



Published on Free Software Magazine (<http://www.freesoftwaremagazine.com>)

Configure a professional firewall using pfSense

Set up multiple subnets to share your broadband Internet with your neighbors and split the cost

By [Sloan Miller](#)

The guide will take you through the setup of the pfSense firewall with one WAN interface, one LAN interface and one Opt1-WiFi Interface.

This guide was written for Linksys, Netgear, and D-link users with no firewall or router experience. No experience is needed with FreeBSD or GNU/Linux to install and run pfSense. When you are finished, management of pfSense will be from a web interface just like any of the SOHO firewall/router appliances.

pfSense is a web-based firewall project that is similar, in terms of functionality, to the software in firewall appliances sold by Linksys, Netgear and D-Link. pfSense covers all the basic requirements offered by those appliances but offers so much more—in fact, it is really in a class by itself since it would be very difficult to find a commercial alternative that would provide what pfSense has to offer (or, anything cheaper than \$2,000–\$5,000).

As mentioned above, in this article I will explain how to setup the pfSense firewall with one WAN interface, one LAN interface and one Opt1-WiFi Interface. This set-up allows you to offer wireless Internet to the surrounding community. The WiFi subnet will not be able to access the LAN: it will be able to connect to the Internet only. You can choose to eliminate the Opt1-WiFi setup: this will leave you with a firewall more similar to the “conventional” appliances.

One of the very unique uses for your new firewall could be to offer wireless Internet to your neighbors at a reduced cost

One of the very unique uses for your new firewall could be to offer wireless Internet to your neighbors at a reduced cost. This connection can be via an encrypted access point, where the network key is only given to approved users, or an open access point where you control access to the Internet with the captive portal function built in to pfSense. A portal landing page will be presented whenever a user tries to connect to the Internet at the beginning of the session. Each user will need to have their user name and password entered into the firewall in advance of the first connection.

There are many advanced features that pfSense can offer with one-click installation which are listed at the end of this article. See the [pfSense's web site](#). There is an [active user forum](#) and an [pfSense Wiki](#).

Two good reasons to use pfSense

Configure a professional firewall using pfSense

1. pfSense is a very powerful and stable project with advanced features. Users of pfSense have reported that it performs well even with hundreds of computers operating behind the firewall. pfSense has all the features of the SOHO units and much more. You can have multiple network subnets separate from each other using firewall rules. For example, you could have separate subnets for each business function; or separate Accounting, Marketing, Sales, and R&D from each other, while giving each one access to the Internet; or set up a HotSpot for your business, allowing users to access the Internet but not the company LAN (which usually contains a POS (Point Of Sale) system and/or proprietary information and non public computer systems).
2. If you are an experienced FreeBSD, GNU/Linux or Unix user you may wish to add applications from the [FreeBSD repository](#). While running additional applications on a firewall can increase your exposure to potential risk of being hacked, it can still be extremely useful to add a few applications to pfSense. Once you get pfSense installed you can find a list of authorized ports under the System Packages tab. These can be installed with one click. The FreeBSD.org packages are added by the user via the shell the way it has been done for years. These FreeBSD.org packages are not officially supported by pfSense.

Install Guide

Download, ISO preparation, and interface selection.

Here is the link to the [pfSense download area](#) This will take you to a mirror near you. This CD we will install from is a Live CD. A Live CD will allow you to test your hardware and pfSense without actually installing onto the hard drive. You will need to change your BIOS to boot from the CD and then boot from the CD image that you create from the ISO image. This CD is also an installer CD—more on this later.

Users of pfSense have reported that it performs well even with hundreds of computers operating behind the firewall

The ISO image for this guide will be `pfSense-Full-Update-1.2-RELEASE.tgz`. You will first need to decompress this file using `gzip` to get to the ISO. Then, create the bootable CD. A good program to use is `cdrecord` via the GNU/Linux command line.

Use this command:

```
sudo cdrecord -v speed=20 dev=/dev/sr0 pfSense-1.2-RC3-LiveCD-Installer.iso
```

If you use Linux, your device (`dev`) may vary. There is also a good utility for Windows for creating ISOs called Deep Burner, which is freeware, but it's *not* released under a free license.

