

# Check Point Firewall 1 on Linux, Part One

*David Del Elson* 2001-02-07

## Check Point Firewall-1 on Linux, Part One

by *David "Del" Elson*

last updated Feb. 7, 2001

---

This is the first in a series of three articles that will examine Check Point Firewall-1 for Linux. This installment will consist of a brief introductory overview of Firewall-1, and a discussion of installation, post-installation tasks, as well as single and multi-system installations. Subsequent articles in this series will focus on concepts such as network objects, firewall rules, address translation rules, and NAT, features and limitations of Firewall-1, file and directory layout, rulesets, migrating existing Firewall-1 installation to Linux, and back-up and standby configurations.

## Introductory Overview

### The Product

Check Point Firewall-1 has been the market-leading firewall system since its introduction in 1994. The main advantage of Firewall-1 is its comprehensive and easy to understand GUI, which has made it a firewall system of choice for many corporate IT managers. Firewall-1 is not a cheap product; however, it is well marketed and product support is available from some of the leading IT vendors and outsourcers. In a recent Internet Security Software survey, IDC estimated that Check Point has a 41 percent market share in the firewall software category, which is a significant consideration for many customers.

### Installing Firewall-1

Installation of Firewall-1 on Linux is not an excessively complicated process and should not be beyond the capabilities of any experienced Linux system administrator. The system is targeted to run on Red Hat Linux version 6.1 and 6.2. I have heard reports of Firewall-1 being installed successfully on other Linux platforms (e.g.: Debian users have managed to turn the RPM files into DEB files for installation); however, I have had a notable lack of success running Firewall-1 on Red Hat version 7.0! When running with Red Hat version 6.2, ensure that all of the latest updates are installed (from Red Hat's FTP site or your nearest mirror).

## Planning

Pre-planning your Firewall-1 installation is quite important. Before you proceed with your installation you should have an idea of what your network looks like, preferably with network diagrams if possible.

Firewall-1 is a-PC based firewall system, and only supports Ethernet interfaces. As a result, if your external Internet connection goes via a different sort of interface (e.g.: a PPP serial link, Frame Relay, or ATM,) you will need a router between your firewall and the Internet. Planning the addresses that you will use on this link is also important. You will probably want to run Firewall-1 on a machine dedicated to the purpose. Generally speaking, a firewall will need at least two Ethernet cards, and if you have a DMZ or other networks attached to your firewall then you will need more than that. (One of the more recent installations of Firewall-1 that I completed was on a machine with 9 Ethernet interfaces!) The PC to be used for Firewall-1 should have at least 64MB of memory, with 128MB recommended. It should have sufficient disk space for the operating system and Firewall-1 software installation, as well as some amount for log files and spare space. A machine with a 4GB or larger hard disk should suffice.

Depending on your required throughput (and the speed of your Internet connection), the CPU requirements for Firewall-1 may vary. I have successfully run and installed the system on a 133MHz Pentium, although it ran somewhat faster on a 600MHz Pentium III! For a firewall with a 2MB circuit to the Internet and approximately 200 users being protected, I found that a 400MHz Pentium II processor was adequate.

## Operating system considerations

Firewall-1 for Linux is designed to run on Red Hat Linux 6.1, with a 2.2.x kernel. Although this distribution is not the latest from Red Hat, Firewall-1 installs and performs quite adequately on Red Hat 6.2. Ensure that you have the latest updates from Red Hat installed, either from the [Red Hat FTP site](#) or your nearest mirror. All recent and current releases of Red Hat Linux have vulnerabilities that should be fixed by applying these updates before installing any third party software or connecting your server to the Internet.

