The Network Sheriff

IP Cop on the Beat

If you are looking for a simple and cheap way to link up your SOHO network to the Internet, a specialized Linux distribution like IPCop [1] might be just what the doctor ordered. The distribution supports i386 and later computers and supports modem, ISDN and DSL based Internet access. BY THOMAS ZELL

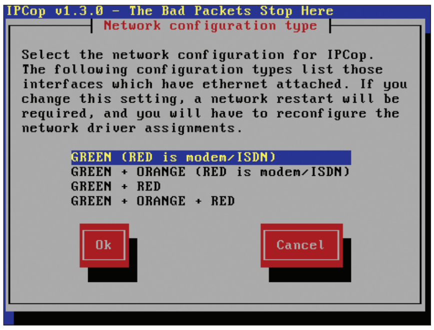
Before you go to the trouble of installing *IPCop* on one of your computers, you will certainly want to know what the distribution has to offer.

- DHCP
- **Intrusion Detection System (IDS)** based on Snort 2.0
- SSH encrypted terminal sessions
- **VPN** based on Super FreeS/Wan 1.99 kb2c
- Linux kernel 2.4.x with *iptables* support
- improved support for DSL modems, ISDN, and analog modems
- neat GUI based view of network traffic

Before You Start Installing

Before you start installing IPCop, you will need to plan your network configuration. Three different network types are supported. And the developers of *IPCop* have assigned them three different colors for you to select during the installation process.

Green represents your secure intranet – packets addressed to this network will be pass through one of the firewall NICs. Red represents the Internet and orange a **DMZ**. The orange network is optional. The Internet connection can use ISDN, a modem, or a second NIC attached to your DSL modem. This allows for four combinations (Figure 1).



```
IPCop v1.3.0 - The Bad Packets Stop Here
            Network configuration type

  Select the network configuration for IPCop.
  The following configuration types list those
  interfaces which have ethernet attached. If you
  change this setting, a network restart will be
  required, and you will have to reconfigure the
  network driver assignments.

           GREEN (RED is modem/ISDN)
           GREEN + ORANGE (RED is modem/ISDN)
           GREEN + RED
           GREEN + ORANGE + RED
```

Figure 1: Network configuration

If you intend to use IPCop with DSL, option three is the right choice for you. Even if you intend to add a server to your DMZ later, you should start with a simple configuration and perform any required changes after testing.

No matter what configuration you choose, you will need to put some thought into the IP addresses used in your Intranet. Your easiest option is to use local network addresses in the range 192.168.0.1 through 192.168.0.254. This will allow you to attach 254 hosts to your network. These so-called **private IP addresses** will be translated by your firewall to the routable addresses provided by your provider.

Servers and routers are typically assigned low addresses, thus 192.168.0.1 is a good choice for your "green" NIC.

Hardware Requirements

To run an IPCop firewall, you will need an older computer to run the firewall software. The PC will need a CD ROM or at least a floppy drive for the installation. You will need a hard disk with at least 125 MBytes and at least twice the RAM size for a swap partition – although it won't hurt if you have more.

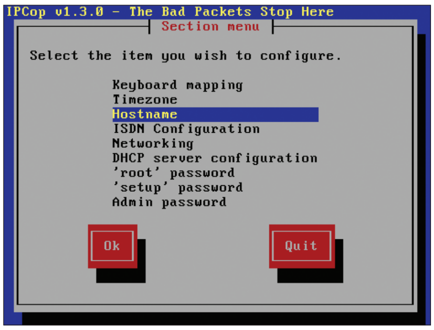
SCSI hard disks are not supported. We have heard of successful *IPCop* installations on as little as 4 MBytes RAM, but 20 MBytes or more will put you on the safe side. In addition to your logon credentials for your Internet provider account and the appropriate hardware (modem, ISDN adapter or NIC for the DSL modem), you will need a network card and appropriate cabling to connect the firewall to your network or host computer.

If your computer is capable of supporting PCI cards, you should invest in a PCI network card. Our installation worked well with NE2000 compatible cards using the Realtek chipset. You can consult [3] to find out whether your hardware is supported.

Installation

The first thing to do, is to obtain a copy of the program – version 1.3 is current. The *IPCop* homepage [1] provides a 22 MBytes **ISO image**. You can launch *IPCop* on the target machine from a bootable CD. You may need to change the boot sequence in your computer's BIOS to boot from CD.

