

Continuity Cloud Virtual Firewall Guide



Version 2.0

September 2016



CONTENTS

INTRODUCTION.....	3
ACCESS THE VIRTUAL FIREWALL.....	4
Hyper-V/VirtualBox Continuity Cloud Nodes	4
VMware Continuity Cloud Nodes	4
CONFIGURE THE LAN INTERFACE	5
CONFIGURE THE DHCP SERVER	6
CONFIGURE FIREWALL RULES & NAT	8
Set outbound traffic.....	8
Port forwarding.....	9
CONFIGURE THE OPENVPN SERVER	12
Add a new certificate authority (CA)	14
Add a new server certificate	15
Configure General OpenVPN Server information.....	16
Configure the Cryptographic Settings for OpenVPN connections.....	17
Configure Tunnel Settings.....	18
Configure Client Settings	19
SET UP REMOTE USER ACCOUNTS	21
DOWNLOAD A CONFIGURED OPEN VPN INSTALLER	23
IPSEC VPN	23
USE STATIC IP ADDRESSES	24
CONCLUSION	25
Additional Assistance.....	25

INTRODUCTION

Each eFolder Continuity Cloud node is provisioned with a virtual firewall to handle internet traffic for your restored virtual machines and provide secure access to your servers.

In this guide, you will learn how to:

- Access your assigned pfSense virtual firewall.
- Configure the LAN interface of the firewall.
- Setup required access rules or NAT translations to support your restored environment.
- OpenVPN configuration for user access.

Additional Assistance

At eFolder, we value feedback from our customers.

Not only do we want to help you quickly resolve your technical issues, we value your input and build our products to incorporate your suggestions.

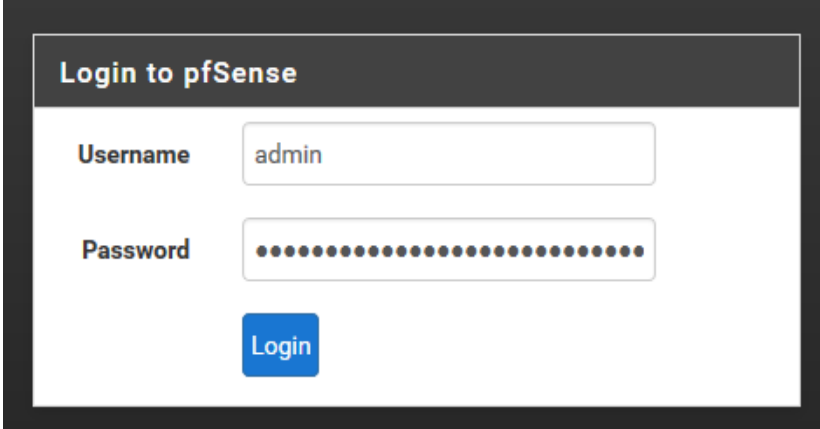
- To contact eFolder Technical Support, call 678-373-0109 or 1-800-352-0248
- Submit questions to support@efolder.net
- For how-to articles and FAQ, see the pfSense documentation at: https://doc.pfsense.org/index.php/Main_Page
- Additional material is available in the [eFolder Partner Portal](#)
- The eFolder Support page is at <http://www.efolder.net/support/>

ACCESS THE VIRTUAL FIREWALL

Use the information provided by eFolder to gain access to the pfSense virtual firewall running on your assigned Continuity Cloud (CC) Node.

Hyper-V/VirtualBox Continuity Cloud Nodes

1. To access the console of your pfSense virtual firewall, first log in to your CC Node using RDP, then open a web browser and go to the WAN Alias IP address of your virtual firewall. (It will look similar to the example shown below.) <https://10.x.x.x:37038>
This is a locally accessible private IP address. There is also a shortcut on the desktop of the CC Node.
2. Next, enter the credentials you received from eFolder for your virtual firewall and click **Login**. Please note that the username and password are case sensitive.



The image shows a web browser window displaying the pfSense login interface. At the top, there is a dark header with the text "Login to pfSense" in white. Below the header, there are two input fields: "Username" with the value "admin" and "Password" with a series of dots representing a masked password. A blue "Login" button is located below the password field.

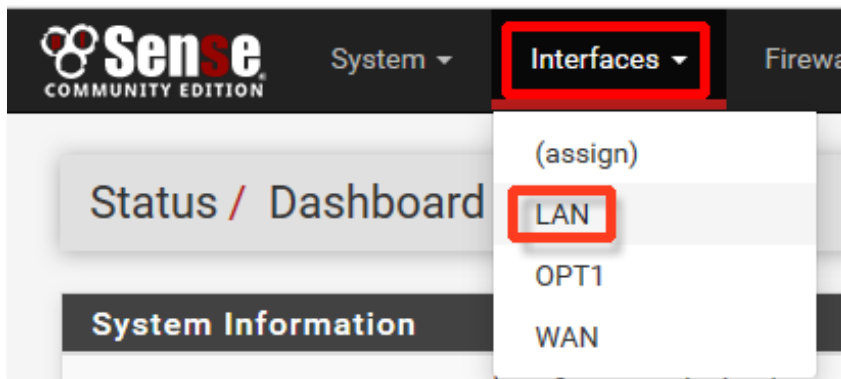
VMware Continuity Cloud Nodes

1. To access the console of your pfSense virtual firewall, open a web browser and go to the link provided by eFolder. It will look similar to the link below. This is a publicly accessible IP address, so you can access this URL from any computer with an internet connection. <https://CCNodeName.cc.sc.efsccloud.net:37038>
2. Next, enter the credentials you received from eFolder for your virtual firewall and click **Login**. Please note that the username and password are case sensitive.

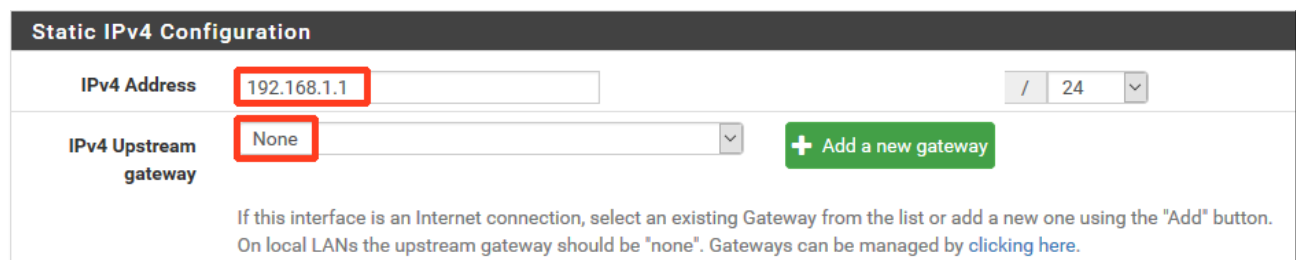
CONFIGURE THE LAN INTERFACE

Configure the LAN interface of the pfSense virtual firewall with the proper IP address and subnet mask required for the virtual machines you are restoring. This IP address will serve as the default gateway for all virtual machines you restore to the Continuity Cloud node.

