Sentry Firewall CD HOWTO

Table of Contents

Table of Contents

Sentry Firewall CD HOWTO

Stephen A. Zarkos, Obsid@Sentry.net

v1.3.1, 2003−08−18

This document is designed as an introduction on how the Sentry Firewall CDROM works and how to get started using the system.

---

1. Introduction

2. How the CD Works (Overview)

3. Obtaining the CDROM

4. Using the Sentry Firewall CDROM

5. Overview of Available Configuration Directives

---

1. Introduction

This is the long−overdue Sentry Firewall CDROM howto. I hope this document helps get you started using the Sentry Firewall CD and answers any questions you might have regarding how the system works. The most current version of this howto can be obtained at the following URL: http://www.SentryFirewall.com/files/howto/.

If you would like to add anything to this document, or if you have any questions or comments please feel free to email me, Obsid@Sentry.net.

1.1 What is the Sentry Firewall CD?

The Sentry Firewall CD is a Linux−based bootable CDROM suitable for use in a variety of different operating environments. The system is designed to be configured dynamically via a floppy disk or over a network. This allows one to configure the system dynamically, eventho much of the actual system is on read−only(CDROM) media.

1.2 Why would I use a CD−based firewall or server?

There are several advantages of using a CDROM based system in various security related environments. The main system is centered around the ramdisk; a compressed file system image which is loaded into RAM at boot time. Any changes to the ramdisk image are temporary, and will be undone upon the next reboot. Furthermore, the ramdisk, kernel, binaries, etc, related to the operating system are kept on read−only media(CDROM). This means that if the security of a box running a CDROM based system is ever compromised the attacker can at best own the box until the next reboot. So there is no real threat of having to go through the tedious task of rebuilding and hardening the system after a successful attack is discovered.

1.3 I'm a Linux newbie, will the Sentry Firewall CD be a good choice for me?

At the moment, there are at least a couple variations of the Sentry Firewall CD that are based on various Linux distributions. You should first choose the Linux distribution you are most familiar with. More information on the different types can be found on the web site − http://www.SentryFirewall.com/.

Basically, the Sentry Firewall CD is meant to be configured just like a normal Slackware or Redhat or whatever Linux system. There are no GUIs, no scripts to do it for you. The idea behind the configuration of the CD is that you are able to reconfigure the system by replacing the startup scripts and the various configuration files normally present on the system at boot time. Most of these are simply text files and shell scripts that you need to edit by hand in order configure properly. There are, however, usually plenty of resources available to assist you in configuring a specific service or daemon(HOWTOs on linux.org, for example).

1.4 What's with all these branches(SENTRYCD/SENTRYCD−RH/SENTRYCD−xxx)? What's the difference between the branches?

First, let me explain briefly how the Sentry Firewall CD works. Basically, there is the "host" system, a Linux system that is based on one of several Linux distributions. Then there are the configuration scripts, written in perl, that run after the kernel boots and help configure the system on the fly. In general, it is possible to create a Sentry Firewall CD system based on nearly any Linux distribution while only modifying one of the five perl scripts.

So, to answer your question, each Sentry Firewall CD branch utilizes similar configuration methods, but are simply based on different Linux distributions. Since I'm a Slackware fan, I used that distribution as the foundation for the original Sentry Firewall CD(the "SENTRYCD" branch). It has always been my desire to utilize other Linux distributions for this project, which is why I created the "SENTRYCD−RH" branche. There will no doubt eventually be other branches and variations.

Sentry Firewall CD Development Branches:

- **SENTRYCD** − Slackware−like Sentry Firewall CD.
- **SENTRYCD−DEB** − Debian−like Sentry Firewall CD. (In Development)
- **SENTRYCD−RH** − RedHat−like Sentry Firewall CD. (Deprecated)

In any case, all the basic functionality is present in each branch. But since different Linux distributions are configured differently, using different rc files or files in /etc/sysconfig for example, some of the configuration directives(explained below) will vary between the two branches.

1.5 Minimum Requirements

- x86 computer with CD−ROM
- BIOS that supports the eltorito standard(booting from the cdrom).
- 32MB RAM(64MB or more recommended)
- Easy access to coffee/tea/soda or equivalent stimulant.
- Floppy disk drive(optional)

1.6 Copyrights and Disclaimer

The current copyright and disclaimer can be found on the website; http://www.SentryFirewall.com/files/COPYRIGHT. It applies to the Sentry Firewall CD, and all the scripts and documentation associated with it.

---

2. How the CD Works (Overview)

This section is just an overview to explain how the Sentry Firewall CD works, that is, from the process of loading the kernel to running the Sentry Firewall CD configuration scripts located on the RAMDisk.

2.1 The Boot Process

Booting from the CDROM is a fairly familiar process. The BIOS execs the bootloader(Syslinux) − which then displays a bootprompt and loads the kernel and ramdisk into memory. Once the kernel is running, the ramdisk is then mounted as root(/).

