CHAPTER 9

How to Secure Your Computer

Linux is widely considered one of the most secure operating systems around. On a basic level, Linux is built from the ground up to be fundamentally sound, and it forces users to work with security in mind. For instance, it enforces the system of ordinary users who are limited in what they can do, thus making it harder for virus infections to occur.

In addition, Linux contains a firewall that is hard-wired into the kernel. It's called iptables (`www.netfilter.org/`), and is considered among the best by practically all computer security experts. Not only that, but it can protect your home PC just as well as it can protect the most powerful supercomputer. But, as with many Linux kernel components, iptables is difficult to use. It requires in-depth knowledge of how networks operate and an ability to hack configuration files, both of which are beyond the skills of many ordinary computer users. Fortunately, several programs act as interfaces to iptables and make it simple to operate (or at least as simple as any equivalent Windows-based software firewall, such as Zone Labs's ZoneAlarm).

As we saw in the "Post-Install Configuration" section of Chapter 5, Fedora allows you to configure and install a firewall. Irrespective of whether you install the firewall and what settings you use, you can use Fedora's Security Level Configuration tool (System ➤ Administration ➤ Firewall and SELinux) to change the firewall settings. This tool is somewhat primitive, in that it doesn't allow for greater control on the various settings.

However, configuring the firewall with a program like Firestarter, which we examine later in this chapter, can be done so quickly and with such little effort that there's no reason *not* to make use of the Linux firewall.

In this chapter, you'll learn how to configure the Linux firewall, but first, you'll spend some time examining more basic security concepts. Following that, we'll look at some elementary steps that you can take to protect your system.

Windows Security vs. Linux Security

If you've switched to Fedora from Windows, there's a very good chance that the security failings of Windows featured in your decision. By any measure, Microsoft's record on security within its products is appalling. A new and serious security warning appears seemingly on an ongoing basis, and a new and devastating virus makes news headlines with similar frequency (usually described as "a PC virus" rather than what it actually is: a Windows virus).

One argument is that Windows is the target of so many viruses merely because it's so popular. Although it's true that some of the underground crackers who write viruses dislike Microsoft, there's also little doubt that Windows has more than its fair share of security issues.

The situation is certainly getting better but, even so, Microsoft's last operating system, Windows XP, provides many good examples of why it's an easy target. Upon installation, the default user is given root powers. True, a handful of tasks can be performed only by the genuine administrator, but the default user can configure hardware, remove system software, and even wipe every file from the hard disk if she pleases. Of course, you would never intentionally damage your own system, but computer attackers use various techniques to get you to run malicious software (by pretending it's a different file, for example) or by simply infecting your computer across the Internet without your knowledge, which is how most worms work. Microsoft Vista, the latest operating system offering from Microsoft, tries to curb some of these defects through improved security measures such as user account control.

Viruses and worms also usually take advantage of security holes within Windows software. As just one example, a famous security hole within Outlook Express allowed a program attached to an e-mail message to run when the user simply clicked a particular message to view it. In other words, infecting a Windows machine was as easy as sending someone an e-mail message!

It's a different story with Linux. Viruses and worms are far rarer than they are on Windows. In fact, the total number of viruses and worms that have been found in the wild infecting Linux systems number far less than 100 (one report published in 2003 put the number at 40, and the number is unlikely to have grown much since then). Compare that to Windows, where according to the Sophos antivirus labs (`www.sophos.com/`), approximately 1,000 new viruses are discovered *every month*! The Sophos antivirus product now guards against about 100,000 viruses.

■ **Note** The high number of Windows viruses may be due to the quantity of Windows PCs out there. After all, for a virus to spread, it needs computers to infect, and it won't have trouble finding other Windows computers.

But while we would love to say that security holes are not found on Linux, the sad truth is that they're a fact of life for users of every operating system. Many so-called rootkits are available, generated by members of underground cracking groups. These are specialized software toolkits that aim to exploit holes within the Linux operating system and its software.

The bottom line is that while writing a virus or worm for Linux is much harder than doing the same thing on Windows, all Linux users should spend time defending their system and *never* assume that they're safe.

Root and Ordinary Users

As we've mentioned in earlier chapters, Linux makes use of something called the *root* user account. This is sometimes referred to as the *superuser* account, and that gives you an idea of its purpose in life: the root user has unrestricted access to all aspects of the system. The root user can delete, modify, or view any file, as well as alter hardware settings.