1. From the menu, click on **Interfaces** and then select **LAN** from the drop-down list:



2. In the *Static IP Configuration* section of the page, enter the IP address for the virtual firewall:

A screenshot of the 'Static IPv4 Configuration' form in pfSense. The 'IPv4 Address' field contains '192.168.1.1' and the 'IPv4 Upstream gateway' dropdown is set to 'None'. Both fields are highlighted with red boxes. A green button labeled '+ Add a new gateway' is visible to the right. Below the form, there is a note: 'If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local LANs the upstream gateway should be "none". Gateways can be managed by clicking here.'

This IP address will become the default gateway IP for virtual machines on your LAN.

In the example shown above, the VM used to be on the network 192.168.1.0/24 (netmask 255.255.255.0) with the default gateway having an IP of 192.168.1.1.

3. Make sure that the *IP Upstream gateway* is set to **None**.



IMPORTANT: Do **not** check the **Block private networks and loopback addresses** option. This would block traffic from the WAN-DMZ. **Leave this box unchecked.**

Reserved Networks

Block private networks and loopback addresses	<input checked="" type="checkbox"/> <p>Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.</p>
Block bogon networks	<input type="checkbox"/> <p>Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. Note: The update frequency can be changed under System->Advanced Firewall/NAT settings.</p>

Click Save when you're finished.

CONFIGURE THE DHCP SERVER

Next, enable and configure the DHCP server (or leave it disabled within your environment.)

1. In the menu at the top of the page, choose **Services > DHCP Server**.

The screenshot shows the top navigation bar of the Sense Community Edition interface. The 'Services' menu is open, and 'DHCP Server' is highlighted with a red box. Other menu items include Captive Portal, DHCP Relay, DHCPv6 Relay, DHCPv6 Server & R, DNS Forwarder, DNS Resolver, Dynamic DNS, IGMP Proxy, Load Balancer, NTP, PPPoE Server, SNMP, UPnP & NAT-PMP, and Wake-on-LAN.

2. Click the LAN tab.

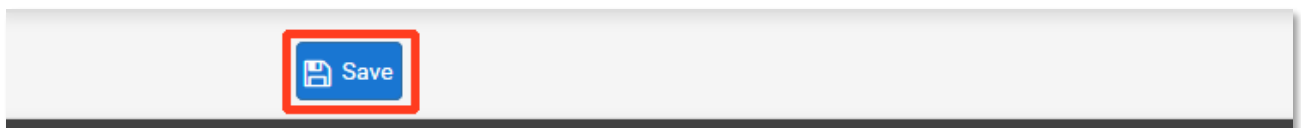
- If you do not want the firewall to act as a DHCP server, uncheck the **Enable** option.
- If you need a DHCP server on the LAN network, click the **Enable** box and then enter the **Range** of IPs the DHCP server should use in its pool.

General Options	
Enable	<input checked="" type="checkbox"/> Enable DHCP server on LAN interface
Deny unknown clients	<input type="checkbox"/> Only the clients defined below will get DHCP leases from this server.
Ignore denied clients	<input type="checkbox"/> Denied clients will be ignored rather than rejected. This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Subnet	192.168.1.0
Subnet mask	255.255.255.0
Available range	192.168.1.1 - 192.168.1.254
Range	<input type="text" value="192.168.1.100"/> <input type="text" value="192.168.1.199"/>
	From To

Note: Typically, you can leave the *DNS servers* entry blank, and eFolder's DNS infrastructure will automatically be used.

Servers	
WINS servers	<input type="text" value="WINS Server 1"/>
	<input type="text" value="WINS Server 2"/>
DNS servers	<input type="text" value="DNS Server 1"/>
	<input type="text" value="DNS Server 2"/>
	<input type="text" value="DNS Server 3"/>
	<input type="text" value="DNS Server 4"/>
Leave blank to use the system default DNS servers: this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the System / General Setup page.	

3. Click the Save button.



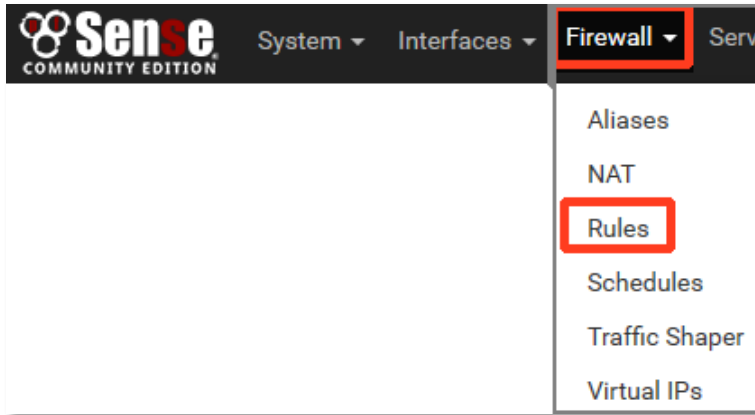
CONFIGURE FIREWALL RULES & NAT

Now, configure required firewall rules to allow external access to services running on your restored virtual machines.

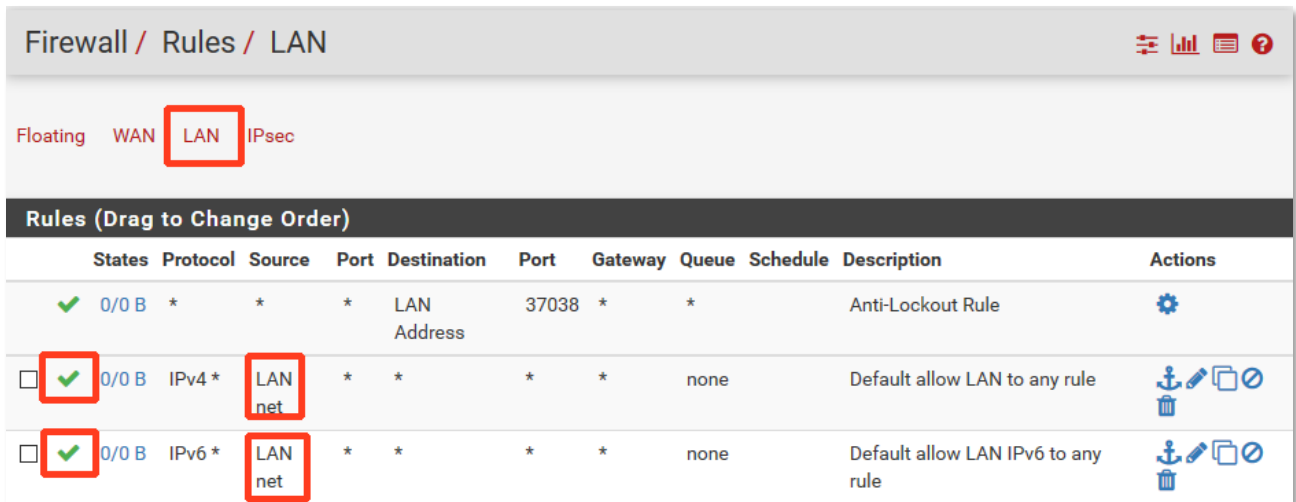
Set outbound traffic

By default, all outbound traffic is allowed.

