pfSense 2.6.0 (OpenVPN Setup)

in pfSense

Published: Aug 17, 2022|Last updated: Aug 18, 2022
This tutorial will walk you through configuring a router using pfSense firmware version 2.6.0.

Before starting, be sure you have downloaded the connection location you would like to use for your connection. For this guide specifically, we have used California, and the associated certificate from the collection labeled **Default**, be sure to decompress the file so you can access the contents.

* Default

* Strong

* Static IP

* TCP

* Strong TCP

Also, decide what DNS servers fit your needs, there are four options:

* 10.0.0.241 — this can provide access to all three of the following

* 10.0.0.242 — DNS only

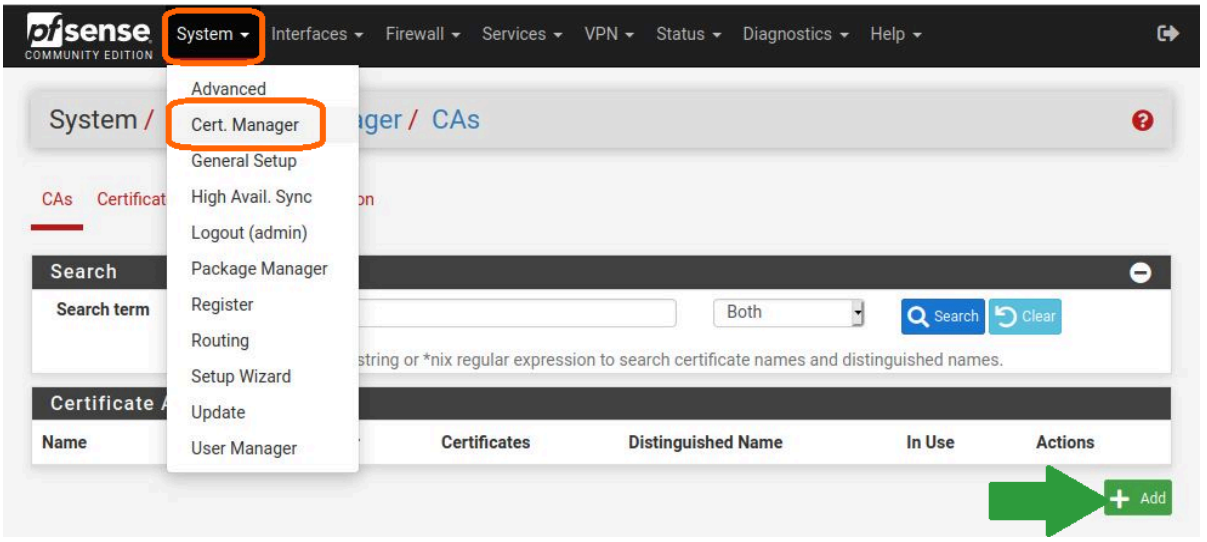
* 10.0.0.243 — forwards streaming domains to the parent proxy for potential access to some streaming services

* 10.0.0.244 — MACE

Step 1. System - Certificate Manager : this interface will allow you to add the security certificate required for the VPN connection. Click on the **System** button on the top bar,

then click on **Cert. Manager** from the dropdown (highlighted in orange in the image below).

