

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

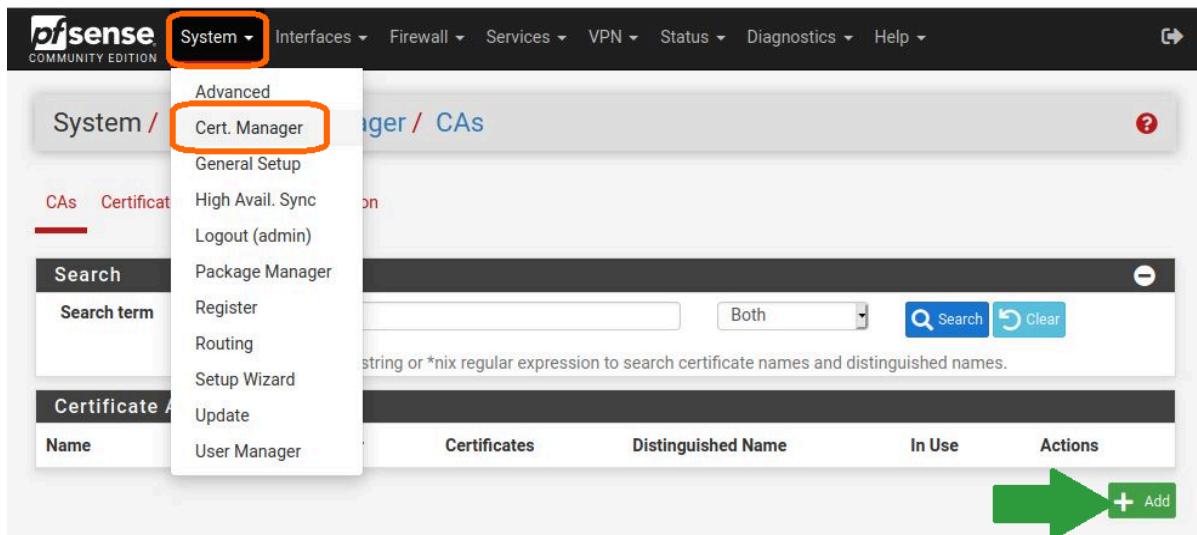
* 10.0.0.243 — forwards streaming domains to the parent proxy for potential access to some streaming services

* 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**.

Create / Edit CA

Descriptive name: PIA.2048

Method: Import an existing Certificate Authority

Trust Store: Add this Certificate Authority to the Operating System Trust Store
When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

Randomize Serial: Use random serial numbers when signing certificates
When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Existing Certificate Authority

Certificate data:

```
-----BEGIN CERTIFICATE-----
MIIEvDCCA3QwDQYJKoZIhvcNAQEBBQADggEAM98Mpy3ayfod2
1wiqteqFkTYoSDctgKMIZ6GdocK9nMroQipIQtpnw4yBDW
yc6Bvlkrq5TQut
YDQ8z9v+DM06iwyIDRiu
-----END CERTIFICATE-----
```

Paste a certificate in X.509 PEM format here.

Certificate Private Key (optional): (Empty text area)

Paste the private key for the above certificate here. This is optional in most cases, but is required when generating a Certificate Revocation List (CRL).

Next Certificate Serial: (Dropdown menu)

Enter a decimal number to be used as a sequential serial number for the next certificate to be signed by this CA.

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.

VPN / OpenVPN / Clients

Servers **Clients** Client Specific Overrides Wizards

OpenVPN

OpenVPN Clients

Interface	Protocol	Server	Mode / Crypto	Description	Actions
-----------	----------	--------	---------------	-------------	---------

+ Add

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 selection 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.

General Information

Description: PIA California

Disabled: Disable this client

Mode Configuration

Server mode: Peer to Peer (SSL/TLS)

Device mode: tun - Layer 3 Tunnel Mode

Endpoint Configuration

Protocol: UDP on IPv4 only

Interface: WAN

Local port: (dropdown)

Server host or address: us-california.privacy.network

Server port: 1198

Proxy host or address: (dropdown)

Proxy port: (dropdown)

Proxy Authentication: none

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 *Dependences Table*.