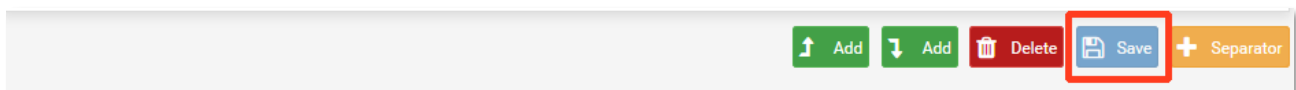
1. To disable all outbound traffic, browse to the *Firewall* menu and select *Rules*.



2. Click the LAN tab.
3. Find the rule(s) from the *Source LAN net* to any destination.
4. Click the green check mark on the left to disable the rule:



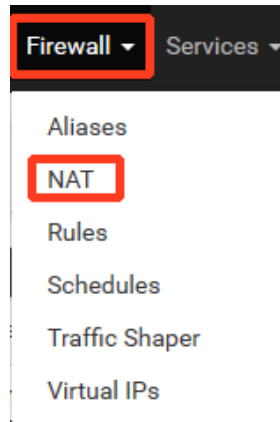
5. Finally, remember to click the *Save* button.



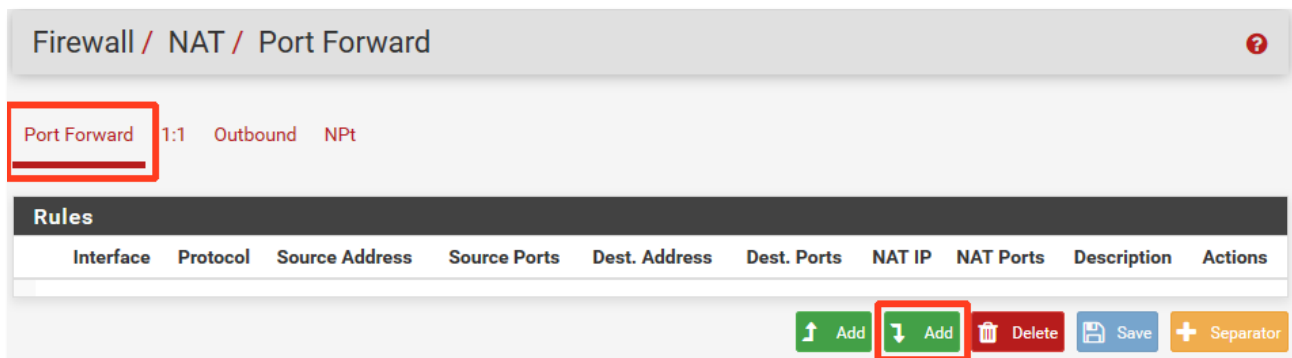
Port forwarding

Next, set up any ports to be forwarded from your assigned public IPs to internal IPs.

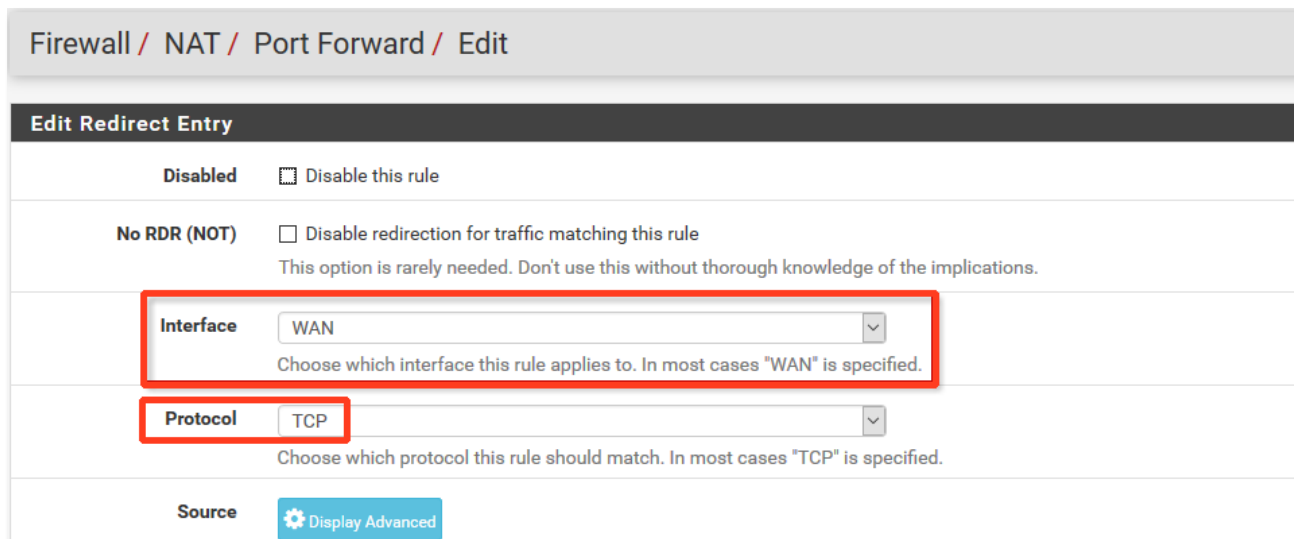
1. Click on **Firewall** in the main menu and select **NAT**.



2. Under the *Port Forward* tab, click the **Add** icon to add a new rule.



Normally, you should leave the *Interface* set to **WAN** and *Protocol* set to **TCP**:



3. For *Destination*, choose the proper IP address that corresponds to your desired public IP.

Note: The **WAN address** entry (shown) is your primary public IP. If you have additional public IP addresses assigned, they will be present at the bottom of the drop-down list.

The screenshot shows a configuration window for a firewall rule. The 'Destination' dropdown menu is open, listing various options. 'WAN address' is highlighted in blue. Other options include 'Any', 'Single host or alias', 'Network', 'This Firewall (self)', 'PPPoE clients', 'L2TP clients', 'WAN net', 'LAN net', 'LAN address', and '10.2.26.94 (Internal MGMT)'. The 'Destination' label is highlighted with a red box. Below the dropdown, there are fields for 'Destination port range' and 'Redirect target IP'.

In this example, we have selected the WAN IP as our **Destination**:

The screenshot shows the same configuration window. The 'Destination' dropdown menu is now closed, and 'WAN address' is selected and displayed in the field. The 'Destination' label and the dropdown menu are highlighted with a red box. Below this, there are fields for 'Destination port range' and 'Address/mask'.

