

Manual for setting up a firewall with pfSense

Table of contents

Introduction.....	3
1. Installation.....	4
2. Allowing connection based on protocol.....	6
3. Syncing one pfSense with another for redundancy (High Availability Cluster)	9

Introduction

This document will explain how to setup a pfSense. This manual is a basic manual, if you want more specific information, you can go to <https://docs.netgate.com/pfsense/en/> this site has a more in-depth explanation.

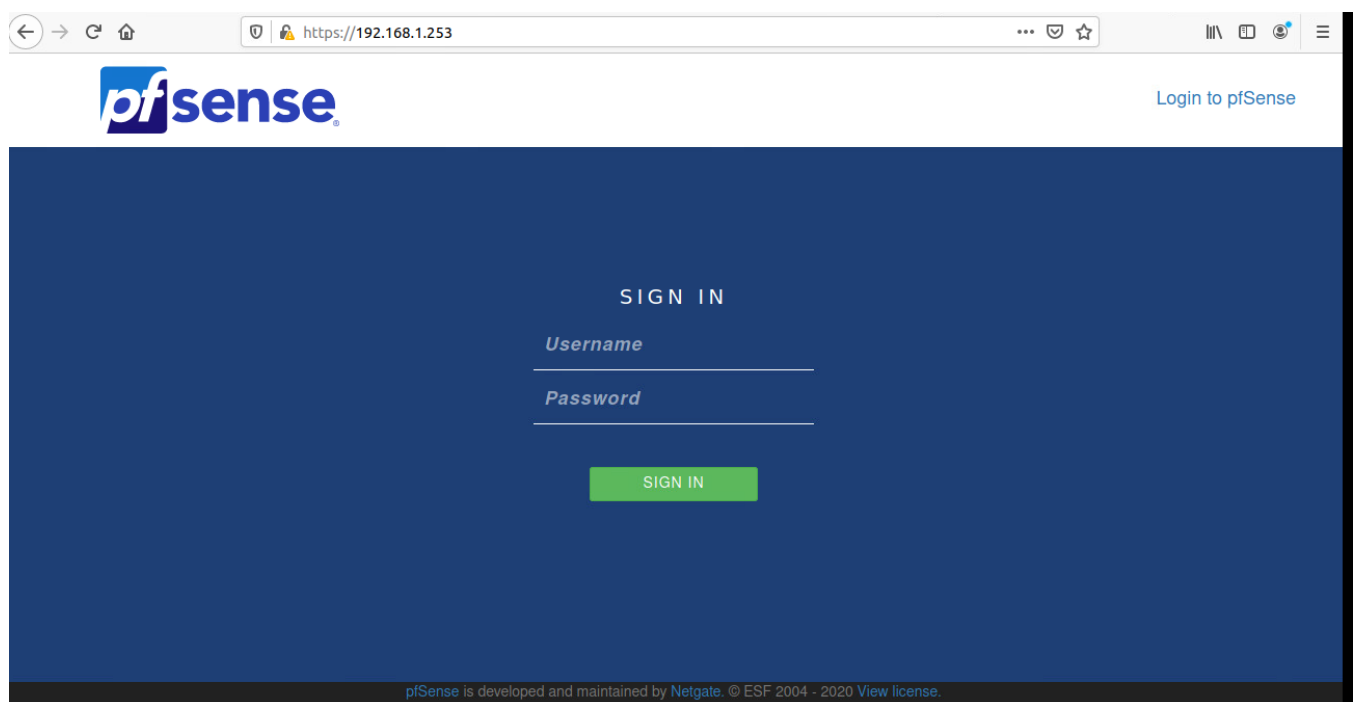
1. Installation

To install Pfsense, you will need to download the iso file which you can find at <https://www.pfsense.org/download/>.