Linux systems also have ordinary user accounts, which are limited in what they can do. Such users are limited to saving files in their own directory within the `/home` directory (although the system is usually configured so that an ordinary user can read files outside the `/home` directory, too). But an ordinary Fedora user cannot delete or modify files other than those that he created or for which he has explicitly been given permission to modify by someone else.

On most Linux systems, it's possible to type `root` at the login prompt and, after providing the correct password, actually log in as root and perform system maintenance tasks. Regular users can also borrow superuser powers whenever they're required. For this to happen, they still need to provide the root login password. With desktop programs, they are prompted to enter the root password, but at the command prompt, users need to use the `su -` command to inherit superuser privileges.

Note Often, people associate the `su` command with *superuser*. The *su* actually stands for *switch user* or *substitute user*. The `su` command can be used to inherit any users' privileges.

Most key operating system files "belong" to root, which is to say that only someone with superuser powers or the root user can alter them. Ordinary users are simply unable to modify or delete these system files, as shown in Figure 9-1. This is a powerful method of protecting the operating system configuration from accidental or even deliberate damage.

Note Along with the root and ordinary user accounts, there is a third type of Linux account, which is similar to a limited user account, except that it's used by the system for various tasks. These user accounts are usually invisible to ordinary users and work in the background. For example, the shutdown subsystem has its own user account that Fedora uses to shutdown Fedora. The concepts of users and files are discussed in more depth in Chapter 14.

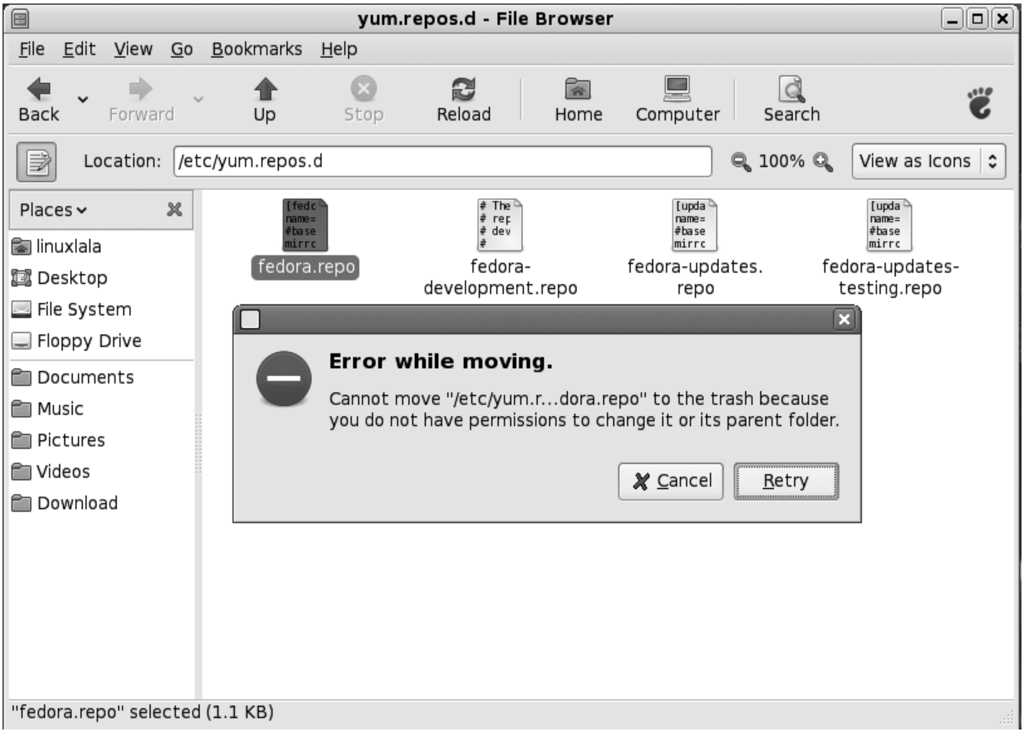
ARE YOU A CRACKER OR A HACKER?

Linux users are often described as *hackers*. This doesn't mean they maliciously break into computers or write viruses. It's simply using the word *hacker* in its original sense from the 1970s, when it described a computer enthusiast who was interested in exploring the capabilities of computers. Many of the people behind multinational computing corporations started out as hackers. Examples are Steve Wozniak, a cofounder of Apple Computer, and Bill Joy, cofounder of Sun Microsystems.

The word *hacker* is believed to derive from model train enthusiasts who "hacked" train tracks together as part of their hobby. When computing became popular in the early 1970s, several of these enthusiasts also became interested in computing, and the term was carried across with them.