User Authentication Settings											
Username	<input type="text" value="p1234567"/> p1234567										
Leave empty when no user name is needed											
Password	<input type="password"/>										
Leave empty when no password is needed											
Authentication Retry	<input type="checkbox"/> Do not retry connection when authentication fails										
When enabled, the OpenVPN process will exit if it receives an authentication failure message. The default behavior is to retry. i											
Cryptographic Settings											
TLS Configuration	<input checked="" type="checkbox"/> Use a TLS Key A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.										
TLS keydir direction	<input type="button" value="Use default direction"/> Use default direction										
The TLS Key Direction must be set to complementary values on the client and server. For example, if the server is set to 0, the client must be set to 1. Both may be set to omit the direction, in which case the TLS Key will be used bidirectionally.											
Peer Certificate Authority	<input type="text" value="PIA.2048"/> PIA.2048										
Peer Certificate Revocation list	No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager > Certificate Revocation										
Client Certificate	<input type="button" value="None (Username and/or Password required)"/> None (Username and/or Password required)										
Data Encryption Negotiation	<input checked="" type="checkbox"/> Enable Data Encryption Negotiation This option allows OpenVPN clients and servers to negotiate a compatible set of acceptable cryptographic data encryption algorithms from those selected in the Data Encryption Algorithms list below. Disabling this feature is deprecated.										
Data Encryption Algorithms	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>AES-128-CFB8 (128 bit key, 128 bit block)</td></tr> <tr><td>AES-128-GCM (128 bit key, 128 bit block)</td></tr> <tr><td>AES-128-OFB (128 bit key, 128 bit block)</td></tr> <tr><td>AES-192-CBC (192 bit key, 128 bit block)</td></tr> <tr><td>AES-192-CFB (192 bit key, 128 bit block)</td></tr> <tr><td>AES-192-CFB1 (192 bit key, 128 bit block)</td></tr> <tr><td>AES-192-CFB8 (192 bit key, 128 bit block)</td></tr> <tr><td>AES-192-GCM (192 bit key, 128 bit block)</td></tr> <tr><td>AES-192-OFB (192 bit key, 128 bit block)</td></tr> <tr><td>AES-256-CBC (256 bit key, 128 bit block)</td></tr> </table> <p>Available Data Encryption Algorithms Click to add or remove an algorithm from the list</p>	AES-128-CFB8 (128 bit key, 128 bit block)	AES-128-GCM (128 bit key, 128 bit block)	AES-128-OFB (128 bit key, 128 bit block)	AES-192-CBC (192 bit key, 128 bit block)	AES-192-CFB (192 bit key, 128 bit block)	AES-192-CFB1 (192 bit key, 128 bit block)	AES-192-CFB8 (192 bit key, 128 bit block)	AES-192-GCM (192 bit key, 128 bit block)	AES-192-OFB (192 bit key, 128 bit block)	AES-256-CBC (256 bit key, 128 bit block)
AES-128-CFB8 (128 bit key, 128 bit block)											
AES-128-GCM (128 bit key, 128 bit block)											
AES-128-OFB (128 bit key, 128 bit block)											
AES-192-CBC (192 bit key, 128 bit block)											
AES-192-CFB (192 bit key, 128 bit block)											
AES-192-CFB1 (192 bit key, 128 bit block)											
AES-192-CFB8 (192 bit key, 128 bit block)											
AES-192-GCM (192 bit key, 128 bit block)											
AES-192-OFB (192 bit key, 128 bit block)											
AES-256-CBC (256 bit key, 128 bit block)											
	AES-128-GCM <p>Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list</p>										
The order of the selected Data Encryption Algorithms is respected by OpenVPN. This list is ignored in Shared Key mode. i											
Fallback Data Encryption Algorithm	<input type="text" value="AES-128-GCM (128 bit key, 128 bit block)"/> AES-128-GCM (128 bit key, 128 bit block)										
The Fallback Data Encryption Algorithm used for data channel packets when communicating with clients that do not support data encryption algorithm negotiation (e.g. Shared Key). This algorithm is automatically included in the Data Encryption Algorithms list.											
Auth digest algorithm	<input type="text" value="SHA1 (160-bit)"/> SHA1 (160-bit)										
The algorithm used to authenticate data channel packets, and control channel packets if a TLS Key is present. When an AEAD Encryption Algorithm mode is used, such as AES-GCM, this digest is used for the control channel only, not the data channel. Set this to the same value as the server. While SHA1 is the default for OpenVPN, this algorithm is insecure.											
Hardware Crypto	<input type="button" value="No Hardware Crypto Acceleration"/> No Hardware Crypto Acceleration										
Server Certificate Key Usage Validation	<input checked="" type="checkbox"/> Enforce key usage Verify that remote host uses a server certificate (EKU: "TLS Web Server Authentication").										