I have attempted an installation of Firewall-1 on Red Hat 7.0, but this was unsuccessful. I suspect that some differences in the as-built kernel or libraries supplied with 7.0 are not compatible with the Firewall-1 software. Note, however, that I did get Firewall-1 successfully

installed and running on a Red Hat 6.2 system with the 2.2.16-3 kernel supplied in the latest 6.2 updates, and this is quite similar to the 2.2.16 kernel supplied with Red Hat 7.0, so your mileage may vary! Note that the main component of Firewall-1 is a loadable kernel module. Although such modules are usually specific to a kernel version, the one that Check Point has shipped appears to load in most of the 2.2.x series kernels that I have tried. It will not load into a 2.4.x kernel!

[It should be noted that after this article was initially published, I received an e-mail from a reader that stated:

"I have gotten firewall-1 4.1 sp2 running on red hat 7.0. The only mod required was to link a couple of libraries thus:

```
cd /usr/lib
ln -s libstdc++-libc6.2-2.so.3 libstdc++-libc6.1-1.so.2"
```

This is the one thing I had missed in attempting to get Firewall-1 running on Red Hat 7.0 - David Elson]

Users of other distributions are on their own, however Phoneboy's Firewall-1 site states:

"Officially, Firewall-1 supports RedHat 6.0 thru 6.2. Some people have had success with SuSE 6.2, Mandrake 7.0, and Debian with a 2.2.12 kernel (the rpm was converted to a deb)."

## Firewall-1 Management Software

The Check Point management software provided with Firewall-1 does not run on Linux. Currently, it runs on Windows NT, Windows 2000, and some UNIX systems (e.g.: Solaris) only. Therefore, to use Firewall-1 you will need an additional workstation to be your management station - unfortunately this must be running on one of the above operating systems. The Firewall-1 management software for Solaris is in fact reasonably poor, and so I would instead recommend that a Windows NT or Windows 2000 workstation be used for the purpose. The Firewall-1 management software must be installed separately from the Firewall-1 gateway software, although both are contained on the same CD-ROM.

## File System Layout

First, a quick note: I install nearly all of my Linux systems using a Red Hat kickstart build. This enables me to very quickly install a Red Hat system from an NFS directory containing the latest

6.2 or 7.0 build with all updates, and not have to touch the system during installation -- all of the installation questions are answered for me in the kickstart file. For more information on Red Hat kickstart builds, see the following section in the documentation on the [Red Hat web site](#).

Generally speaking, a Linux system used for Firewall-1 will need the following partitions:

- / (root), which contains the basic system structure. This should be around 100 - 200MB.
- A swap partition. This should be approximately as large as the amount of memory you have.
- Although there is some debate about this, I prefer to have a separate /usr partition. /usr is where most of the base software supplied with Red Hat Linux gets installed, and it is useful to have this partition as separate as it is mostly static (executable programs, libraries, fonts, etc). On a Red Hat Linux system I like to have about 1GB of space in /usr.
- I also find it useful to have a separate /var partition. This is mostly dynamic data, e.g.: spool files, system configuration data, log files, etc. On a Red Hat system using Firewall-1, the Firewall-1 log files are in fact stored in /opt, not in /var. For this reason I like to have about 200MB of space in /var.
- Firewall-1 is installed into /opt. This directory contains the Firewall-1 software (about 20MB) plus log files, configuration files, etc. On a Firewall-1 system this should be your largest partition, occupying most of the disk.

All of the above partitions can be created manually if you are installing the system from CD (or any other manual installation method). My kickstart (ks.cfg) file for installing Firewall-1 systems has the partitions defined as follows:

```
part / --size 200
part swap --size 128
part /usr --size 1000
part /var --size 200
part /opt --size 1 --grow
```

Note the use of the "--grow" parameter in the definition of the /opt partition, allowing the partition to use all of the remaining available disk space.

