



PF SENSE SETUP

Start by downloading our CA certificate file from <https://www.privateinternetaccess.com/openvpn/ca.rsa.2048.crt>. We'll be using this later. You can also find the hostnames of our gateways on our Network page here: <https://www.privateinternetaccess.com/pages/network/>.

CA Installation:

- 1 System -> Cert Manager -> CA
- 2 Descriptive Name: Your choice, or use PIAVPN

System: Certificate Authority Manager



- 3 Method: Import an existing Certificate Authority
- 4 Certificate Data: Paste all content from the ca.rsa.2048.crt file, opened in notepad, downloaded from: <https://www.privateinternetaccess.com/openvpn/ca.rsa.2048.crt>
- 5 Save, Private Key, and Serial should both be blank.

Certificate Setup:

- 1 System -> Cert Manager -> CA -> Add
- 2 Descriptive Name: Your choice, or use Internal CA

- 3 Method: Create an internal CA
- 4 Key Length: 2048 bits
- 5 State/City/Org/E-mail: All set to your choice, can be invalid data.
- 6 Common Name: internal-ca
- 7 System -> Cert Manager -> Certificates -> Add
- 8 Create Internal Certificate
- 9 Descriptive Name: Your choice, I use PIA Client
- 10 Method: Create an internal Certificate
- 11 Key Length: 2048 bits
- 12 Certificate Type: User Certificate
- 13 State/City/Org/E-mail: All set to your choice, can be invalid data.
- 14 Common Name: PIA-Client
- 15 Click Save

System: Certificate Authority Manager

CAs Certificates Certificate Revocation

Descriptive name

Method

Existing Certificate Authority

Certificate data



-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----

Paste a certificate in X.509 PEM format here.

Certificate Private Key (optional)



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

Serial for next certificate

Enter a decimal number to be used as the serial number for the next certificate to be

OpenVPN Setup:

- 1 Diagnostics -> Command Prompt
- 2 Execute the following: `echo "username" > /etc/openvpn-passwd.txt; echo "password" >> /etc/openvpn-passwd.txt`
- 3 Above should have username/password replaced with your provided PIA username/password.
- 4 Click the Save button

Diagnostics: Edit file

File successfully loaded.

Save / Load from path:

```
username
password
```

- 5 Create OpenVPN Client

- 6 Select menu: VPN->OpenVPN
- 7 Select Client tab
- 8 Click Plus symbol to add client
- 9 Configure as follows:
- 10 Disabled = unchecked
- 11 Server Mode = Peer To Peer (SSL/TLS)
- 12 Protocol = UDP
- 13 Device Mode = tun
- 14 Interface = WAN
- 15 Local Port = (leave blank)
- 16 Server host or address = us-texas.privateinternetaccess.com (or any server you choose that we offer)
- 17 Server Port = 1198
- 18 Proxy host or address = (leave blank)
- 19 Proxy port = (leave blank)
- 20 Proxy authentication extra options = none
- 21 Server host name resolution = checked, Infinitely resolve server
- 22 Description = PIA OpenVPN (or whatever you desire)
- 23 TLS Authentication = unchecked, Enable authentication of TLS packets
- 24 Peer Certificate Authority = PIAVPN
- 25 Client Certificate = webConfigurator default *In use
- 26 Encryption cipher = AES-128-CBC

- 27 Hardware Crypto = No Hardware Crypto Acceleration
- 28 IPv4 Tunnel Network = (leave blank)
- 29 IPv6 Tunnel Network = (leave blank)
- 30 IPv4 Remote Network/s = (leave blank)
- 31 IPv6 Remote Network/s = (leave blank)
- 32 Limit outgoing bandwidth = (leave blank)
- 33 Compression = checked, Compress tunnel packets using the LZO algorithm
- 34 Type-of-Service = unchecked
- 35 Advanced = (enter the following into the text field, one item per line with a semi-colon separating each):
auth-user-pass /etc/openvpn-passwd.txt;
verb 5;
remote-cert-tls server
- 36 Click the Save button

OpenVPN: Client

Server	Client	Client Specific Overrides	Wizards
--------	--------	---------------------------	---------

General information

Disabled	☐ Disable this client Set this option to disable this client without removing it from the list.
Server Mode	Peer to Peer (SSL/TLS)
Protocol	UDP
Device mode	tun
Interface	WAN
Local port	 Set this option if you would like to bind to a specific port. Leave this blank or enter 0 for a random dynamic p
Server host or address	us-texas.privateinternetaccess.com
Server port	1198
Proxy host or address	
Proxy port	
Proxy authentication extra options	Authentication method : none
Server host name resolution	☒ Infinitely resolve server Continuously attempt to resolve the server host name. Useful when communicating with a server that is not connected to the Internet.
Description	 You may enter a description here for your reference (not parsed).