However, in recent years, the media has subverted the term *hacker* to apply to an individual who breaks into computer systems. This was based on ignorance, and many true hackers find the comparison extremely offensive. Because of this, the term *cracker* was invented to clearly define an individual who maliciously attacks computers.

So, don't worry if an acquaintance describes herself as a Linux hacker, or tells you that she has spent the night hacking. Many Linux types use the term as a badge of honor.



Location: /etc/yum.repos.d

Error while moving.

Cannot move "/etc/yum.r...dora.repo" to the trash because you do not have permissions to change it or its parent folder.

"fedora.repo" selected (1.1 KB)

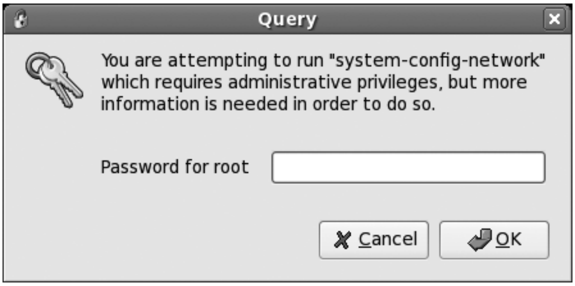
Figure 9-1. *Ordinary users are simply unable to modify or delete essential system files under Linux.*

Common-Sense Security

As you start to understand how Fedora works, you'll become more and more aware of common-sense methods that will protect your system. However, we'll outline a few of these now to get you started:

Entering your password: Be very wary if you're asked to enter the root password. You'll be asked to provide the root password when following many of the configuration steps within this book, for example, and this is acceptable and safe. But if you're asked to do so out of the blue, then you should be suspicious. If the root password prompt dialog box appears when you run a file that shouldn't really need root permissions, such as an MP3 or OpenOffice.org file, then you should treat the situation with caution. Each time the root password dialog appears (shown in Figure 9-2), you should read what it says carefully. It often informs you why the root password is required.

Installing new software: Be careful in choosing programs to download and install. Because Linux works on the basis of open source code, anyone can theoretically tamper with a program and then offer it for download to the unwary. This very rarely happens in real life. Even so, it's wise to avoid downloading programs from unofficial sources, such as web sites you find online via a search engine and whose authenticity you cannot totally trust. Instead, get software from the web site of the people who made it in the first place or, ideally, from the official Fedora software repositories or other trusted repositories (discussed in Chapter 8).



Query

You are attempting to run "system-config-network" which requires administrative privileges, but more information is needed in order to do so.

Password for root

Figure 9-2. *Beware if you're asked to type your password out of the blue or for no apparent reason.*

Updating your system: Always ensure that your system software is completely up to date. As with Windows, many Fedora programs have bugs that lead to security holes. Crackers target such vulnerabilities. Downloading the latest versions of Fedora software ensures that you not only get the latest features, but also that any critical security holes are patched. As with most versions of Linux, updating Fedora is easy and, of course, it's also free of charge. You'll learn how to get online updates in the next section.

Locking up your PC: Limit who has physical access to your computer. Any Fedora system can be compromised by a simple floppy boot disk, by a LiveCD distribution, or from the GRUB boot loader. Booting a PC using such disks gives anyone complete root access to your system's files, with no limitations. This is for obvious reasons; the idea of a boot disk is to let you fix your PC should something go wrong, and you cannot do this if you're blocked from accessing certain files. When Linux is used on servers that hold confidential data, it's not uncommon for the floppy and CD-ROM drives to be removed, thus avoiding booting via a boot disk. Such computers are also usually locked away in a room or even in a cupboard, denying physical access to the machine.

Securing GRUB

The GRUB boot loader has a security feature that disallows people from using it to become the root user. The GRUB boot loader can be used to enter Fedora as the root user, without ever having to enter a password. To do this, at the GRUB menu, highlight the Fedora entry and press E. This allows you to edit the entry. Highlight the kernel entry using the arrow keys and press E again. Now type the word `single` at the end of the line, as follows:

```
rhgb quiet single
```

Now press Enter and then B to boot into Fedora. You will soon be dropped to the root shell. There will be no graphical desktop, but you will have complete access to the system.

To stop this from happening, you can password protect the GRUB boot loader such that you are prompted to enter a password to boot into Fedora, or even if you wish to edit the GRUB entries. Follow these steps to create a GRUB password:

1. Open a terminal (Applications ➤ System Tools ➤ Terminal).
2. Run the command `/sbin/grub-md5-crypt`.
3. You will be asked for a password. This will be used on the GRUB boot loader, so be careful of what you use.