## Before Installing Firewall-1

After Linux is successfully installed, you might want to take a few minutes to secure your system. In particular, here are a few things that I always do on a Red Hat Linux system before exposing it to the Internet:

- Edit /etc/inetd.conf, and turn off all unwanted services. Usually, I remove access to all services listed here. This includes telnet, which I replace with the use of OpenSSH (provided with Red Hat 7.0 or available at <http://www.openssh.com/>)
- Use ntsysv to turn off any unwanted services. In particular, your Firewall-1 system should not be running most of the standard services ... I leave atd, crond, network, random, sshd, and syslog running, and turn off everything else.
- Reboot your system with the reduced set of services, and use "netstat -a" to see what ports are open on your machine (these will be the ones marked "LISTEN"). You should investigate if you see anything unexpected!
- Ensure that all network cards are installed and operational (you may want to use "netconf" for this), and that your route table is correct. At this point, it would probably be useful to "ping" a few hosts on your network to ensure that your system is networked correctly, as this will mean that it will be easier to diagnose problems later.

## Firewall-1 Installation

Check Point has provided an installation script that is compatible with all UNIX systems that Firewall-1 can be installed on. To install Firewall-1 using this script, first ensure you have the correct CD-ROM, this should be marked "Check Point 2000 Enterprise Suite v4.1.2". This includes service pack 2 of Firewall-1 v4.1, which is required for running Firewall-1 on Linux. Earlier releases of the Check Point 2000 CD-ROM did not include this service pack, so if you have an earlier release, contact your Check Point vendor for an upgrade CD.

Mount the CD-ROM into your CD-ROM drive using:

```
mount /mnt/cdrom
```

... and install the software using the following commands:

```
cd /mnt/cdrom ./InstallU
```

The installation script will take you through several steps, including:

- Reading and accepting the license agreement.
- Choosing an installation type. The options are (1) VPN-1 & FireWall-1 Stand Alone Installation, or (2) VPN-1 & FireWall-1 Distributed Installation. For a single firewall, you should choose option (1). Where you have multiple

distributed firewalls managed from a central firewall management console (more about this later), you will need to choose option (2). Make sure that you have sufficient Firewall-1 licenses!

- Choosing a Firewall-1 module. The options are (1) VPN-1 & FireWall-1 - Limited hosts (25, 50, 100, 250), (2) VPN-1 & FireWall-1 - Unlimited hosts, and (3) VPN-1 & FireWall-1 - SecureServer. If you have an unlimited IP address license, you will need to choose option (2). If you have (or plan to purchase) a license that is limited by IP addresses, then you should choose option (1).
- Do you wish to start VPN-1 & FireWall-1 automatically from /etc/rc.d/rc3.d and /etc/rc.d/rc5.d (y/n) [y] ? Answer yes to this question.
- Configuring Licenses. Do not add any licenses at this point, I have had limited success doing so. You are better to use the "fw putlic" command obtained with your license, mentioned earlier.
- Configuring Administrators. You will need to add at least one administrator at this point, for example "fwadmin" with a password that you're unlikely to forget (and others are unlikely to guess). You will want to assign write ("W") permissions to your first administrator.
- Configuring GUI clients. You should add at least one GUI client at this point. This will need to be the IP address of your Firewall-1 management station.
- Configuring the SMTP server. Firewall-1 has the capability of sending some alerts via e-mail. If you want to use this facility, then you may want to configure the values in this section. I normally do not use e-mail notification of firewall alerts, as I have quite enough e-mail to read in an average working day without being nagged periodically by my firewalls!
- Configuring the SNMP extension. For security purposes I do not recommend using the SNMP extensions to Firewall-1: however, in a managed network environment then you may wish to do so.
- Configuring groups. This allows you to set up users (within a group) other than root that can start or stop the Firewall-1 software. I do not recommend doing this.
- Configuring IP Forwarding. This allows you to disable the IP Forwarding option at boot time. I recommend that you should select this option.
- Configuring Default Filter. This allows you to ask Firewall-1 to install a default filter at boot time. I have had limited success with systems where I've done this, often this appears to corrupt the network stack so that the system doesn't boot correctly. Select (N). Your mileage may vary.
- Configuring Random Pool. This asks you to type some characters on your keyboard at random so that Firewall-1 can initialize the random number pool.
- Starting Firewall-1. Provided that your management station is operational, you can start Firewall-1 at this point. You will probably see an error message saying "FW-1: only 25 internal hosts allowed". This is because you have not yet installed your Firewall-1 license.

