

## Re: Configuring PF

**Source:** <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/questions/2005-02/3142.html>

---

**From:** Pat Maddox ([pergesu\\_at\\_gmail.com](mailto:pergesu_at_gmail.com))

**Date:** 02/20/05

Date: Sun, 20 Feb 2005 11:42:41 -0700  
To: "Loren M. Lang" <[lorenl@alzatex.com](mailto:lorenl@alzatex.com)>

On Sun, 20 Feb 2005 06:23:39 -0800, Loren M. Lang <[lorenl@alzatex.com](mailto:lorenl@alzatex.com)> wrote:

> *On Mon, Feb 14, 2005 at 09:32:25PM -0700, Pat Maddox wrote:*  
> > *I want to install a firewall on my system. First of all, is PF the*  
> > *one I should be using? It seems to get the most recommendations.*  
> >  
> > *I don't actually seem to have any problems configuring it - I just*  
> > *have some problems testing the configuration. I can ssh to the box,*  
> > *and I can access port 80...but I'd like to be able to just scan it to*  
> > *quickly see what's up. When PF is disabled, I can nmap it in about 9*  
> > *seconds. When I turn it on, it takes over 3 minutes to do. These*  
> > *machines are on the same network, so the connection is obviously fast.*  
>  
> *This is a good thing, IMHO. Think about all those script kiddies*  
> *sitting out there looking for a nice, juicy server to compromise. If it*  
> *takes them 3 minutes to port scan your machine, they'll probably cancel*  
> *it before it's finished and move on.*

That makes sense to me. I'd still like to be able to scan it the first time around to make sure everything's working, then I can just set it to drop packets, so it takes longer.

I'd still like to find a good example config file that works well for a web server.

>  
> *I believe what's happening is that all ports that aren't open are*  
> *configured to drop packets instead of reject them like is default.*  
> *Reject means send back an error message saying port is closed where*  
> *dropping just ignores it. The port scanner sends out a request and*  
> *waits for a response, either "Hello," or "Sorry, I'm closed." It will*  
> *wait quite a while before it decides that nothings there.*  
>  
> >  
> > *Are there any good, pretty simple guides on setting up PF? I'm having*  
> > *a tough time understanding what the rule*