If you have a PC with the popular Asus BIOS, press the [Del] key while booting and use the space key to navigate the BIOS menu. The [PgUp] and [PgDn] keys will change the values in the menu. When prompted to *Save values and exit?* press [y] to confirm. If your computer cannot boot from CD, you will need to create a bootable floppy. Refer to [2] for a howto.



```
IPCop v1.3.0 - The Bad Packets Stop Here
                 Section menu

  Select the item you wish to configure.

            Keyboard mapping
            Timezone
            Hostname
            ISDN Configuration
            Networking
            DHCP server configuration
            'root' password
            'setup' password
            Admin password
```

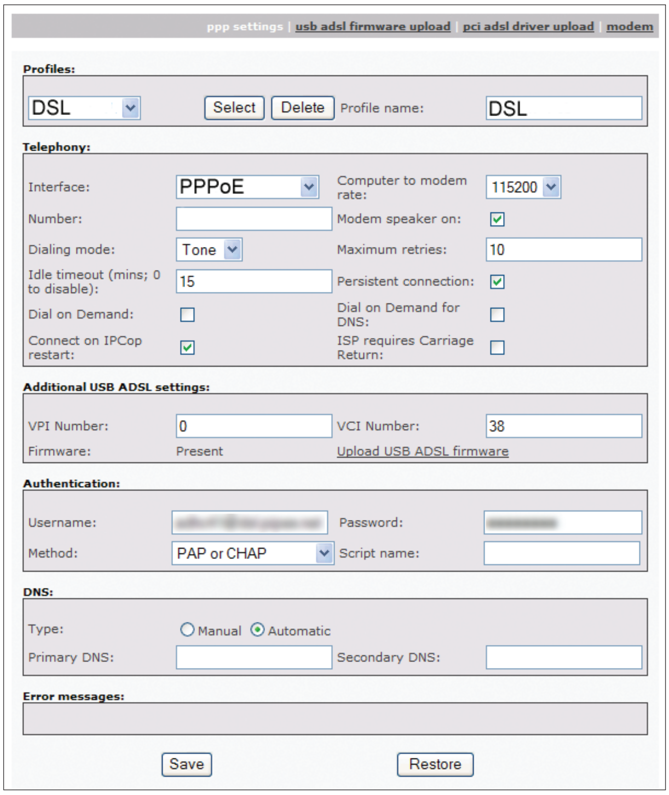
Figure 2: Options for the "setup" user

A welcome screen appears when you boot, warning you that any data on your hard disk will be destroyed by the installation steps. If you are sure that you have not left any important data on your hard disk, you can ignore the warning and run the installation.

Select the required language and indicate that you want to install from CD. IPCop will then copy the software packages to your hard disk, and after a short delay, you can start configuring the firewall. Enter the IP address you decided to assign to the "green" network. This is 192.168.0.1 in our example.

You will use another computer for many of the configuration tasks by pointing your browser at 192.168.0.1:81 (that is port 81). If you discover that you have made a mistake, or if your network card is not recognized correctly, you will need to access the firewall console directly to remedy the situation. In this case, log on with the *setup* user account and supply the password you assigned to access an well-organized screen with the configuration options.

The Linux powers that be still require some more work from you before you can reboot. You will be prompted to remove the installation media and enter your keyboard type. This is typically *us-latin1-nodeadkeys*. You can now add the time zone (for example *Europe/London*), and the hostname for your computer, or simply use the default, *ipcop*. Three user accounts are available on the machine.



ppp settings | usb adsl firmware upload | pci adsl driver upload | modem

Profiles:

DSL Select Delete Profile name: DSL

Telephony:

Interface: PPPoE
Computer to modem rate: 115200
Number:
Modem speaker on: ☑
Dialing mode: Tone
Maximum retries: 10
Idle timeout (mins; 0 to disable): 15
Persistent connection: ☑
Dial on Demand: □
Dial on Demand for DNS: □
Connect on IPCop restart: ☑
ISP requires Carriage Return: □

Additional USB ADSL settings:

VPI Number: 0
VCI Number: 38
Firmware: Present
Upload USB ADSL firmware

Authentication:

Username: [redacted]
Password: [redacted]
Method: PAP or CHAP
Script name:

DNS:

Type: ○ Manual ● Automatic
Primary DNS:
Secondary DNS:

Error messages:

Save Restore

Figure 3: Important details for accessing the Internet

Each account has its own password and access privileges to the firewall. The *admin* user can only log on remotely, *root* and *setup* can only log on locally. This would allow parents to tell their children the *admin* password, without any danger of them changing the firewall configuration.