4. You will be invited to enter the password again. This is to ensure that you didn't mistype the first time:

   ```
   [root@localhost ~]# grub-md5-crypt
   Password:
   Retype password:
   $1$diwIw1$I5iFKODj2Ve99FOLwr5.A/
   ```

5. The last line in the preceding listing is the encrypted form of the password typed in. The encrypted string might have a dot or a slash at the end, as in the preceding case. This is part of the encrypted password.

6. From the terminal, run the command `gedit /boot/grub/grub.conf` and enter the encrypted string under the `initrd` line, like so:

```
title Fedora Core (2.6.18-1.2798.fc6)
       root (hd0,0)
       kernel /vmlinuz-2.6.18-1.2798.fc6 ro root=/dev/VolGroup00/LogVol00 rhgb quiet
       initrd /initrd-2.6.18-1.2798.fc6.img
password --md5 $1$diwIw1$I5iFKODj2Ve99FOLwr5.A/
```

7. Save the file and close Gedit. Now whenever you boot into Fedora or try to edit the GRUB entry, you'll be asked to enter the password. Just type in the original password and press Enter. GRUB will then compare the password with the encrypted string, and if they match, you will be able to boot into Fedora.

■ **Caution** Remember that anyone with physical access to your computer can still bypass the GRUB security with the aid of a LiveCD Linux distribution. A BIOS password, however, can render a LiveCD distribution useless for this purpose.

WHERE'S THE ANTIVIRUS?

At first glance, it may appear that there are very few Linux antivirus programs. Actually, many of these exist, but they're designed to work on server computers and primarily guard against Windows viruses, in addition to the handful of Linux viruses. The idea is that they protect Windows users who access the server.

Very few antivirus products are aimed at the Linux desktop. However, one example includes F-Secure's Anti-Virus for Linux Workstations. This costs around $60 dollars and is available from `www.f-secure.com/products/fsavcsl.html`. AVG (`www.grisoft.com/`) and Kaspersky (`http://www.kaspersky.com/linux`) also produce Linux workstation versions of their antivirus products.

The main issue with all of these programs is that they're not open source, as with most of the Linux software included in Fedora. If you absolutely must have your entire system running free software, consider ClamAV (`www.clamav.net/`). This is a product designed to work on Linux servers but is flexible enough to run on desktop computers, too. ClamAV is included in the Fedora software repository, and so is available via Pirut Package Manager. Be aware that ClamAV is a command-line program, however. You'll need to read its man page to learn how it works. In addition, you might choose to read the online documentation at `www.clamav.net/doc/`.

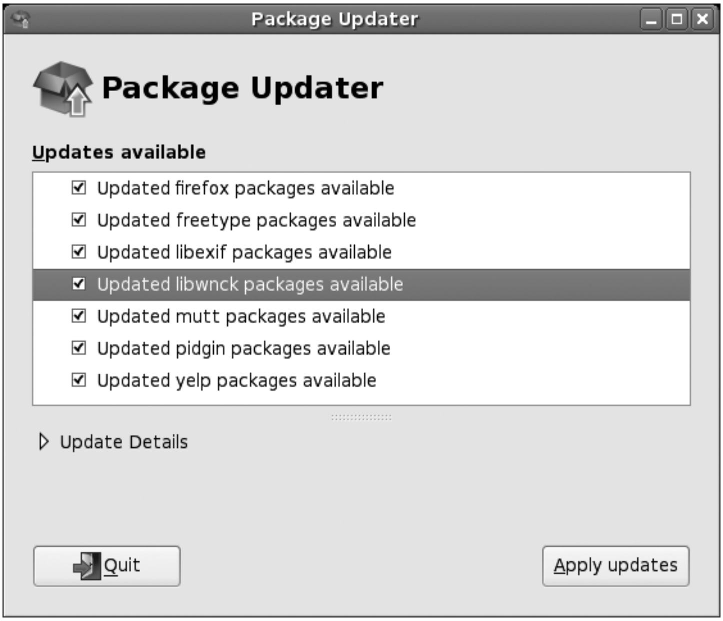
Online Updates

The Fedora notification area (the equivalent of the Windows system tray) contains a program called Puplet that automatically monitors the package repositories and tells you when updates are available.

Puplet runs each time you boot Fedora. If there are updates available, an icon appears in the notification area that informs you of available updates. In addition, each time you boot, you will see a speech bubble telling you whether updates are available.