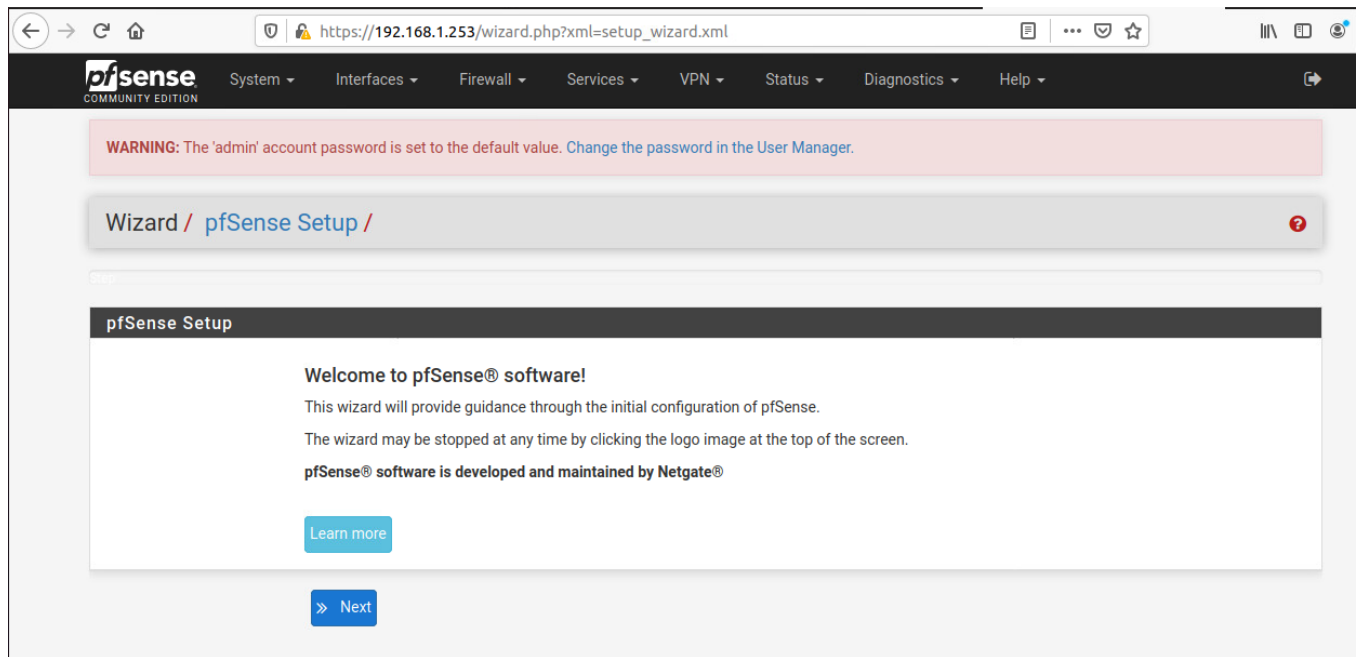
After you've done the installation of pfSense, you will be prompt with some questions.

First you have to choose which network adapter is the WAN and which one is the LAN. After that you can assign the ip address by giving in the number 2 and press enter.

After you've setup the ip address, you can surf via the LAN address to the website of the pfSense for setting up.



The default username is admin and the password is pfSense, it is recommended to change the default password for security reasons. After you've logged in, there is a possibility to use the install wizard, but we will setup the pfSense without it.



2. Allowing connection based on protocol

With pfSense all connection will be dropped by default. You will have to open some ports. Allow for example HTTPS connection, click on the firewall tab and click on rules.

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Firewall / Rules / Edit

Edit Firewall Rule

Action Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

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

Interface WAN
Choose the interface from which packets must come to match this rule.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol TCP
Choose which IP protocol this rule should match.

Source

Source ☐ Invert match any Source Address /

[Display Advanced](#)

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination ☐ Invert match any Destination Address /

Destination Port Range HTTP (80) HTTP (80)
From Custom To Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

