate with MFA.

To change this time out, go to the Advanced Configuration, Custom options and use the "reneg-sec" command to the required time, this example of 43200 is 12 hours.

Complete the setup of your pfSense by configuring the required policy that allows traffic from the SSL VPN interface to the internal Lan, for further assistance please refer to your pfSense documentation.

User Experience

At the time of release, the OpenVPN client does not fully support challenge-response. When a user connects to the pfSense VPN, they will enter their Active Directory Username and Password.



The OpenVPN will provide a ”soft.auth-failure” leave the username the same but now enter the OTP, and your authentication request will be successful.