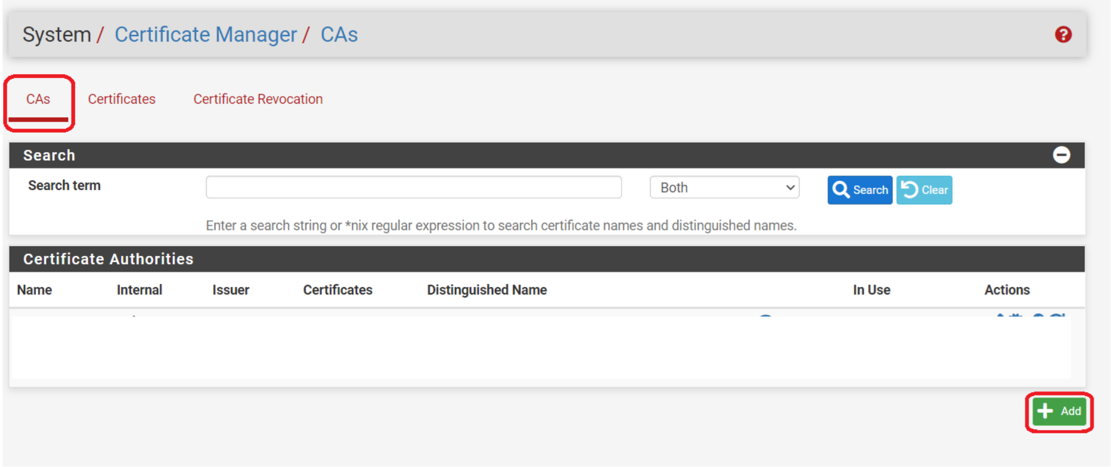
OpenVPN between pfSense and Vigor Router

Vigor2927, Vigor2865 and other Vigor routers running firmware version 4.2.2 support OpenVPN with pfSense firewall.

This article documents how to create an OpenVPN tunnel between a Vigor Router and a pfSense firewall.

pfSense OpenVPN server configuration

1. Go to System>Cert. Manager and add a CA



System / Certificate Manager / CAs

Search

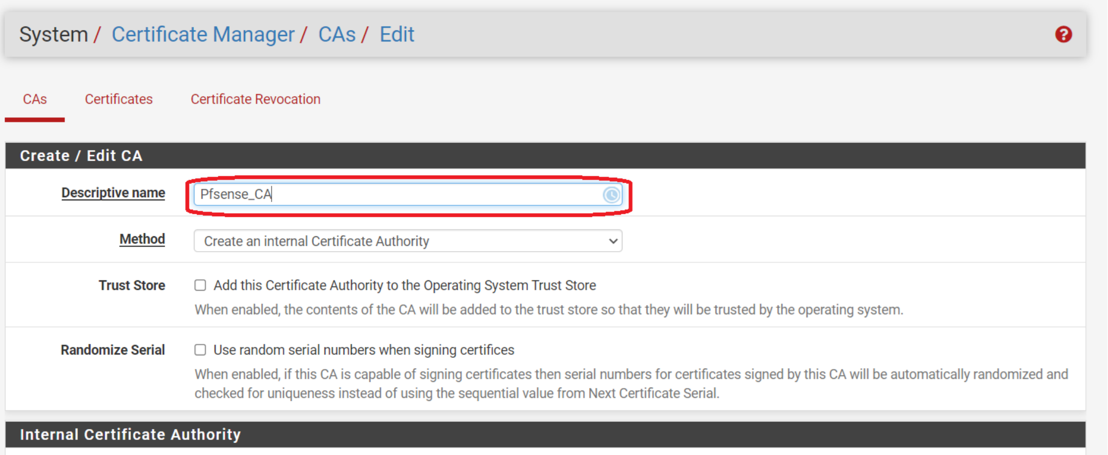
Search term: Both

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificate Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions

2. Give a Descriptive name, CA subject components and click Save to generate a CA



System / Certificate Manager / CAs / Edit

Create / Edit CA

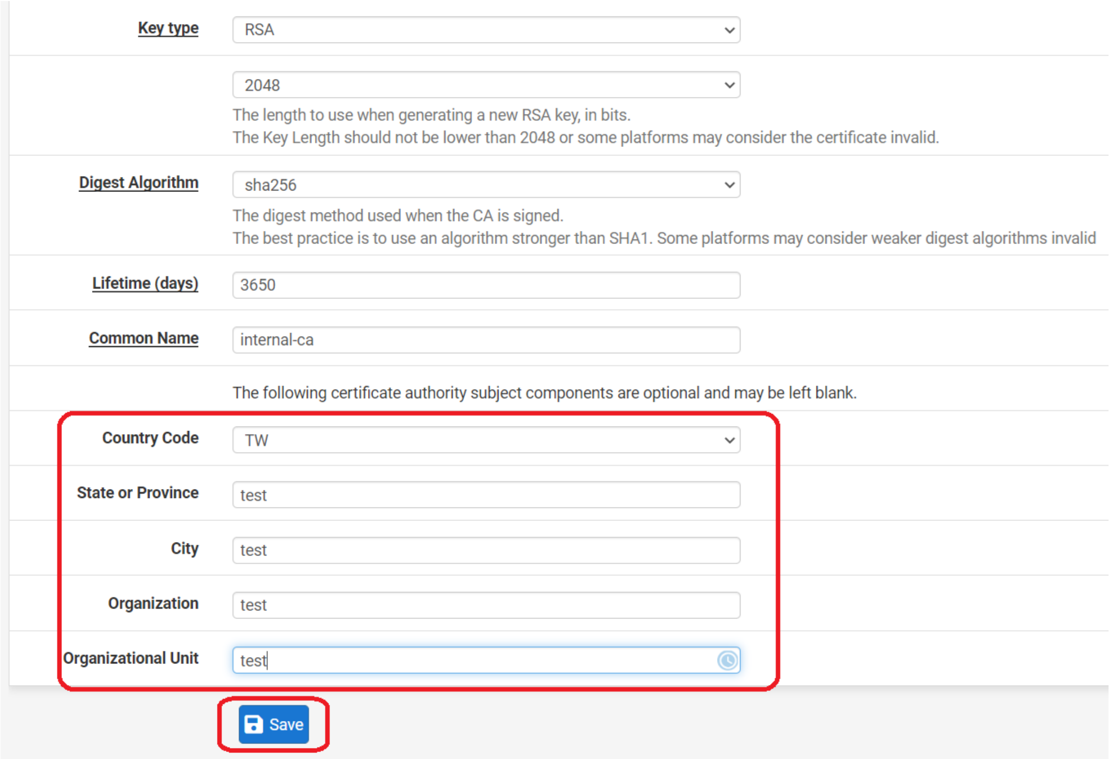
Descriptive name: Pfsense_CA

Method: Create an internal 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.

