

15 May 2006

By: Bogdan Radulescu, Editor, Linux Software Reviews



[Guarddog Review](#)

Protect your computer with a cute little dog.

There is a general belief that when you are using Linux you are automatically protected from the threats that are on the Internet. This is somehow true, but not entirely. You are indeed protected from viruses and worms and this is very cool because most of the problems come from here. Other problems can come from intruders. Your computer stores a lot of data that would be helpful to some people. There are the popular credit card data and a lot more that some computers have to offer. There are also e-mail addresses, passwords and who knows what other valuable data. For this type of threats we have firewalls. The subject of this review is Guarddog, a simple and efficient firewall. **What do I like about Guarddog?** First of all I like that it uses ipchains or iptables to set the rules. Guarddog actually generates a rc.firewall file that is somehow standard in Linux. I encountered a problem because the script that chooses whether to use ipchains or iptables chose ipchains for me and it wasn't installed. I fixed this problem easily by installing ipchains too. Guarddog is a perfect application that can allow a newbie to do the job of an experienced network administrator with just a few clicks. I used iptables and ipchains to block the access to some ports and I'm pretty sure I will not use the manual approach unless I have to. Guarddog does everything easily and when I use it there is no need to know what port uses ICQ or Squid or whatever. Actually you don't even need to know what is a port. You just have to click in a check button if you want to allow a protocol. This philosophy is excellent because everything that you don't need will be automatically denied. **The Interface** The interface is made of four tabs. The first one has the defined network zones. By default Guarddog has two zones defined: one for the Internet and one for the local machine. In most cases those two are enough but in some cases, where several NICs are available, we have to add more zones. Adding a new zone is a snap. I said before that you don't need to know any port number. Guarddog has a comprehensive list with protocols and what ports are used for each one of them. It also gives a short description and the security risk they present. The list with the protocols is grouped in several categories so users can easily find the ones they want to unblock. Logging is supported through syslog. When a packet is blocked or rejected an entry it's written in the system log. A cool feature is that you can set a rate limiting. Without this feature it wouldn't be hard to get attacked with a DOS (Denial Of Service). Several logging options are set by default and I advice that you leave it that way because without them the logs would become useless. In the end of the discussion about logging I also feel obliged to advice you not to log the aborted TCP connections because usually they have nothing to do with the attackers and just mess up the log file. The last tab is named "Advanced". I would call this one "Extra" but this is not my shot. The most interesting features include support for defining a new protocol and for importing and exporting the configuration file. Those two features are a must have in a firewall program. Defining a new protocol is very important in a firewall because sometimes you might be accessing a service on a different port than the standard one. For example, a SQL server uses port 3306 but some people decide to make it run on 3307 or maybe something else. This is also true for custom applications or some that are not popular. Importing and exporting is very good when you want to use the same firewall configuration for several computers. **The Good** The easy to use GUI is the best thing about this program. A complete newbie should be able to set its own firewall in just a few clicks. The firewall script generated is very clean and can easily be converted in a skeleton for the use with future firewall scripts. Where a graphical interface is missing the skeleton would really come in handy. **The Bad** I would have liked to be able to choose between iptables and ipchains.

The program chooses for me and it does it bad. An Internet connection sharing would have been a great addition to this program. I think that some bugs regarding logging are available. **The Truth**At the moment I think Guarddog it's the best firewall configuration utility. It is not the best because of its features. It's the best because of its simple and efficient interface and because it depends on very few programs to work. Firestarter is another firewall that has more features and maybe a nicer interface but it's harder to get it running. Now I'll definitely go with Guarddog. *Check out the screenshots below:*