

Instructions for configuring pfSense 2.0 Cluster using CARP

pfSense is an open source application with routing functions for free and powerful firewalls that will allow you to expand your network without compromising security.

TipsMake.com - pfSense is an open source application that has routing functions for free and powerful firewalls, which will allow you to expand your network without compromising security. With its many advantages, it should be popular everywhere, from private homes to businesses. In the following article, I will show you how to configure a pfSense 2.0 Cluster using CARP Failover.

System requirements

To accomplish this process we need two identical computers, with a minimum of 3 network cards and a subnet dedicated to network traffic synchronization.

For example, the IP address will be used in the article:

Network configuration:

Firewall 1

WAN IP: 192.168.100.1

SYNC IP: 10.155.0.1

LAN IP: 192.168.1.252 Firewall 2

WAN IP: 192.168.100.2

SYNC IP: 10.155.0.2

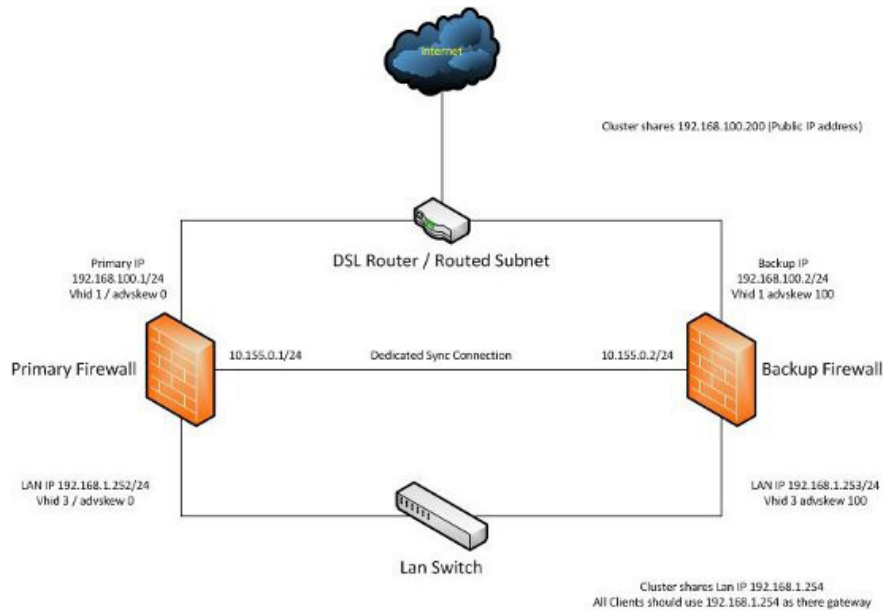
LAN IP: 192.168.1.253

The following two IP addresses are used for sharing between firewalls:

1. IP virtual WAN: *192.168.100.200*
2. Virtual LAN IP: *192.168.1.254*

This tutorial assumes that you have pfSense preinstalled on both computers and network cards configured with IP addresses . and experienced users work with pfSense (mostly around interfaces). Webmasters).

Illustrative example of the model we build:



Building Cluster

First you need to configure a firewall rule on both boxes to allow firewalls to communicate with each other on the **SYNC** card.

To do this, click on " **Firewall | Rules** ", select **SYNC** at **Interface** . Click the **Plus** button to add a new firewall rule entry. Set " **Protocol** "for" **any** ", add a description to be able to identify Click **Save** , then click **Apply Changes** if necessary.

Firewall: Rules: Edit	
Action	Pass <small>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. Reject only works when the protocol is set to either TCP or UDP (but not "TCP/UDP") below.</small>
Disabled	<input type="checkbox"/> Disable this rule <small>Set this option to disable this rule without removing it from the list.</small>
Interface	SYNC <small>Choose on which interface packets must come in to match this rule.</small>
Protocol	any <small>Choose which IP protocol this rule should match. Hint: in most cases, you should specify TCP here.</small>

Still on the firewall backup, here we need to configure **CARP** synchronization and configure it to be just a copy. Click " **Firewall | Virtual IPs** "> " **Firewall | Virtual Ips** ", check the box " **Synchronize Enabled** ". Select " **Synchronize Interface to SYNC** ", then save this change.

Services: CARP Settings: Edit

Virtual IPs	CARP Settings
Synchronize Enabled	<input checked="" type="checkbox"/> 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. NOTE: Clicking save will force a configuration sync!
Synchronize Interface	SYNC If Synchronize State is enabled, it will utilize this interface for communication. NOTE: We recommend setting this to a interface other than LAN! A dedicated interface works the best. NOTE: You must define a IP on each machine participating in this fallover group. NOTE: You must have an IP assigned to the interface on any participating sync nodes.

Completing the configuration of the firewall backup, we now proceed to configure CARP synchronization on the main firewall.

Log in to your main firewall, click " **Firewall | Virtual Ips** ", switch to the " **CARP Settings** " tab and check the " **Synchronize Enabled** " box. In the **Synchronize Interface** section, select " **SYNC** " as the default, check the boxes under " *Synchronize Rules* ", " *Synchronize NAT* ", " *Synchronize Virtual IPs* ".

