The Bad packets stop here

IPCOP FIREWALL

IPCop firewall isn't as well known as firewall proxying software such as Freesco or E-Smith but even in its early stages it has some good features that you might not see somewhere else. Richard Ibbotson takes a closer look

IPCop Linux is a complete Linux Distribution, which has the sole purpose of protecting the networks it is installed on. By implementing existing technology, outstanding new technology and secure programming practices, IPCop is the Linux Distribution for those wanting to keep their computers/networks safe. Whether for your home or SOHO, IPCop may be all the firewall you will ever need.

At the time of writing there is a 0.1.1 stable release, which you can register after downloading. You don't have to register but it's worth it for the support and help that you will receive. Releases 0.1.x are IPChains-based and when 0.2.x appears it will be IPTables-based.

To install the software, download it from the UK Linux Web site or alternatively you can also get it from this month's coverdisc. Like most instant firewall software, you can create a floppy disk and then boot the computer you intend to use as a firewall from this disk. To make a floppy disk use the command:

```
dd if=/mnt/cdrom/images/boot.img ➥
   of=/dev/fd0 bs=1k count=1440
```

Or if you are lucky enough to have a CD burner you can put your downloaded ISO image on to a CD and boot your computer from that. For more info about this see the online installation documents, which are extensive and extremely helpful.

Before going any further with the installation, or perhaps before you even begin, you might like to consider the ways in which you are using your network now and the ways in which you may need to change things in order to improve security of your data. To make sure that you are doing things in the right way you might want to write a few things down and make a few mental notes in order to get things straight. It's good to think about network security in this way so that you don't have to completely re-install everything later on. You might even find that more haste and less speed will take care of some of the holes that are presently in your network or home computer. Wisdom and network security go and hand in hand.

After your first boot you'll see the lilo boot screen, which welcomes you to IPCop. You can then press Return to continue. You will then see the all too familiar Linux boot messages scrolling down the screen. Language selection is next and then you'll be asked if you want to install from the Internet or from CD-ROM. At the next screen the installation program, which looks a lot like the Red Hat one, will tell you that it will now format the hard disk. There is a colour-coded scheme that may help you to understand what to do with your various network interfaces.

A brief feature list

- Analogue/ISDN/ADSL modem support
- PPtP ADSL support
- PPPoE support
- USB ADSL firmware upload area
- Integrated Java-based SSH shell area
- DHCP server
- Intrusion Detection System – Snort
- DMZ pin-holing capacity for publicly accessible servers
- Creates a virtual private network easily
- Full status display
- Full traffic graphs
- Full connections information
- Full system logs
- Web proxy logs
- Firewall logs
- Remote shutdown/reboot area
- IPCop GNU/Linux updates area

There are many more features, which you can read about by having a look at the IPCop Web site.

Red, gold and green

IPCop uses a familiar method of describing the various parts of your network, colour-coded to highlight the dangers imposed by where they are in that network. First of all, the IPCop computer is classified as RED and connects to the untrusted Internet. This is the most dangerous part of your network and should be treated with contempt until proved otherwise.

Once past this part of the network you have your protected computers, which are considered a GREEN

network, so if IPCop has been configured correctly these should be safe and secure. Any further parts of the network that you might want to be available to the outside world such as Web and FTP servers are classified as an ORANGE network. This ORANGE network is only permitted access to the GREEN network by a secure channel, with the firewall maintaining security.

In the IPCop computer you will need a minimum of one Network Interface Card (NIC) connected to your GREEN network. If you are using a cable modem then that requires another NIC and if you have an ORANGE network then another NIC for that system is also needed.

In the simplest of networks you have one RED computer running IPCop in addition to your home computer. You would connect your home machine to the IPCop machine via a twisted-pair Ethernet cable. If you have more than one computer in your GREEN network then you would connect these via a hub rather than a twisted pair cable.

First things first

After you have given IPCop some basic values for netmask and network addresses the software will install. It will then ask you for things like your location, time zone and the name of the machine. You will also be asked for things like the name of an ISDN card or perhaps a USB-based ADSL modem. If you get lost with any of this check the IPCop Web site: there's plenty of installation help. There is also an excellent online administration manual, which is written by Charles Williams who is the project manager for IPCop.

After finishing your installation you can then connect to your IPCop machine with a browser across your home or small business network. You can view the status of data packets moving across your protected network interface to the outside world.

In the Administration Window (AW), there is a dial-up section, which allows you to control a 56K modem, ISDN interface or ADSL interface. You can also change the dial-up number and DNS settings. There is even an SSH section, which allows you make remote access to your firewall by SSH a possibility (or not if that's what you want). This option is disabled by default so if you are a bit forgetful then you don't need to worry about it. Web proxying can be done in the AW section as well. Most people recommend that if you are using a dial-up firewall then it should be a caching proxying firewall. One of the nicer points of the AW section is the easy configuration of Snort, which is an intrusion detection system. Quite a few people who are new to Snort spend a lot of time learning how to use it. It's a very comprehensive piece of software and quite good when it's used properly. There is a rather nice shutdown and reboot feature built into the AW for remote administration, which finishes off the suite of tools that are available. This means that you can then remove the monitor and keyboard from the IPCop machine. Updates can be obtained through the built-in updates AW. This is similar in operation to the Debian GUN/Linux or BSD update tool.

Patchwork

Recent IPCop patches have seen the following fixes:

- Shadow passwords are enabled
- VPN Config can be succesfully restored
- Netmask 255.255.255.255 is valid
- FTP Masquerading Module is loaded with the correct in_ports option
- Snort rulesets are updated
- Squid FTP vulnerability fixed
- Squid SNMP vulnerability fixed
- Squid HTCP vulnerability fixed
- Bug fixed where log rotate did not compress rotated logs

This highlights the fact that the IPCop developers aren't content with things the way they are. Their intention is to improve the software as quickly as is possible.

Conclusion

Did we encounter any problems with the software while it was being tested? Not really. The only thing that we found slightly annoying was that some of the higher ports are left open by default. It is thought that in later versions this will be changed. After installing the software you can get help and support from the various IPCop mailing lists.

If you're a developer and you want to be involved then you might like to know that IPCop is going through a major re-write just now. There is a developer's list just for you and you can actively discuss the future and improvements in IPCop.

If you have tried all of the others and they didn't work then why not try IPCop. You'll be presently surprised. It's a quick and easy way of making your home or office network more secure than it was.

Info

IPCop homepage: *http://www.ipcop.org*
Installation and configuration: *http://www.ipcop.org/cgi-bin/twiki/view/IPCop/IPCopInstallv01#Caveats*
Administration manual: *http://www.ipcop.org/cgi-bin/twiki/view/IPCop/IPCopAdministrationv01*
Security issues: *http://www.securityfocus.com*
Download: *http://mirror.uklinux.net/ipcop*
ftp://mirror.uklinux.net/ipcop/
Mailing lists for support: *http://www.ipcop.org/cgi-bin/twiki/view/IPCop/IPCopMailingLists*
IRC channel #ipcop on: *http://irc.openprojects.net*

The author

Richard is the chairman and organiser for Sheffield Linux User's Group. You can view its Web site at – *http://www.sheflug.co.uk*