You can apply all the updates by clicking the icon and selecting Apply. You can use the Pup package updater program to see a list of all the available updates, as shown in Figure 9-3, click Applications ➤ System Tools ➤ Software Updater (you'll be asked for the root password). After selecting a package, you can click Update Details to see details about the update—whether it is a bug fix, a feature upgrade, a new version of the software, or security fix. Additionally, Update Details informs you whether an update requires you to restart the computer.

By default, all updates are set to be installed. Remove the check from the check box if you don't want to apply an update. Clicking the Apply Updates button will install all the selected updates.



Package Updater

Package Updater

Updates available

☑ Updated firefox packages available
☑ Updated freetype packages available
☑ Updated libexif packages available
☑ Updated libwnck packages available
☑ Updated mutt packages available
☑ Updated pidgin packages available
☑ Updated yelp packages available

Figure 9-3. *You'll be informed if your system is in need of updates, and Pup can take care of everything for you.*

Be aware that some updates can be large and might take some time to download, particularly if you're doing it for the first time after installing Fedora.

Once the downloads have finished, you probably won't need to reboot unless the kernel file has been updated.

The Fedora Firewall

A *firewall* is a set of programs that protects your PC when it's online. It does this by watching what data attempts to enter your PC from the Internet and allowing in only what it is sure is secure (which usually is what you've asked for). It also attempts to close off various aspects of your Internet connection so that crackers don't have a way in should they target your system.

Although Fedora includes a powerful firewall in the form of iptables, you'll also need a program that can manage it. Here, we'll show you how to use Firestarter, available from the Fedora software repository, for this purpose. Together with the built-in firewall, this really does provide industrial-level protection.

The benefit of configuring the firewall is that even if your system has security vulnerabilities because of buggy software, crackers will find it a lot harder to exploit them across the Internet. When someone attempts to probe your system, it will appear to be virtually invisible.

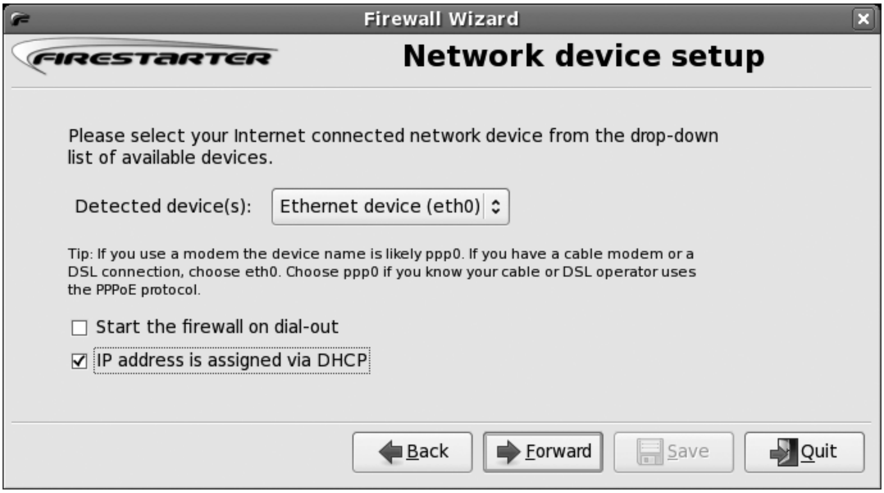
Caution Although software firewalls such as the one built into Linux offer a high level of protection, it's best to use them in concert with a hardware firewall, such as that provided by most DSL/cable broadband routers (curiously, some of these routers actually use Linux's iptables software as well). Many security experts agree that relying solely on a software firewall to protect a PC affords less than the best level of protection.

Installing Firestarter

Let's get started by downloading and installing Firestarter. Follow these steps:

1. Select System ➤ Applications ➤ Add/Remove Software. Click the Search button and enter **firestarter** as a search term. In the list of results, locate the program and click the check box. Then choose to install the package.
2. You'll find Firestarter under the Applications ➤ System Tools menu. Alternatively, you can start Firestarter from the command-line. Open a terminal and type **su -c 'firestarter'**. When you run Firestarter for the first time, it will walk you through a wizard.
3. Click the Forward button to continue the wizard beyond the introductory page.
4. The first step asks which network interface Firestarter should configure, as shown in Figure 9-4. If you use an Ethernet card, have a wireless card, or attach a broadband modem directly to your computer, the answer will probably be `eth0` or `wlan0`. However, if you use a modem, the answer is `ppp0`.
5. Put a check in the "IP address is assigned via DHCP" check box, *unless you're using a modem*.
6. You're asked if you want to enable Internet connection sharing. This allows you to turn your computer into an Internet router and can be very useful in certain circumstances. You can activate this later on by running the wizard again (to rerun the wizard, simply click Firewall on Firestarter's main window, and then click Run Wizard).
7. Save your settings. The Firestarter main window then opens.