Then enter the *SYNC IP address* of the firewall copy into the " **Synchronize to IP** " box and set the password at the " **Remote System Password** " box.

Services: CARP Settings: Edit

Virtual IPs	CARP Settings
Synchronize Enabled	<input checked="" type="checkbox"/> 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. NOTE: Clicking save will force a configuration sync!
Synchronize Interface	SYNC If Synchronize State is enabled, it will utilize this interface for communication. NOTE: We recommend setting this to a interface other than LAN! A dedicated interface works the best. NOTE: You must define a IP on each machine participating in this fallover group. NOTE: You must have an IP assigned to the interface on any participating sync nodes.
pFSync sync peer IP	<input type="text"/> Setting this option will force pFSync to synchronize its stable tables to this IP address. The default is directed multicast.
Synchronize rules	<input checked="" type="checkbox"/> When this option is enabled, this system will automatically sync the firewall rules over to the other CARP host when changes are made.
Synchronize NAT	<input checked="" type="checkbox"/> When this option is enabled, this system will automatically sync the NAT configuration to the other CARP host when changes are made.
Synchronize Virtual IPs	<input checked="" type="checkbox"/> When this option is enabled, this system will automatically sync the CARP Virtual IPs to the other CARP host when changes are made.
Synchronize to IP	10.155.0.2 Enter the IP address of the firewall you are synchronizing with.
Remote System Password	***** Enter the webGUI password of the system that you are synchronizing with.

Click **Save** to save the changes.

Next we configure Virtual IP address for both firewalls to use. To do this go to " **Firewall | Virtual IPs** " and switch to the " **Virtual Ips** " tab.

First, set the IP address for the **WAN** of **Interface** section, click the **Plus** button to add a new IP IP, make sure the IP type is set at **CARP** . This WAN address will be used throughout your system regardless of whether the

primary firewall or replica is enabled.

Next create a password in the " **Virtual IP Password** " box, keep the value of " **VHID Group** " and the " **Advertising Frequency** " value **0** , add a little description in the **Description** and click Save to save.

Firewall: Virtual IP Address: Edit

Type	<input type="radio"/> Proxy ARP <input checked="" type="radio"/> CARP <input type="radio"/> Other
Interface	WAN
IP Address(es)	Type: Single address Address: 192.168.100.200 / 24 <small>This is the network's subnet mask. It does not specify a CIDR range.</small>
Virtual IP Password	Enter the VHID group password.
VHID Group	1 Enter the VHID group that the machines will share
Advertising Frequency	0 The frequency that this machine will advertise. 0 = master. Anything above 0 designates a backup.
Description	Virtual IP - WAN Address You may enter a description here for your reference (not parsed).

Similarly, we configure **Virtual IP address** for **LAN** in **Interface** section. The steps are not different from the above instructions for the WAN, the ' **VHID Group** ' instead of **3** , put another description and click **Save** to save the changes.

Firewall: Virtual IP Address: Edit

Type	<input type="radio"/> Proxy ARP <input checked="" type="radio"/> CARP <input type="radio"/> Other
Interface	LAN
IP Address(es)	Type: Single address Address: 192.168.1.254 / 24 <small>This is the network's subnet mask. It does not specify a CIDR range.</small>
Virtual IP Password	Enter the VHID group password.
VHID Group	3 Enter the VHID group that the machines will share
Advertising Frequency	0 The frequency that this machine will advertise. 0 = master. Anything above 0 designates a backup.
Description	Virtual IP - LAN Address You may enter a description here for your reference (not parsed).

And now you will see in the " **Firewall | Virtual IPs** " section a list of two virtual IPs appears in the type of **CARP** .

Firewall: Virtual IP Addresses

Virtual IPs **CARP Settings**

Virtual IP address	Type	Description
192.168.100.200/24 (vhid 1)	CARP	Virtual IP - WAN Address
192.168.1.254/24 (vhid 3)	CARP	Virtual IP - LAN Address

Note:
The virtual IP addresses defined on this page may be used in NAT mappings.
You can check the status of your CARP Virtual IPs and interfaces here.

If you log into the backup site's web interface and click on " **Firewall | Virtual IPs** " you will see **virtual IPs** in sync with the backup firewall.

Now is the time to see how it works. Two pfSense firewalls will continuously synchronize their rules, NAT, virtual IPs and any other settings you've selected in the Synchronize option. For some reason the main firewall is deactivated, its copy still works continuously.

Under test conditions, copies of the firewall will receive for a minimum of 10 seconds, because the freeBSD operating system will apply virtual IP addresses to the interface once it is disconnected from the main firewall.

Test Failover

You can test it by unplugging the network cable or turning off the main firewall while continuously pinging the IP address of the LAN or WAN. You will see the IPs drop to a few seconds in other firewalls.

You finished reading the article "**Instructions for configuring pfSense 2.0 Cluster using CARP**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.