An obvious necessity for deploying CDROM based systems is the ability to dynamically configure the system for various environments with different configurations, which is what a good majority of this project is dedicated to building. A simple way to do this is to give the user the ability to customize the startup scripts located in /etc/rc.d before they are actually used, as well as the ability to customize other important system configuration files.

At boot time, the /etc and /etc/rc.d directories are nearly empty. On a Slackware system the first rc file to run is /etc/rc.d/rc.S − and it is from this file where we run the configuration scripts that look for a configuration file(sentry.conf), and place the proper configuration and system files in /etc and various subdirectories under /etc. On other Linux systems, such as RedHat, the configuration scripts would be run from rc.sysinit. If there is not a configuration directive for a specific file, or if a configuration file cannot be found, then the default system files are used − which are located in /etc/default/* on the ramdisk.

2.2 ISOLINUX

Early versions of the Sentry Firewall CD utilized the 2.88MB floppy emulation method, along with either lilo or syslinux to boot the kernel and load the ramdisk. This method proved very limiting for two reasons; A) the total size of the compressed ramdisk AND kernel was limited to 2.88MB, and B) it was quite slow compared to the current method.

The Sentry Firewall CD is currently utilizing the isolinux.bin boot record with no emulation in order to properly boot the CDs. This allows us to use a much larger ramdisk and offer a choice of several kernels to boot at boot time.

More information about syslinux can be found at syslinux.zytor.com.

2.3 The CD Configuration Scripts

As previously mentioned, our configuration scripts which reside in /etc/rc.d/SENTRY/ on the ramdisk are generally run from an rc script in /etc/rc.d/. The first script to run is called 'cd−config.pl', which is essentially the mainline for the entire program. The other scripts that are used are called 'get_config.pl', 'process_conf.pl', 'do_config.pl' and 'networking.pl'. These scripts were written specifically for this project, and are essentially the mainstay of the entire configuration process.

In depth review of these scripts is a little beyond the scope of this document, but is covered a bit in the file called 'DOCUMENTATION' available on the website (http://www.SentryFirewall.com/). The files are written in perl, and do several important things; read in and parse the configuration file(sentry.conf), locate and retrieve the important files detailed in the sentry.conf file, and replace the system default files with the ones the user has defined in the configuration file.

3. Obtaining the CDROM

3.1 Downloading

The CDROM is distributed as a gzip or bzip2 compressed iso image, and is generally between 95−105MB in size. ISO images for the sentyrcd−RH branch are generally much larger, between 150−200MB in size. Available download mirrors are listed on the websites; http://www.SentryFirewall.com/ or http://Sentry.Sourceforge.net/.

3.2 Purchasing

Although the iso image is free to use and distribute, copies of the Sentry Firewall CD mailed to you at a minimal cost. Custom versions of the CD and support can also be made available and tailored to a specific network configuration.

For more information about these services, please email me.

3.3 Burning the CDROM

This section will attempt a general overview on how to burn the CD iso image once you have obtained it from one of the mirrors. All the commands presume you're working in Linux. Buring ISO images in Windows is not covered in this howto. If you are using windows then check out the CD Burning Howto

First, let's decompress the iso image:
NOTE: Make sure you have enough disk space, the decompressed iso image can be somewhere between 250MB and 400MB.

```
blah@wherever:~$ gzip −d sentrycd.iso.gz

or

blah@wherever:~$ bzip2 −d sentrycd.iso.bz2
```

Verify the integrity of the iso image,

```
blah@wherever:~$ md5sum −b sentrycd.iso
```

Now, let's try to burn the CD. You'll need the 'cdrecord' utility available, it can be obtained here. You will want to run 'cdrecord −scanbus' in order to find the 'dev' value required for the following command. You will also need to know the write speed of your CDRW. Details on how to set this all up are beyond the scope of this document, please refer to the CD Writing HOWTO for more details.

```
blah@wherever:~$ DEV="DEV_LINE_HERE" SPEED="SPEED"
blah@wherever:~$ cdrecord −v −data speed=$SPEED dev=$DEV sentrycd.iso
```

That's it, you now have a Sentry Firewall CDROM. By the way, you may have to be 'root' to do all this.

Keep in mind, if you simply want to look at the ISO image without actually burning the CD, you can mount the image on a loopback device;

```
blah@wherever:~$ mount -o loop ./sentrycd.iso /MOUNT_POINT
```

Where "MOUNT_POINT" is where you would like the CD mounted. You may then 'cd' to the MOUNT_POINT directory and poke around – don't forget to 'umount' the image once you're finished. This assumes you have support in your kernel for the loopback device. You probably do, but once again, recompiling kernels is beyond the scope of this document.

4. Using the Sentry Firewall CDROM

4.1 Introduction

The configuration scripts which are run from /etc/rc.d/rc.S first look for a configuration file called 'sentry.conf' on a floppy disk which, if present, will be mounted on /floppy. In order to configure the Linux system for use in any particular environment the user must have the ability to replace the system default files with his/her own copies. The 'sentry.conf' file basically tells the configuration scripts which files it should replace and where those files are.