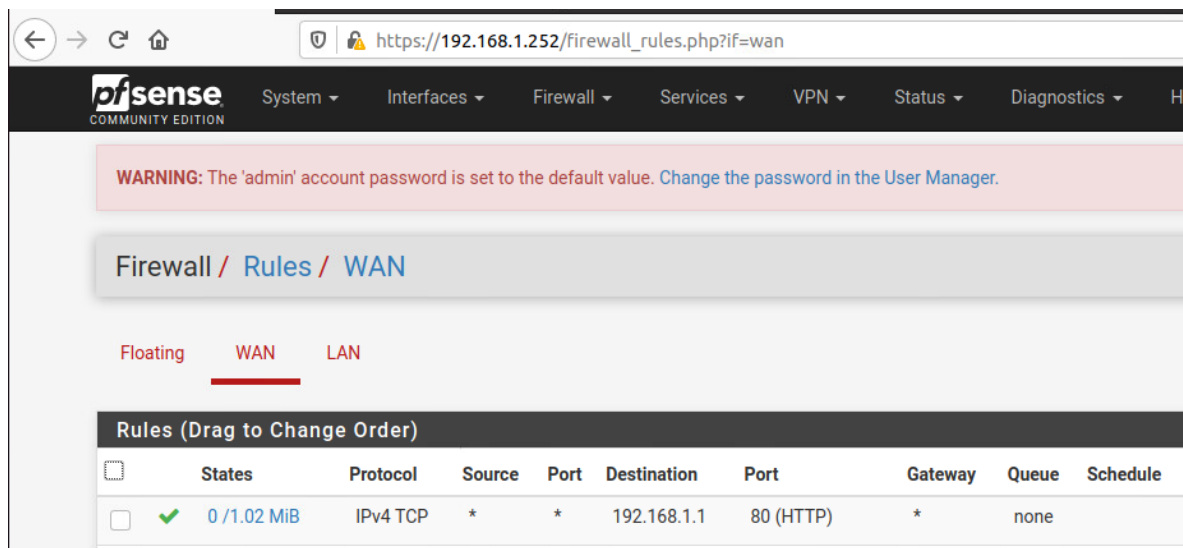
Extra Options

Log ☐ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description

Click on save to use the settings.

You can now see the rule has been added.



For our system in particular, we are going to use port forwarding NAT. Click on the tab firewalls and then on NAT.

Here you can add a rule for port forwarding. For example we want a HTTP connection to connect our internal server with ip address 192.168.1.1

You can click on add to add a rule. Next you will see a page where you can setup the rule.

Here you can put the ports and ip addresses. The redirect target IP should be the address of the internal ip address if the server you want it to connect to.

Destination port range Other Other
From port Custom To port Custom
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP
Enter the internal IP address of the server on which to map the ports.
e.g.: 192.168.1.12

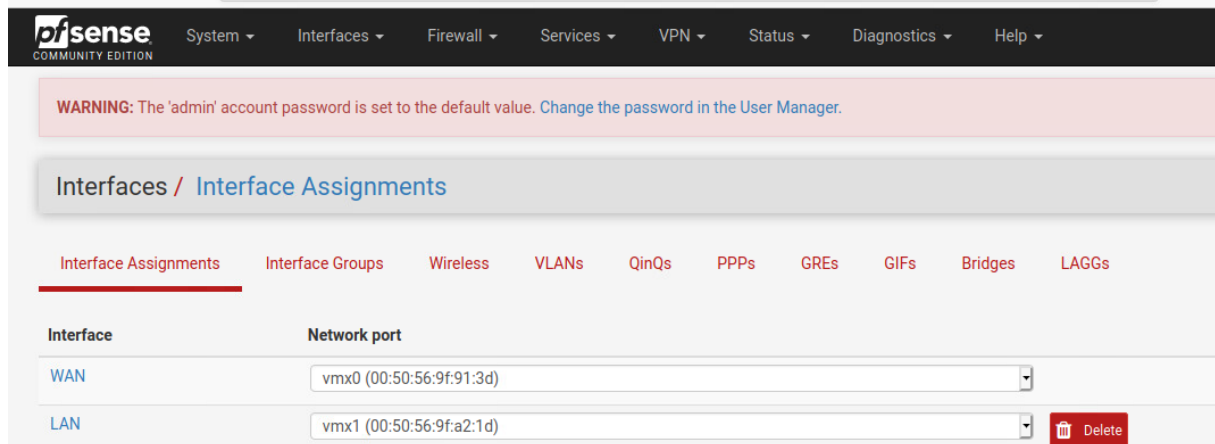
Redirect target port Other
Port Custom
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
This is usually identical to the "From port" above.

For example if you want to connect to website on a server via WAN with an internal address of 192.168.1.1. Then this would be your setting.

Protocol	TCP		
Choose which protocol this rule should match. In most cases "TCP" is specified.			
Source	Display Advanced		
Destination	<input type="checkbox"/> Invert match.	WAN address	
		Type	Address/mask
Destination port range	HTTP		HTTP
	From port	Custom	To port
	Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.		
Redirect target IP	192.168.1.1		
	Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12		
Redirect target port	HTTP		
	Port	Custom	
	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.		

3. Syncing one pfSense with another for redundancy (High Availability Cluster)

You can create a dedicated interface on both pfSense for synchronisation, this would be more preferable. In the interface tab you can add more interfaces to the settings.