1. Click the **Add+** button to create a new certificate entry.

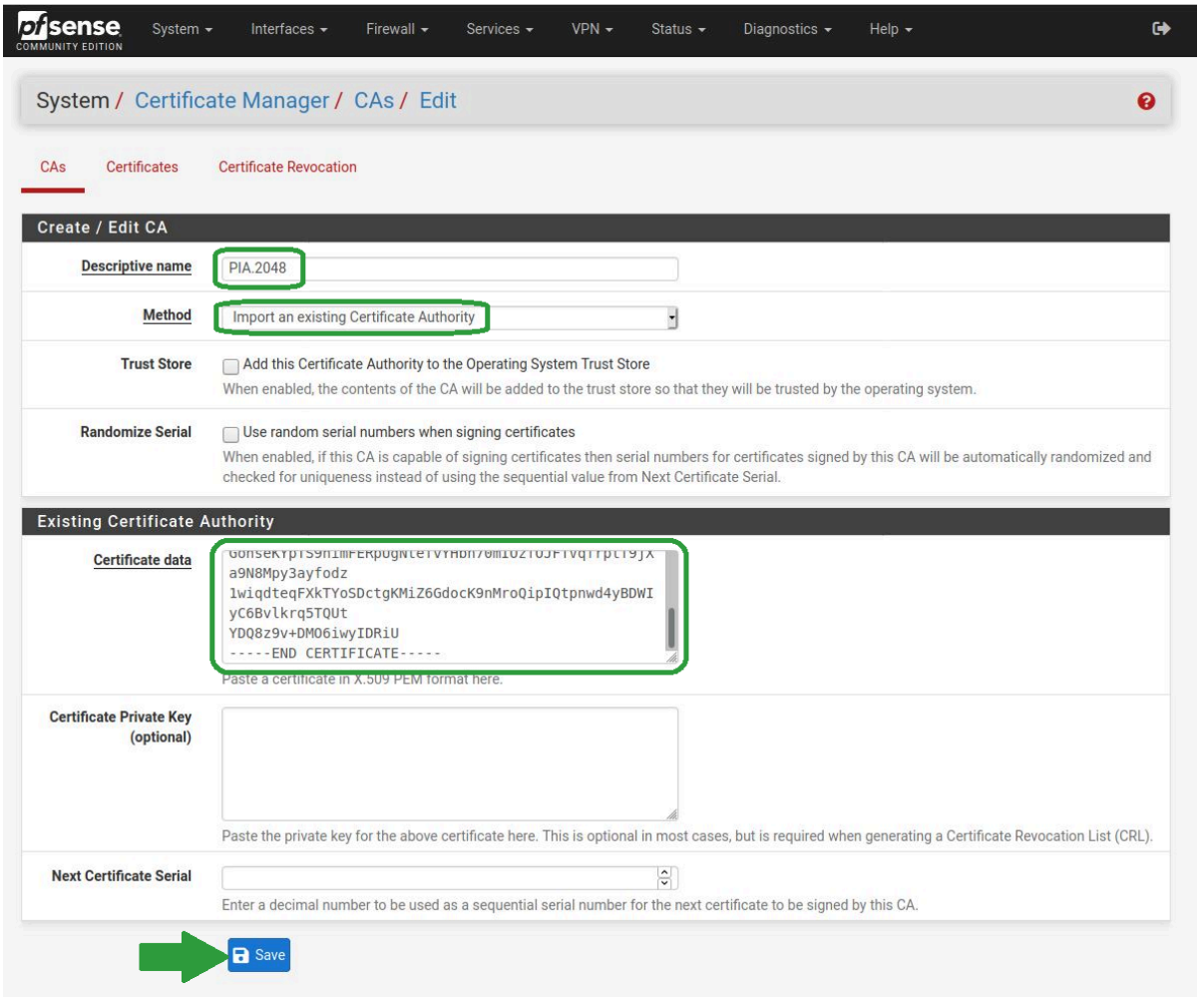


2. Set the **Descriptive name** to something that will be easy to identify, we have used ***PIA.2048***

3. From the **Method** dropdown, select **Import an existing Certificate Authority**

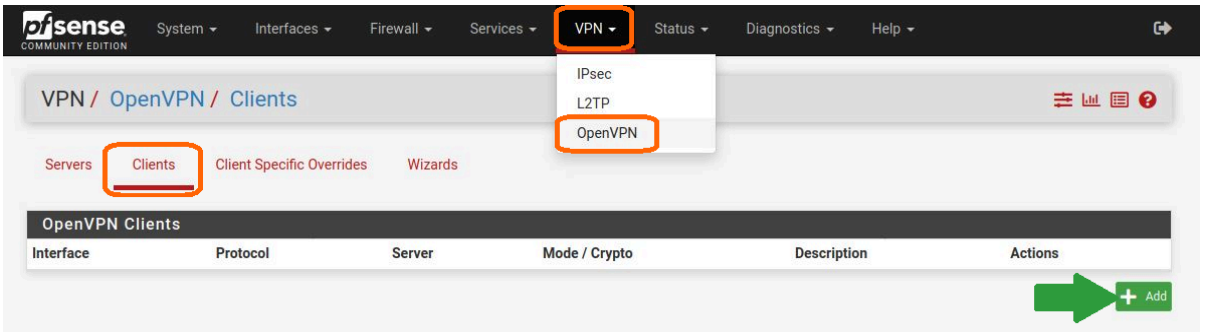
4. You will need to copy the contents of the security certificate specific to the encryption settings you are using, which is provided in the file you downloaded before starting. Open the certificate in a text editor and copy the contents into the **Certificate data** field. (Note : The contents of this must include the *begin* and *end* certificate lines as well, be sure to copy the whole thing.)

5. Click **Save**.



Step 2. VPN - OpenVPN - Clients : this interface will allow you to input all configuration details required for the OpenVPN connection. Navigate to **VPN** in the top navigation bar, click on **OpenVPN** and in the interface that appears, select **Clients** from the options shown (these are all highlighted orange in the image below.)