Note If you haven't enabled your firewall, click System ➤ Administration ➤ Firewall and SELinux, and choose to enable the firewall.



Network device setup

Please select your Internet connected network device from the drop-down list of available devices.

Detected device(s): Ethernet device (eth0)

Tip: If you use a modem the device name is likely ppp0. If you have a cable modem or a DSL connection, choose eth0. Choose ppp0 if you know your cable or DSL operator uses the PPPoE protocol.

□ Start the firewall on dial-out

☑ IP address is assigned via DHCP

Figure 9-4. *Firestarter includes a wizard to walk you through the basics of firewall configuration.*

Configuring Firestarter

Firestarter works by controlling the data that goes in and out of your computer via your Internet or network connection. By default, it blocks every type of uninvited inbound connection but allows every type of outbound connection. This needs some explanation.

Whenever you click a link on a web page, your computer sends a request for data to the web server hosting the web page. Within a few milliseconds, that data will be sent to your computer. This is an *inbound* data connection. The Linux firewall is clever enough to realize that the data was requested by you, so it is allowed through. However, any uninvited connections are turned away. If, out of the blue, someone attempts to connect to your computer via the popular Secure Shell (SSH) tool, as just one example, he won't be allowed to make that connection. This is a good thing because it makes your computer secure. Crackers are turned away whenever they try to connect, no matter *how* they try to connect.

But in some circumstances, allowing uninvited connections is useful. For example, if you create a shared folder for other computers in your office to connect to, they will frequently make uninvited inbound connections to your computer. And if you want to make use of SSH to connect to your computer remotely, you will need to allow such incoming connections. Therefore, Firestarter lets you allow certain types of inbound connections.

Outbound traffic is any kind of data originating on your computer that is sent out on the network and/or Internet. By default, Firestarter allows out all data, no matter what it is. This is described as a *permissive* policy. But Firestarter can be configured to block all outgoing connections *apart from those you opt to allow through*. This is described as a *restrictive* policy and can be useful in blocking certain types of programs that "phone home" with personal data about you, such as spyware. It can also prevent certain types of viruses and worms from spreading. You are much safer on Linux than Windows considering that spyware is very rare in Linux.

The downside is that you must configure Firestarter to take into account every type of outgoing data connection, such as those for web browsers, instant messaging programs, and so on. You can configure Firestarter by clicking the Policy tab in the main program window. Click the Editing drop-down list and choose to configure either the inbound traffic policy or the outbound traffic policy.

■**Note** Firestarter is used only to configure the built-in firewall and doesn't need to be running for the firewall to work. Once you've finished configuration, you can quit the program. You'll need to use it again only if you wish to reconfigure the firewall.

Setting Inbound Rules

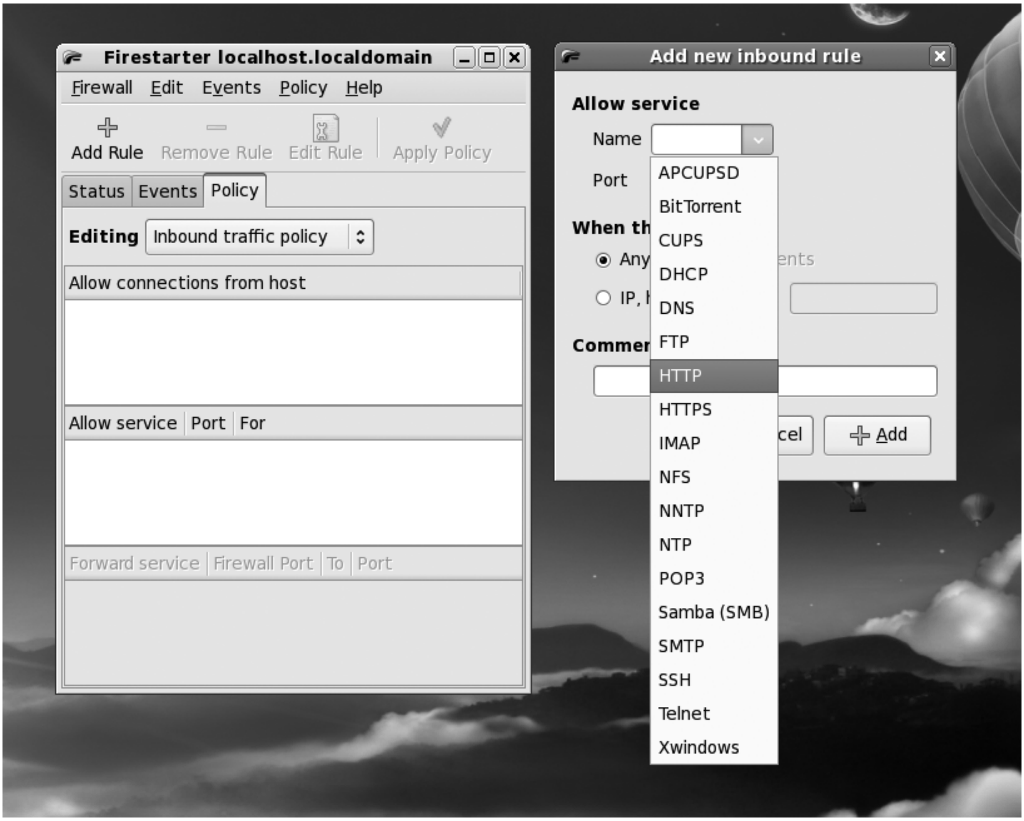
For most users, Firestarter's default inbound traffic policy will be perfectly acceptable. It configures the firewall to disallow all uninvited incoming data, apart from certain diagnostic tools, such as ping, traceroute, and so on. You can choose to disallow those as well, as described shortly in the "Turning Off Diagnostic Services" section.

