Guarddog Firewall Configuration

Your very own guard dog against malicious crackers and "script kiddies".

PHIL BARNETT

Does the name Guarddog bring an image to mind? A brown leather collar with spikes around the neck of a large, muscled, snarling canine? Perhaps we need to reduce your anxiety about having a guard dog. This one won't eat you out of house and home, and it won't be aggressive with the neighbors. It will sit when you tell it to and will roll over only on your command. What we are talking about here is a guard dog for your computer.

Firewalls are now installed on just about every computer, and for good reason. The Internet is not a safe place to go barefoot. It hasn't been for a long time. Geeks have been making firewalls for years. Really geeky firewalls. Firewalls that almost nobody understands. A question often asked is, "How well can a firewall protect me if I don't understand how it works?" Probably not as much as it could if you had better control of it.

In mid-2000, Simon Edwards put the first version of his firewall configuration tool, Guarddog, on the Internet for everyone to use. Since that time, Simon has released a new version once or twice a month. This series of improvements has culminated with his most recent stable release, the December 16, 2004 2.4.0 version.

I wrote to Simon to get a little background on why he started the project. Here's his response:

> I've had a strong interest in usability and GUI design for a long time, and about the time that Guarddog started, I was also very interested in computer security. What I learned from computer security is that many security problems are simply caused by errors in the configuration of the software by the user, what people might refer to as a "human error".
>
> Another important principle in computer security, this time directed more toward the design of network firewalls in particular, is whitelisting. This idea is simply, "Better to block everything and allow what is known to be good through, instead of the other way around, for example, filtering with a blacklist."
>
> Looking at the firewall programs and scripts available for Linux at the time, I saw that for securing a small network, all available programs failed one or both principles.
>
> So that is how Guarddog started. It is my attempt to create a really paranoid firewall that also tackles the difficult configuration error problem with good user-interface design. Guarddog was designed starting from the point of view of the user, and not from the underlying network filtering system. This is why Guarddog is so different, and easier to use than every other firewall program or script on Linux.

Simon has done a great job of removing the complexity of configuring a firewall. Instead of using an editor to make changes to a cryptic looking text file that the firewall uses, you use a graphical interface and you tell it what tasks you want to accomplish. The Guarddog Project motto is: "Protecting your computer with a cute little dog".

INSTALLATION

If you are running a Linux distribution that has a package management system, your first stop should be to find out if your distribution already has Guarddog installed, or a Guarddog package on the CD or in an Internet repository ready for you to install. If you can install Guarddog that way, you will save time. If this is the case, you can use that install method and jump directly to the Planning section of this article.

If your distribution doesn't support a Guarddog install, you can download an installation file for several distributions at http://www.simonzone.com/software/guarddog/#download.

FOR GEEK EYES ONLY

And, of course, the ultimate installation file is there as well, the tarball. The tarball file has been a longtime method of distribution of source code that is packaged in

a way to be installed on many different platforms. Installing a tarball is a five-step process. Download, uncompress, configure, compile and install.

If you didn't find an install by one of the two easier methods above, then you'll have to download and install the tarball file. As I write this article, the name of the current tarball file is http://www.simonzone.com/software/guarddog/guarddog-2.4.0.tar.gz.

You need to be logged in as root to install this kind of system utility. In my last article [July 2005], I talked about logging in only as a regular user most of the time. This is one of those times that you need to be a system administrator to perform the install. To become the system administrator, open a command shell and run the Switch User command (note the hyphen):

```
su -
```

After you enter this command, you'll be asked for the root password. Enter it correctly, and you are now the system administrator and you'll be in the /root directory. Most systems change the prompt from $ to # when you are logged in as the system administrator.

Almost all systems now have the wget command available, and it's a great way to grab a file. So, here's the command (you'll need to correct it if a new version is available):

```
wget http://www.simonzone.com/software/guarddog/guarddog-2.4.0.tar.gz
```

This command fetches the file and brings it to your local directory. If you don't have wget, be creative. There are dozens of ways to fetch a file. Use one of them.