4. Using the two **Destination port range** drop-down lists, select the protocol you want to forward from and to. You can also manually enter a range of ports. In this example, we are forwarding remote desktop:

The screenshot shows the configuration window with the 'Destination port range' section. Both the 'From port' and 'To port' dropdown menus are set to 'MS RDP'. Both dropdown menus are highlighted with a red box. Below this, there are fields for 'From port' and 'To port'.

- For the *Redirect target IP* and *Redirect target port*, enter the virtual LAN IP address of the server that should receive the forwarded traffic.

Note: The **Redirect target port** is normally the same as the **destination port**. (In this example, remote desktop):

Redirect target IP	<input type="text" value="192.168.1.12"/>
	Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12
Redirect target port	<input type="text" value="MS RDP"/> <input type="button" value="Custom"/>
	Port
	Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically). This is usually identical to the "From port" above.

- Typically, *NAT reflection* should be enabled with the **Use system default** setting.

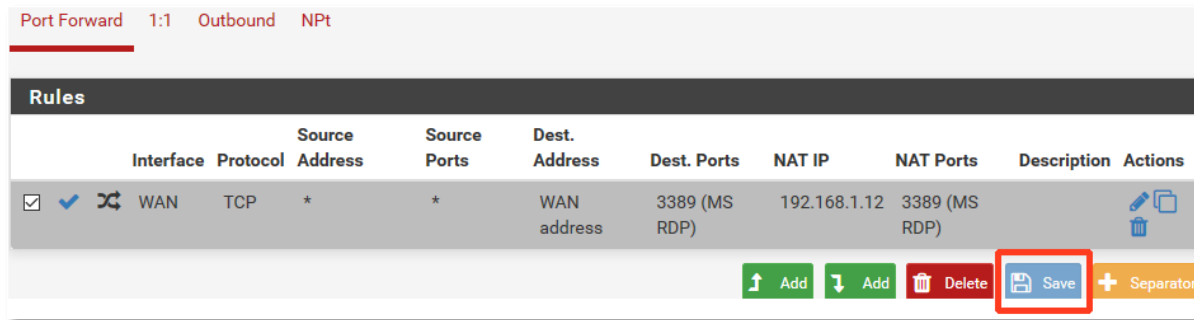
This allows servers in your internal LAN to connect to forwarded ports using your assigned public IPs. (This is sometimes called *NAT loopback*.) Note that this may not work in all scenarios.

NAT reflection	<input type="text" value="Use system default"/>
Filter rule association	<input type="text" value="Add associated filter rule"/>
	The "pass" selection does not work properly with Multi-WAN. It will only work on an interface containing the default gateway.

- The *Filter rule association* setting determines whether to automatically add a firewall rule allowing port-forwarded traffic. Select **Add associated filter rule**.

NAT reflection	<input type="text" value="Use system default"/>
Filter rule association	<input type="text" value="Add associated filter rule"/>
	The "pass" selection does not work properly with Multi-WAN. It will only work on an interface containing the default gateway.

8. After configuring the port forward rule, click **Save**. Then click **Apply Changes**.

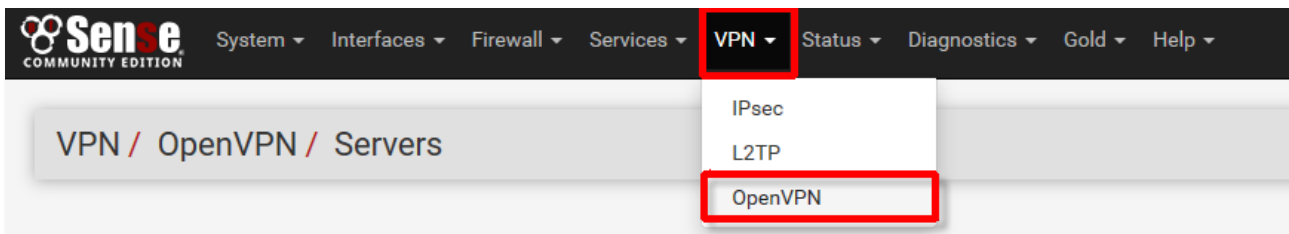


Repeat this for all ports that you want to forward. **Note:** You can also setup 1:1 NAT if desired. Normally you do not need to customize Outbound NAT.

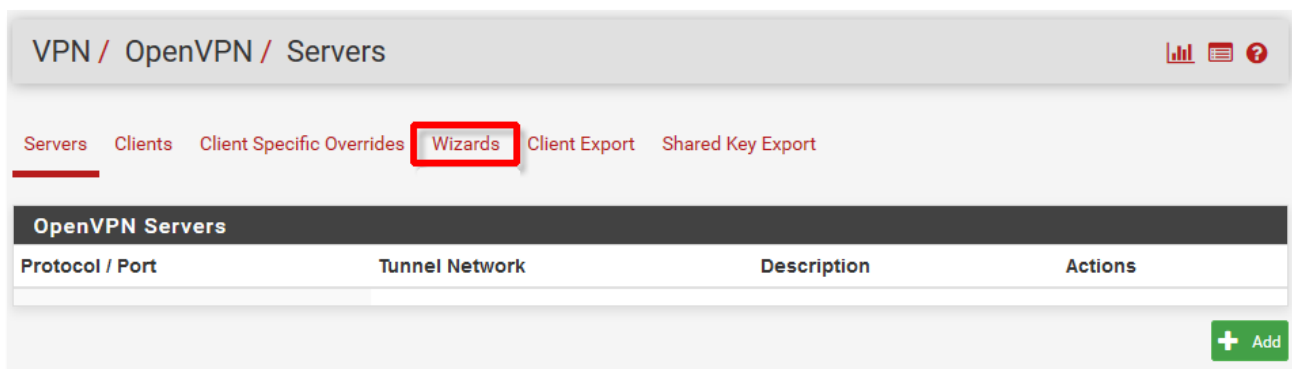
CONFIGURE THE OPENVPN SERVER

Configuring an OpenVPN Server allows remote users to access resources on the LAN side of the virtual firewall.

1. To access the OpenVPN configuration, go to the **VPN** drop-down menu on the main navigation bar and select **OpenVPN**.