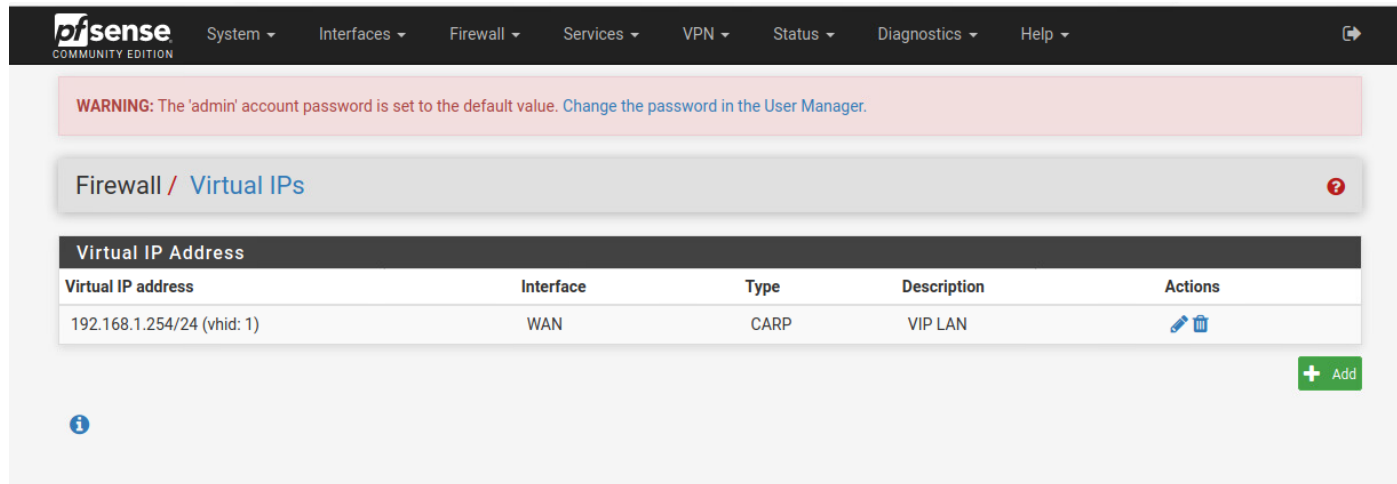


After you've setup the interfaces, you will have to allow them to communicate with each other. You can do this by making a firewall rule between the two interfaces.

Next we need a virtual ip address for CARP. This allows the use of one 1 ip address for the 2 firewalls. One pfSense will be active and the other will be on standby.

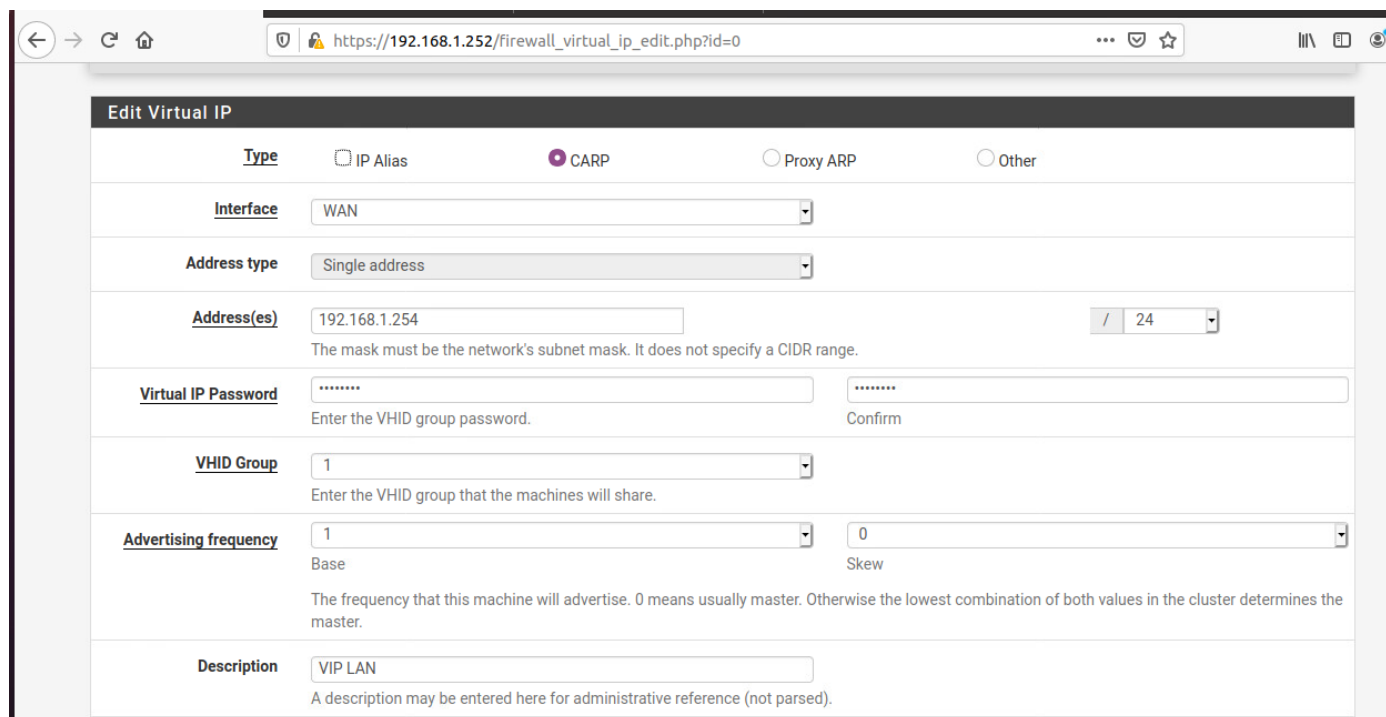
We also will be needing synchronisation, this allows us to only setup one pfSense and the other pfSense will have the same configuration/rules.