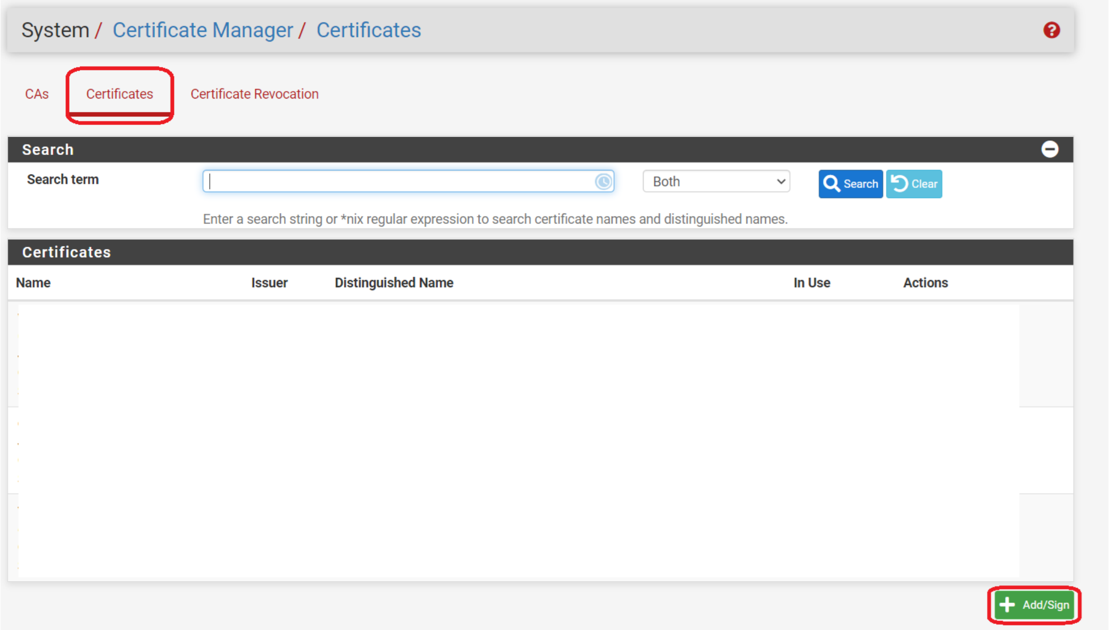
Randomize Serial: □ Use random serial numbers when signing certificates
When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate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

Internal Certificate Authority



Key type	RSA
	2048 The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.
Digest Algorithm	sha256 The digest method used when the CA is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid
Lifetime (days)	3650
Common Name	internal-ca
	The following certificate authority subject components are optional and may be left blank.
Country Code	TW
State or Province	test
City	test
Organization	test
Organizational Unit	test

3. Go to Certificate and add a certificate



System / Certificate Manager / Certificates

Search

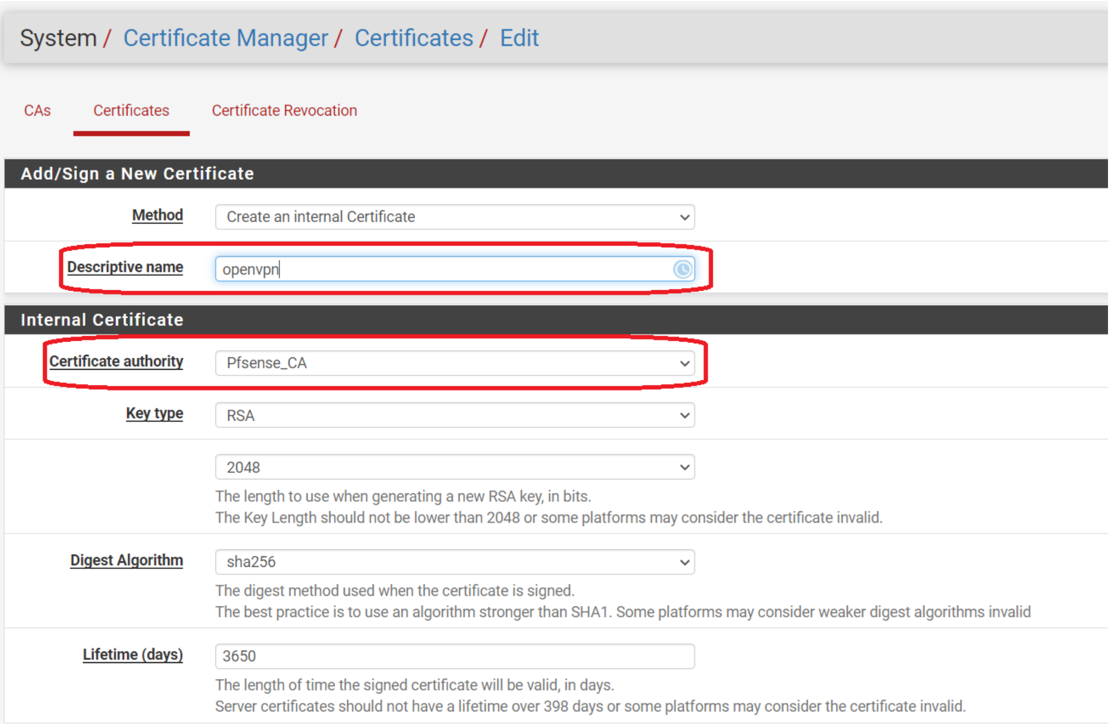
Search term

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificates

Name	Issuer	Distinguished Name	In Use	Actions

4. Give a Descriptive name and select the CA just created as Certificate authority, then save it to create a server certificate



System / Certificate Manager / Certificates / Edit

Add/Sign a New Certificate

Method: Create an internal Certificate

Descriptive name: openvpn

Internal Certificate

Certificate authority: Pfsense_CA

Key type: RSA

2048

The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

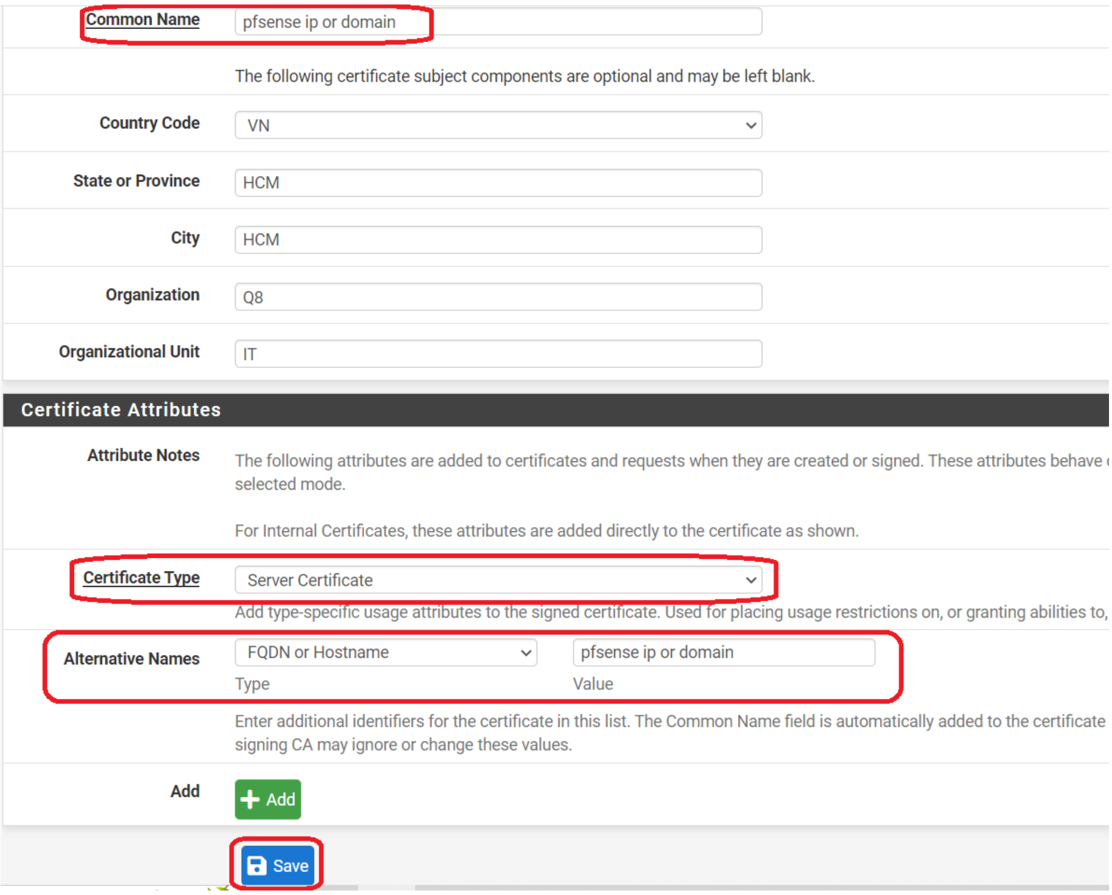
Digest Algorithm: sha256

The digest method used when the certificate is signed.
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid

Lifetime (days): 3650

The length of time the signed certificate will be valid, in days.
Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.

Use pfSense Internet IP or Domain as Common name and Alternative Names



Common Name: pfsense ip or domain

The following certificate subject components are optional and may be left blank.