1. Click **Add+** to create a new VPN Client configuration.

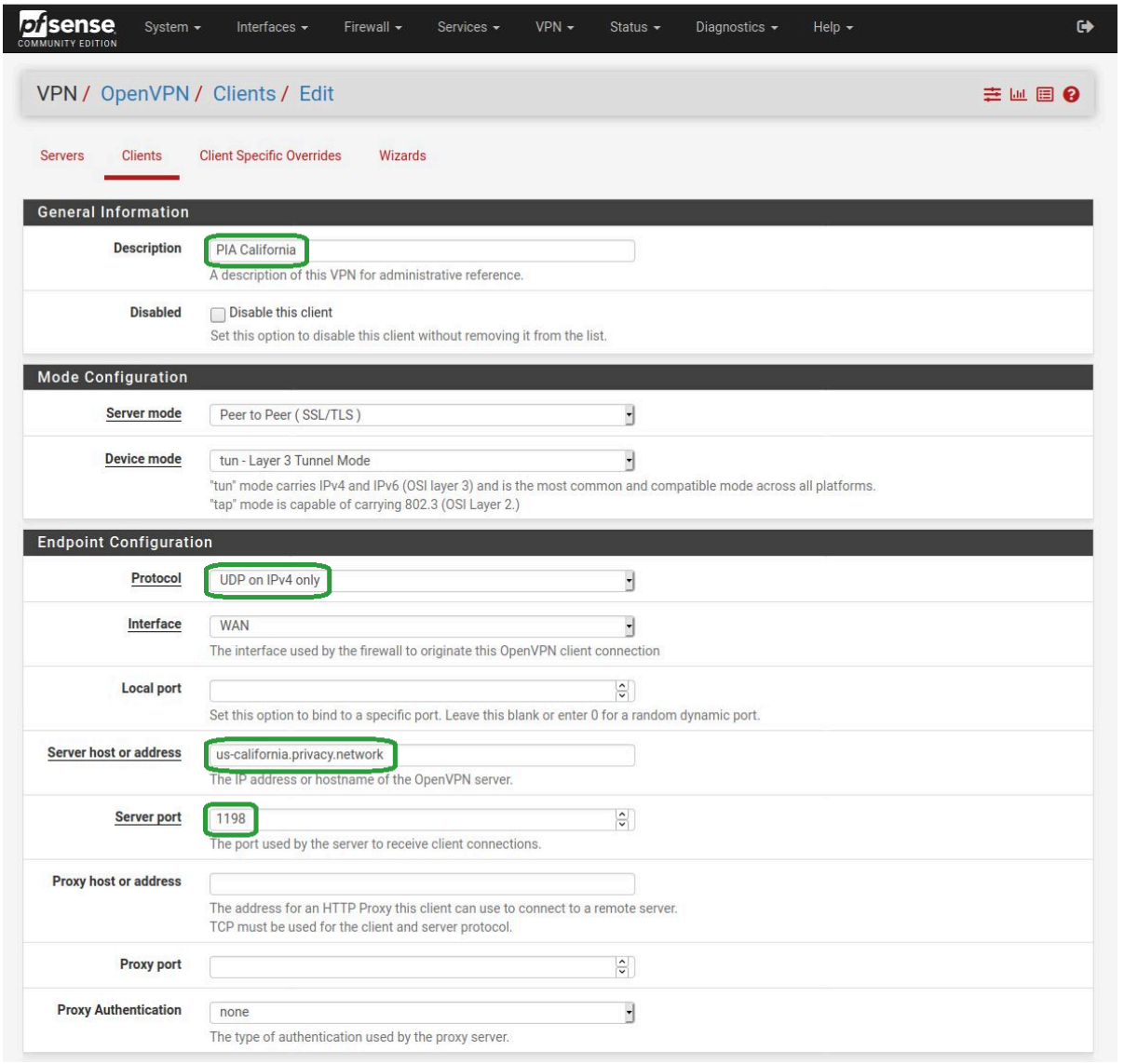


2. The **Description** allows you to specify an identifying name for this VPN configuration.

3. Set the **Protocol** you want to use for your connection, you will select **UDP on IPv4 only** or **TCP on IPv4 only**. The decision will be based upon the settings you want to use from your file selecction beginning of this guide. (Note: there are many settings available here, only the ones that need to be changed from default values are mentioned. If you are experiencing issues, be sure the unmentioned settings match the screenshot provided in this guide.)

4. **Server host or address** is where you will input the PIA server that you would like to connect to, the server locations available for the generation of servers you are connecting to is available in the collection you downloaded at the start. The information you are looking for is found on the fourth line of the OpenVPN configuration file; in this case "remote **us-california.privacy.network** *1198*". The text "us-california.privacy.network" is the input for the server address, and "1198" is the input for the server port in the next step.

5. For the **Server port** setting you will input the required port for the chosen configuration — 1198 from the step above.



6. In the **Username** field, input your PIA username — that is always in the format of p1234567 and cannot be replaced with any other information.