Here you can see an example.



The screenshot shows the pfSense web interface. At the top is a navigation bar with links: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below the navigation bar is a warning message: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." The main content area is titled "Firewall / Virtual IPs". Below this is a table titled "Virtual IP Address". The table has five columns: "Virtual IP address", "Interface", "Type", "Description", and "Actions". There is one row in the table with the following data: "192.168.1.254/24 (vhid: 1)", "WAN", "CARP", "VIP LAN", and a link icon. At the bottom right of the table is a green button with a plus sign and the text "Add".

Virtual IP Address	Interface	Type	Description	Actions
192.168.1.254/24 (vhid: 1)	WAN	CARP	VIP LAN	Edit Delete



The screenshot shows the "Edit Virtual IP" form in the pfSense web interface. The form is for a CARP virtual IP on the WAN interface. The form has the following fields and values:

- Type:** CARP (selected)
- Interface:** WAN
- Address type:** Single address
- Address(es):** 192.168.1.254 / 24
- Virtual IP Password:** (password field) Confirm
- Vhid Group:** 1
- Advertising frequency:** 1 (Base) 0 (Skew)
- Description:** VIP LAN

The form also includes a note: "The mask must be the network's subnet mask. It does not specify a CIDR range." and "A description may be entered here for administrative reference (not parsed)."

You will also have to create a WAN VIP address.

What we now have to do is turn on high availability sync. Click on systems and then on high availability sync.

One your first pfSense you setup, you will have to use the ip address of you second pfSense

And you will also need to give the login and password of the second pfSense.

System / High Availability Sync

State Synchronization Settings (pfsync)

Synchronize states

☒ pfsync transfers state insertion, update, and deletion messages between firewalls.
Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table.
This setting should be enabled on all members of a failover group.
Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)

Synchronize Interface

If Synchronize States is enabled this interface will be used for communication.
It is recommended to set this to an interface other than LAN! A dedicated interface works the best.
An IP must be defined on each machine participating in this failover group.
An IP must be assigned to the interface on any participating sync nodes.

pfsync Synchronize Peer IP

Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

Configuration Synchronization Settings (XMLRPC Sync)

Synchronize Config to IP

Enter the IP address of the firewall to which the selected configuration sections should be synchronized.

XMLRPC sync is currently only supported over connections using the same protocol and port as this system - make sure the remote system's port and protocol are set accordingly!
Do not use the Synchronize Config to IP and password option on backup cluster members!

Remote System Username

admin

Enter the webConfigurator username of the system entered above for synchronizing the configuration.
Do not use the Synchronize Config to IP and username option on backup cluster members!

Remote System Password

Enter the webConfigurator password of the system entered above for synchronizing the configuration.
Do not use the Synchronize Config to IP and password option on backup cluster members!

Confirm

On the second pfSense you will just have to fill in the first part, with the ip address of the first pfSense. (Only State sync settings)

You should now see on the second pfSense that the rules of pfSense 1 has been added to the second pfSense.

The pfSense have now been setup and you now have firewall protection.