

Check Point Firewall-1 on Linux, Part Three

David Del Elson 2001-03-28

Check Point Firewall-1 for Linux, Part Three

by David "Del" Elson

last updated March 28, 2001

This is the third and final article in a series devoted to the exploration of Check Point Firewall-1 for Linux. In the first article we discussed single and multi-system installation and post-installation tasks. The second article explored Firewall-1 concepts such as network objects, firewall rules, address translation rules, and NAT, as well as features and limitations of Firewall-1. In this installment, we will go over aspects of Firewall-1 such as file and directory layout, rulesets, migrating existing Firewall-1 installations to Linux, and backup and standby configurations.

Inside Firewall-1

File and Directory Layout

Firewall-1 on Linux is installed into a directory on /opt. This directory is symbolically linked as /etc/fw, and all directories, commands, and files are accessed relative to /etc/fw. Inside /etc/fw/ there are the following important subdirectories:

- the bin directory, which contains the Firewall-1 binaries (executable programs);
- the conf directory, which contains the configuration files, rulesets, etc.;
- the log directory contains the Firewall-1 log files;

... plus several others.

The Conf Directory

The conf directory contains the most user-serviceable parts, and is where a Firewall-1 hacker might spend most of his or her time. Inside the conf directory there are a number of files, including:

- *.W files, which are the editable versions of the rule sets;
- *.pf files, which are the compiled versions of the rule sets;

- `objects.C`, which contains the network objects; and,
- `rulebases.fws`, which contains the rule sets in a format that is used by the Policy Editor; and,
- `gui-clients`, which lists the IP addresses of any management stations.

File Formats

Most of the files in the `conf` directory are ASCII text, and rather than using the GUI Policy Manager program, it is possible to interface directly with Firewall-1 from the command line. The basic Firewall-1 rulesets are stored in `*.W` files, which are in a easily readable text format. These files correspond to the rule sets defined in the Policy Manager, with each policy being stored in a separate file, and each line in a policy stored in a set of lines in the `*.W` file.

The format of the `*.W` files is not complex, and if you are an experienced firewall administrator then some experimentation will explain the language used in the files. It is possible to copy the `*.W` files, edit a copy, and revert to the old copy if your edits go astray or cause problems.

Network Objects

The network objects are stored in the `objects.C` file. This file is, again, ASCII text and can be edited with a text editor such as `vi`. The network objects for all rule sets are stored in the same `objects.C` file, so be careful when editing it.

Rulesets (.W and .pf files)

Generating a firewall ruleset from one of the `*.W` files can be done from the command line. The command to do this is:

```
fw gen myrules.W > myrules.pf
```

This generates an inspection (`*.pf`) file from the `*.W` language used by the Policy Manager. Note that it is possible to edit the `*.pf` files directly, as they are ASCII text as well. The `*.pf` files are in a language called INSPECT, which is described in chapter 3 of the Firewall-1 Reference Guide. The Reference Guide is available in PDF format in the `Docs` directory on the CD-ROM.

Ruleset Generation

Once you have generated an INSPECT file from a *.W file, it is possible to load this into the running firewall using a command such as:

```
fw load myrules.pf
```

Note that loading an INSPECT file reads both the inspect script and the objects.C file, so if you have hand-edited both files and not kept them in sync, you could encounter problems at this stage.

Migrating an Existing Firewall-1 Installation To Linux

If you have an existing Firewall-1 installation on, for example, Windows NT, it is possible to upgrade to the latest version of Firewall-1 by using the standard Firewall-1 installation program. This upgrades previous versions of the rulesets to new versions, adds any required network objects to the objects.C file and installs the new software. If you have an existing installation on Windows NT and wish to migrate this to a Linux installation, there are several steps that you will need to follow.

Pre-Planning and Preparation

Firstly, upgrading a machine from Windows NT to Linux is going to involve some (possibly considerable) period of down time. Assuming that you have a running firewall, and that it is in a production environment, you may wish to consider building a second machine to migrate your NT firewall onto, rather than re-installing the production firewall. One other advantage of this is that it gives you a chance to fall back should things go wrong. It also means that once you are finished you may possibly have a spare machine for redundancy or disaster recovery purposes.

Your new firewall system should be of sufficient capability and performance to cater for your organisation's growth over a period of, perhaps, 2 - 3 years.

ASCII Files

Firstly, one warning: ASCII files on Windows NT and ASCII files on Linux are not exactly the same format. On Windows NT, each line of an ASCII file is terminated by a CR/LF sequence, which is 2 bytes. An ASCII file on Linux is terminated by a single LF byte. Firewall-1 on Linux uses ASCII files in the Linux format, while Firewall-1 on NT uses ASCII files in the NT format. They will not be able use each other's files directly. There are many utilities around that are

capable of converting a NT (or DOS) format text file to a Linux (or UNIX) format file. The one I prefer to use is the old faithful vi (actually vim, with the -b flag):

```
vi -b some-dos-file
```

On loading a DOS text file, you will see that each line has a hanging "^M" sequence at the end. The command to remove these is:

```
:%s/<ctrl-V><ctrl-M>//g
```

where <ctrl-V><ctrl-M> means "hold down the Ctrl key, hit V, then hit M". You will see a "^M" sequence appear in vi when you do this.

