Take your old PC and turn it into a $5,000 firewall, for free.

Get others to pay for your Broadband Using Free pfSense firewall. While protecting your home LAN from access.

By Sloan Miller

At the end of this guide you will be able to set up the Open Source (free) firewall pfSense to allow you to share the cost of your broadband internet and prevent those other users from accessing your LAN home network. This guide contains screen shots and Graphical tutorials. When you are finished you will have a firewall that is just as robust, easier to use and has a set of features unmatched by commercial alternatives.

This guide is intended for users who are from the Linksys, Netgear, D-link etc. firewall/router background. No experience is needed with FreeBSD or Linux/Unix to install and run pfSense. When you are finished, management of the pfSense firewall will be from a web interface just like any of the SOHO firewall/router appliances. The pf in pfSense stands for Packet Filter.

Reasons for switching to pfSense. A Very powerful and Stable platform on which you run a firewall with optional advanced features. It has been reported by pfSense users that it performs well with hundreds of Computers operating behind the pfSense firewall. pfSense has all the features of the SOHO units and much more. Have multiple network subnets separated by the firewall from each other. Example: have one protected/unprotected wireless access-point for friends and neighbors to access your internet connection. Split the cost of your internet connection with your neighbors and prevent them from accessing your home network. Additional packages are implemented with one click. If you are an experienced FreeBSD, Linux or Unix user you may wish to add even more applications from the FreeBSD repository at FreeBSD.org. http://www.freebsd.org/ports/master-index.html

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 apps 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.

This guide is divided into sections. The first section, Phase 1 is about where to go to find the download you will need to install pfSense onto the hard drive of an old PC. Phase 2 will walk you through the install screens and the selections necessary to complete the install onto the entire hard drive. Then you will be guided through the configuration of pfSense through the web-interface. Phase 3 is how to setup your wifi access-points. At the end of the guide I will tell you about some of the more advanced Packages and Features of pfSense.

PHASE 1

Here is the link to the pfSense download area. Near the top of the page there is a link 'LiveCD'. 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 cdrom and then boot from the cd image that we create from the .iso image. This CD is also an installer CD, more on this later.
http://www.pfsense.com/index.php?id=22

The .iso image for this guide will be pfSense-1.2-RC3-LiveCD-Installer.iso.gz You will first need to decompress this file using gzip to get to the ISO. Then create the ISO. I use 'cdrecord' via the Linux command line.

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

I use Ubuntu your device 'dev' may vary . There is also a good free utility for Windows for creating ISO's called Deep Burner. Here is the link   http://www.deepburner.com/?r=download
Deep Burner is free.

Now that you have set your bios to boot from cdrom and you have created your ISO we can boot into pfSense on your PC. You will need to have at least two network card installed into the PC, I recommend 3. One for the WAN (your ISP), one for your private LAN and one for your WiFi only subnet.

Check the FreeBSD hardware compatibility list first to make sure your hardware is supported.

http://www.freebsd.org/releases/6.0R/hardware-i386.html

Now we boot into pfSense. As the bootloader comes into the 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 'fxp0'. Next I am asked to

“Enter your WAN interface name”

I enter 'fxp1'.   The next option “Enter the Optional 1 interface name”, here I enter my last 'dc0'.

Then we see “The interfaces will be assigned as follows:”
LAN -> fxp0
WAN -> fxp1
OPT1 -> fxp2

You can do the same for the opt1 interface now or wait till we configure the Wifi via the GUI.

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.   If you choose to login the username is 'admin' and the password is 'pfsense'.

PHASE 2

Hard Drive Install.

We will now transition to the console where we will begin the Hard Drive installation.
This section is “pfsense console setup” We select 99) Install pfSense to a hard drive/memory drive, etc.

This is a curses based install. You are best using an entire hard disk or memory that you can write over. Make sure if there is any data on the disk that you have copied it to another location. Now you can as a rule of thumb accept the default settings that are presented during the curses based install.

Pictures of this process are available for download here.

http://forum.pfsense.org/index.php/topic,7356.0.html

Remember to remove the cd-rom from the drive when you reboot.

Now we have rebooted and are 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 select option 8 and explore via a Shell.

Make sure your computers interface is in the 192.168.1.1 subnet, because 'pfSenses' LAN interface is by default 192.168.1.1.

The defualt user name/password for the web GUI is 'admin' 'pfsense'.

Now we are going to select System > Setup Wizard.

At this point you can switch to the Wink tutorial. This will walk you through the rest of the configuration.

http://computerpro.bz/Complete%20Final.htm

PHASE 3

This is the money section. Here I will explain how to set up one or more WiFi Access Points to share your broadband connection to the internet. You can use your old SOHO router/firewall that you will be replacing with pfSense for this purpose.

Run a cat 5 cable from your opt interface to the access point you plan to have on its own subnet. This subnet is separated from you 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. 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 this will regulate how many IP addresses you will give out. When you select the save button this will alert us to an error I made during configuration of the Opt 1 interface. We will need to go back to the Interfaces Opt 1 menu. And change the netmask to /24 instead of the /32 that I mistakenly accepted on the initial setup. PfSense was kind enough to alert me to my error.

This tutorial shows how to create the firewall rule to allow open wifi traffic from the 192.168.2.1 subnet out to the internet but not access the 192.168.1.1 subnet.

***** 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 out purposes would not work.*******

If you need to increase the range of your access point to adequately cover your neighbors house you can deploy two routers that come with WDS. Put one in your neighbors house and one in or on your house. WDS acts as a wireless cat5 networking cable linking the two AP's together. A directional antenna properly placed and attached to your firewall router can also accomplish this task.

If you are in need of help pfSense has a forum full of very knowledgeable helpful people who can help.

http://forum.pfsense.org/index.php

I use this same process outlined above on my LAN for a second access point with an ip address in the same LAN subnet that is encrypted. This wireless network connection is for my use only not my neighbors. I disable the DHCP server on the second Access Point and let pfsense handle that funtion.

I 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 pass-phrase to select people.

Advanced Features:

Install with one click	
Load Balancer	
Failover	
Captive Portal	Control Access to the internet. Like coffee shops use with free WiFi.
Snort	Lightweight network intrusion detection system.
Squid	High performance web proxy cache
FreeRadius	Implementation of the RADIUS protocol
imspector	IMSpector is 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