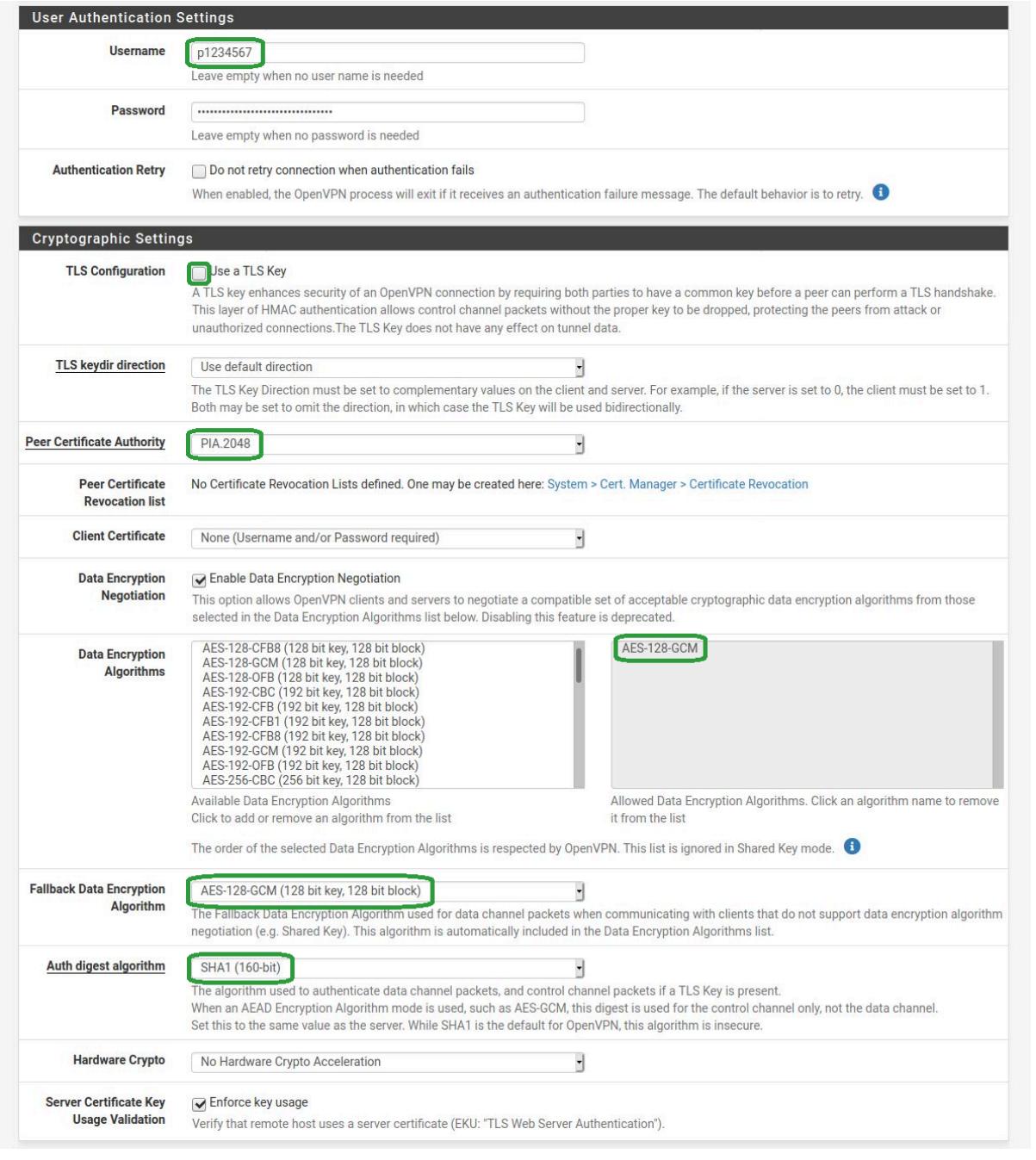
7. The Password field requires the input of the password for your PIA account, which is assigned to you, but you have the ability to customize in the client control panel. The interface will require that you input this password twice as attempted error prevention.

8. The checkbox for **Use a TLS key** will be checked by default **uncheck** this.

9. From the dropdown for **Peer Certificate Authority** select the **Descriptive name** for the security certificate you created in **Step 2**.

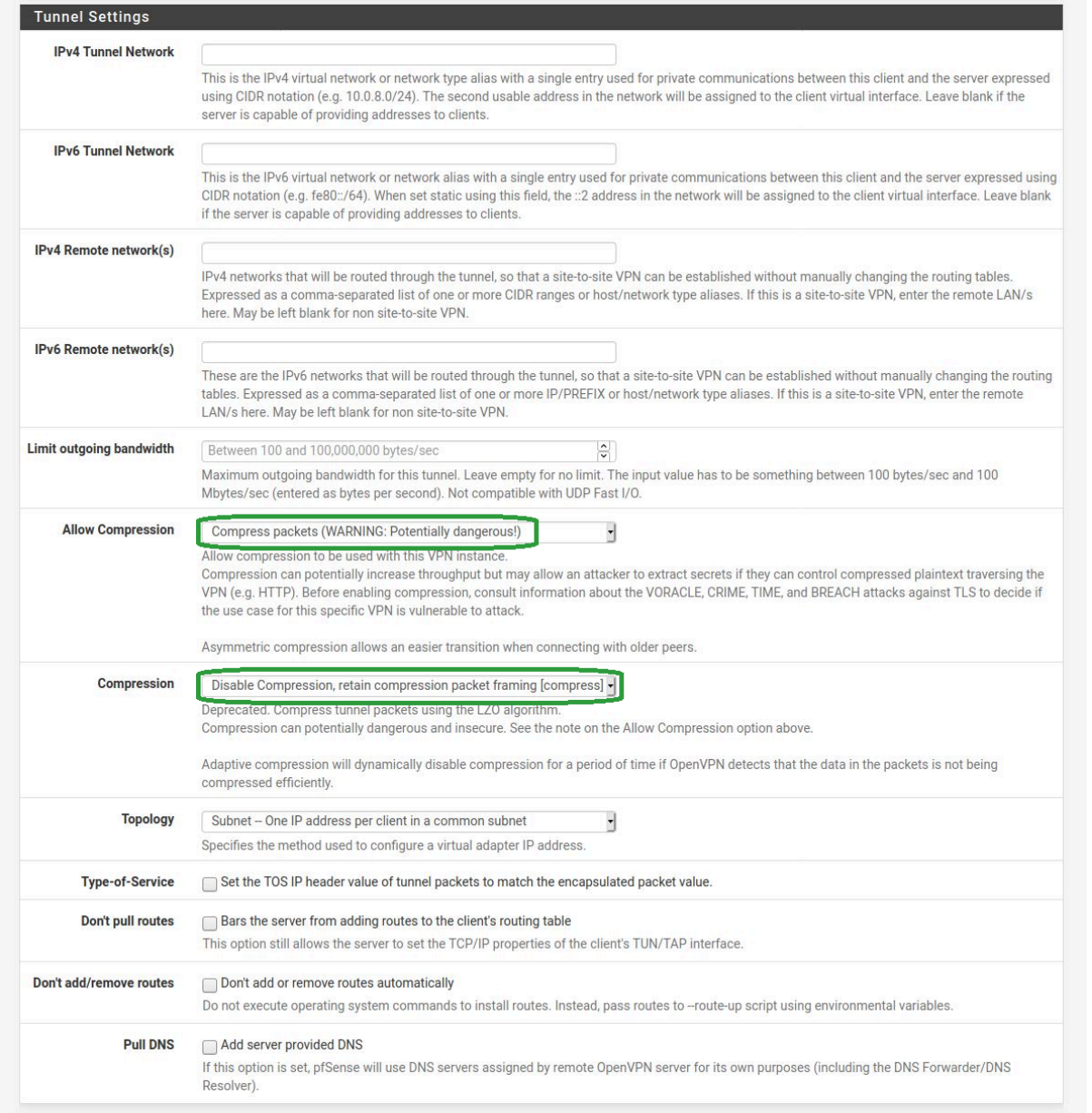
10. For **Encryption Algorithm** select the option appropriate to your configuration. In general, we suggest using GCM over CBC.