Country Code: VN

State or Province: HCM

City: HCM

Organization: Q8

Organizational Unit: IT

Certificate Attributes

Attribute Notes: The following attributes are added to certificates and requests when they are created or signed. These attributes behave
selected mode.

For Internal Certificates, these attributes are added directly to the certificate as shown.

Certificate Type: Server Certificate

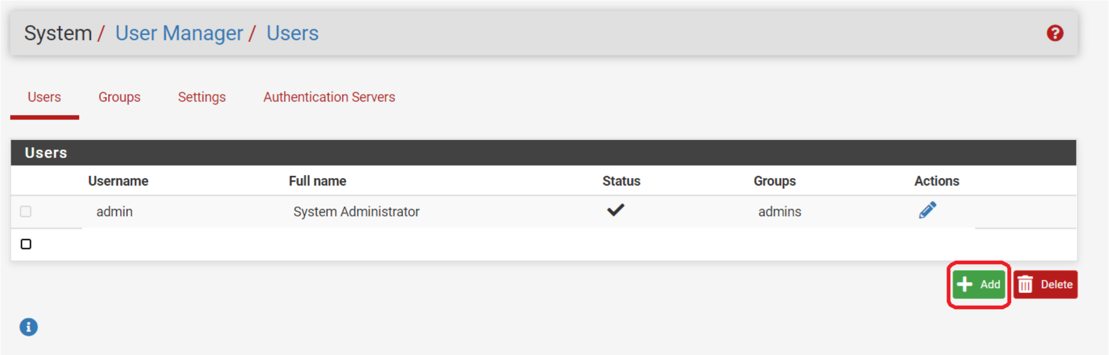
Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to,

Alternative Names: FQDN or Hostname (Type) pfsense ip or domain (Value)

Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate
signing CA may ignore or change these values.

Add: + Add

5. Go to System>User Manager and add an user



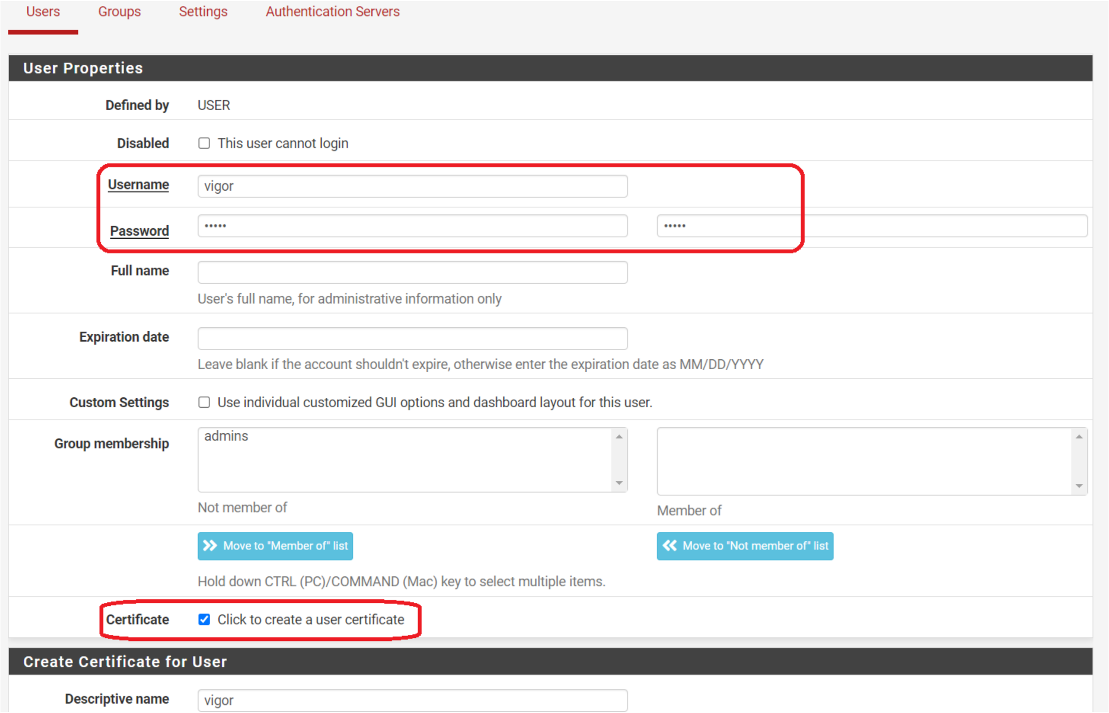
System / User Manager / Users

Users | Groups | Settings | Authentication Servers

Users

	Username	Full name	Status	Groups	Actions
□	admin	System Administrator	✓	admins	✎
□					

6. Enter Username, Password and create a user certificate



Users | Groups | Settings | Authentication Servers

User Properties

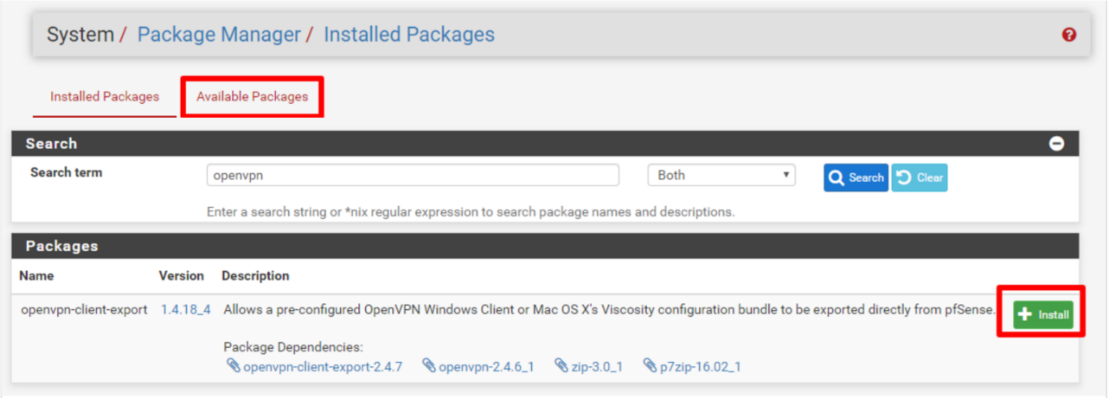
Defined by	USER
Disabled	□ This user cannot login
Username	vigor
Password	••••• •••••
Full name	User's full name, for administrative information only
Expiration date	Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY
Custom Settings	□ Use individual customized GUI options and dashboard layout for this user.
Group membership	Not member of: admins Member of:
	Move to "Member of" list Move to "Not member of" list Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.
Certificate	☑ Click to create a user certificate

Create Certificate for User

Descriptive name	vigor

7. Go to System>Package Manager, search openvpn in available package and

install openvpn-client-export



System / Package Manager / Installed Packages

Installed Packages | Available Packages

Search

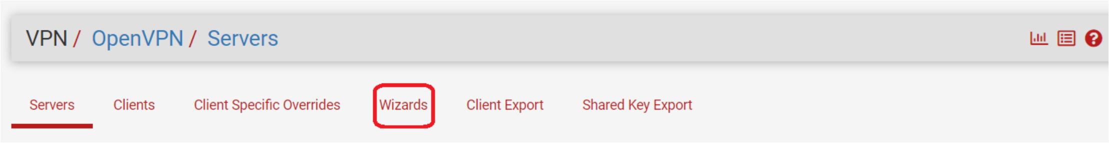
Search term: openvpn | Both

Enter a search string or *nix regular expression to search package names and descriptions.