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

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

Tunnel Settings	
IPv4 Tunnel Network	<input type="text"/>
This is the IPv4 virtual network or network type alias with a single entry used for private communications between this client and the server expressed using CIDR notation (e.g. 10.0.8.0/24). The second usable address in the network will be assigned to the client virtual interface. Leave blank if the server is capable of providing addresses to clients.	
IPv6 Tunnel Network	<input type="text"/>
This is the IPv6 virtual network or network alias with a single entry used for private communications between this client and the server expressed using CIDR notation (e.g. fe80::/64). When set static using this field, the ::2 address in the network will be assigned to the client virtual interface. Leave blank if the server is capable of providing addresses to clients.	
IPv4 Remote network(s)	<input type="text"/>
IPv4 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases. If this is a site-to-site VPN, enter the remote LAN/s here. May be left blank for non site-to-site VPN.	
IPv6 Remote network(s)	<input type="text"/>
These are the IPv6 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more IP/PREFIX or host/network type aliases. If this is a site-to-site VPN, enter the remote LAN/s here. May be left blank for non site-to-site VPN.	
Limit outgoing bandwidth	<input type="text"/> Between 100 and 100,000,000 bytes/sec
Maximum outgoing bandwidth for this tunnel. Leave empty for no limit. The input value has to be something between 100 bytes/sec and 100 Mbytes/sec (entered as bytes per second). Not compatible with UDP Fast I/O.	
Allow Compression	<input checked="" type="checkbox"/> Compress packets (WARNING: Potentially dangerous!)
Allow compression to be used with this VPN instance. Compression can potentially increase throughput but may allow an attacker to extract secrets if they can control compressed plaintext traversing the VPN (e.g. HTTP). Before enabling compression, consult information about the VORACLE, CRIME, TIME, and BREACH attacks against TLS to decide if the use case for this specific VPN is vulnerable to attack.	
Asymmetric compression allows an easier transition when connecting with older peers.	
Compression	<input checked="" type="checkbox"/> Disable Compression, retain compression packet framing [compress]
Deprecated. Compress tunnel packets using the LZ4 algorithm. Compression can potentially dangerous and insecure. See the note on the Allow Compression option above.	
Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.	
Topology	<input type="text"/> Subnet – One IP address per client in a common subnet
Specifies the method used to configure a virtual adapter IP address.	
Type-of-Service	<input type="checkbox"/> Set the TOS IP header value of tunnel packets to match the encapsulated packet value.
Don't pull routes	<input type="checkbox"/> Bars the server from adding routes to the client's routing table
This option still allows the server to set the TCP/IP properties of the client's TUN/TAP interface.	
Don't add/remove routes	<input type="checkbox"/> Don't add or remove routes automatically
Do not execute operating system commands to install routes. Instead, pass routes to --route-up script using environmental variables.	
Pull DNS	<input type="checkbox"/> Add server provided DNS
If this option is set, pfSense will use DNS servers assigned by remote OpenVPN server for its own purposes (including the DNS Forwarder/DNS Resolver).	

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**.

Ping settings

Inactive: 0
Causes OpenVPN to exit after n seconds of inactivity on the TUN/TAP device.
Activity is based on the last incoming or outgoing tunnel packet (not control or keep-alive packets).
A value of 0 disables this feature.

WARNING: Use with caution. When triggered, the client process will exit and it will not automatically restart.

Ping method: keepalive – Use keepalive helper to define ping configuration
keepalive helper uses interval and timeout parameters to define ping and ping-restart values as follows:
ping = interval
ping-restart = timeout

Interval: 10
Timeout: 60

Advanced Configuration

Custom options:
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

Enter any additional options to add to the OpenVPN client configuration here, separated by semicolon.

UDP Fast I/O: Use fast I/O operations with UDP writes to tun/tap. Experimental.
Optimizes the packet write event loop, improving CPU efficiency by 5% to 10%. Not compatible with all platforms, and not compatible with OpenVPN bandwidth limiting.

Exit Notify: Retry 1x
Send an explicit exit notification to connected servers/peers when restarting or shutting down, so they may immediately disconnect rather than waiting for a timeout. This value controls how many times this instance will attempt to send the exit notification.