Any files (objects.C, *.W, or rulebases.fws) copied from an NT system to a Linux system must be put through this process.

Migrating the Network Objects

Copying the network objects from an NT system to a Linux system is relatively straightforward. You just copy the objects.C file on NT to a floppy disk and copy it back into the conf directory on Linux.

Remember to convert the file to UNIX format, as mentioned above!

Migrating the Rulesets

As mentioned earlier, the Firewall-1 rulesets are stored in a group of text files, which are *.W on Windows NT. You need to copy all of these files from your NT firewall to your Linux firewall and put them in the conf directory.

There is one other file you will need to copy: rulebases.fws. This file contains a conglomeration of all of the rule sets, in a format used by the Policy Editor. Without the rulebases.fws file, you will be able to manually compile and load *.W files but you will not be able to see them in the GUI.

Migrating from a v4.0 Installation

If you have an existing Firewall-1 installation on NT that is Firewall-1 version 4.0, and you want to migrate that to a Linux installation, then you will have two tasks. The first is migrating from NT to Linux, the second is to upgrade to Firewall-1 version 4.1 (as version 4.0 does not run on Linux).

The migration process is very similar, with a few catches. Firstly, there are some additional objects in the version 4.1 objects.C file that you must capture as you migrate to Linux. These will be in the default objects.C file when you install Firewall-1 on Linux, so it is important not to lose this file when you copy your objects.C file from Windows NT.

Instead of copying the file directly across from NT, copy it to a new file called objects.C.old. You then will have two files, objects.C.old which has come from NT, and objects.C which was provided with Firewall-1 on Linux.

After converting the objects.C.old file to UNIX format, you can merge these two files into one by using the following command:

```
fw confmerge objects.C.old objects.C > objects.C.new
```

You now have an objects.C.new file that contains all of the necessary network objects. Rename this to objects.C using:

```
mv objects.C.new objects.C
```

Additionally, you will want to copy both the rulebases.fws and the *.W files from your version 4.0 system to your new version 4.1 system. These can be copied across directly. I suggest loading each rule set into the Policy Manager and saving it after you have done this, this will update them into their new version 4.1 formats if required.

Migrating From a v3 or Earlier Installation

I would recommend against upgrading from Firewall-1 version 3.0 to 4.1 and migrating across platforms at the same time. Provided that you have all of the necessary software and media, I would instead recommend the following procedure:

- upgrade your existing Firewall-1 version 3.0 installation on NT to version 4.1 on NT, using the version 4.1 installation media; and,

- migrate from Firewall-1 version 4.1 on NT to Linux, using the procedures that I have outlined above.

Note that Check Point states that it is not possible to upgrade from a version prior to 3.0 to a version 4.1 firewall. You need to upgrade from your prior version to version 3.0, and then from 3.0 to 4.1. If you are migrating to Linux at the same time then you will probably have a 3 step process. Plan for plenty of downtime while you are doing this!

Migrating Multi-System Installations

Note that migrating a system from NT to Linux is not significantly more complicated if you have a multi system installation than a single system installation. The first step is to migrate the master firewall (aka the management server, or machine running the fwm module). While doing so, you should refrain from applying any ruleset changes to any of the slave Enforcement Modules. The Enforcement Modules can then be migrated one at a time. While you are migrating an Enforcement Module, there is no need to migrate any of the rulesets (rulebases, fws, objects.C, or *.W files), as these can be propagated to the Enforcement Module once it has been installed. Essentially, you should set up an "empty" Enforcement Module, and use the Management Module to propagate a rule set to it, just as you did when you first installed the module.

Backup and Standby Configuration

Some Firewall-1 administrators on NT have set up standby configurations of Firewall-1, using such software as StoneBeat. This is not really possible with the Linux version of Firewall-1, although there are some pieces of software that are emerging to perform failover and High Availability on Linux. I haven't tested any of these with Firewall-1, however.

An alternative to having a hot standby is to have a spare machine, configured (hardware and software) similarly to your primary firewall. This can be left running, off-line, or even switched off and locked in a safe. Periodically, it would pay to back up the conf directory of your primary Firewall-1 system and restore it onto your spare machine, or even just restore the objects.C and rulebases.fws files, from which most of the rest of the configuration can be regenerated.

Summary

Without getting into the good or bad points of commercial software (I tend to use a mix of commercial and free software myself, whatever suits my needs best tends to get the green light), it can be said that Firewall-1 is a fast, reliable, and popular piece of software that does the job of creating a firewall with an easy to manage GUI on Linux. Existing Firewall-1 customers with an interest in Linux will be pleased to note that Firewall-1 performs more than adequately on Linux. The performance of Firewall-1 on Linux appears to noticeably exceed that of Firewall-1 on NT, even from anecdotal evidence gained from the small handful of installations that I have performed. Firewall-1 customers with an NT based firewall who are concerned about performance may well be advised to migrate away from Windows NT and on to Linux.

Relevant Links

[Check Point Firewall-1 for Linux, Part One](#)

David "Del" Elson, SecurityFocus.com

[Check Point Firewall-1 for Linux, Part Two](#)

David "Del" Elson, SecurityFocus.com

[Check Point Firewall-1](#)

Check Point

[Privacy Statement](#)

Copyright 2006, SecurityFocus