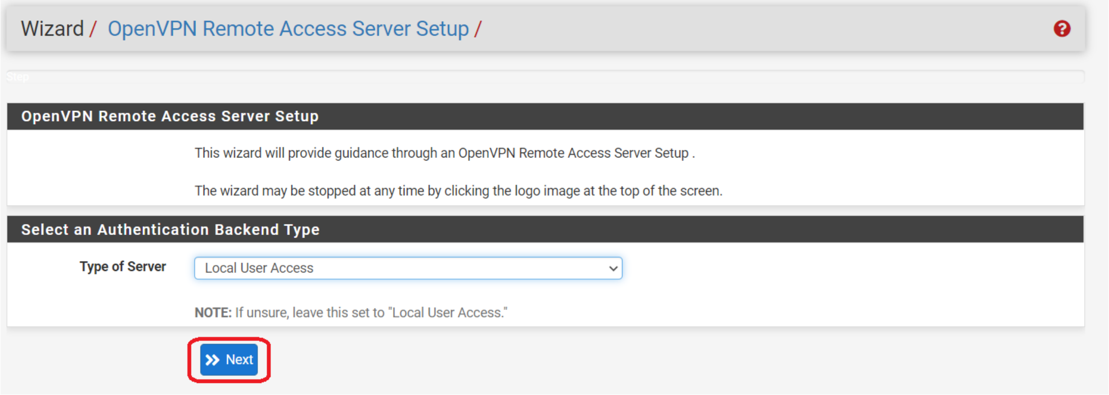
Packages

Name	Version	Description	
openvpn-client-export	1.4.18_4	Allows a pre-configured OpenVPN Windows Client or Mac OS X's Viscosity configuration bundle to be exported directly from pfSense. Package Dependencies: openvpn-client-export-2.4.7 openvpn-2.4.6_1 zip-3.0_1 p7zip-16.02_1	Install

8. Go to VPN>OpenVPN and click Wizard


VPN / OpenVPN / Servers

9. Select Local User Access as Type of Server and go next


Wizard / OpenVPN Remote Access Server Setup /

OpenVPN Remote Access Server Setup

This wizard will provide guidance through an OpenVPN Remote Access Server Setup .

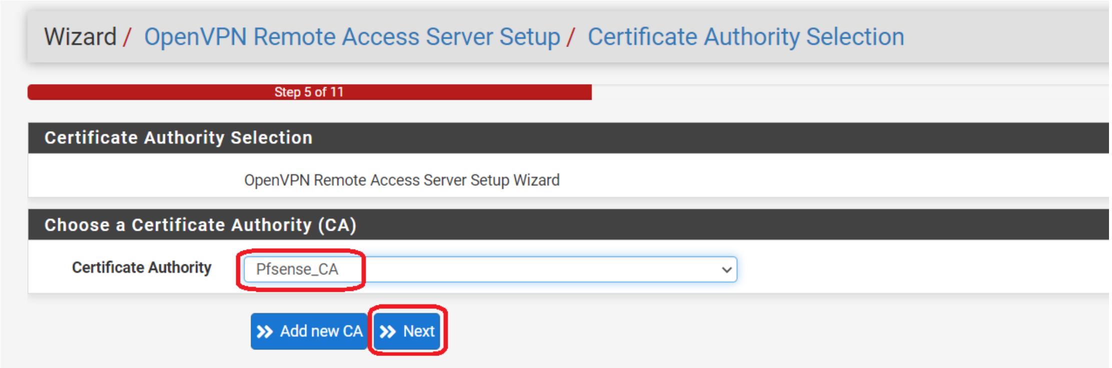
The wizard may be stopped at any time by clicking the logo image at the top of the screen.

Select an Authentication Backend Type

Type of Server: Local User Access

NOTE: If unsure, leave this set to "Local User Access."

Select the CA and certificate created in step2 and 4


Wizard / OpenVPN Remote Access Server Setup / Certificate Authority Selection

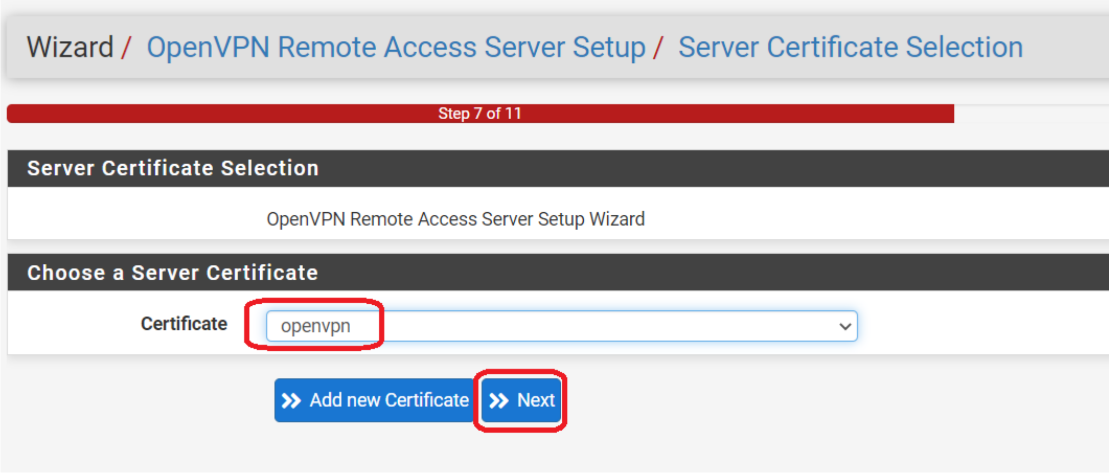
Step 5 of 11

Certificate Authority Selection

OpenVPN Remote Access Server Setup Wizard

Choose a Certificate Authority (CA)

Certificate Authority: Pfsense_CA


Wizard / OpenVPN Remote Access Server Setup / Server Certificate Selection

Step 7 of 11

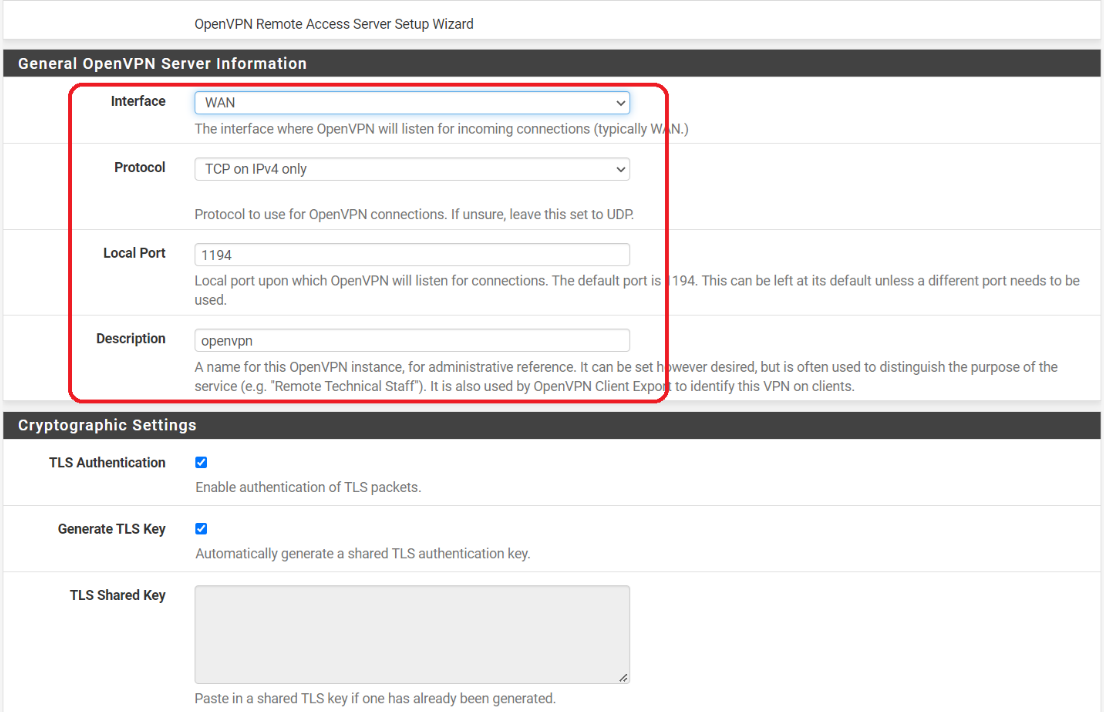
Server Certificate Selection

OpenVPN Remote Access Server Setup Wizard

Choose a Server Certificate

Certificate: openvpn

Select WAN as Interface, TCP/UDP(UDP recommended) and OpenVPN port



OpenVPN Remote Access Server Setup Wizard

General OpenVPN Server Information

Interface: WAN
The interface where OpenVPN will listen for incoming connections (typically WAN.)