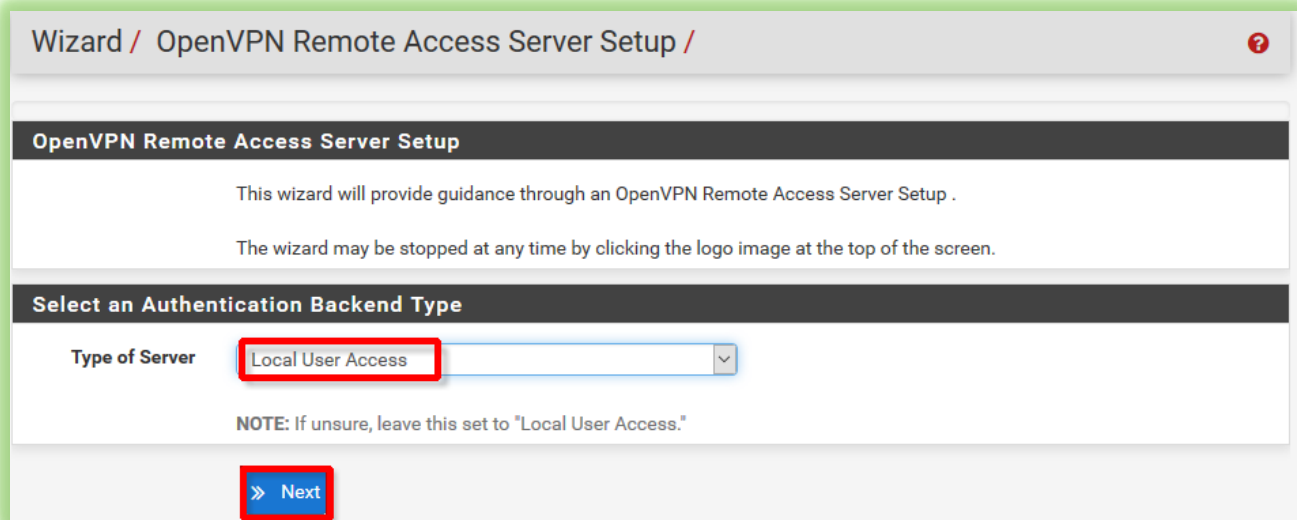


2. Any configured OpenVPN servers will be displayed. If none are present (as in the screenshot below), click on the **Wizards** tab on top to begin configuring a new server.



3. The *OpenVPN Remote Access Server Setup Wizard* will launch.

Under the *Type of Server* menu, select **Local User Access** and then click **Next**.



Add a new certificate authority (CA)

1. Enter your information in the form to generate a **new certificate authority (CA)**.
 - Ensure the **Key length** is set to 4096 bit.
 - All fields are required.

Create a New Certificate Authority (CA) Certificate

Descriptive name
A name for administrative reference, to identify this certificate. This is the same as common-name field for other Certificates.

Key length
Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see keylength.com

Lifetime
Lifetime in days. This is commonly set to 3650 (Approximately 10 years.)

Country Code
Two-letter ISO country code (e.g. US, AU, CA)

State or Province
Full State or Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario).

City
City or other Locality name (e.g. Louisville, Indianapolis, Toronto).

Organization
Organization name, often the Company or Group name.

E-mail
E-mail address for the Certificate contact. Often the e-mail of the person generating the certificate.

2. After all fields are complete, click **Add new CA**.

Add a new server certificate

1. Enter your information in the form to generate a **new server certificate**.
 - Ensure the Key length is set to 4096 bit.
 - All fields are required.

Create a New Server Certificate

Descriptive name	<input type="text" value="OpenVPNCert"/>
	A name for administrative reference, to identify this certificate. This is also known as the certificate's "Common Name."
Key length	<input type="text" value="4096 bits"/>
	Size of the key which will be generated. The larger the key, the more security it offers, but larger keys are generally slower to use.
Lifetime	<input type="text" value="3650"/>
	Lifetime in days. This is commonly set to 3650 (Approximately 10 years.)
Country Code	<input type="text" value="US"/>
	Two-letter ISO country code (e.g. US, AU, CA)
State or Province	<input type="text" value="GA"/>
	Full State of Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario).
City	<input type="text" value="Atlanta"/>
	City or other Locality name (e.g. Louisville, Indianapolis, Toronto).
Organization	<input type="text" value="eFolder"/>
	Organization name, often the Company or Group name.
E-mail	<input type="text" value="address@efolder.net"/>
	E-mail address for the Certificate contact. Often the e-mail of the person generating the certificate.

2. After all of the fields are complete, click **Create new Certificate**.

Configure General OpenVPN Server information

1. Set *Interface* to **WAN**.
2. Set *Protocol* to **TCP**.
3. Make sure the *Local Port* is set to **1194**.
4. Enter a **Description** for the OpenVPN server.

General OpenVPN Server Information	
Interface	<input type="text" value="WAN"/> ▼ The interface where OpenVPN will listen for incoming connections (typically WAN.)
Protocol	<input type="text" value="TCP"/> ▼ Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.
Local Port	<input type="text" value="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	<input type="text" value="CC Node 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.

Configure the Cryptographic Settings for OpenVPN connections

Use the settings as shown in the following screenshot:

1. Check the box by **TLS Authentication** to enable it.
2. Check the box by **Generate TLS Key** to enable it.
3. No *TLS Shared Key* is required. You may leave this field blank.
4. *DH Parameters Length* should be set to **4096 bit**.
5. Set *Encryption Algorithm* to **AES-256-CBC (256-bit)**.
6. For *Auth Digest Algorithm*, select **SHA1 (160-bit)**.
7. Select **No Hardware Crypto Acceleration** for *Hardware Crypto*.

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.

DH Parameters Length 4096 bit

Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure commu
larger values are more secure, but may be slower in operation.

Encryption Algorithm AES-256-CBC (256-bit)

The algorithm used to encrypt traffic between endpoints. This setting must match on the client
Certain algorithms will perform better on different hardware, depending on the availability of su

Auth Digest Algorithm SHA1 (160-bit)

The method used to authenticate traffic between endpoints. This setting must match on the cli
desired.

Hardware Crypto No Hardware Crypto Acceleration

The hardware cryptographic accelerator to use for this VPN connection, if any.

Configure Tunnel Settings

Use the settings as shown in the following screenshot:



Notes: Set *Tunnel Network* to the unique private network used for communication between the remote hosts and this OpenVPN server.

- Set *Local Network* to the LAN subnet of your pfSense firewall. This is the network that will be accessible to your remote hosts that connect to the Open VPN server.
- Ensure that *Concurrent Connections* is set high enough to accommodate the number of expected remote hosts.

All remaining fields should be left at their defaults, as shown below:

Tunnel Settings	
Tunnel Network	<input type="text" value="192.168.2.0/24"/> <small>This is the virtual network used for private communications between this server and client hosts. The first network address will be assigned to the server virtual interface. The remaining network addresses will be available to the clients. (see Address Pool)</small>
Redirect Gateway	<input type="checkbox"/> Force all client generated traffic through the tunnel.
Local Network	<input type="text" value="192.168.1.0/24"/> <small>This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. This is the local network through this tunnel on the remote machine. This is generally set to the LAN network.</small>
Concurrent Connections	<input type="text" value="50"/> <small>Specify the maximum number of clients allowed to concurrently connect to this server.</small>
Compression	<input type="text" value="No Preference"/> <small>Compress tunnel packets using the LZO algorithm. Adaptive compression will dynamically detect and compress data in the packets if it detects that the data in the packets is not being compressed efficiently.</small>
Type-of-Service	<input type="checkbox"/> Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.
Inter-Client Communication	<input type="checkbox"/> Allow communication between clients connected to this server.
Duplicate Connections	<input type="checkbox"/> Allow multiple concurrent connections from clients using the same Common Name. <small>NOTE: This is not generally recommended, but may be needed for some scenarios.</small>

Configure Client Settings

1. Enable **Dynamic IP** by checking the box.
2. Enable **Address Pool** by checking the box.
3. Set **Topology** to **Subnet – One IP address per client in a common subnet**.
4. Set **DNS Default Domain** to the domain name you want appended to the connection for remote hosts.
5. Set **DNS Server 1** to the IP address of the remote DNS server you want remote hosts to use for name resolution.