A good example of a sentry.conf file can be found on the Sentry Firewall CD in the directory /SENTRY/scripts/cd–config/. Configuration floppy disk images(1.44M) can also be found in /SENTRY/images/ on the CD. These files are also available on the website, http://www.SentryFirewall.com/

4.2 The sentry.conf file

The main configuration file for the system is called 'sentry.conf'. It will first be looked for on a floppy disk(/dev/fd0). The file accepts several configuration directives, many of which will be discussed below.

Example

A basic configuration file looks like the following (everything after a '#' sign is interpreted as a comment):

```
----snip----
## Basic Sentry Firewall CD config file(sentry.conf)

rc.local = /floppy/config1/rc.local
fstab = /floppy/config1/fstab

passwd = /floppy/config1/passwd
shadow = /floppy/config1/shadow

# EOF #
```

```
----snip----
```

The syntax is pretty simple, the default 'rc.local' file will be replaced with the user defined 'rc.local' file located in the '/floppy/config1/' directory. Same goes for 'fstab', 'passwd', and the 'shadow' file. But it is important to remember, the first place the sentry.conf file will be looked for is on /dev/fd0, which if found, will be mounted on /floppy. This is why all these files appear to be located in the /floppy directory, it is simply the mount point for the floppy disk.

NOTE: As of version 1.3.0, a user may now omit the `/floppy' prefix. So, for example a line in sentry.conf that says the following:

```
shadow = config1/shadow
```

Will be assumed to mean(in most cases) the following:

```
fstab = /floppy/config1/shadow
```

As long as /floppy/config1/shadow exists.

Unfortunately, you cannot arbitrarily replace files, for example the following will likely not be parsed correctly:

```
foo.conf = /floppy/config1/foo.conf
```

The configuration scripts only recognize a certain number of configuration files, so it probably won't know what to do with "foo.conf". There are other very easy ways to copy configuration files into their proper location, however. These methods will be discussed below.

4.3 Network Configuration

As of version 1.0.5, a new syntax for the configuration directives are recognized; those with an "http://" or "ftp://" prefix. This basically means that the following syntax is now supported:

```
inetd.conf = ftp://[user:pass@]123.123.123.123/config1/inetd.conf
hosts = http://[user:pass@]123.123.123.123/config1/hosts
```

As of version 1.3.0, "https://", "scp://", and "sftp://" URLs are also supported. For example:

```
shadow = scp://<user>:<pass>@123.123.123.123/dir/shadow
passwd = sftp://<user>:<pass>@123.123.123.123/dir/passwd
fstab = https://[user:pass@]123.123.123.123/dir/fstab
```

NOTE: The username and password fields are required when retrieving files via scp or sftp. Empty passwords are not permitted.

In order to accomplish this the configuration scripts need to have the ability to set up an ethernet interface, as well as obtain nameserver information from the sentry.conf file. The syntax to accomplish this is the following:

```
device{1..10} = <device>:<driver>:<IP address>[|Gateway_IP]

or..

device{1..10} = <device>:<driver>:dhcp[|Hostname]
```

And to set up a nameserver:

```
nameserver = <IP_ADDRESS>
```

Additionally, when retrieving files using "http", "https", or "ftp", you may also set up a proxy server. The following directives will allow you to do so (they may not all be required for your setup):

```
http_proxy = http://<hostname>/
ftp_proxy = http://<hostname>/
proxy-user = <PROXY_USER>
proxy-passwd = <PROXY_PASSWORD>
```

Passive FTP may also be required. If so, use the 'passive-ftp' option, ie:

```
passive-ftp = <on|off>  ## Default == off
```

So, for example to set up an interface called "eth0", which uses the "tulip" driver and can obtain its ip address from a DHCP server, we can use the following line:

```
device1 = eth0:tulip:dhcp
```

As you can see, a total of 10 devices are allowed. Let's say we now want to set up an interface "eth1" that uses an "rtl8139" chip, and has a static IP(192.168.1.2) and a default gateway(192.168.1.1):

```
device2 = eth1:8139too:192.168.1.2|192.168.1.1
```

NOTE: It is important to keep in mind that whatever devices you set up during the configuration process will be promptly taken down after the configuration is complete. This setup is only used so you can retrieve configuration files over the network, via http(s)/ftp/scp/sftp. For more permanent network configuration, please use the rc.inet1 file.