Now that you have set your BIOS to boot from CD and you have created your bootable CD, you can boot into pfSense on your PC. You will need to have at least two network cards installed—although I recommend three. The third is necessary for the WiFi subnet, giving you:

- one for the WAN (your ISP);
- one for your private LAN;
- one for your WiFi internet-access-only subnet.

Check the [FreeBSD hardware compatibility list](#) first to make sure your hardware is supported.

Configure a professional firewall using pfSense

You can now boot into pfSense. As the bootloader comes up the Free BSD screen 7 options are listed. You can wait for the default option (1) to boot up. Take a sheet of paper and write down the initials for the “valid interfaces”: you will need them in a moment. Mine are `fxp0`, `fxp1`, and `fxp2`. The next choice you will be asked to make is “Do you want to set up VLAN’s now [y|n]?” Select “no” or “n”.

Then you are asked to “Enter your LAN interface name”, enter one from the sheet of notes you just created. I enter ‘`fxp1`’.

Next you are asked to “Enter your WAN interface name”. I enter `fxp2`. The next option is “Enter the Optional 1 interface name”. Here I enter my last ‘`fxp0`’.

You should then see:

```
The interfaces will be assigned as follows:  
LAN -> fxp1  
WAN -> fxp2  
OPT1 -> fxp0
```

```
Do you want to proceed [y|n]?
```

(Make sure you enter “y” here).

pfSense is now running in RAM and almost fully functional. If you wish you may plug your LAN interface into a hub or switch and connect via the web interface. pfSense is by default assigned an IP of 192.168.1.1. Open your browser and check it out, or proceed to the hard drive install. To run from RAM you can skip to the “Web interface configuration” section of this guide.

pfSense is now running in RAM and almost fully functional

If you choose to login, the user name is “admin” and the password is “pfsense”.

Hard drive install

Here is how to complete a hard drive installation.

Transition to the console in order to begin the “hard drive installation”. This section is “pfsense console setup”: Select “99”.

This is a curses based install. It works best if you use an entire hard disk. If there is any data on the disk, make sure that you have copied it to another location. You can, as a rule of thumb, accept the default settings that are presented during the curses-based installation.

Pictures of the [pfSense installation](#) are available in pfSense’s forums.

Here is a list of operations, shown graphically by the tutorial:

- Note: If you would like to see the instructions as a Wink tutorial, you can see pfSense’s [Wink tutorial](#). However, the instructions here follow.
- Remember to remove the CD from the drive when you reboot.
- After rebooting, you should be presented with the “pfsense console setup” for a second time. At this moment you can unplug your monitor cable and manage this firewall via a browser, or you could

Configure a professional firewall using pfSense

select option 8 and explore it using a shell.

- Make sure your computer's interface is in the 192.168.1.0 subnet, because pfSense's LAN interface is by default 192.168.1.1. The default username and password for the web GUI are "admin" "pfsense".
- Select System Setup Wizard now.
- This wizard will guide you through the initial installation of pfSense. Click "next"
- General Information: enter primary and secondary DNS (name servers) if you wish. Click "next"
- Select TimeZone and then Click "next"
- On the Wide Area Network Information page scroll down and click "next"
- On the LAN interface page you may select a Subnet IP address of your choice or stay with the default of 192.168.1.1. If you stay with the default, you will need to configure your computers so that they are on the same subnet, or have DHCP enabled on your network PCs.
- The password page: you should select a password that consists of at least 8 letters and numbers, lowercase and uppercase. Save this new password in a secure place. Now that you have selected a new password you will be required to login again.
- Go to "Interfaces" tab on the top row and select "Opt 1: *Enable the opt 1 interface*". Enter the IP of the Opt 1 interface under the IP Configuration section, "192.168.2.1". Scroll to the bottom and select "save"
- On the top bar, select "Firewall Rules"; select the "Opt 1" tab; and click on the plus to add a rule. Change protocol to "any". Under "Destination", check the "not" box. In "Type", select "LAN subnet". In "Description", enter allow all to net - > ! LAN subnet. Save the changes, and then in the next window, select "Apply Changes".
- Go to the Top row and select *Status Interfaces*
- Move the cable from your current firewall to the WAN port for pfSense and connect the LAN cable to the LAN port on you new pfSense firewall. At this point you should power cycle your Broadband provider's equipment (turn it off for 30 seconds, then turn it back on). Sometimes when your MAC address changes on your firewall, your broadband provider will need to be involved to reset your configuration.
- Under the WAN interface section, you may see your external IP address. If this is the case you are, most likely, good to go.
- Go to the "Services" tab, then "DHCP server". Select the "Opt 1" tab and enable the DHCP server for that interface. In the "Range" section, enter the IP address range for your DHCP server.
- Scroll to the bottom to select "save", and you are ready to go.

