

# IPCop: An Overview

David "Del" Elson 2002-03-13

## IPCop: An Overview

by David "Del" Elson

last updated March 13, 2001

---

## Introduction

IPCop is a cut-down Linux distribution that is intended to operate as a firewall, and only as a firewall. It has some advanced firewalling features, including VPNs using IPsec. This article describes the set-up and use of IPCop, and contains a few comments about its features.

This article is based on IPCop version 0.1.1, which was in turn derived from SmoothWall version 0.9.9.

## Features

IPCop's main feature is as a firewall system for small offices or home networks. Being licensed under the GPL, it is free to use and therefore the only costs in getting it running are the hardware. IPCop supports up to three network interfaces, and includes the following features:

- IPChains-based firewall
- External interface can be an Analog modem, an ISDN modem, or an ADSL modem, and can support PPTP or PPPoE ADSL connections to Ethernet or USB modems.
- DMZ Support
- Web-based GUI Administration System
- SSH server for Remote Access
- DHCP server
- Caching DNS
- TCP/UDP port forwarding
- Intrusion detection system ([Snort](#))
- IPsec based VPN Support ([FreeSWAN](#)) with Control Area and support for Check Point SecuRemote

IPCop is a complete firewall installation, taking control of the machine and replacing any other

operating system that is installed. Therefore, it is not similar to packages like ipchains or any of the GUI firewall administration tools. It is not an additional security service you would run on your machine; rather, it is a complete operating system and firewall administration kit in a box that the user would dedicate a single machine to house and run as an Internet gateway.

## Where to Find IPCop

IPCop can be found at [SourceForge](#), at or at [the IPCop home page](#). The home page is fairly easy to navigate, and contains the source code, a downloadable ISO image, and some documentation including installation and administration guides.

## IPCop and SmoothWall

IPCop is derived from the [SmoothWall project](#) but was forked as a separate project for a two main reasons:

- To provide better, and more friendly support. Because the SmoothWall authors have both a GPL and a commercial product, it is obviously in their interests to support the commercial version more than the GPL version. The IPCop authors are providing support for a GPL product.
- To provide some additional features. There are some additional features planned for the commercial version of SmoothWall, which the IPCop authors have plans to implement in their GPL-ed product.

## Differences between SmoothWall and IPCop

The scripts and installer in IPCop were derived from SmoothWall. The OS underneath it has been rebuilt from the Red Hat 7.2 RPMs. A rebuild was required as both IPCop and SmoothWall use a 2.2 kernel instead of the 2.4 kernel used in Red Hat's distribution.

The code has been modified to run on an ext3 (journalled) filesystem, for added reliability. Some additional fixes and feature enhancements to the SmoothWall product have been made, notably in the area of ADSL support.

Of course, most of what is said in this article applies to the current version of SmoothWall as well as IPCop. If you would prefer to run SmoothWall or require a commercially supported product, then see the [SmoothWall home page](#).

# Installing IPCop

What you will need:

- The IPCop distribution, which is a 28MB ISO image downloadable from the IPCop Web site.
- A CD burner (optional, as IPCop can be installed across a network from a boot floppy disk).
- A PC on which to install the IPCop system.

## Finding a PC

This is often the hard bit of the installation. IPCop doesn't require a highly powered PC to run on. Since machines are often at a premium in many small offices, a trip to your nearest PC recyclers or second hand shop may be an ideal way to get hold of a PC to use for IPCop.

Of course, it will need to be running and have a reasonable amount of memory (say, 64MB would be useful for a machine that is doing caching as well, although 128MB would be great), and a good-sized hard disk if you plan to Web cache, but processing speed is not important.

Since IPCop is almost completely manageable by the Web interface (requiring the console only to change network interface parameters), it can run happily without a keyboard, monitor, mouse, or any of the other paraphernalia attached to a PC. Most PC suppliers and/or recyclers can be convinced to sell PCs equipped without these items.

## Installation

The installation process is incredibly simple and is well documented in the installation manual. The installation manual can be found by following the Documentation links from the IPCop home page, or directly via this link: <http://www.ipcop.org/cgi-bin/twiki/view/IPCop/IPCopInstallv01>.