Example

```
----snip----
## Basic Sentry Firewall CD config file to retrieve files via HTTP(s)/FTP/SCP/SFTP.

device1 = eth0:tulip:192.168.1.2|192.168.1.1
nameserver = 123.123.123.123  ## This should be the IP of your DNS server.

rc.M = ftp://user:pass@config.sentry.net/node1/rc.M
rc.inet1 = http://user:pass@config.sentry.net/all_nodes/rc.inet1

passwd = scp://user:pass@config.sentry.net/all_nodes/passwd
shadow = sftp://user:pass@config.sentry.net/node1/shadow
```

```
# EOF #
----snip----
```

4.4 Other Useful Configuration Directives

Copy file /floppy/someconfig.conf to /etc/someconfig.conf –

```
/floppy/someconfig.conf |= /etc/someconfig.conf

OR, this does the same thing -

/etc/someconfig.conf = /floppy/someconfig.conf

and this is also possible(v1.3.0) -

/etc/someconfig.conf = ftp://<server>/someconfig.conf
```

Make a symlink called /etc/someconfig.conf that points to /etc/otherconfig.conf –

```
/etc/someconfig.conf => /etc/otherconfig.conf
```

The include directive. Grabs another sentry.conf file either from another location –

```
include = ftp://user:pass@config.sentry.net/node1/sentry.conf
```

Keep in mind, however, that the include directive is one of the first directives to be parsed. Any configuration directives parsed from the included sentry.conf file that conflict with directives in the previously parsed sentry.conf files will clobber the old ones.

4.5 Putting it all together, managing multiple nodes from a single location.

In order to manage multiple nodes at a single location, you can use a bare sentry.conf file located on a floppy disk, and then grab files from your ftp or http servers.

```
----snip----
## Basic Sentry Firewall CD config file.

device1 = eth0:tulip:dhcp
nameserver = <DNS_IP>
include = ftp://user:pass@config.sentry.net/node1/sentry.conf

----snip----
```

The included sentry.conf file will then be parsed, and files replaced via http or ftp if you like. You can now edit your sentry.conf and configuration files at a central location.

4.6 Example sentry.conf and disk images

An example configuration disk image is available on the CDROM. The disk is an ext2 formatted disk, and is located in the '/SENTRY/images/' directory on the CD. There is also a very complete sentry.conf file on the disk which may help clarify alot of these directives. Use a command like the following to create the configuration disk:

```
blah@wherever:~$ dd if=/cdrom/SENTRY/images/ext2-144.img of=/dev/fd0
2880+0 records in
2880+0 records out
```

The disk images and a sample sentry.conf file can also be found on the website, http://www.SentryFirewall.com/

---

5. Overview of Available Configuration Directives

5.1 Replacing rc/config files

To replace a file that is supported by the configuration scripts, you may use the following syntax:

```
filename_directive = /location/of/filename
```

Where "filename_directive is one of the directives listed below, and the location of the file is often '/floppy/filename'. The file location can also be a URL. The supported prefixed include "http://", "https://", "ftp://", "sftp://", and "scp://".

As previously mentioned, there are at least two Sentry Firewall CD branches with varying names like "SENTRYCD" and "SENTRY−RH". The only difference between these branches is the "host" Linux distribution that is utilized. And since Linux distributions utilize different files during bootup, the accepted directives for the two branches vary. For example, a Slackware system utilizes files such as "rc.S" and "rc.M" to boot into single and multi−user modes. Other Linux distributions, such as Red Hat, utilize different files such as "rc.sysinit" and various files located in /etc/rc.d/init.d/. Therefore, when running a sentrycd−RH system, which is not Slackware based, it would be pointless to have a directive that states the following:

```
rc.M = /floppy/rc.M
```

since a non−Slackware system wouldn't know to do with a file called "rc.M". In any case, it is for this reason that the configuration directives vary a bit between branches. The directives that are available can be found in the sentry.conf file in the SENTRY/scripts/cd−config/ directory, or on the website.

The "sysconf_dir" and "xinetd_dir" are unique to the "SENTRYCD−RH" branch. Unlike the other directives, these are used to replace the files located in the /etc/xinetd.d/ and the /etc/sysconfig/ directories. The /etc/sysconfig/ directory contains most of the configuration files used by the init scripts(in /etc/rc.d/init.d/) on systems such as Red Hat systems.

Example:

```
sysconf_dir = /floppy/sysconfig
or
sysconf_dir = ftp://123.123.123.123/node1234/sysconfig
```

Please note that "/floppy/sysconfig" and "/node1234/sysconfig" are *directories* that contain files you want placed in /etc/sysconfig/. The "xinetd_dir" directive is used in the same way.

NOTE: To replace files not supported by the configuration scripts, use the '|=' file copy directive discussed below.