Protocol: TCP on IPv4 only
Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.

Local Port: 1194
Local port upon which OpenVPN will listen for connections. The default port is 1194. This can be left at its default unless a different port needs to be used.

Description: openvpn
A name for this OpenVPN instance, for administrative reference. It can be set however desired, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff"). It is also used by OpenVPN Client Export to identify this VPN on clients.

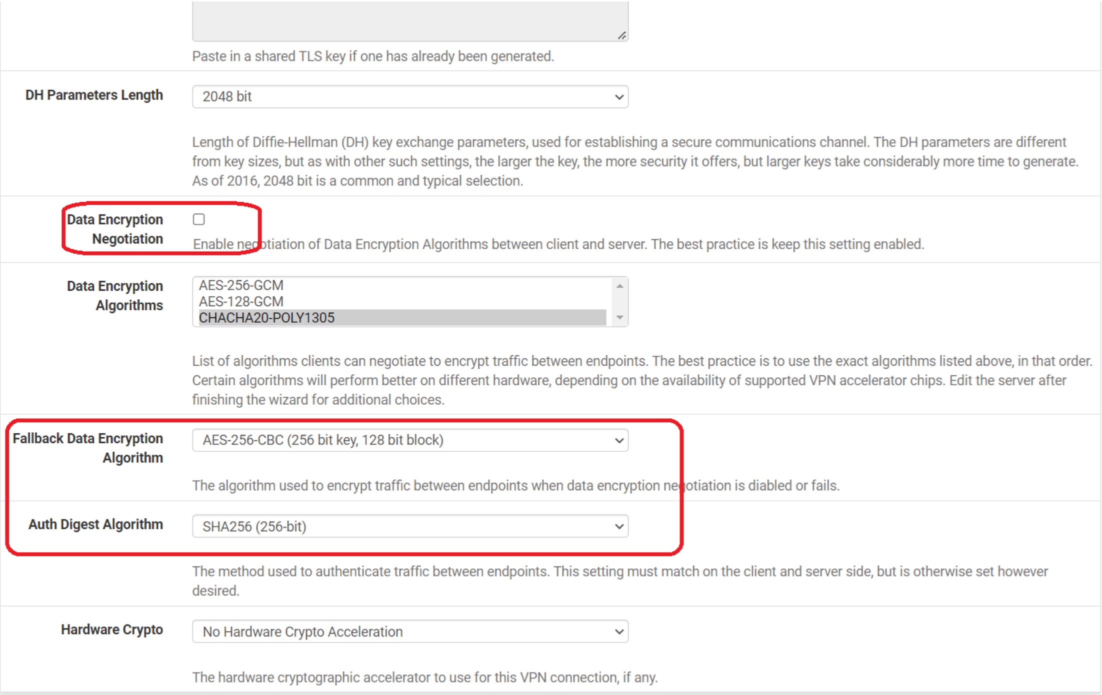
Cryptographic Settings

TLS Authentication: ☑
Enable authentication of TLS packets.

Generate TLS Key: ☑
Automatically generate a shared TLS authentication key.

TLS Shared Key:
Paste in a shared TLS key if one has already been generated.

Disable Data Encryption Negotiation and use AES-256-CBC and SHA256



Paste in a shared TLS key if one has already been generated.

DH Parameters Length: 2048 bit
Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure communications channel. The DH parameters are different from key sizes, but as with other such settings, the larger the key, the more security it offers, but larger keys take considerably more time to generate. As of 2016, 2048 bit is a common and typical selection.

Data Encryption Negotiation: ☐
Enable negotiation of Data Encryption Algorithms between client and server. The best practice is keep this setting enabled.

Data Encryption Algorithms: AES-256-GCM
AES-128-GCM
CHACHA20-POLY1305
List of algorithms clients can negotiate to encrypt traffic between endpoints. The best practice is to use the exact algorithms listed above, in that order. Certain algorithms will perform better on different hardware, depending on the availability of supported VPN accelerator chips. Edit the server after finishing the wizard for additional choices.

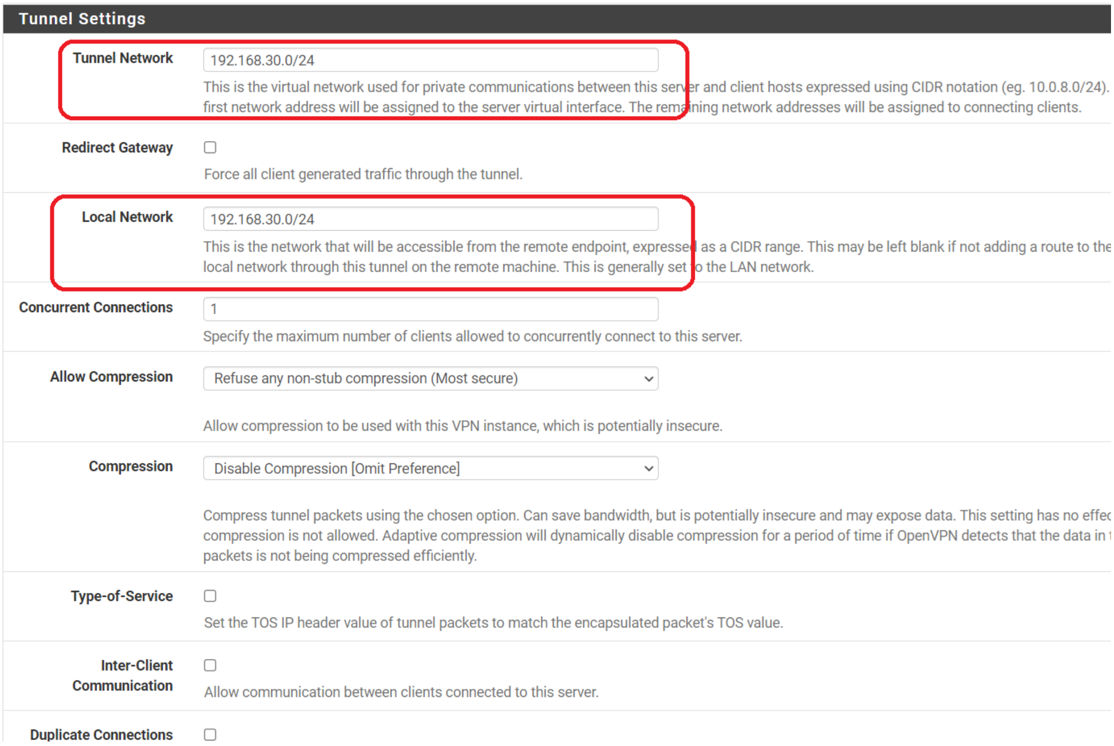
Fallback Data Encryption Algorithm: AES-256-CBC (256 bit key, 128 bit block)
The algorithm used to encrypt traffic between endpoints when data encryption negotiation is diabled or fails.

Auth Digest Algorithm: SHA256 (256-bit)
The method used to authenticate traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired.

Hardware Crypto: No Hardware Crypto Acceleration
The hardware cryptographic accelerator to use for this VPN connection, if any.

Enter the pfSense local network for Vigor to access in Tunnel Network and Local

Network



Tunnel Settings

Tunnel Network: 192.168.30.0/24
This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.

Redirect Gateway: □
Force all client generated traffic through the tunnel.

Local Network: 192.168.30.0/24
This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.

Concurrent Connections: 1
Specify the maximum number of clients allowed to concurrently connect to this server.

Allow Compression: Refuse any non-stub compression (Most secure)
Allow compression to be used with this VPN instance, which is potentially insecure.