11. For **Auth digest algorithm** select the option appropriate to your configuration, shown in the *Dependenices Table*.



12. Set the **Allow Compression** dropdown to **Compress Packets**.

13. Set **Compression** to **Disable Compression, retain compression packet framing**.



14. The **Custom options** section will require multiple specific lines of text; copy and paste the following into this field:

```
persist-key

persist-tun

remote-cert-tls server

reneg-sec 0

auth-retry interact
```

```
dhcp-option DNS 10.0.0.241

dhcp-option DNS 10.0.0.243
copy
```

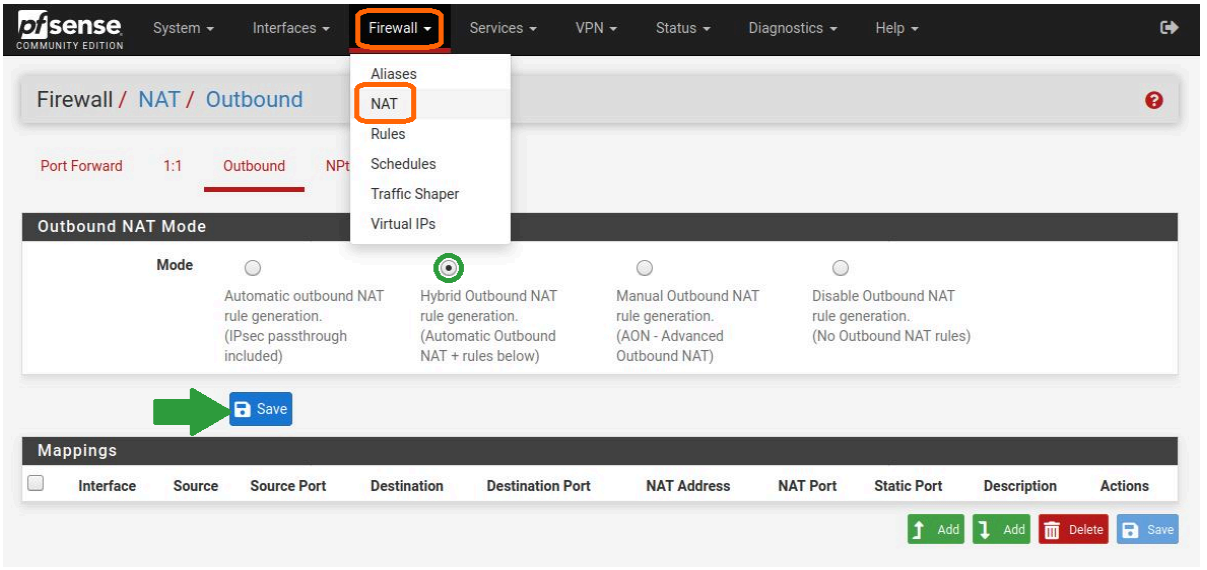
14. For the **Gateway Creation** setting, select the radio button for **IPv4 only**.

15. Click **Save**.

Step 3. Firewall — NAT — Outbound : this interface will allow you to manually create the outbound NAT rules to utilize the OpenVPN configuration you have created. Click on **Firewall**From the top navigation bar, select **NAT** from the options that appear, and on the page that loads, select **Outbound** from the options at the top; all those items are highlighted in orange in the image below.