You might wish to allow an incoming connection if you intend to connect to your computer via SSH from a remote location or if you have a shared folder created for other computers in your office. It's a must if you're running the BitTorrent file sharing application. Additionally, if you run a web, e-mail, or other type of server on your computer, you will need to allow the correct type of incoming connection here.

Here's how to set inbound connection rules:

1. In the Firestarter main window, click the Policy tab. Select Inbound Traffic Policy in the Editing drop-down list.
2. Right-click in the second box on the Policy tab (with the headings Allow Service / Port / For), and then select Add Rule.
3. The Add New Inbound Rule dialog box appears. In the Name drop-down list, select the type of outgoing connection you want to allow, as shown in Figure 9-5. To allow others to access shared folders on your computer, select Samba (SMB). To allow SSH or BitTorrent connections to your computer, select the relevant entry from the list. Selecting the service will automatically fill in the Port box, which you shouldn't alter unless you know exactly what you're doing.
4. If you know the IP address of the computer that's going to make the incoming connection, you can click the IP, Host or Network radio button, and then type in that address. However, the default of Anyone will allow anyone using any IP address to connect to your computer.
5. Click Add. Back in the main Firestarter window, click the Apply Policy button.

■**Note** You'll need to return to Firestarter whenever you activate new services on your computer. For example, in Chapter 12, we will look at accessing Windows shares across a network, and you'll need to enable SMB incoming and outgoing access for this to work. In Chapter 33, we will look at using the SSH service, which will have to be allowed through the firewall. In other words, securing your computer isn't something you can do once and then forget about. It's a continual process.



Editing: Inbound traffic policy

Name: HTTP

Figure 9-5. *Creating an inbound rule enables computers to connect to your PC uninvited.*

Setting Outbound Rules

By default, Firestarter allows all types of outgoing connections and, as with its incoming connections policy, this is by no means a bad choice for the average user. It's certainly the option that involves the least fuss. However, by opting to go with a restrictive traffic policy, you can completely control what kind of data leaves your computer. Any type of data connection that isn't authorized will be refused; as far as the program sending the data is concerned, it will be as if your computer did not have a network or Internet connection.

Here's how to set outbound connection rules:

1. In the Firestarter main window, click the Policy tab. Select Outbound Traffic Policy in the Editing drop-down list.
2. Click the Restrictive by Default, Whitelist Traffic radio button.
3. In the second empty box at the bottom of the Policy tab, right-click and select Add Rule.

4. The Add New Outbound Rule dialog box appears. Select the type of data connection you wish to allow. At the very least, you should select HTTP. This will allow your web browser to operate correctly (it's also needed to allow the Pirut Package Manager and Package Updater programs to work). You should also add a rule for POP3 and another for SMTP, without which your e-mail program won't work. Selecting the type of service will fill in the Port box automatically. You shouldn't alter this unless you know what you're doing.
5. Click the Add button to add the rule. Back in the Firestarter main window, click Apply Policy.
6. Test your settings with a program that uses the services you've just authorized.