5.2 'device' directive support

Set up an ethernet device to use during configuration.

```
     device[#] = [device_name]:[driver_name]:[IP_Address]<|gateway>
     device[#] = [device_name]:[driver_name]:dhcp<|hostname>

     NOTE: 1) <hostname> and <gateway> are optional, but sometimes required.
           2) Most ethernet devices are supported.  If you find one that isn't
              and you think it should be, please let me know.
           3) "device1" to "device10" are supported.

Examples:
     device1 = eth0:tulip:192.168.1.50|192.168.1.1
     device2 = eth1:via-rhine:dhcp
```

5.3 'nameserver' directive

Set up a nameserver to use during configuration.

```
     nameserver = <DNS_IP>
```

5.4 Proxy Support Directives

Set up a proxy for pulling files via http(s), or ftp.

```
     http_proxy = http://<hostname>/
     ftp_proxy = http://<hostname>/
     proxy-user = <PROXY_USER>
     proxy-passwd = <PROXY_PASSWORD>
```

5.5 Passive FTP Support

Use passive ftp instead of active ftp to retrieve files.

```
passive-ftp = <on|off>  ## Default == off
```

5.6 'include' directive

Retrieve and parse another 'sentry.conf' file.

```
include = </location/of/sentry.conf>

Or, with network support -

include = <ftp|http>://[<user>:<pass>@]<SERVER_IP></path/to/sentry.conf>
```

5.7 Copying files (|=)

Copy file from one location to the other.

```
     Syntax: source_file |= dest_file, OR
             dest_file = source_file

Example:  Copy file /floppy/daemon.conf to /etc/daemon.conf

          /floppy/daemon.conf |= /etc/daemon.conf
          or
          /etc/daemon.conf = /floppy/daemon.conf
          or
          /etc/daemon.conf = scp://<user>:<pass>@<server>/config/daemon.conf
```

NOTE: http(s)/(s)ftp/scp support is only available with Sentry Firewall CD versions >= 1.3.0.

5.8 Making Symlinks (=>)

Create a symlink

```
     Syntax: dest_file => source_file(where the symlink points to)

Example:
     Make symlink called /etc/somefile.conf that points to /etc/otherfile.conf
     /etc/somefile.conf => /etc/otherfile.conf
```

5.9 'cdrom' directive

Defines which device the CDROM is. Most of the time the CDROM is detected and mounted using the /etc/rc.d/rc.cdrom script. But this makes the process less error–prone.

```
     Syntax: cdrom = <DEVICE>

Example:
     cdrom = /dev/hdc
```

5.10 'cron' directive

Replace a user's crontab file(located in /var/spool/cron/crontabs/).

```
Syntax: cron:<USERNAME> = </LOCATION/OF/CRONTAB_FILE>
```

5.11 hostname

Defines the hostname of the local machine. This directive can be used to either point to a file containing the hostname of the local machine, or to define the hostname itself.

```
     Syntax: hostname = </path/to/file>
             or
             hostname = MYHOSTNAME
```

5.12 Other SENTRY–{RH,DEB} Specific Directives

Besides the "xinetd_dir" and "sysconf_dir" directives, mentioned above, there is another directive that is unique to the sentrycd–RH branch.

Start/Stop a Service or Daemon

This directive gives you the ability to start or stop a service at bootup. The syntax looks like the following:

```
     service:[start|stop] = <path/to/service_init_file>
```

For example:

```
     httpd:stop
     or
     httpd:start = /floppy/config/httpd
```

In the above example, we are telling the Sentry Firewall CD to either start or stop the http daemon at bootup. The optional argument "<path/to/service_init_file>" is usually not necessary, but is used to actually replace the startup script located in /etc/rc.d/init.d/, in case you ever wanted to do so.

To get a better idea of how this works, please take a look at the sample "sentry.conf" file located either on the CD or online at http://www.sentryfirewall.com/files/sentrycd−rh−devel/scripts/cd−config/sentry.conf

---

6. Setting Up a Firewall

6.1 Starting the Firewall

Ok, so the project is called the Sentry *Firewall* CD. So where's the firewall? Well, it's important to note that this system is capable of quite a bit more than your standard bootable floppy or CD firewall. In fact it is a pretty complete Linux system on a CD, and as with any Linux system the "firewall" is set up using scripts and various userland utilities such as ipchains or iptables.

IPChains or IPTables firewall scripts generally take the form of shell scripts that are customized by the user and run at boot−time. If you already have a ruleset for your firewall simply edit the "rc.firewall" directive in your "sentry.conf" file to point to your firewall script on your floppy or on a remote HTTP(S)/FTP/SCP/SFTP server as explained above. The firewall will then be run at boot time.

6.2 Using FWBuilder with the Sentry Firewall CD

FWBuilder(http://www.FWBuilder.org/) is a firewall configuration and management system. The advantage to this application is that it provides a graphical user interface to develop and modify firewall rulesets on various platforms using various utilities. The Firewall rulesets that are created with FWBuilder are completely compatible with the Sentry Firewall CD, and with just about any Linux firewall.

As with most Linux firewalls there are no X11 binaries or libraries on the Sentry Firewall CD, so you will need to develop the firewall ruleset on a separate workstation using fwbuilder and then upload the ruleset to the various firewalls/routers/nodes on the network. The following are the basic steps required to get your new fwbuilder ruleset running on the Sentry CD:

- Configure your new firewall to your liking with fwbuilder(duh).
- Save your firewall. Choose File−>Save As, and choose an appropriate name. The file will normally be saved as "whatever.xml".
- Compile the firewall. Choose Rules−>Compile. The ruleset will be compiled and turned into a shell script called "whatever.fw".
- You will then want to copy "whatever.fw" to your configuration floppy and use the "rc.firewall" configuration directive in your sentry.conf file to point to your new firewall script. The firewall script will be copied to /etc/rc.d/rc.firewall during the configuration process and run at boot−time.