1. Click the radio button for **Hybrid Outbound Rule Generation**.

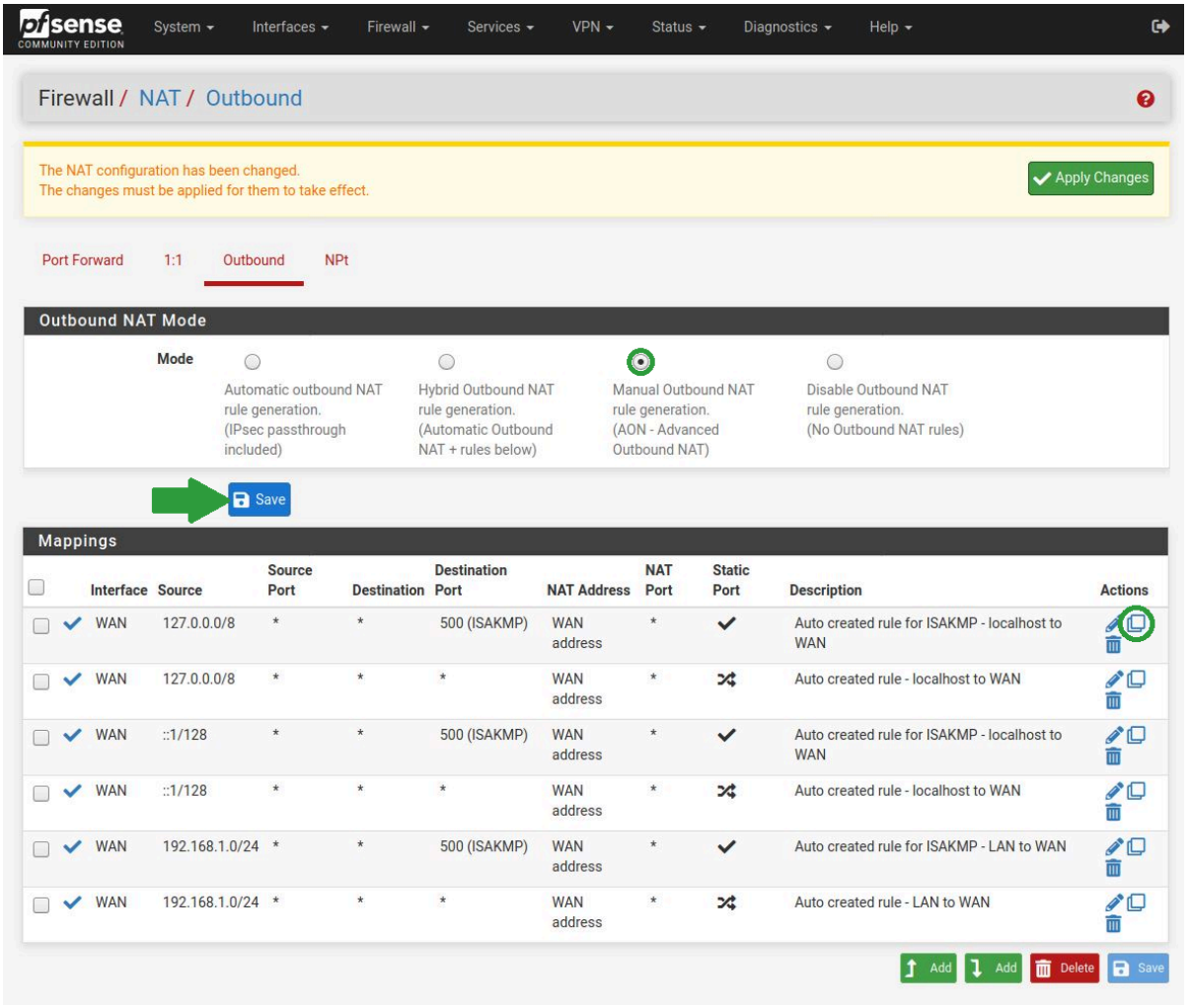
2. Click **Save**. (This will auto-generate rules we need to expand upon).