Cryptographic Settings

TLS Authentication	☐ Enable authentication of TLS packets.
Peer Certificate Authority	PIAVPN
Client Certificate	webConfigurator default *In Use
Encryption algorithm	AES-128-CBC
Hardware Crypto	No Hardware Crypto Acceleration

Tunnel Settings

IPv4 Tunnel Network	
---------------------	----------------------

- 37 Create OpenVPN interface
- 38 Select menu: Interfaces->(assign)
- 39 Click the Plus button to add new interface. The new interface will be named OPT1 with a network port of ovnc1().
- 40 Click on OPT1 to edit the interface
- 41 Configure as follows:
- 42 Enabled = checked

- 43 Description = PIAVPN
- 44 IPv4 Configuration Type = none
- 45 IPv6 Configuration Type = none
- 46 MAC address = (leave blank)
- 47 MTU = (leave blank)
- 48 MSS = (leave blank)
- 49 Block private networks = unchecked
- 50 Block bogon networks = unchecked
- 51 Click the Save button

The screenshot shows the 'General configuration' section of the PF Sense web interface. It includes fields for 'Enable' (checked), 'Description' (PIAVPN), 'IPv4 Configuration Type' (None), 'IPv6 Configuration Type' (None), 'MAC address' (empty), 'MTU' (empty), and 'MSS' (empty). Below this is the 'Private networks' section with checkboxes for 'Block private networks' and 'Block bogon networks', both of which are unchecked. At the bottom are 'Save' and 'Cancel' buttons.

General configuration

Enable ☒ **Enable Interface**

Description
Enter a description (name) for the interface here.

IPv4 Configuration Type

IPv6 Configuration Type

MAC address
Insert my local MAC address
This field can be used to modify ("spoof") the MAC address of this interface (may be required with some cable connections)
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank

MTU
If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in circumstances.

MSS
If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus header size) will be in effect.

Private networks

☐ **Block private networks**
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option turned off unless your WAN network lies in such a private address space, too.

☐ **Block bogon networks**
When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets you receive.

Note: The update frequency can be changed under System->Advanced Firewall/NAT settings.

Nat Settings

- 1 On new page, click Apply Changes
- 2 Configure NAT Rules
- 3 Select menu: Firewall->NAT
- 4 Select Outbound tab
- 5 Check the radio button: Manual Outbound NAT rule generation (AON - Advanced Outbound NAT)
- 6 Click the Save button

At this point, automatic rules that were in use in Automatic outbound NAT will be generated. It will look like the following, with the exception that the Source IP subnet will match your LAN IP subnet.

Port Forward 1:1 Outbound NAT

Mode: ☐ Automatic outbound NAT rule generation (IPsec passthrough included) ☒ Manual Outbound NAT rule generation (AON - Advanced Outbound NAT)

Mappings:

	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
☐	WAN	192.168.1.0/24	*	*	500	WAN address	*	YES	Auto created for ISAK - LAN to WAN
☐	WAN	192.168.1.0/24	*	*	*	WAN address	*	NO	Auto created for LAN WAN
☐	WAN	127.0.0.0/8	*	*	*	WAN address	1024:65535	NO	Auto created for local to WAN

- 7 The next step is to duplicate each of these rules, but change the NAT Address from WAN to PIAVPN. Start with the first rule by clicking the Plus sign immediately to the right of the line "to add a new NAT based on this one." A new page will open. Configure as follows:
- 8 Do not NAT = unchecked
- 9 Interface = PIAVPN
- 10 Protocol = (do not change)
- 11 Source = (do not change)
- 12 Destination = (do not change)

- 13 Translation = (do not change)
- 14 No XMLRPC Sync = (no dot change)
- 15 Description = Auto created rule for ISAKMP - LAN to PIAVPN

Firewall: NAT: Outbound: Edit

Edit Advanced Outbound NAT entry	
Do not NAT	☐ Enabling this option will disable NAT for traffic matching this rule and stop processing Outbound NAT Hint: in most cases, you won't use this option.
Interface	PIAVPN Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.
Protocol	any Choose which protocol this rule should match. Hint: in most cases, you should specify any here.
Source	Type: Network Address: 192.168.1.0 / 24 Enter the source network for the outbound NAT mapping. Source port: (leave blank for any)
Destination	☐ not Use this option to invert the sense of the match. Type: any Address: / 24 Enter the destination network for the outbound NAT mapping. Destination port: 500 (leave blank for any)
Translation	Address: Interface address Packets matching this rule will be mapped to the IP address given here. If you want this rule to apply to another IP address rather than the IP address of the interface above, select it here (you will need to define Virtual IP addresses on the interface first). Port: Enter the source port for the outbound NAT mapping. Static-port: ☒
No XMLRPC Sync	☐ Hint: This prevents the rule on Master from automatically syncing to other CARP members. This does the rule from being overwritten on Slave.
Description	Auto created rule for ISAKMP - LAN to PIAVPN You may enter a description here for your reference (not parsed).
Save Cancel	