Please note that it is not necessary to reboot the Sentry Firewall CD every time you update your firewall script. You may simply upload the new script to the Sentry Firewall and run it. But just make sure that you copy the final draft of your script to the configuration floppy so that it will be run at boot−time.

6.3 Using Webmin with the Sentry Firewall CD

As of version 1.5.0−rc3 Webmin(http://www.webmin.com/) is available on the CD. Among many of the other default modules available with webmin − of which not all have been fully tested − Webmin includes two modules for generating and managing your firewall setup. These modules are located in the "Networking" section of the webmin interface. In this section you will see the "Linux Firewall" and "Shorewall Firewall" modules, either of which are available for your use.

The addition of Webmin also adds four new configuration directives −

```
start_webmin = <enable | disable>           ## enable|disable webmin.  Default == disable.
webmin_config = <path/to/config>            ## Main webmin config(/etc/webmin/config).
miniserv.conf = <path/to/miniserv.conf>     ## Config file for webmin http(s) daemon.
miniserv.pem = <path/to/miniserv.pem>       ## SSL cert for webmin http(s) daemon.
                                            ## An SSL cert will be created by rc.webmin if
                                            ## one is not specified.
miniserv.users = <path/to/miniserv.users>   ## Password file used for webmin.
                                            ## Default user:pass is sentry:SENTRY.
                                            ## NOTE: If this file is not replaced webmin
                                            ## will NOT start!
```

Note: The modifications made by these web interface tools are, of course, not permanent. Any files altered will need to be placed on a floppy or on a remote server and declared in your sentry.conf file as explained in previous sections.

Many of these web interface tools do not simply generate a firewall script, but rather set up a firewall and use the 'iptables−save' and 'iptables−restore' utilities to dump and load the firewall. The file created by 'iptables−save' must be loaded using 'iptables−restore', it cannot be run like a shell script. By default this file is placed in "/etc/rc.d/rc.firewall.save". Once you configure your firewall to your liking you will need to place the rc.firewall.save file on a floppy or a remote server and declare its location using the "rc.firewall.save" directive in the sentry.conf file. With the sentrycd and sentyrcd−devel branches, the rc.firewall and rc.firewall.save files are normally run automatically at boot−time from rc.inet2.

As of verions 1.5.0−rc3 the Shorewall(http://www.shorewall.net/) firewall scripts are available on the Sentry Firewall CD. Webmin also comes with a module to configure and set up Shorewall, although Shorewall can be configured manually as well. Shorewall utilizes a number of configuration files located in /etc/shorewall. The sentry.conf file recognizes the "shorewall.conf" configuration directive, but if any of the other configuration files in /etc/shorewall need to be replaced you will need to do so manually using the "|=" configuration directive.

6.4 Other Sample Firewall Scripts and Tools

Sample firewall scripts can be found in the /SENTRY/scripts/firewall directory on the CD. These are just a few firewall scripts I found on the Internet and have put here for your convenience. If you do a search on google or freshmeat.net you will probably find several others pretty easily.

I have also added "Easy Firewall Generator" (http://easyfwgen.morizot.net/) and "IPTables Script Generator" (http://iptables.linux.dk/) to the CD. These are PHP scripts that can assist you in creating a ruleset for your Sentry Firewall CD system. In order to view these you will need to start the Apache web server on a running Sentry Firewall CD system, and then direct your browser to the IP address of your Sentry Firewall. The scripts should be available in the "firewall" directory.

Please note that these web−based scripts will often generate a script for you, but you will still need to take that generated script and place at on a floppy or on a remote server and edit the "rc.firewall" directive in the sentry.conf file to point to your new script.

6.5 Links to Other Firewall Resources

Netfilter HOWTO
Netfilter FAQ
Netfilter Tutorials

If there are any other resources you think I should add to this section, please email me at Obsid@Sentry.net.

---

7. Troubleshooting

7.1 Booting Problems

Booting problems are generally rare, and generally only occur on old and buggy, or somehow non−compliant hardware. Booting problems can be associated with a number of problems, depending upon at what point during the boot process the failure occurs. The following are possible causes of failure when booting from a CD.

- Old or buggy BIOSes that do not fully support the eltorito standard. System may fail to load the isolinux bootloader or the kernel.
- Problematic CDROM drives can cause various problems when booting the CD. CD may or may not boot, and will generally have trouble accessing files on the CD.
- Damaged CD, obviously can cause a number of problems, similar symptoms as above.
- Insufficient hardware resources. Please see the "Minumum Requirements" section of this howto for more information on what is required to boot the CD.
- In the case of booting the Sentry Firewall CD, old or buggy floppy disk drives or damaged floppy disks can also result in serious problems, including curruption of the data on the floppy disk. The inability for the configuration scripts to read and parse files contained on the floppy disk can seriously inhibit the capability of the system to configure itself properly.