This option is ignored in Peer-to-Peer Shared Key mode and in SSL/TLS mode with a /30 tunnel network as it will cause the server to exit and not restart.

Send/Receive Buffer: Default
Configure a Send and Receive Buffer size for OpenVPN. The default buffer size can be too small in many cases, depending on hardware and network uplink speeds. Finding the best buffer size can take some experimentation. To test the best value for a site, start at 512KiB and test higher and lower values.

Gateway creation: Both IPv4 only IPv6 only
If you assign a virtual interface to this OpenVPN client, this setting controls which gateway types will be created. The default setting is 'both'.

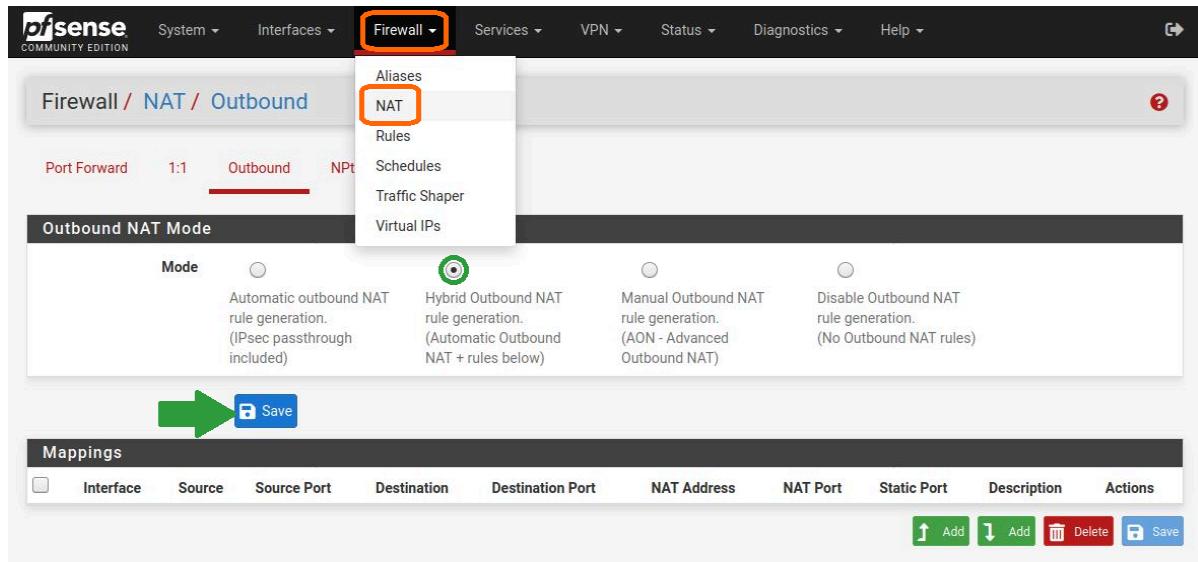
Verbosity level: default
Each level shows all info from the previous levels. Level 3 is recommended for a good summary of what's happening without being swamped by output.

None: Only fatal errors
Default through 4: Normal usage range
5: Output R and W characters to the console for each packet read and write. Uppercase is used for TCP/UDP packets and lowercase is used for TUN/TAP packets.
6-11: Debug info range

 **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.

pfSense COMMUNITY EDITION

Firewall / NAT / Outbound

The NAT configuration has been changed.
The changes must be applied for them to take effect.

Port Forward 1:1 **Outbound** NPt

Outbound NAT Mode

Mode	Automatic outbound NAT rule generation. (IPsec passthrough included)	Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)	Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)	Disable Outbound NAT rule generation. (No Outbound NAT rules)
------	---	--	---	--

 **Save**

Mappings

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
WAN	127.0.0.0/8	*	*	500 (ISAKMP)	WAN address	*	✓	Auto created rule for ISAKMP - localhost to WAN	 
WAN	127.0.0.0/8	*	*	*	WAN address	*	✗	Auto created rule - localhost to WAN	 
WAN	::1/128	*	*	500 (ISAKMP)	WAN address	*	✓	Auto created rule for ISAKMP - localhost to WAN	 
WAN	::1/128	*	*	*	WAN address	*	✗	Auto created rule - localhost to WAN	 
WAN	192.168.1.0/24	*	*	500 (ISAKMP)	WAN address	*	✓	Auto created rule for ISAKMP - LAN to WAN	 
WAN	192.168.1.0/24	*	*	*	WAN address	*	✗	Auto created rule - LAN to WAN	 