The next few details can be entered directly on the firewall, or you can reboot the computer and use the Web interface for the remaining configuration options.

A Question of Trust

The main advantage of a distribution like IPCop is its remote control capability. You can use *SSH* to log on; the IPCop distribution runs the SSH daemon on port 222. The computer additionally provides a Web interface. The address is the IP address of your firewall and port 81 for http or port 445 for https. To avoid the need to type the IP address each time you access the firewall, you can add the appropriate IP address/hostname mapping to */etc/hosts* file on the computer where you launch the browser.

However, before doing so, you will need to log on to the firewall using the *admin* account, and supply the password you assigned previously. Your friendly neighborhood IPCop sheriff needs a few details before he can get on with the job of connecting your network to the Internet. In other words, nothing will happen if you do not supply your user name and password for your provider account.

You can define multiple profiles to support multiple providers or access methods. Figure 2 shows the settings for DSL. To avoid having to establish the Internet connection manually, you can check the "Dial On Demand Mode" checkbox, or tell your firewall to establish a connection to the Internet on booting – this is the recommended procedure for flat-rate users. *IPCop* will take the connection down after a pre-defined "inactivity timeout".

You can use the other defaults below *Phone number* area; they will not cause any harm if you are a DSL user, and actu-

GLOSSARY

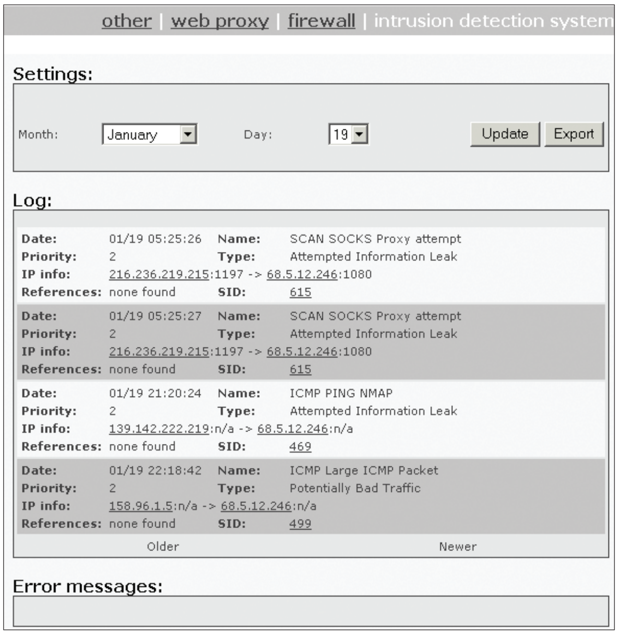
Intrusion Detection System (IDS): *An IDS provides you with a second line of defense behind your firewall. It searches network traffic at packet level, looking for suspicious patterns that might indicate an attempted intrusion into your network. A ruleset is used to specify what the IDS will view as suspicious. When ever the IDS recognizes a pattern defined as suspicious by the ruleset, it writes an entry to a logfile /var/log/messages. In contrast to a firewall, an IDS will not block traffic, but instead alert the system administrator if it notes potentially malevolent activities.*

Virtual Private Network (VPN): *A VPN is used to connect a network. The computers are attached via a connection that works like a tunnel through a hostile network segment such as the Internet allowing users to exchange confidential data as the network traffic within the VPN is encrypted.*

DMZ: *A DMZ ("demilitarized zone") is a network that is accessible from the Internet and is not directly attached to the "green" Intranet. Allowing access from the Internet to a Web server in your "green" network could compromise the security of your network. A software bug on your server could leave a gaping hole for attackers to exploit.*

Private IP addresses: *RFC 1918 specifies private IP addresses reserved for computers without a direct Internet connection. Additional information is available from [2], Appendix A.2.*

ISO Image: *A file containing a complete CD image. A CD burning program like cdrecord for the command line or xcdroast for X can use the image to create a CD.*



Settings:

Month: January Day: 19

Log:

```
Date:       01/19 05:25:26  Name:    SCAN SOCKS Proxy attempt
Priority:   2               Type:    Attempted Information Leak
IP info:    216.236.219.215:1197 -> 68.5.12.246:1080
References: none found      SID:     615
Date:       01/19 05:25:27  Name:    SCAN SOCKS Proxy attempt
Priority:   2               Type:    Attempted Information Leak
IP info:    216.236.219.215:1197 -> 68.5.12.246:1080
References: none found      SID:     615
Date:       01/19 21:20:24  Name:    ICMP PING NMAP
Priority:   2               Type:    Attempted Information Leak
IP info:    139.142.222.219:n/a -> 68.5.12.246:n/a
References: none found      SID:     469
Date:       01/19 22:18:42  Name:    ICMP Large ICMP Packet
Priority:   2               Type:    Potentially Bad Traffic
IP info:    158.96.1.5:n/a -> 68.5.12.246:n/a
References: none found      SID:     499
```

Error messages:

Figure 4: Who's been knocking at my door?

ally make sense if you use a modem. In this case, you will need to supply your provider's dial-up number – this is not required for DSL users. You can typically ignore the area below *Additional PPPOE Settings* and *Additional PCI ADSL Settings*.