Setting up your Wi-Fi for the Opt1-Wi-Fi interface

Run a cat-5 cable from the Opt1-Wifi interface that you set up earlier to the access point you plan to have on its own subnet. This subnet is separated from your LAN via firewall rules. This AP will connect directly to the internet and have no access to your LAN. Many of the SOHO firewall/routers have a default IP address of 192.168.0.1 or 192.168.1.1. Change this to a different IP address so it will work on this install, and not have the same IP address as your new pfSense box. I selected 192.168.2.5.

You can use this same process on your LAN for a second access point with an IP address on the same LAN subnet that is encrypted

Then, disable the DHCP server on this appliance so your pfSense box can now hand out the addresses. This way when you are looking under *Diagnostic ARP* tables you can easily see who is on your connection. Enable the DHCP server under the *Services DHCP server*, tab click on the Opt 1 interface, and on the top, check the box "enable DHCP Server". You will need to set the Range of the DHCP server which will regulate how many IP addresses you will give out.

Configure a professional firewall using pfSense

The key to this functioning properly is to make sure that when the firewall rule is set up for the `Opt1 Wifi` interface is that the protocol section be set to “any”. By default when the rule is set up it is TCP. If this is not set properly access will be limited and for our purposes would not work.

You can use this same process on your LAN for a second access point with an IP address on the same LAN subnet that is encrypted. This wireless network connection is for your use only, not your neighbors. Disable the DHCP server on the second Access Point and let pfSense handle that function. You can regulate access by using the built in captive portal capability found under *Services Captive Portal*. An equally effective way for an encrypted network is to only give your network key passphrase to select people.

Get help

If you encounter difficulty you can post questions related to the [pfSense forums](#).

Advanced Features for pfSense

This section outlines some of the advanced features available in pfSense. These are features that in the past were generally available on proprietary and expensive firewalls.

- Traffic Shaping - This gives you the ability to prioritize traffic. For example if you use VOIP you will want to give that top priority. Also you may want to move torrent traffic down the priority list so that it does not slow down web surfing traffic
- Clustering - Linking two or more computers into a separate network to take advantage of parallel processing of those computers
- Load Balancing - If you are running multiple web servers you can spread the traffic evenly to each server. This will help to prevent any one server from becoming overburdened
- Failover - You can set up two firewalls with pfSense if one fails the other will automatically kick in. If you have multiple Internet connections and one fails the other will take over
- Captive Portal - Control Access to the internet. Like coffee shops use when they offer free WiFi
- The below services will install with one click in pfSense. Installing these features is a snap. There are tutorials available for some of the below packages on the pfSense [wiki](#). If no tutorial is available help is available on the pfSense [forums](#)
- Snort - Lightweight network intrusion detection system
- Squid - High performance web proxy cache
- FreeRadius - Implementation of the RADIUS protocol
- IMSpector - an Instant Messenger proxy with logging capabilities
- nmap - A utility for network exploration or security auditing
- ntop - Shows network usage in a way similar to top
- Darkstat - A packet sniffer and a network statistics gatherer and much much more.

pfSense will also allow you to add packages from the standard FreeBSD repository, although any unofficial packages are not supported by pfSense.

Resources

- [HOWTO Add a Wireless Interface](#). You can skip this tutorial if you are planning on adding an external Access Point as outlined above. This tutorial is for those who want an internal WiFi interface.

Configure a professional firewall using pfSense

*Graphical Tutorials

Biography

Sloan Miller (/user/47747" title="View user profile.): Open Source Software user for about 12 years. Patiently waiting for Open source software to take over the world.

Copyright information

Verbatim copying and distribution of this entire article is permitted in any medium without royalty provided this notice is preserved.

Source URL:

http://www.freesoftwaremagazine.com/articles/configure_professional_firewall_using_pfsense