3. Click the radio button for **Manual Outbound Rule Generation**.

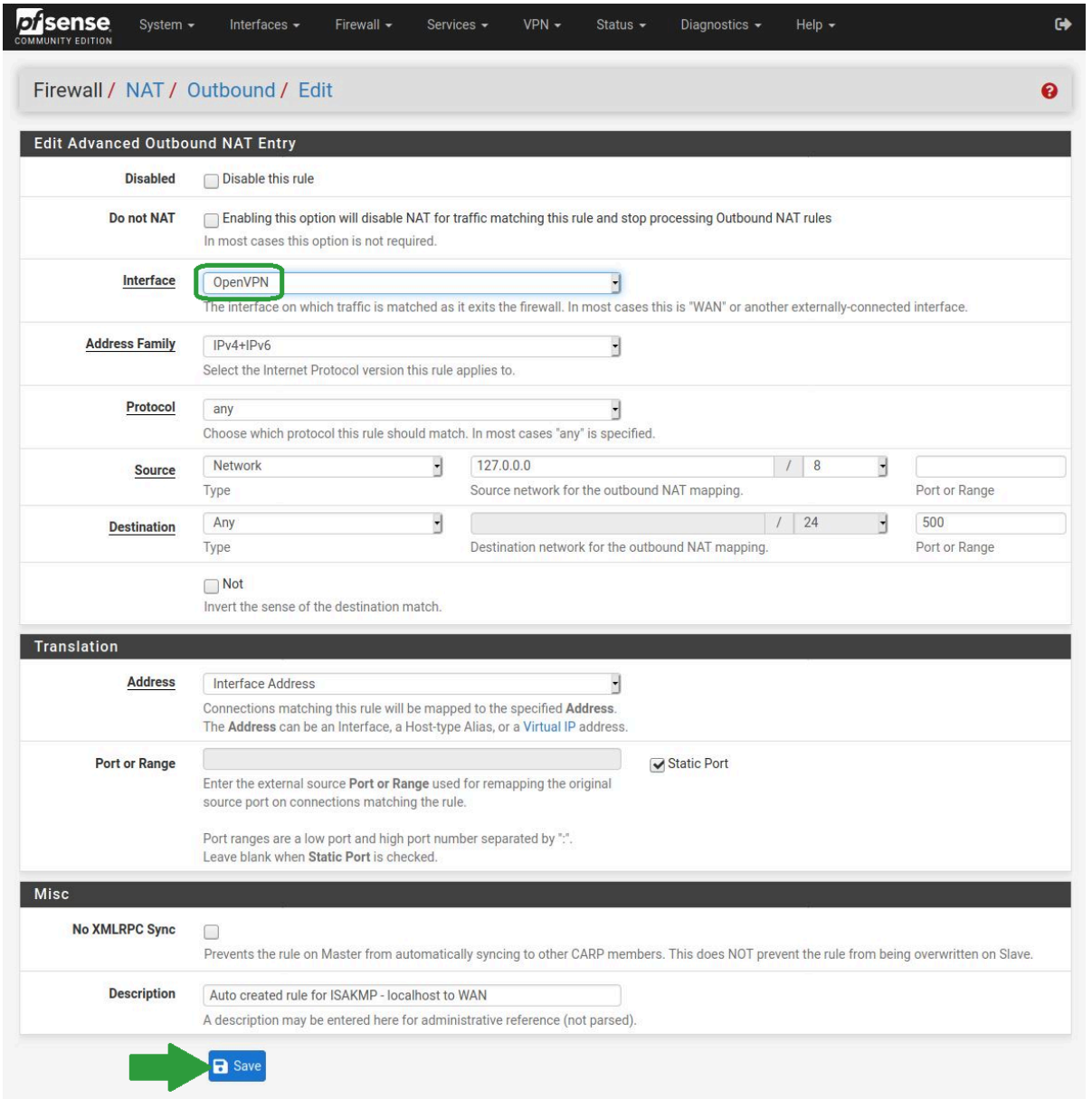
4. Click **Save**.

5. You will need to duplicate each of the interfaces that are present by default, the first step to this is clicking on the **Add a new mapping based on this one** button in the **Actions** column.



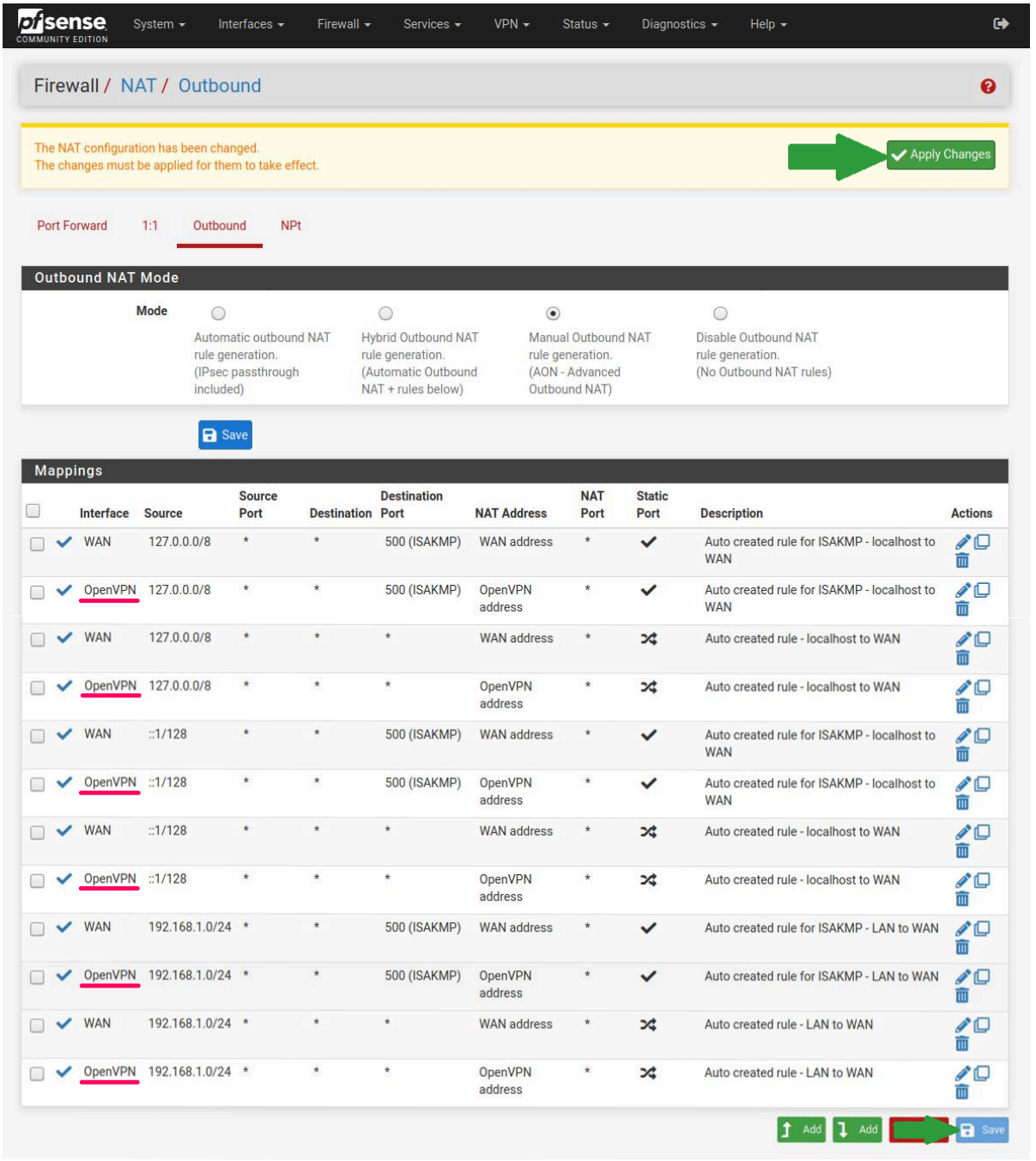
6. Change the **Interface** this new connection is using to **OpenVPN**.