Client Settings

Dynamic IP Allow connected clients to retain their connections if their IP address changes.

Address Pool Provide a virtual adapter IP address to clients (see Tunnel Network).

Topology Subnet – One IP address per client in a common subnet
Specifies the method used to supply a virtual adapter IP address to clients when using Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Conn Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may requir

DNS Default Domain domainname.com
Provide a default domain name to clients.

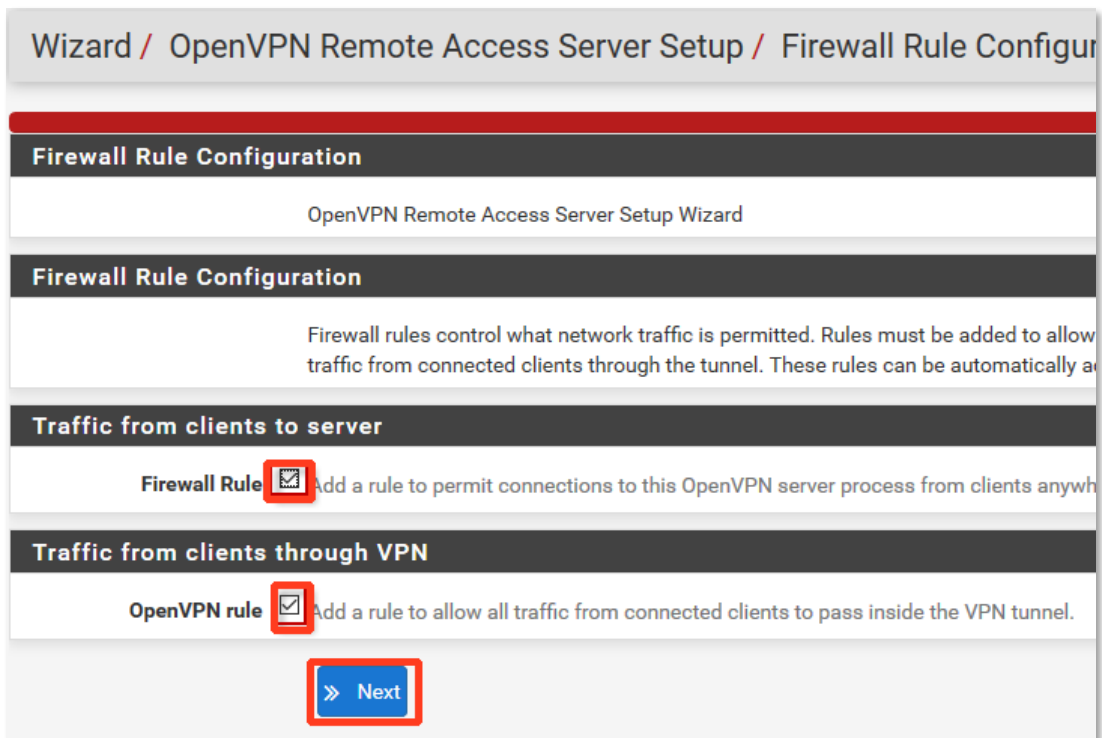
DNS Server 1 192.168.1.1
DNS server IP to provide to connecting clients.

6. Enable **NetBIOS over TCP/IP** to allow for propagation of NetBIOS traffic over the VPN connection.

NetBIOS enable Enable NetBIOS over TCP/IP
If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.

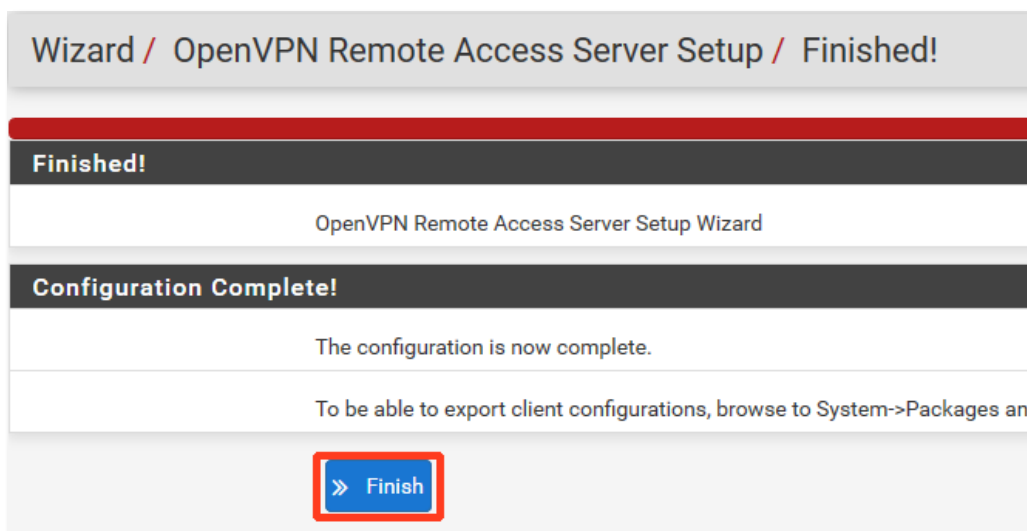
After all *Client Setting* fields are configured, click **Next**.

7. On the *Firewall Rule Configuration* screen:
 - a) Check the **Traffic from clients to server** checkbox.
 - b) Check the **Traffic clients through VPN** checkbox.
 - c) Then click **Next**.