Caution If you created an inbound rule, you'll need to create a matching outbound rule. If you created an incoming rule for BitTorrent, for example, you'll need to create an outgoing rule for BitTorrent, too.

You can delete both incoming and outgoing rules by right-clicking their entries in the list.

Turning Off Diagnostic Services

Certain network tools can be misused by crackers in order to break into a computer or just cause it problems. In the past, the traceroute and ping tools, among others, have been used to launch denial-of-service (DoS) attacks against computers.

Fedora is set to allow these tools to operate by default. If you want to adopt a belts-and-braces approach to your computer's security, you can opt to disable them. If you don't know what ping and traceroute are, you're clearly not going to miss them, so there will be no harm in disallowing them. Here's how:

1. In the Firestarter main window, click Edit ➤ Preferences.
2. On the left side of the Preferences window, click ICMP Filtering. Then click the "Enable ICMP filtering" check box, as shown in Figure 9-6. *Don't* put a check in any of the boxes underneath, unless you specifically want to *permit* one of the services.
3. Click the Accept button to finish.

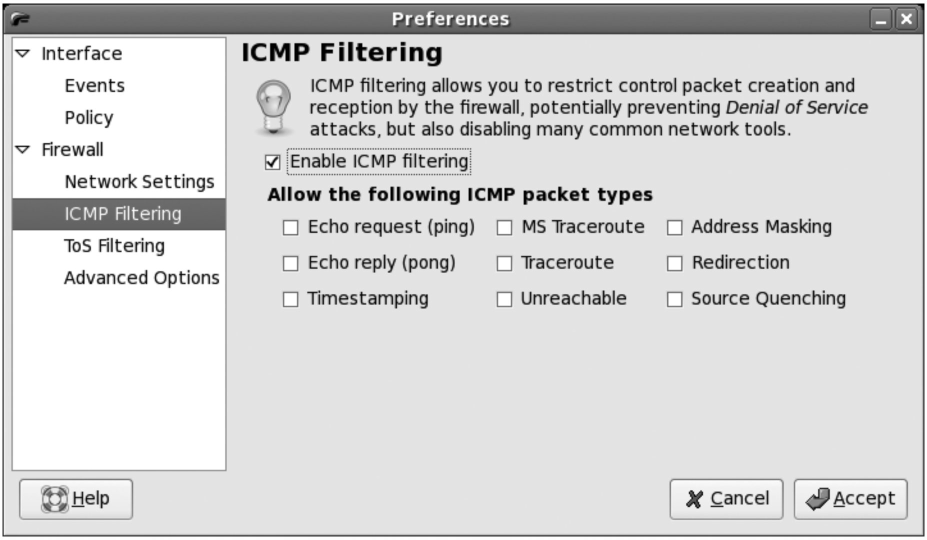
PARANOIA AND SECURITY

There's a fine line between security and paranoia. Using Firestarter gives you the opportunity to ensure your system is secure, without needing to constantly reassess your system for threats and live in fear.

When considering your system security, remember that most burglars don't enter a house through the front door. Most take advantage of an open window or poor security elsewhere in the house. In other words, when configuring your system's security, you should always select every option and extra layer of security, even if it might not appear to be useful. You should lock every door and close every window, even if you don't think an attacker would ever use them.

Provided a security setting doesn't impact your ordinary use of the computer, you should select it. For example, deactivating the ping response of your computer might sound like a paranoid action, but it's useful on several levels. First, it means your computer is less easy to detect when it's online. Second, and equally important, it means that if there's ever a security flaw in the ping tool (or any software connected with it), you'll be automatically protected.

This illustrates how you must think when configuring your system's security. Try to imagine every situation that might arise. Remember that you can never take too many precautions!



ICMP Filtering

ICMP filtering allows you to restrict control packet creation and reception by the firewall, potentially preventing *Denial of Service* attacks, but also disabling many common network tools.

☑ Enable ICMP filtering

Allow the following ICMP packet types

☐ Echo request (ping) ☐ MS Traceroute ☐ Address Masking
☐ Echo reply (pong) ☐ Traceroute ☐ Redirection
☐ Timestamping ☐ Unreachable ☐ Source Quenching

Figure 9-6. *By deactivating traceroute, ping, and other services, you can add extra protection to your PC.*

Summary

In this chapter, we've looked at what threats your system faces and how security holes can be exploited by malicious interests. You learned about measures you can take to protect your system, such as updating it online and configuring the system's firewall. We also discussed some common-sense rules you can follow to keep your system safe.

In the next chapter, we move on to looking at how your Fedora system can be personalized and how to set up everything to suit your own preferences.