

Building Firewalls with OpenBSD and PF

Building Firewalls with OpenBSD and PF

Jacek Artymiak

Second Edition

Lublin

5.6.3 GUI Tools for Writing Rulesets with a Mouse

Recently, some brave developers wrote ‘clickable’ GUI applications for easy ruleset creation. They look promising and may evolve into some very interesting tools. To have a wider appeal, GUI *pf.conf* configurators must provide additional value to the administrators. For example, a GUI-based ruleset tester/simulator and an integration with CVS would be nice to have. Knowing the worldwide open source software community, it won’t be long before such tools are available.

5.6.4 Scripting *pf.conf*

When you have to manage more than one firewall, or when you need to dynamically adjust firewall rulesets, it pays to learn scripting tools like shell, AWK, Perl, Tcl, or Python. You will find plenty of free information available online. If you prefer to learn from books, Addison-Wesley, Prentice-Hall, and O’Reilly & Associates publish very good general-purpose programming books as well as more specialist titles targeted specifically to system administrators.

5.7 Managing *pf.conf* Versions with CVS

Pf(4) rules change quite often when you are fine-tuning the firewall and it is a good idea to keep a track of the changes you make with *cvsv(1)*. While many people think of it as a programmer’s tool, CVS is not limited to storing source code of programs and scripts. Any kind of file, text or binary can be stored in CVS.

Working with CVS is quite easy. The CVS repository can reside anywhere you choose. You could create a CVS repository of *pf.conf* files in */root* on the firewall machine, but a more secure solution would be to keep it on the computer you usually work on. When the repository is kept up to date and well-commented, you will quickly create a collection of rules that you will be able to go back to when you need to add a new firewall, or change the existing network configuration. If you are managing more than one firewall, create separate repositories for each machine’s *pf.conf*.

To create a repository, first create a directory where all your firewall repositories will be held, e.g.:

```
$ mkdir ~/cvsv
```

Next, create a temporary directory into which you'll import the initial version of *pf.conf* from host `fw0`:

```
$ mkdir ~/tmppfconf
```

This could be anywhere, but it's probably most convenient to create it in your home directory. Just in case you asked, the name of the repository and the name of the directory where CVS keeps repositories are two different things.

Then, change the present working directory to this new directory you've just created, export the `CVSROOT` environment variable (used by all CVS commands; must contain the path to the CVS repository), and initialize your new CVS repository:

```
$ cd ~/tmppfconf
$ export CVSROOT=/usr/joe/cvsdir
$ cvs init
```

Before you copy */etc/pf.conf* to the machine that you will keep its CVS history on, copy it to the ordinary user's home directory and change its privileges (the following procedure assumes that you are logged as an ordinary user on the firewall host and that user `joe` belongs to group `wheel`, see Chapter 4, *Configuring OpenBSD* for more information):

```
$ su
# cp ./etc/pf.conf /home/joe/
# chmod 0660 /home/joe/pf.conf
# exit
```

You can now log off the firewall host and copy *pf.conf* from the firewall with `scp` to `~/tmppfconf` and commit (add) it to the repository:

```
$ cd ~/tmppfconf
$ scp joe@fw0.example.com:/home/joe/pf.conf ~/tmppfconf/
$ cvs import -m 'Initial configuration of fw0.' fw0 joe start
```

The *pf.conf* that you have just imported into the CVS repository will be stored in the `fw0` module (when you download configuration files from other hosts, place them in the temporary directory and import with a

module name that's different from `fw0`). To begin working with it, do the following:

```
$ cd ..  
$ cvs co fw0  
$ cd fw0
```

Every time you make changes to *pf.conf*, use the following command to store them in the CVS repository, so you will have a trace of the changes you've done and will be able to go back to earlier versions of *pf.conf*:

```
$ cvs ci -m 'Added NAT rules for the DMZ.' ./pf.conf
```

In the future, when you want to checkout the last revision from the repository, use:

```
$ cvs co pf.conf
```

What if you want to checkout one of the revisions committed to the repository before the last one? Use the `-r` option followed by the number of the revision, as in:

```
$ cvs co -r 1.17 pf.conf
```

If you want to see the repository log for a file, use this command:

```
$ cvs log pf.conf
```

When you want to transfer a modified version of *pf.conf* to the firewall host, do the following:

```
$ scp ./pf.conf joe@fw0.example.com:/home/joe/pf.conf
```

Then, log on the firewall and:

```
$ cd /home/joe  
$ su  
# cp ./pf.conf /etc/pf.conf
```

```
# chmod 0600 ./etc/pf.conf
```

And reload the ruleset with *pfctl(8)*.

This is only a short intro to CVS, you can learn more from *cvst(1)*. And if you really want to get into CVS (as you should) read [Vesperman 2003]. A very good (and free) CVS manual can be found at:

<http://www.cvshome.org>

(CVS home)