The DSL username for xyz customers is put together as follows:

```
Phone number - 012345678901
Matching xyz number - 9876543210
Co-User number/suffix - 0001
```

Concatenate the numbers in the order phone number/xyz number/suffix and add *@xyz.com*. This will allow you to connect to the Internet.

Users with modems or ISDN cards should enter the username and password for their provider account and additionally supply the dial-up number.

Safety First

If required, Snort can notify you of connection attempts by other computers and also indicate the risk factor involved. An access attempt is not necessarily malevolent.

Lots of alerts are caused by badly configured computers. The *Logs* menu also allows you to check how long your computer has been on the Internet and what volume of traffic has been transferred, or which computer is accessing which Internet site.

Of course you can also view *normal* status information typical of Linux computers, such as your uptime, kernel warnings or cryptic *pppd* messages.

Gateway to the Internet

So you have finally got IPCop up and running, and now want to access the Internet through the firewall. Computers with Linux or other Unix type operating systems will need a gateway entry for the IPCop host. Log on as *root*, and launch the GUI network setup tool, or edit the */etc/gateways* file manually to create the required entry.

If you notice that you cannot use intuitive names, such as *http://www.linux-magazine.com*, to access hosts on the Internet, but you use the IP address, you can assume that your computer needs an entry for the nearest DNS server. The */etc/resolv.conf* file should contain only one entry, that is *nameserver 192.168.0.1*, assuming that this is the IP address of your IPCop PC.

Additionally, for any Microsoft Windows computers you may have on your network, you will need to supply DNS information and the address of your "Standard Gateway". The easiest way to supply this kind of information to all your clients is to use DHCP.

For more details on configuring the Windows network environment, refer to [4]. You can launch DHCP on your firewall via the Services menu. You will need to specify a start and end address for the address pool you want to use for your clients. We used 192.168.0.2 and 192.168.0.254 on our lab network. Specify the IP address of your firewall as the DNS server address.

More Software

Besides the software already mentioned in this article, IPCop also provides the proxy server, Squid, software for setting up virtual private networks, pre-configured scripts, for DynDNS support for example, with lots more tools which are beyond the scope of this article.

If you are interested in learning more, why not take a look at the IPCop homepage [1], browse the FAQ at [6] or use IRC [8] to chat directly with the developers, after reading the documentation, of course.

Conclusion

IPCop is one of many router/firewall distributions, but as such it does offer more tools than most. If you have a lot of Linux experience there is nothing to stop you configuring a firewall of your own design, by installing Debian, and deinstalling any services and software you do not need, setting up your own filtering rules and updating your software.

But if that sounds like too much work IPCop is the right choice for you. The installation procedure normally runs without any glitches, updates are easy to install, an the Web interface provides convenient access. And, should problems occur, competent help is available via the mailing list [5]. ■

INFO

[1] IPCop Homepage: *http://www.ipcop.org*

[2] IPCop Installation guide: *http://www.ipcop.org/1.3.0/en/install/html/*

[3] IPCop Hardware Compatibility List: *http://www.ipcop.org/cgi-bin/twiki/view/IPCop/IPCopHCLv01*

[4] Windows networks: *http://www.computing.net/*

[5] Information on the IPCop mailing list: *https://lists.sourceforge.net/lists/listinfo/ipcop-user/*

[6] IPCop FAQ: *http://www.ipcop.org/cgi-bin/twiki/view/IPCop/IPCopFAQ*

[7] Current documentation: *http://www.ipcop.org/cgi-bin/twiki/view/IPCop/IPCopDocumentationv01*

[8] IPCop IRC: *irc.openprojects.net* channel: *#ipcop*

THE AUTHOR

Thomas Zell lives in Berlin. His interest in Unix and Linux was raised in 1998. Having tried many distributions he finally developed his own version of the WinDowMaker desktop which can be found at http://www.allroy.de.