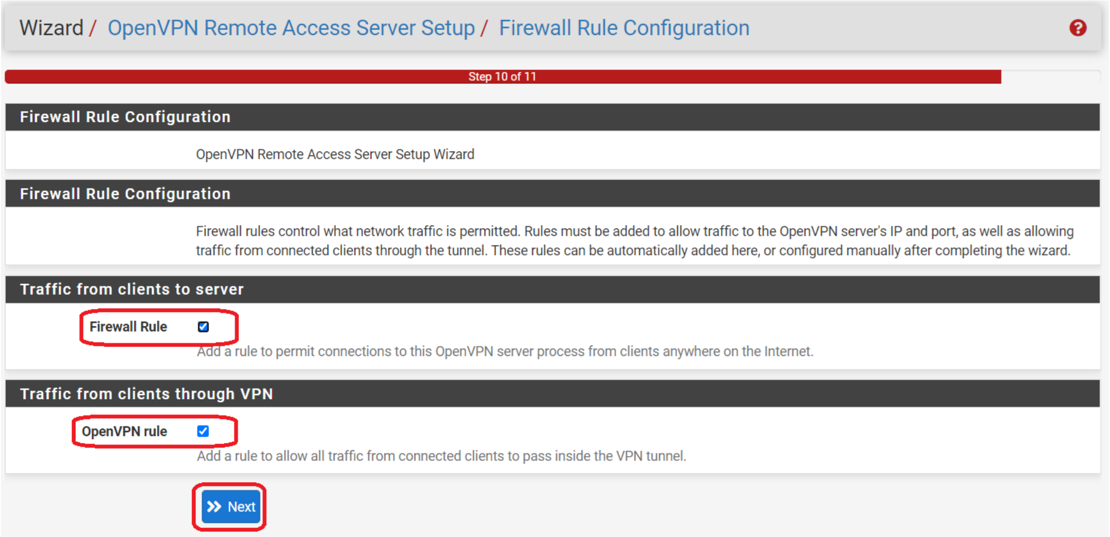
Compression: Disable Compression [Omit Preference]
Compress tunnel packets using the chosen option. Can save bandwidth, but is potentially insecure and may expose data. This setting has no effec compression is not allowed. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in t packets is not being compressed efficiently.

Type-of-Service: □
Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.

Inter-Client Communication: □
Allow communication between clients connected to this server.

Duplicate Connections: □

Add a Firewall Rule and OpenVPN Rule, then Finish the wizard



Wizard / OpenVPN Remote Access Server Setup / Firewall Rule Configuration

Step 10 of 11

Firewall Rule Configuration

OpenVPN Remote Access Server Setup Wizard

Firewall Rule Configuration

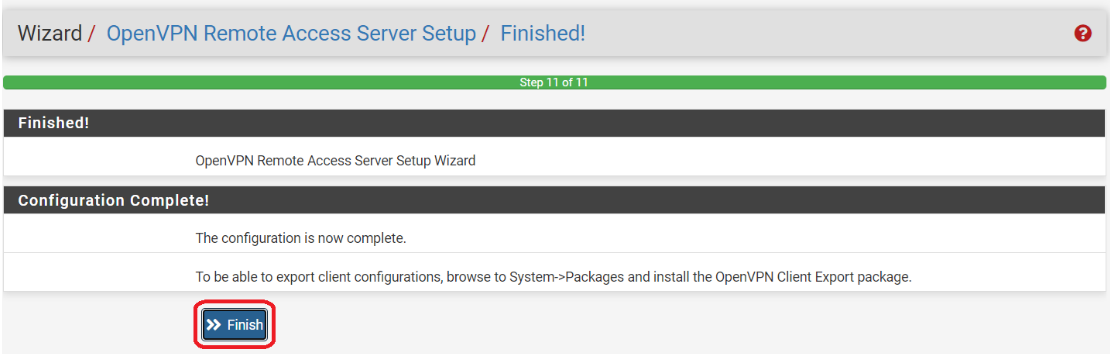
Firewall rules control what network traffic is permitted. Rules must be added to allow traffic to the OpenVPN server's IP and port, as well as allowing traffic from connected clients through the tunnel. These rules can be automatically added here, or configured manually after completing the wizard.

Traffic from clients to server

Firewall Rule: ☑
Add a rule to permit connections to this OpenVPN server process from clients anywhere on the Internet.

Traffic from clients through VPN

OpenVPN rule: ☑
Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.



Wizard / OpenVPN Remote Access Server Setup / Finished!

Step 11 of 11

Finished!

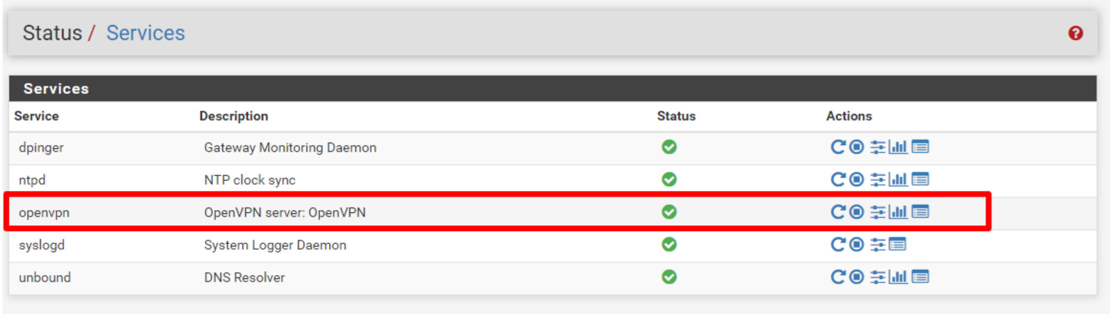
OpenVPN Remote Access Server Setup Wizard

Configuration Complete!

The configuration is now complete.

To be able to export client configurations, browse to System->Packages and install the OpenVPN Client Export package.

10. Go to Status>Services to check OpenVPN is running

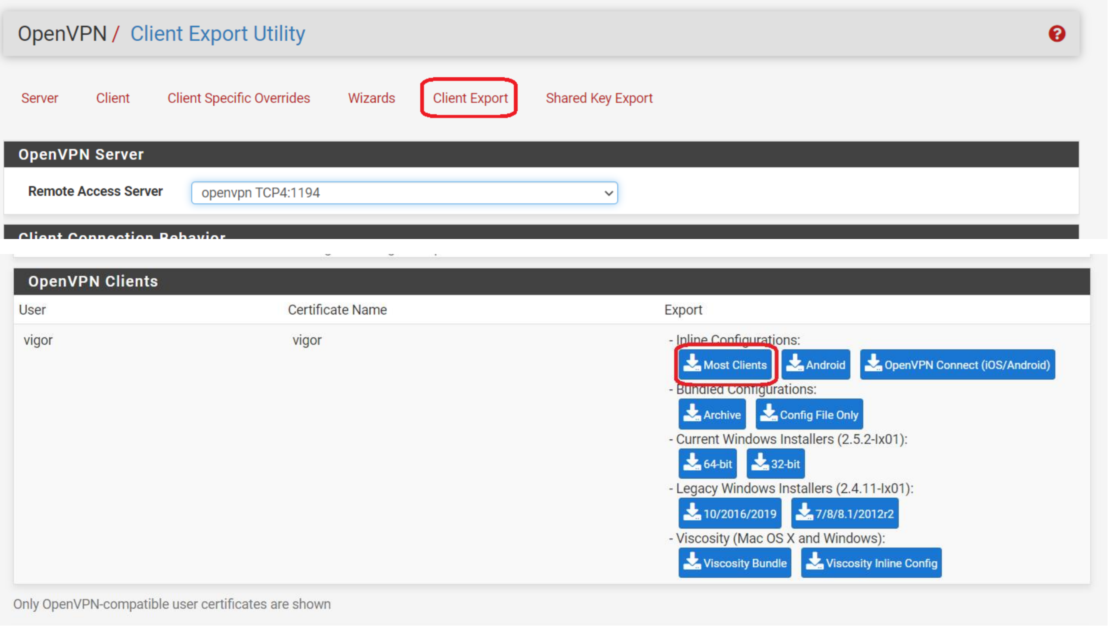


Status / Services

Services

Service	Description	Status	Actions
dpinger	Gateway Monitoring Daemon	✓	
ntpd	NTP clock sync	✓	
openvpn	OpenVPN server: OpenVPN	✓	
syslogd	System Logger Daemon	✓	
unbound	DNS Resolver	✓	