 Add  Add  Delete  Save

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

7. Click **Save**.

bisense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾ 

Firewall / NAT / Outbound / Edit 

Edit Advanced Outbound NAT Entry

Disabled	<input type="checkbox"/> Disable this rule
Do not NAT	<input type="checkbox"/> Enabling this option will disable NAT for traffic matching this rule and stop processing Outbound NAT rules In most cases this option is not required.
Interface	<input type="text" value="OpenVPN"/> 
The Interface on which traffic is matched as it exits the firewall. In most cases this is "WAN" or another externally-connected interface.	
Address Family	<input type="text" value="IPv4+IPv6"/>
Select the Internet Protocol version this rule applies to.	
Protocol	<input type="text" value="any"/>
Choose which protocol this rule should match. In most cases "any" is specified.	
Source	<input type="text" value="Network"/> <input type="text" value="127.0.0.0"/> / <input type="text" value="8"/>
Type Source network for the outbound NAT mapping. 	
Destination	<input type="text" value="Any"/> <input type="text" value=""/> / <input type="text" value="24"/> <input type="text" value="500"/>
Type Destination network for the outbound NAT mapping. 	
<input type="checkbox"/> Not Invert the sense of the destination match.	
Translation	
Address	<input type="text" value="Interface Address"/>
Connections matching this rule will be mapped to the specified Address . The Address can be an Interface, a Host-type Alias, or a Virtual IP address.	
Port or Range	<input type="text"/> 
Enter the external source Port or Range used for remapping the original source port on connections matching the rule.	
Port ranges are a low port and high port number separated by ":". Leave blank when Static Port is checked.	
Misc	
No XMLRPC Sync	<input type="checkbox"/>
Prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.	
Description	<input type="text" value="Auto created rule for ISAKMP - localhost to WAN"/>
A description may be entered here for administrative reference (not parsed).	

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.**

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Firewall / NAT / Outbound

The NAT configuration has been changed.
The changes must be applied for them to take effect.

Port Forward 1:1 **Outbound** NPt

Outbound NAT Mode

Mode	Automatic outbound NAT rule generation. (IPsec passthrough included)	Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)	Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)	Disable Outbound NAT rule generation. (No Outbound NAT rules)
------	---	--	---	--

Mappings

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
WAN	127.0.0.0/8	*	*	500 (ISAKMP)	WAN address	*	✓	Auto created rule for ISAKMP - localhost to WAN	
OpenVPN	127.0.0.0/8	*	*	500 (ISAKMP)	OpenVPN address	*	✓	Auto created rule for ISAKMP - localhost to WAN	
WAN	127.0.0.0/8	*	*	*	WAN address	*	✗	Auto created rule - localhost to WAN	
OpenVPN	127.0.0.0/8	*	*	*	OpenVPN address	*	✗	Auto created rule - localhost to WAN	
WAN	::1/128	*	*	500 (ISAKMP)	WAN address	*	✓	Auto created rule for ISAKMP - localhost to WAN	
OpenVPN	::1/128	*	*	500 (ISAKMP)	OpenVPN address	*	✓	Auto created rule for ISAKMP - localhost to WAN	
WAN	::1/128	*	*	*	WAN address	*	✗	Auto created rule - localhost to WAN	
OpenVPN	::1/128	*	*	*	OpenVPN address	*	✗	Auto created rule - localhost to WAN	
WAN	192.168.1.0/24	*	*	500 (ISAKMP)	WAN address	*	✓	Auto created rule for ISAKMP - LAN to WAN	
OpenVPN	192.168.1.0/24	*	*	500 (ISAKMP)	OpenVPN address	*	✓	Auto created rule for ISAKMP - LAN to WAN	
WAN	192.168.1.0/24	*	*	*	WAN address	*	✗	Auto created rule - LAN to WAN	
OpenVPN	192.168.1.0/24	*	*	*	OpenVPN address	*	✗	Auto created rule - LAN to WAN	

Add Add Save

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

Status / OpenVPN

Client Instance Statistics

Name	Status	Connected Since	Local Address	Virtual Address
PIA California UDP4	up	Tue Aug 16 20:18:27 2022	192.168.1.5:61774	10.12.112.119

Status

- 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

Bytes Sent Bytes Received Service

Bytes Sent	Bytes Received	Service
:1198 3 KiB	7 KiB	✓ C O