Next in the process is to uncompress the tarball:

```
tar -xzvf guarddog-2.4.0.tar.gz
```

This will uncompress the files into their original layout as the author created them. In this case, the author put his files into a directory, so we need to move into it to continue:

```
cd guarddog-2.4.0
```

Once this is done, the next step is to run a script that determines how your machine is set up and configures Guarddog to be ready to compile on your machine. This is typical of the tarball compiling process. Run it now:

```
./configure
```

When the script completes, you are ready to compile. If the script stopped early, it will tell you what is missing from your system. Generally, you go get the missing package and try again. Most systems will have everything needed. After you have successfully run the configure script, it's time to compile Guarddog. So, do it:

```
make
```

Now, that wasn't too hard was it? Your computer compiles all of the Guarddog source code. The amount of time this process takes depends on how powerful your computer is. It took about a minute on my Athlon XP 2500+. You've just compiled a tarball, but it's not installed yet. The final step is to run the installer. In a tarball, the installer is generally part of the make process. You add a parameter and the files get installed to their final destination. In this case, the command is:

```
make install
```

And you are done! You can type:

```
which guarddog
```

to see where it is installed. The default installation is /usr/bin/guarddog. You are done with the system administration part of this install, so it's time to exit from your root login by running the exit command now:

```
exit
```

If you installed from a tarball, you will need to create an icon to run Guarddog. In KDE, right-click the desktop and select Create New→File→Link to Application. This pops up the application link wizard.

You need to fill in four things here to make the icon work properly. First, you need a caption for the icon. Replace the words Link to Application with