## Post Installation Tasks

After Firewall-1 is installed, you should perform the following tasks:

- Immediately log out and log in again. The Firewall-1 installation program installs some extra scripts into /etc/profile.d which modify your default path to include the location of the Firewall-1 executable programs (/etc/fw/bin). Logging out and logging in again re-reads this directory and sets up your path correctly.
- Install the Firewall-1 license, using the command that was e-mailed to you in your Firewall-1 license certificate.
- Log in to your management station, install the Check Point management clients (if not already installed), run the Policy Editor, and connect to your firewall.
- Create some network objects and rules!

## Single system and multi system installations

Firewall-1 has the ability to control multiple firewalls from a single management module. Before I discuss this, I will explain a few concepts:

- Management Station. This is a workstation (e.g.: running Windows NT or Windows 2000) which runs the Check Point management software. This allows a user to view, edit, and delete firewall rules, and communicate these to the Firewall-1 management module.
- Firewall-1 Management Module. This is a daemon called "fwm" which runs on one or more Firewall-1 systems. This accepts connections from the management station, accepts rule updates, and distributes these amongst one or more enforcement modules.
- Enforcement Module. This is a daemon ("fwd") and kernel module ("fwmod.2.2.x") that enforces a rule set. It runs at your Internet gateway.

It is normal practice to run the Firewall-1 Management Module (fwm), and the Enforcement Module on the same machine, being your Internet gateway. This is not required, however, especially where you have multiple Internet gateways, or perhaps multiple gateways between networks of various levels of trust.

Two installation types were presented during the installation sequence, these were:

1. VPN-1 & FireWall-1 Stand Alone Installation, or;
2. VPN-1 & FireWall-1 Distributed Installation.

The Firewall-1 stand alone installation installs the Management Module and the Enforcement Module on the same machine. The Distributed Installation allows you to specify some combination of Management Module and Enforcement Module (i.e. either one or both) to be installed.

For example, Company X has a wide area network covering the USA. They have a Frame Relay WAN connecting most of their sites, with offices around the country. They have two sites that have their own separate Internet connections, one in San Francisco and one in New York. It would be possible for them to set up a distributed installation, with the management module and enforcement module both installed in New York, but only the Enforcement Module installed in San Francisco. They could control both firewalls from a central management console, and connect only to the New York firewall to update the rule set covering both firewalls.

Ensure that you have the correct installation type selected before installing Firewall-1. The stand-alone installation will give you error messages if you attempt to apply a rule set that covers more than one enforcement module! This might require some pre-planning of your network layout and Internet connections.

## **Installing the User Interface (on Windows)**

The Firewall-1 GUI should be installed on a Windows system before or immediately after you have installed the firewall modules on Linux. To do this, you should insert the CD-ROM into your Windows workstation, and follow the set up instructions in the installation program that is automatically started.

If the installation program does not automatically start then you may run it manually from the CD-ROM (use the SETUP.EXE program in the \windows\CPMgmtCInt-41 directory on the CD).

## **In the Next Episode**

This article has offered a brief overview of the Check Point Firewall-1 for Linux, including pre-installation procedures, installation and post-installation procedures. The next article in this three-part series will cover Firewall-1 concepts such as network objects, firewall rules, address translation rules, and NAT, as well as features and limitations of Firewall-1. The final article will then discuss aspects of Firewall-1 such as file and directory layout, rulesets, migrating existing

Firewall-1 installation to Linux, and back-up and standby configurations.

To read **Check Point Firewall-1 on Linux, Part Two**, click [here](#).

[Privacy Statement](#)

Copyright 2006, SecurityFocus