In general, hardware issues cause the majority of problems during the boot process of the Sentry Firewall CD, and may not always be easy to diagnose. Generally, the first step in debugging a general boot problem is to try and boot another CD in the same machine to attempt to rule out a hardware problem. And then attempt to boot the Sentry Firewall CD in another machine to attempt to rule out damage to the CD. If both these tests produce no negative results, then perhaps swap out the CDROM drives in the two machines, if possible, and do the test again. Then perhaps check out the general mailing list(mentioned below) for further assistance.

7.2 Configuration Problems

This section deals with configuration problems with the "sentry.conf" file. The sentry.conf configuration file, as mentioned in previous sections, tells the configuration scripts what to do during boot time to configure the running system. Syntax errors in the script can cause a file to be misplaced, or for the directive to not be parsed at all.

Error messages during the boot process of the Sentry Firewall CD can help greatly in diagnosing potential syntax or other types of errors. So watch the CD boot and write down any error messages that may pop up. Also, during bootup a logfile detailing the configuration process is created at /var/log/SENTRY_LOG. If you can log in to the system after it has booted, then take a look at this file for any obvious error messages.

7.3 Frequently Asked Questions

A FAQ is currently being maintained on the Sentry Firewall website, it can be accessed via the following URL: http://Sentry.SourceForge.net/files/FAQ.

7.4 Mailing List

Thanks to SourceForge.net, there are mailing lists available for the Sentry CD. You can look through the archives, or subscribe to the general mailing list to ask questions or make comments. The following are links for the general Sentry−Users mailing list. Other mailing lists are listed at SentryFirewall.com.

- Subscribe to Sentry−Users
- Sentry−Users Archives

---

8. Building a Custom Sentry CD

8.1 Introduction

This section will attempt to describe how to create a custom Sentry Firewall CDROM. Unfortunately, I do not have time to go into every detail. But at the very least I will try and provide for you an overview of the CD creation process.

8.2 The development system(How I do it)

My development system consists of two separate Linux installations of the same distribution, depending on what branch I'm working on. First, I have a very complete <insert Linux distro here> installation on my main hard drive(/dev/hda). I then have /dev/hdb1, upon which I have another, bare bones, installation − this installation generally has no compiling tools or X stuff.

I usually have /dev/hdb1 mounted on /mnt, that's not a critical element, but I thought I'd mention it since I will refer to /mnt alot from now on. I then have a directory called /CD−FW on the /dev/hdb1 installation, that is, if /dev/hdb1 is mounted on /mnt, then the directory would be called /mnt/CD−FW/. Throughout this entire process, the installation on /dev/hda is the live running system, and it is from here that I compile the needed tools, kernels, etc and basically run everything.

To make this easy for you, the Sentry Firewall CD ISO is basically an exact copy of what's in /mnt/CD−FW/ on my hard drive. I simply use the 'mkisofs' utility on /mnt/CD−FW to create the ISO image.

If you simply want to get started, perhaps try the following steps:

- Install a basic slackware system on some other partition, /dev/hdb1 perhaps.
- Reboot into your normal(linux) system and mount this new partition, let's say on /mnt.
- Mount the Sentry CD somewhere, let's say on /mnt2
- **type:** mkdir /mnt/CD−FW
- **type:** cp −Rdp /mnt2/* /mnt/CD−FW/
- **type:** find /mnt/CD−FW/ −name 'TRANS.TBL' −type f −print | xargs rm −f
  This removes those 'TRANS.TBL' files that are created by mkisofs.
- Unmount /mnt2
- Run the following commands(in a script if you like) to update the /mnt/CD−FW/ directory:

```
cp -Rdp /mnt/bin /mnt/CD-FW/
cp -Rdp /mnt/sbin /mnt/CD-FW/
cp -Rdp /mnt/lib /mnt/CD-FW/
cp -Rdp /mnt/usr/bin /mnt/CD-FW/usr/
cp -Rdp /mnt/usr/sbin /mnt/CD-FW/usr/
cp -Rdp /mnt/usr/local/bin /mnt/CD-FW/usr/local/
cp -Rdp /mnt/usr/lib /mnt/CD-FW/usr/
cp -Rdp /mnt/usr/libexec /mnt/CD-FW/usr/
cp -Rdp /mnt/usr/share /mnt/CD-FW/usr/
cp -Rdp /mnt/usr/man /mnt/CD-FW/usr/
```

NOTE: The above commands may spit out errors when working with certain files(ie. hard links). These errors are annoying, but they're not critical at all.