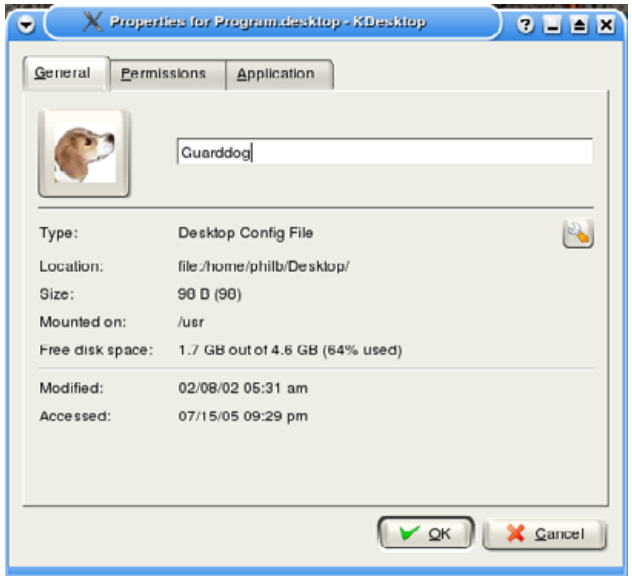

Figure 1. Creating the Guarddog Icon

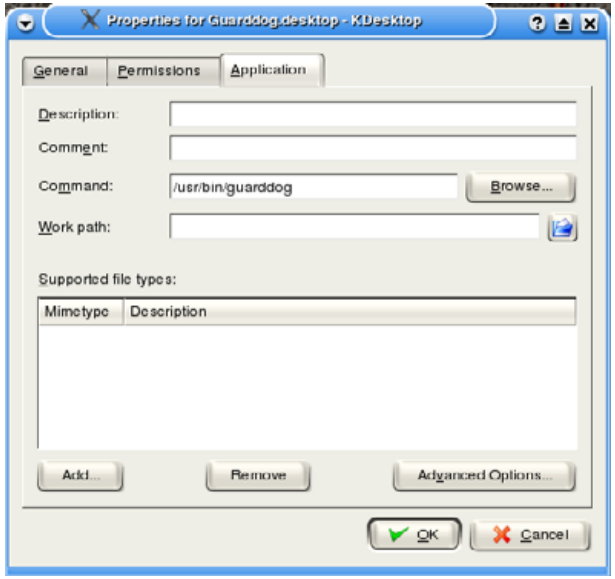

Figure 2. Entering the Command

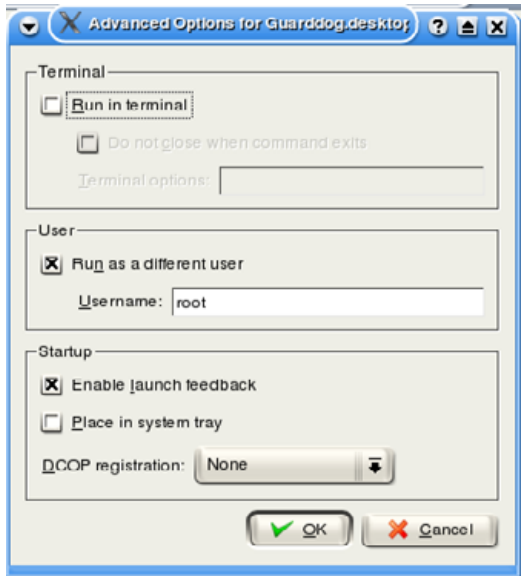

Figure 3. Using the Advanced Options Tab

Guarddog. To the left of that, you will see a Blue Gear. When you click on it, a screen opens that allows you to select a new icon (Figure 1). More than a hundred icons are available here, or you can download an icon from the Internet and link it in here. Look and you'll find the one named Guarddog. If it's not there, your installation may have put one on the disk somewhere. I did find one in the System icon files, but when I looked around, I also found a copy of the Guarddog icon that the installer put in /usr/share/icons/hicolor/32x32/apps/guarddog.png. If you didn't find one from your install, you can select any icon.

Next, click on the application tab and put `/usr/bin/guarddog` in the command field (Figure 2).

Because this tool needs to run as root, you need to tell the icon to ask you for the root password and to run it as root. To accomplish this, click on the Advanced Options button (Figure 3). Mark the box for Run as a different user and fill in the user name root.

Select Ok to save the icon configuration.

BACK TO THE NON-GEEKS: PLANNING

Remember what Simon said about whitelisting? Guarddog is designed so that nothing can access into or from the network unless you specify it. Guarddog assumes you will be implementing a default block all policy.

With that in mind, we should make a small list of the things we expect to do with our computer.

From my computer, I browse Web pages, do on-line banking, send and receive electronic mail, send and receive files using FTP, use VNC to view other computer screens, use secure shell and set the time on my computer. Your list will be different, and that is not a problem for Guarddog. That list can be translated directly to the services I want to allow to operate from my machine to the Internet (listed in the order as mentioned above): http, https, pop3, smtp, ftp, vnc, ssh and ntp.

We need to tell Guarddog that it's okay to do those things from our computer.

How about the things I want to be able to access on my computer from the outside world? I have a Web server I would like to be able to see from browsers at client locations. I would like to be able to access my computer via secure shell. These translate to the following services I want to allow in from the Internet: http and ssh.

We need to tell Guarddog that it's okay to do those two things from the Internet.

CONFIGURATION

Now that you have your planning done, you'll need to configure Guarddog for your plan. Let's start up Guarddog by clicking the icon you built earlier. If you set up the icon properly, it will ask you for the root password. Enter the root password and press Enter.

Guarddog should start up. If you have never started your firewall before, Guarddog will ask you if you want to start it now. Go ahead and start the firewall. If you want to shut the firewall off at any time, it's easy in one of the Guarddog configuration screens.

When you start Guarddog for the first time, you will see the default zones in the Zone tab. The Internet and the Local zones are the only zones we will use in our configuration (Figure 4).

The real action happens on the Protocol tab (Figure 5). When you select the Protocol tab, you will see the two zones in the Defined Network Zones box. Select the Internet Zone. To the right, you will see a window labeled Zone Properties. This is a tree view of all of the protocols and software that you can teach Guarddog to allow you to use on the Internet.

In Figure 5, you can see how I have checked the http and https services. This allows my machine to reach Web and on-line banking pages.

You need to scan through the different protocols and software packages represented in Guarddog and check the boxes that you want your machine to have access to. When you get to mail, if you are not sure, check them all. Once you get mail working, you can uncheck things one at a time until you get to a minimum that it takes to get it working.

After you have checked all of the protocols that you want to allow out to the Internet, you need to select the protocols you want to allow in from the Internet. Many of you will not do anything in this step, but in our scenario above, we are going to allow http and ssh protocols to access our machine from the Internet. First, select the Local zone. Then, in the protocol window, select http and ssh (Figure 6). You will find http under File Transfer and ssh under Interactive Session.