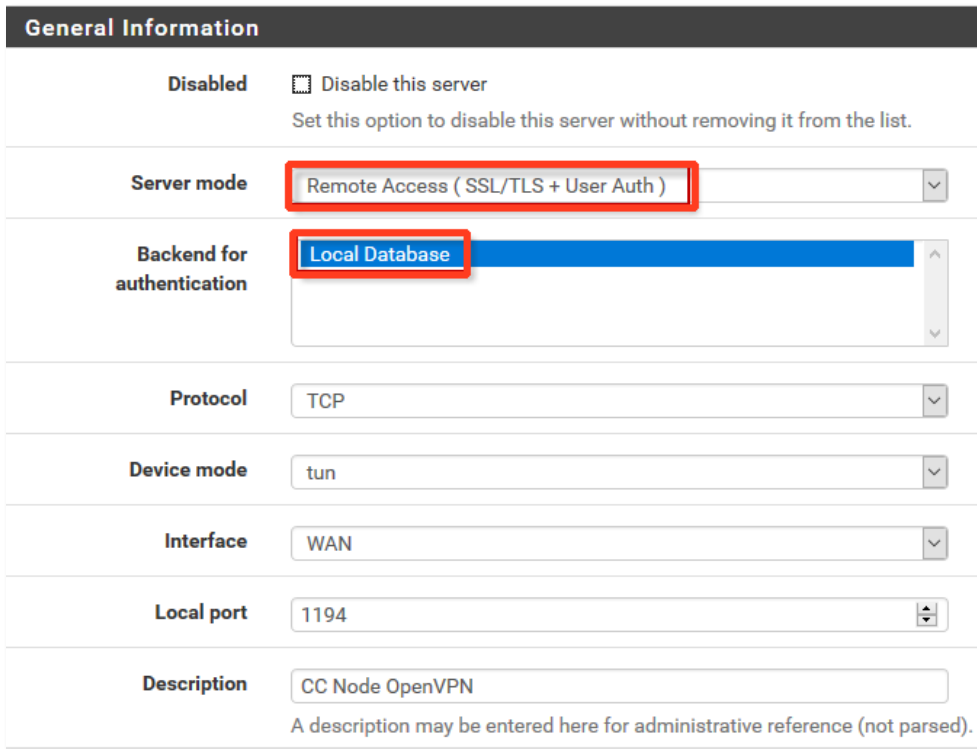


These settings open all traffic to and from remote hosts connected over the VPN connection.

Next, click **Finish** on the completion screen.



8. Finally, verify these two settings:
 - a. OpenVPN server has *Server mode* set to **Remote Access (SSL/TLS+User Auth)**
 - b. **Local Database** is selected as *Backend for authentication*.



General Information

Disabled Disable this server
Set this option to disable this server without removing it from the list.

Server mode Remote Access (SSL/TLS + User Auth)

Backend for authentication Local Database

Protocol TCP

Device mode tun

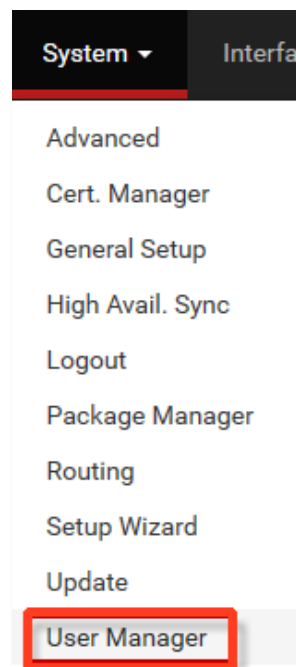
Interface WAN

Local port 1194

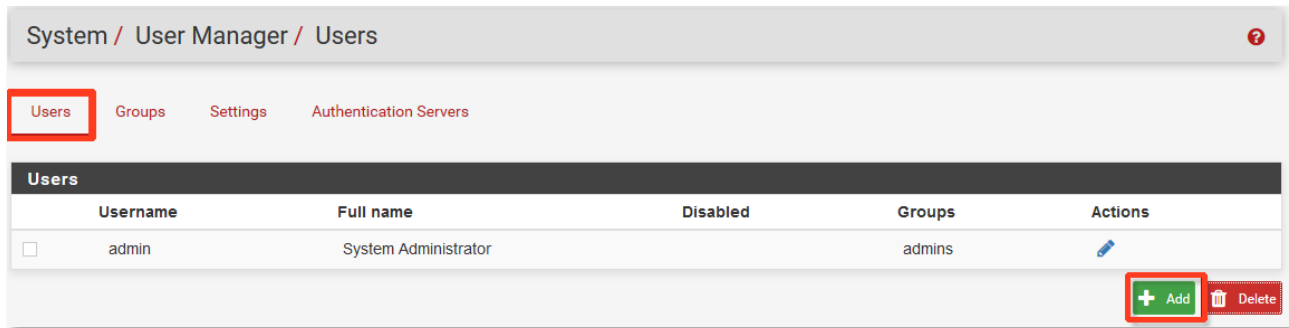
Description CC Node OpenVPN
A description may be entered here for administrative reference (not parsed).

SET UP REMOTE USER ACCOUNTS

1. Hover over *System* in the navigation bar and select **User Manager**:



2. On the Users tab, select the add user button in the bottom right corner.



3. Set the Username and Password for the new user. Enter a Full name for reference, if needed.

User Properties

Defined by USER

Disabled This user cannot login

Username

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

Then click Save.

Keys

Authorized SSH Keys

Enter authorized SSH keys for this user

IPsec Pre-Shared Key

Save

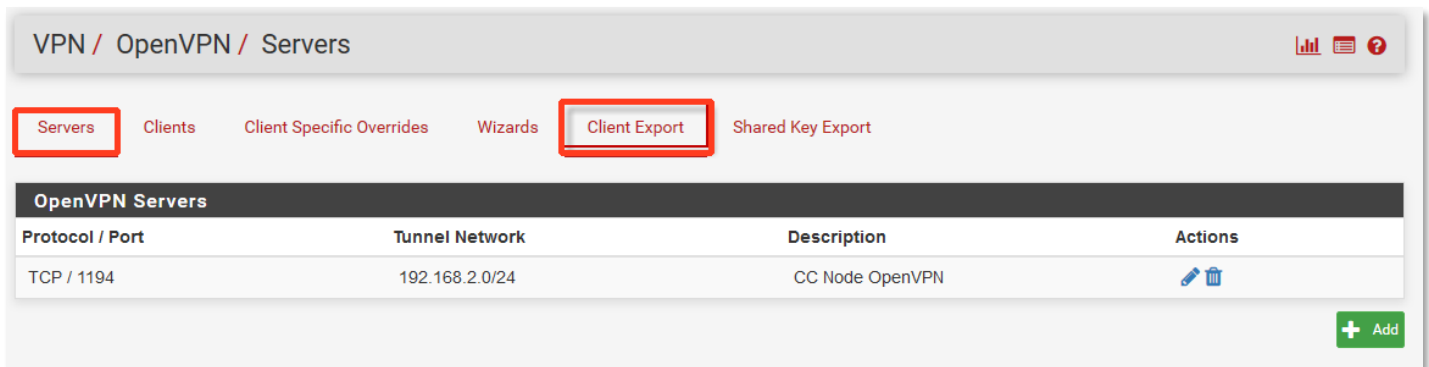
The new user account will now be listed under the Username tab of the User Manager.

Username	Full name	Disabled
<input type="checkbox"/> admin	System Administrator	
<input checked="" type="checkbox"/> testuser	Test User	



DOWNLOAD A CONFIGURED OPEN VPN INSTALLER

1. To download a fully configured OpenVPN Client software installer, browse to the *OpenVPN Server manager* and click the **Client Export** tab.