You now have a development system like, or similar to, my own :−)

Now, if you ever want to install an rpm update or a Slackware package update(with upgradpkg), you can do the following:

```
root@mybox:~# cd /mnt; chroot /mnt

root@mybox:/# upgradepkg update.tgz
or
root@mybox:/# rpm --upgrade update.rpm

$ exit
```

Then, all I need to do is re−run the script mentioned above, the one that copies all those files, to update the /mnt/CD−FW directory.

8.3 The RAMdisk Image

That's all nifty, but now comes the hard part... making the ramdisk. If you take a look at the /isolinux directory on the CDROM, you will see a bunch of files, one of them is called 'initrd.img' − there are several others as well, such as isolinux.cfg, message.txt, and isolinux.bin. These files are required by isolinux in order to work properly. Take a look at those files and the documentation that comes with syslinux to get a better idea of what all that does. In any case, the 'initrd.img' file is, in fact, the compressed ramdisk image.

To take a look at the image, do something like the following:

```
blah@wherever:~$ cp /cdrom/isolinux/initrd.img /tmp/initrd.img.gz
blah@wherever:~$ gzip -d /tmp/initrd.img.gz
blah@wherever:~$ mount -o loop /tmp/initrd.img /MOUNT_POINT
```

In a nutshell, I use the file '/SENTRY/scripts/MK−CD/mkrootdsk.sh' to create the rootdisk. Please read that file and the disclaimer before you decide to use it. It runs perfectly on my system, but may not run well at all on yours. It basically attempts to create a rootdisk image to use with the Sentry CD, but it is very long and may be somewhat difficult to comprehend at times. This is what happens when I start hacking around and fail to utilize proper child safety restraints.

8.4 Making the ISO Image

The next file I use is called 'mkiso.sh'. The script generally just declares a few variables and runs the 'mkisofs' utility. The command I normally run looks like the following:

```
root@mybox:~# cd /mnt/CD-FW
root@mybox:/mnt/CD-FW# mkisofs -o sentrycd.iso -R -V "Sentry Firewall CD [v1.x.x]" -v \
   -T -d -D -N \
   -b isolinux/isolinux.bin \
   -c isolinux/eltorito.cat \
   -no-emul-boot -boot-load-size 4 -boot-info-table \
   -A "Sentry Firewall CD v1.x.x" .
........
```

And that's it, I burn the CD and test it. For reference, the following files are available on the CDROM and online at http://www.SentryFirewall.com/

- /SENTRY/scripts/MK−CD/mkrootdsk.sh (builds the rootdisk)
- /SENTRY/scripts/MK−CD/mkiso.sh (builds final ISO image)
- /SENTRY/scripts/MK−CD/record−cd.sh (burns the ISO to a CD)

9. More About the Sentry Firewall Project

9.1 Goals

The general goal of this project is mentioned several times within the documentation. That is simply, to build a bootable CDROM−based system that can be easily and dynamically configured. In the end, I wanted the configuration to rival that of any commercial router that utilizes configuration files(ie. Cisco). I also wanted the system to be simple, secure, and highly functional in a large number of operating environments − not just as a firewall. This, of course, has proven to be a difficult balance to maintain.

At the present time, the basic goals have been fulfilled. However, I believe there is still a great deal of development that can and needs to be done in order for the Sentry Firewall to be a truly diverse Linux distribution.

9.2 Supporting the Project

There are various ways one can support this project. The easiest and most common way is to simply utilize the system in a test or production environment and send me suggestions, bugs, or other such feedback. For those interested in assisting with the enhancement of any of the Sentry Firewall CD branches, please check out the TODO file located in /SENTRY/docs/TODO on the CD image, or online at http://www.SentryFirewall.com/files/sentrycd/docs/TODO or http://www.SentryFirewall.com/files/sentrycd−rh/docs/TODO.

I do, on occasion, make the Sentry Firewall CD available for purchase. I also accept donations including hardware, software, currency, or anything else that you feel can help. Revenues from such donations or CD sales will help support the continued development of the project. If you are interested in supporting this project please feel free to contact me at the information provided below, or email me at Obsid@Sentry.net.

9.3 About the Author

The Sentry Firewall project has only ever had a single developer, Stephen Zarkos(me) of Bellevue, Washington(USA). I began work on the project around April of 2000, probably ruining 200 CD−Rs before I got my first stable Sentry Firewall CD. And for the last two years I have been continuing to develop, enhance and maintain the project − give or take a few months here and there while I took a short hiatus(marriage, education, etc).

From the beginning, this project has proven to be quite popular, and has received a great deal of support and feedback from its loyal users. This kind of support has proven invaluable, and has kept me motivated to continue to develop this project. There is nothing I would rather do right now than work on and enhance this system, however since I do not get paid to develop this project, it is only a part−time endeavor. Even so, the positive comments and feedback I receive has without a doubt made this the most enjoyable project I have ever been a part of.

9.4 Contacting the Author

Mailing Address:
Sentry Firewall CD Project
C/O Stephen A. Zarkos
P.O. Box 6133
Bellevue, WA 98008

Email: Obsid@Sentry.net