11. Go to VPN>OpenVPN>Client Export, find the user created in step6, and export the client config by Inline Configuration>Most Clients



OpenVPN / Client Export Utility

OpenVPN Server

Remote Access Server: openvpn TCP4:1194

Client Connection Behavior

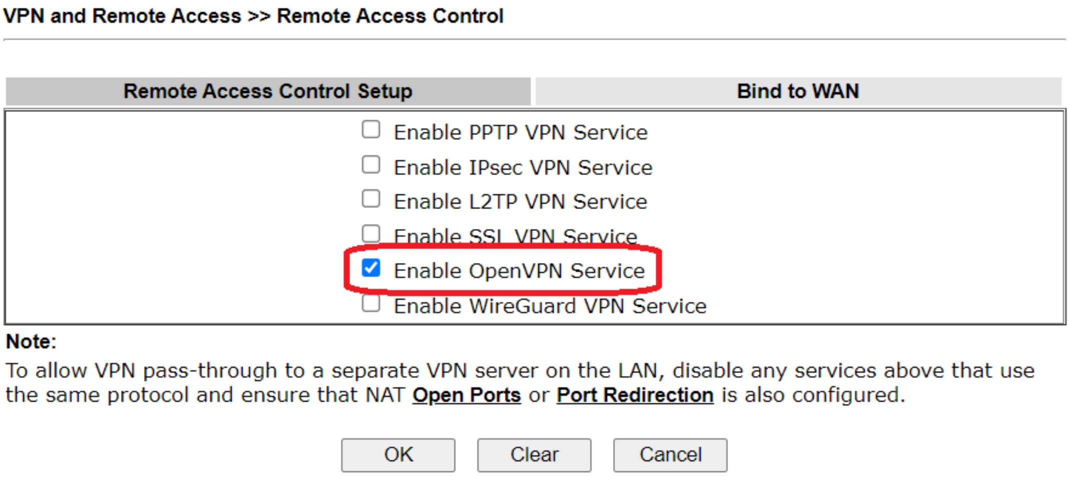
OpenVPN Clients

User	Certificate Name	Export
vigor	vigor	- Inline Configurations: Most Clients · Android · OpenVPN Connect (iOS/Android) - Bundled Configurations: Archive · Config File Only - Current Windows Installers (2.5.2-Ix01): 64-bit · 32-bit - Legacy Windows Installers (2.4.11-Ix01): 10/2016/2019 · 7/8/8.1/2012r2 - Viscosity (Mac OS X and Windows): Viscosity Bundle · Viscosity Inline Config

Only OpenVPN-compatible user certificates are shown

Vigor Router Configuration

1. Go to VPN and Remote Access>Remote Access Control, enable OpenVPN service

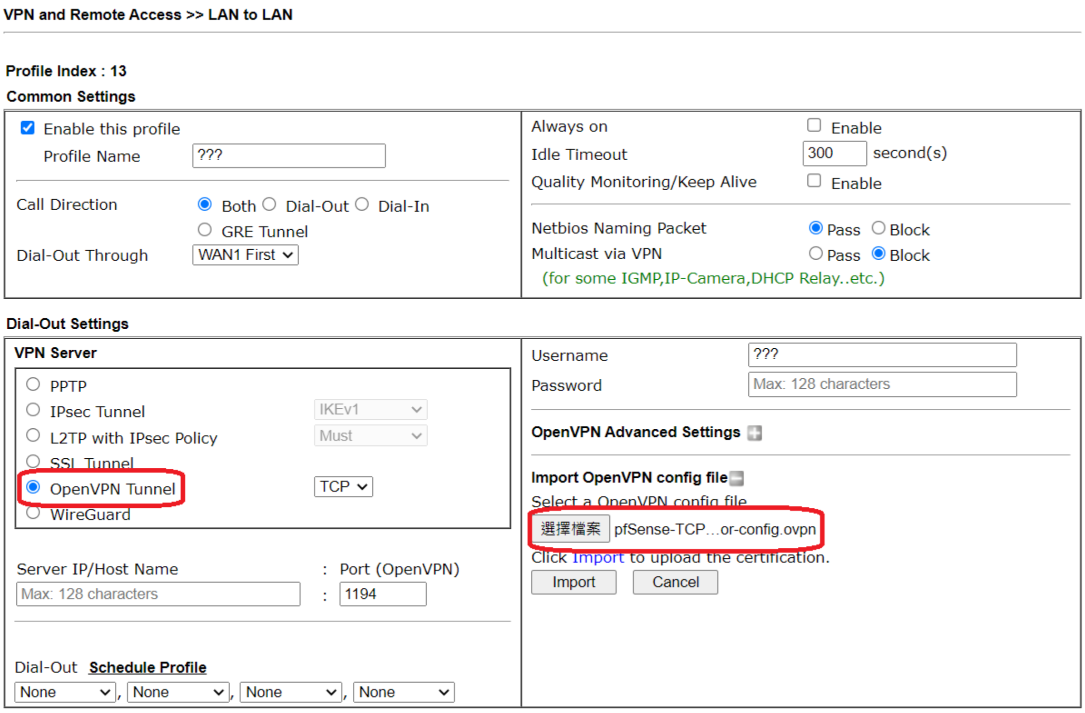


VPN and Remote Access >> Remote Access Control

□ Enable PPTP VPN Service
□ Enable IPsec VPN Service
□ Enable L2TP VPN Service
□ Enable SSL VPN Service
☑ Enable OpenVPN Service
□ Enable WireGuard VPN Service

Note:
To allow VPN pass-through to a separate VPN server on the LAN, disable any services above that use the same protocol and ensure that NAT **Open Ports** or **Port Redirection** is also configured.

2. Go to VPN and Remote Access>LAN to LAN, click a profile and select OpenVPN to import the client config



VPN and Remote Access >> LAN to LAN

Profile Index : 13
Common Settings

☑ Enable this profile
Profile Name: ???
Call Direction: ● Both ○ Dial-Out ○ Dial-In ○ GRE Tunnel
Dial-Out Through: WAN1 First

Always on: □ Enable
Idle Timeout: 300 second(s)
Quality Monitoring/Keep Alive: □ Enable
Netbios Naming Packet: ● Pass ○ Block
Multicast via VPN: ○ Pass ● Block
(for some IGMP,IP-Camera,DHCP Relay..etc.)

Dial-Out Settings

VPN Server
○ PPTP
○ IPsec Tunnel IKEv1
○ L2TP with IPsec Policy Must
○ SSL Tunnel
● OpenVPN Tunnel TCP
○ WireGuard

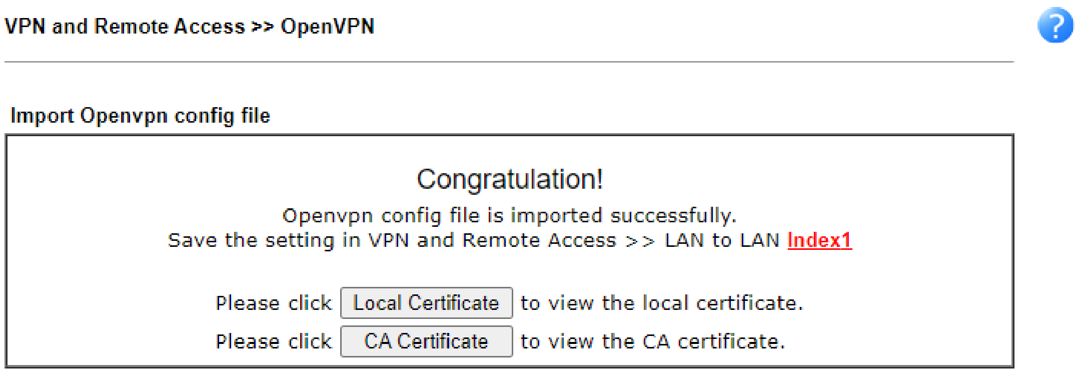
Server IP/Host Name: Max: 128 characters
Port (OpenVPN): 1194

Dial-Out **Schedule Profile**
None, None, None, None

Username: ???
Password: Max: 128 characters

OpenVPN Advanced Settings

Import OpenVPN config file
Select a OpenVPN config file
選擇檔案 pfSense-TCP…or-config.ovpn
Click Import to upload the certification.