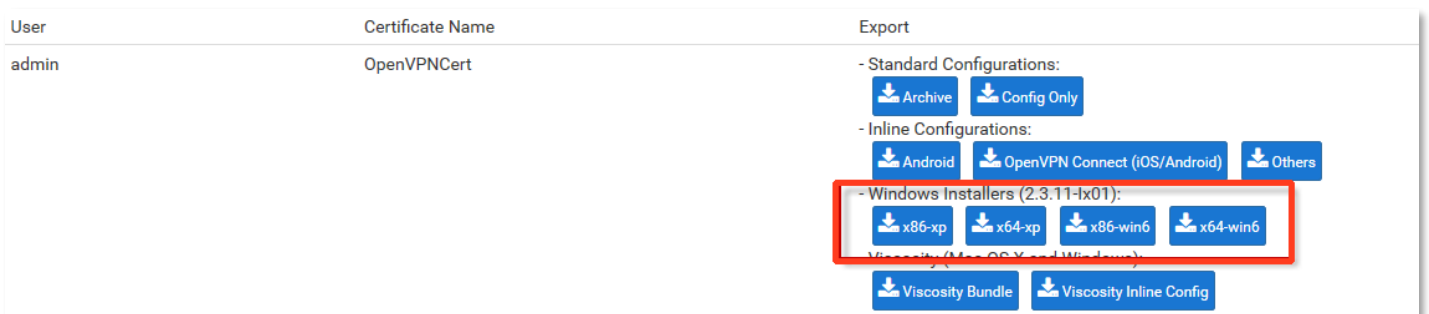
NOTE: This installer will fully install and configure the client software to a remote host. Users will only need to enter their username and password after installation.






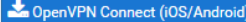


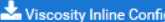
The screenshot shows the 'VPN / OpenVPN / Servers' interface. The 'Client Export' tab is highlighted with a red box. Below the tabs, there is a table of OpenVPN Servers. The table has four columns: Protocol / Port, Tunnel Network, Description, and Actions. One server is listed: TCP / 1194, 192.168.2.0/24, CC Node OpenVPN. A green '+ Add' button is visible at the bottom right.

Protocol / Port	Tunnel Network	Description	Actions
TCP / 1194	192.168.2.0/24	CC Node OpenVPN	 

2. Under the *Client Install Packages* section, select the appropriate x86 or x64 client software installer that you want to distribute to your remote users.



The screenshot shows the 'Client Install Packages' section. The 'Export' column contains several download buttons. The 'Windows Installers (2.3.11-ix01)' section is highlighted with a red box. It includes buttons for x86-xp, x64-xp, x86-win6, and x64-win6.

User	Certificate Name	Export
admin	OpenVPNCert	<p>- Standard Configurations:  </p> <p>- Inline Configurations:   </p> <p>- Windows Installers (2.3.11-ix01):    </p> <p>Viscosity (Mac OS X and Windows)  </p>

IPSEC VPN

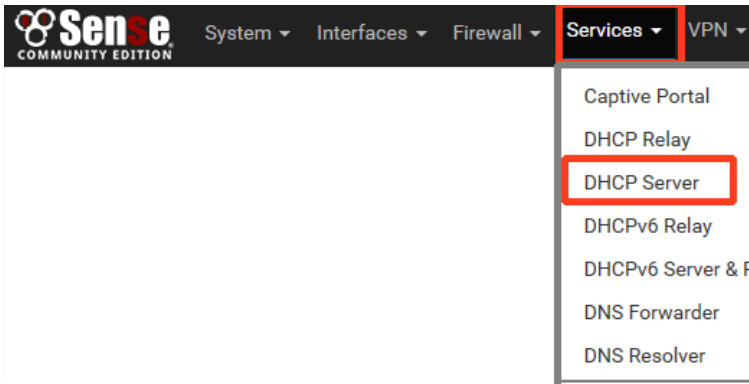
If you want to tie your virtual LAN to your actual LAN through an IPsec site-to-site VPN tunnel, please see the detailed instructions at:

http://doc.pfsense.org/index.php/VPN_Capability_IPsec

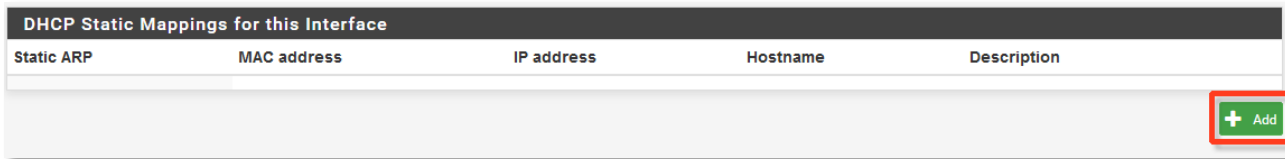
USE STATIC IP ADDRESSES

You can set up pfSense to allow servers with static IP's access to the internet.

1. Identify the MAC address of the VM you'll be assigning a static IP address to.
2. Login into pfSense.
3. Click on the *Services* tab then select DHCP Server.



4. Once the DHCP server screen comes up, click the LAN tab in the upper left.
5. Make note of the DHCP range. (Usually between 192.1681.100 and .199).
IPs that are to be statically assigned to servers must not fall within the DHCP range.
6. Scroll down to *DHCP Static Mappings for this Interface*.
7. Click Add to add a static IP entry.



8. In the **MAC Address** field (a) add the MAC address of the computer assigned the static IP address, then (b) add the IP address assigned to the computer on the IP address sections.

A screenshot of the 'Static DHCP Mapping on LAN' form. The 'MAC Address' field is highlighted with a red box and contains 'XXXXXXXX:XXXX'. Below it is a 'Copy My MAC' button. The 'IP Address' field is also highlighted with a red box. Below the IP field is a note: 'If an IPv4 address is entered, the address must be outside of the pool. If no IPv4 address is given, one will be dynamically allocated from the pool.' Other fields include 'Client Identifier', 'Hostname', and 'Description'.



9. Click Save

10. Test the server with the static IP assigned to it. At this point, you should have internet access.

CONCLUSION

Congratulations! You have now completed the eFolder Continuity Cloud Virtual Firewall setup.

If you have any problems during this procedure or notice errors in the log file, please call eFolder Technical Support at 678-373-0109 or 1-800-352-0248 or submit questions to support@efolder.net.

Additional Assistance

At eFolder, we value feedback from our customers.

Not only do we want to help you quickly resolve your technical issues, we value your input and build our products to incorporate your suggestions.

- To contact eFolder Technical Support, call 678-373-0109 or 1-800-352-0248
- Submit questions to support@efolder.net
- For how-to articles and FAQ, see the pfSense documentation at: https://doc.pfsense.org/index.php/Main_Page
- Additional material is available in the [eFolder Partner Portal](#)
- The eFolder Support page is at <http://www.efolder.net/support/>