Guarddog also allows you to control how you log blocked and rejected packets. If you select the Logging tab, you will see that you can adjust these and other options in Guarddog (Figure 7). The defaults seem quite sane, and I found no need to change any of them, but you may want to experiment with the way logging occurs. If you intend to ignore the logs, you can turn them off entirely. In Linux, these logs are rotated and compressed weekly, so it's not a big deal if you leave them on. You may need them to prosecute an attempted

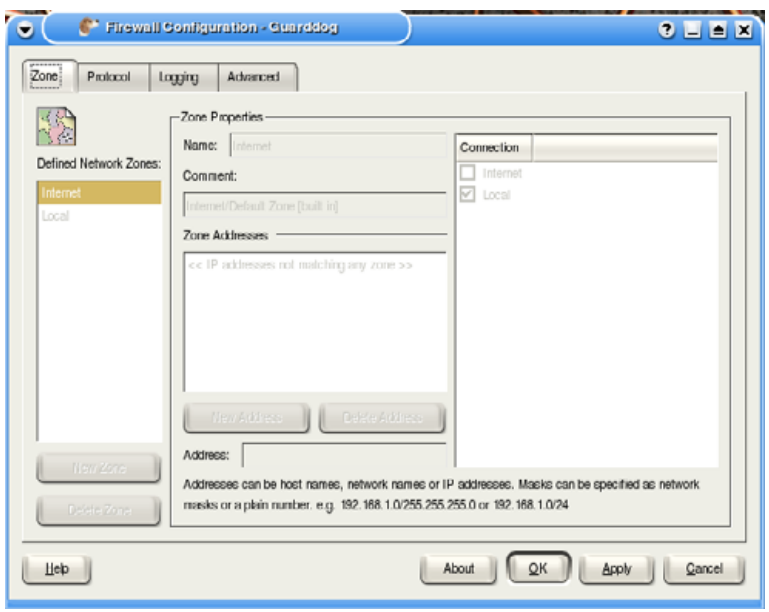

Figure 4. The Zone Tab

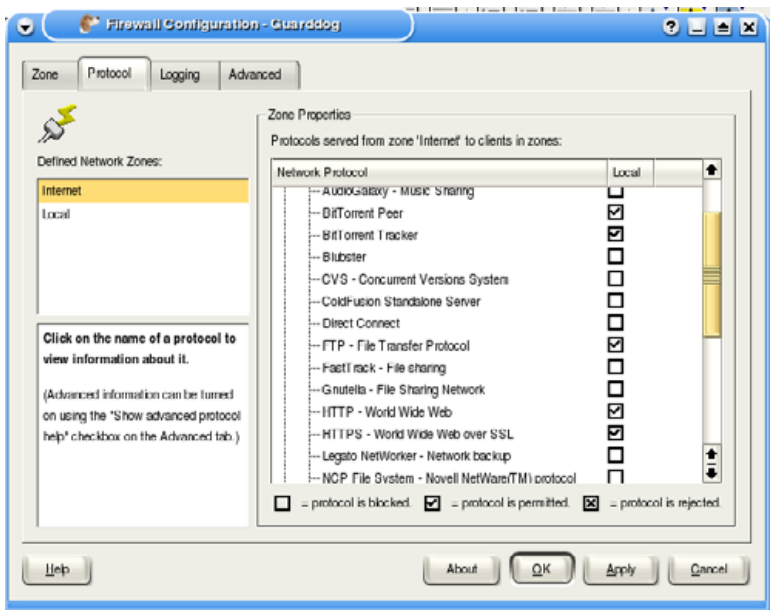

Figure 5. The Protocol Tab

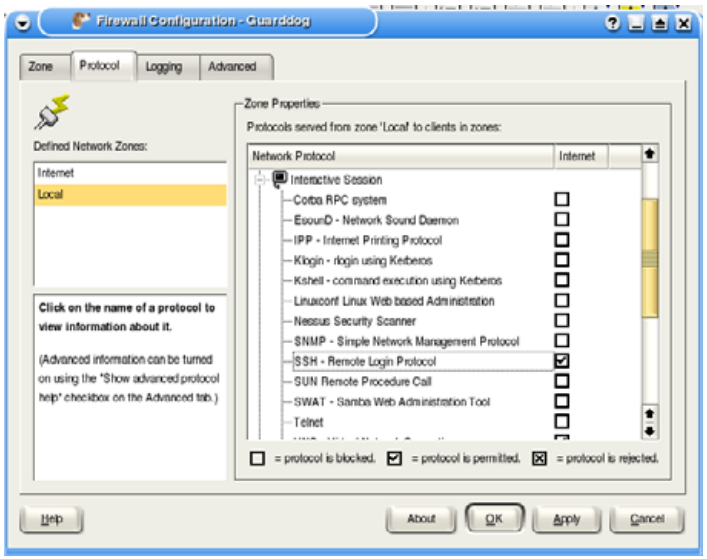

Figure 6. Enabling SSH

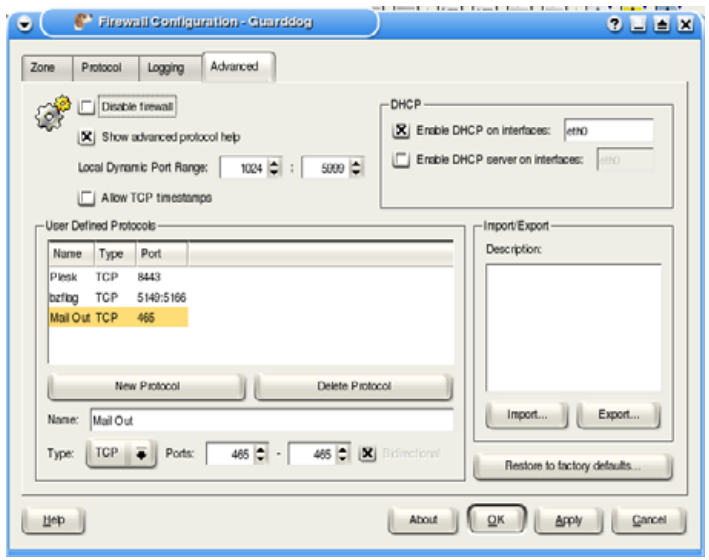

Figure 8. The Advanced Tab

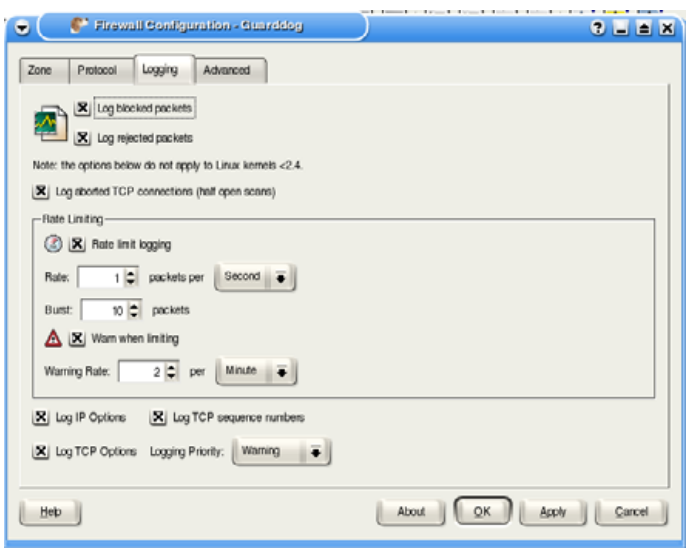

Figure 7. Logging

break-in. Personally, I have better things to do.

I did tell you that there's an easy way to turn the firewall on and off in Guarddog, so let's discover that and our tour is over. On the Advanced tab, you will see a selection for Disable Firewall (Figure 8). If you check that box and confirm with OK, your firewall is off.

GETTING HELP

On every Guarddog screen, there is a Help button in the lower-left corner. This leads to The Guarddog Handbook, which contains extensive help, concepts and tutorials. If you are having problems or feel you need help, be sure to read the excellent help files and perform the tutorials.

There is a support mailing list for Guarddog you can join if you have questions about installation or configuration. I have found that asking questions directly into support groups for the programs I am using gets me quick and accurate answers. If you do this, make sure to describe your installation in detail, like what distribution you are using and how you installed as well as what problem you are having. The more details you include in your requests for help, the better the answers you get will be.

You can access the Guarddog support list at https://lists.sourceforge.net/lists/listinfo/guarddog-user.

There are many advanced features in Guarddog, but what I've shown you will get you on your way. It's a great program that lets you have total control over your personal firewall without having to invest years in the study of firewalls and security.■

Phil Barnett is a Senior Programmer-Analyst at Walt Disney World where he has spent the last ten years working with corporate software and computer security projects. Six years ago, he helped incorporate the popular Florida Linux User Group, Linux Enthusiasts and Professionals, which he considers his greatest Linux accomplishment (http://www.leap-cf.org). Besides Linux and computers in general, his other hobbies include woodworking and amateur radio communications.