- 16 Click the Save button

Repeat this process for the other two rules. When completed, it should resemble the following:

Port Forward 1:1 Outbound NAT

Mode: ☐ Automatic outbound NAT rule generation (IPsec passthrough included) ☒ Manual Outbound NAT rule generation (AON - Advanced Outbound NAT)

Mappings:

	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
☐	WAN	192.168.1.0/24	*	*	500	WAN address	*	YES	Auto created for ISAK - LAN to WAN
☐	PIA/VPN	192.168.1.0/24	*	*	500	PIA/VPN address	*	YES	Auto created for ISAK - LAN to PIA/VPN
☐	WAN	192.168.1.0/24	*	*	*	WAN address	*	NO	Auto created for LAN to WAN
☐	PIA/VPN	192.168.1.0/24	*	*	*	PIA/VPN address	*	NO	Auto created for LAN to PIA/VPN
☐	WAN	127.0.0.0/8	*	*	*	WAN address	1024:65535	NO	Auto created for local to WAN
☐	PIA/VPN	127.0.0.0/8	*	*	*	PIA/VPN address	1024:65535	NO	Auto created for local to PIA/VPN

- 17 Finally, click the Apply Changes button

Verify OpenVPN Service

- 1 At this point, your system is configured. The only thing you may need to do is restart your OpenVPN Service.
- 2 Select menu: Status->OpenVPN
- 3 Status should be UP (but it may be DOWN)
- 4 Our recommendation is to click on the Restart OpenVPN Service button no matter what the status is. It's the middle button to the right of the service.

Verify OpenVPN Logs:

- 1 Select menu: Status->System Logs
- 2 Click on OpenVPN tab
- 3 Look for confirmation in your logs:
- 4 `openvpn[65701]: Initialization Sequence Completed`

EASY Setup Guides for Alternate Configurations (Advanced):

! PPTP/L2TP/SOCKS Security

The PPTP/L2TP/SOCKS5 protocols are provided for devices lacking compatibility with the Private Internet Access application or OpenVPN protocol. PPTP/L2TP/SOCKS5 should be used for masking one's IP address, censorship circumvention, and geolocation.

If you need encryption, please use the Private Internet Application or OpenVPN protocol with our service.

⊖ Advanced OpenVPN SSL Usage Guides

[Windows OpenVPN Setup](#)

[Mac OS X OpenVPN Setup](#)

[Mac OS X Viscosity Setup](#)

[Ubuntu 12.04 OpenVPN Setup](#)

[Robolinux 7.5.3 OpenVPN Setup](#)

[iOS \(iPad/iPhone/iTouch\) OpenVPN Setup](#)

[Android 4.0+ OpenVPN Setup](#)

[DD-WRT OpenVPN Setup](#)

[DD-WRT OpenVPN \(Older Builds\)](#)

[Tomato OpenVPN Setup](#)

[PfSense OpenVPN Setup](#)

[OpenVPN Configuration Files \(Recommended Default\)](#)

[OpenVPN Configuration Files \(Strong\)](#)

+ L2TP/IPSec Usage Guides



+ Advanced OpenVPN SSL Restrictive Configurations

+ PPTP VPN Instant Setup Guides



+ SOCKS5 Proxy Usage Guides



+ Port Forwarding

+ IPv6 Leak Protection

+ DNS Leak Protection

+ Internet Kill Switch

+ Advanced Router Setup

+ Regional Gateways

WHY

Hide My IP
Browse Anonymously
Public Wifi Security
Identity Protection
Internet Security
Internet of Things Security
Prevent Data Theft
Hide My Location
FaceNiff and Firesheep
Tor vs VPN vs Proxy
Free vs Paid
UN Recommends Encryption

NAVIGATION

VPN Service
What's my IP?
VPN Encryption
VPN Reviews
About Us
Client Support
Downloads
VPN Forum
VPN Blog
VPN Affiliates
Companies We Support
Work For Us
PIA Site Map
PIA In The Media
PIA Android App
PIA iOS App

LEGAL

Terms Of Service
Privacy Policy
DMCA Policy
Export Control Policy

ABOUT

Private Internet Access is the leading VPN Service provider specializing in secure, encrypted VPN tunnels which create several layers of privacy and security providing you safety on the internet. Our VPN Service is backed by multiple gateways worldwide with VPN Tunnel access in 24+ countries, 36+ regions.

Map data provided by Google.

Copyright© London Trust Media, Inc. All Rights Reserved.

SOCIAL**PAYMENT METHODS**