7. Click **Save**.

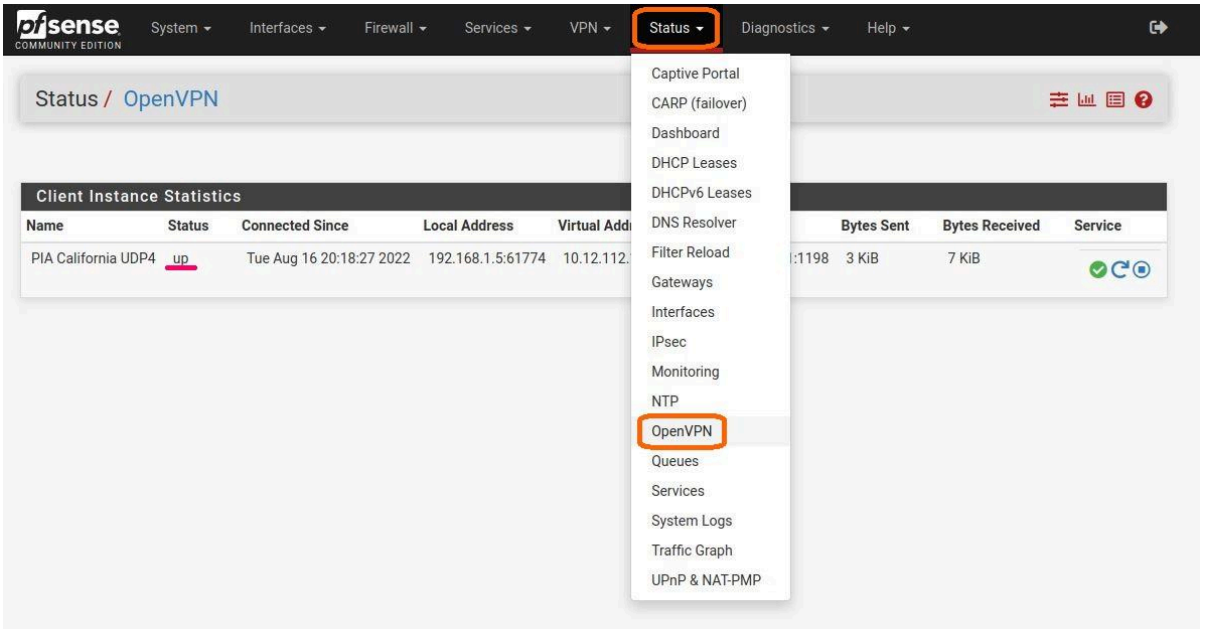


7. **Repeat the previous three actions (3.5, 3.6, and 3.7) for each of the six connections.** Once all interfaces have been duplicated and set to use OpenVPN, click **Save**

8. Click **Apply Changes** in the top right to initiate use of the new setup.



You have successfully completed the OpenVPN setup for pfSense. You can confirm the status of your connection in the **Status - OpenVPN** interface. If you find that you are not connected initially, restarting the router may be necessary for all your settings to be properly invoked.


pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Status / OpenVPN
Client Instance Statistics
Name
Status
Connected Since
Local Address
Virtual Addr
Bytes Sent
Bytes Received
Service
PIA California UDP4
up
Tue Aug 16 20:18:27 2022
192.168.1.5:61774
10.12.112.
:1198
3 KiB
7 KiB
Captive Portal
CARP (failover)
Dashboard
DHCP Leases
DHCPv6 Leases
DNS Resolver
Filter Reload
Gateways
Interfaces
IPsec
Monitoring
NTP
OpenVPN
Queues
Services
System Logs
Traffic Graph
UPnP & NAT-PMP