VPN and Remote Access >> OpenVPN

Import Openvpn config file

Congratulation!

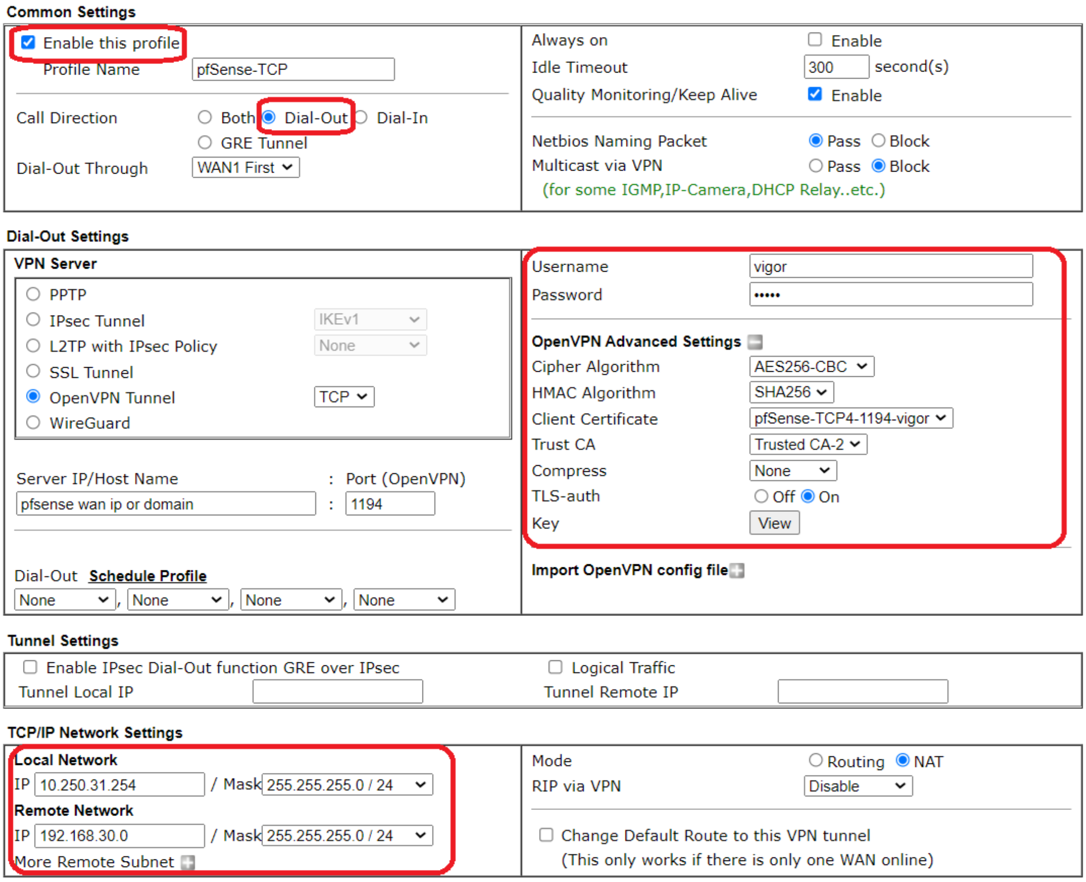
Openvpn config file is imported successfully.
Save the setting in VPN and Remote Access >> LAN to LAN Index1

Please click Local Certificate to view the local certificate.

Please click CA Certificate to view the CA certificate.

3. Enable the profile, select Dial-Out, Enter Username and Password and

Enter pfSense Local Network as Remote Network



Common Settings

☑ Enable this profile		Always on	□ Enable
Profile Name	pfSense-TCP	Idle Timeout	300 second(s)
		Quality Monitoring/Keep Alive	☑ Enable
Call Direction	○ Both ● Dial-Out ○ Dial-In ○ GRE Tunnel	Netbios Naming Packet	● Pass ○ Block
Dial-Out Through	WAN1 First	Multicast via VPN	○ Pass ● Block
		(for some IGMP,IP-Camera,DHCP Relay..etc.)	

Dial-Out Settings

VPN Server
- ○ PPTP
- ○ IPsec Tunnel — IKEv1
- ○ L2TP with IPsec Policy — None
- ○ SSL Tunnel
- ● OpenVPN Tunnel — TCP
- ○ WireGuard

Server IP/Host Name: pfsense wan ip or domain : Port (OpenVPN) 1194

Dial-Out Schedule Profile: None, None, None, None

Username	vigor
Password	•••••

OpenVPN Advanced Settings

Cipher Algorithm	AES256-CBC
HMAC Algorithm	SHA256
Client Certificate	pfSense-TCP4-1194-vigor
Trust CA	Trusted CA-2
Compress	None
TLS-auth	○ Off ● On
Key	View

Import OpenVPN config file

Tunnel Settings

□ Enable IPsec Dial-Out function GRE over IPsec — □ Logical Traffic

Tunnel Local IP — Tunnel Remote IP

TCP/IP Network Settings

Local Network
IP 10.250.31.254 / Mask 255.255.255.0 / 24

Remote Network
IP 192.168.30.0 / Mask 255.255.255.0 / 24

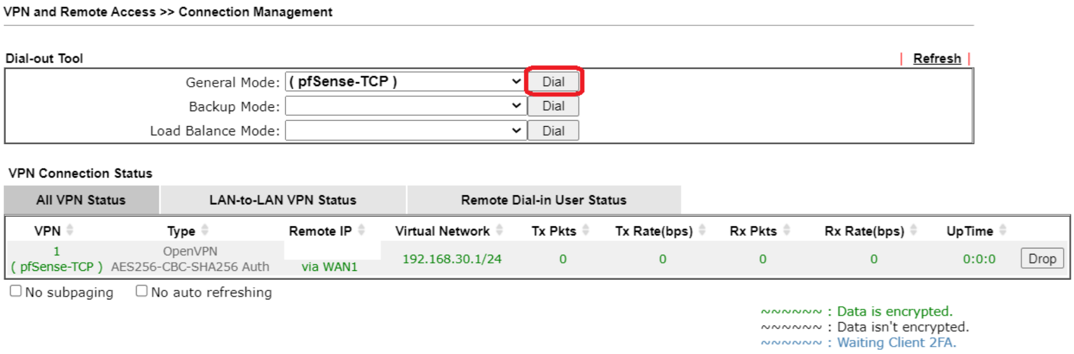
More Remote Subnet

Mode	○ Routing ● NAT
RIP via VPN	Disable

□ Change Default Route to this VPN tunnel
(This only works if there is only one WAN online)

4. Go to VPN and Remote Access>Connection Management, and click Dial.

OpenVPN will be up in few seconds



VPN and Remote Access >> Connection Management

Dial-out Tool | Refresh |

General Mode: (pfSense-TCP) Dial

Backup Mode: Dial

Load Balance Mode: Dial

VPN Connection Status

All VPN Status | LAN-to-LAN VPN Status | Remote Dial-in User Status

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(bps)	Rx Pkts	Rx Rate(bps)	UpTime	
1 (pfSense-TCP)	OpenVPN AES256-CBC-SHA256 Auth	via WAN1	192.168.30.1/24	0	0	0	0	0:0:0	Drop

□ No subpaging □ No auto refreshing

~~~~~~ : Data is encrypted.
~~~~~~ : Data isn't encrypted.
~~~~~~ : Waiting Client 2FA.
~~~~~~