The installation manual contains complete screen shots of the entire installation process. Rather than repeat or paraphrase the installation manual here, I will simply list the main points:

- Read the section titled "Decide On Your Configuration" fairly carefully. You need to decide on your network interfaces, of which there can be up to three. IPCop calls these "RED", for the Internet / exposed interface, "ORANGE" for the DMZ interface (this is optional), and "GREEN" for the internal or protected interface.
- You can burn the CD-ROM image onto a CD using just about any CD writing software. I have successfully used Adaptec Easy-CD on Windows, or cdrecord on Linux. The CD-ROM image supplied by IPCop is bootable, and so if you have a reasonably recent system with a bootable CD-ROM drive supported in the BIOS, you do not need a boot floppy disk.
- If you are like me, and have multiples of the same type of network cards for the three interfaces, then all of your network cards will become active when you probe for the GREEN interface (this is because I happen to like one particular brand of network card). You still need to activate the other network interfaces during initial system configuration - this is done after the step where you configure any external modems, ADSL interfaces, or ISDN cards.
- When you see the "Network configuration menu", select "Network configuration type", specify the number of interfaces you have, and the installation system will then ask you for IP address parameters, etc, for those interfaces. This was a step that I accidentally skipped over more than once during various IPCop installations.
- If you need to change network configuration details later, you can do so by logging on to the IPCop system as the "set-up" user. The installation program will ask you for a password for this user account, you must remember this password if you want to re-run the set-up program as reconfiguring network parameters is not possible via the GUI Web interface.
- As well as the set-up password, the installation system will ask you for "root" and "admin" passwords. The "root" password is only used for logging on to the console and performing a few shell-based administration tasks. The "admin" password is used for connecting to the IPCop system via the Web-based interface.

## Network Interfaces and the DMZ

IPCop supports up to three network interfaces. This may be an issue in larger organizations, as I have seen firewalls with as many as 15 network interfaces in the past.

Generally you would run IPCop with at least two interfaces, which would be RED and GREEN, but you may also want to use an ORANGE interface as well, which allows you to have a DMZ (de-militarized zone).

The IPCop documentation clearly explains why you should use an ORANGE interface for the DMZ. An Internet-exposed Web server, for example, should probably live on the ORANGE interface rather than the GREEN interface. Why? Well, this is as a fallback measure. A server on the DMZ, if protected by the ORANGE interface, cannot access anything on the GREEN interface unless a pinhole is specifically created for it. This would usually be done between a Web server on the DMZ and a database server (for example) on the GREEN network.

This means that if a cracker were to somehow bypass the firewall, intrusion detection measures, and other systems that you have in place to protect your Web server, and managed to gain root access on it, they would still be unable to attack your internal network. Sure, they would be able to access the database that you have specifically allowed access to, but they would be unable, for example, to attack your NFS servers, your domain controllers, or other more sensitive devices on your LAN.

## Finishing the Installation

Ideally, IPCop would be running on a low profile machine, which would be hidden in a network cabinet somewhere away from prying eyes (and fingers).

You should unplug any keyboard, mouse, and monitor, and do the environment a favour by re-using them elsewhere on your network.

## Configuring IPCop

Just about everything that can be said about administering IPCop is in the administration manual, which is available at the [IPCop home page](#), or directly via the [IPCop User Administration Manual](#).

### The Basics

Installed out of the box, IPCop is pretty much a blank although functional template. It has the necessary rules in place to allow access from your protected network to the Internet, and deny access from the Internet inwards to your network.

There are a few things that need configuring once IPCop is running, however:

- Enable additional services, such as the Web proxy, DHCP, and the snort intrusion detection system.
- Set up port forwarding and external service access.
- Enable any required DMZ pinholes.

## Starting the Administration Interface

Administering IPCop is a simple matter of using a Web browser, from anywhere on the GREEN network. You need to know the GREEN network interface address that was assigned when you set up your IPCop server. Simply start your preferred Web browser and access the address `http://<green_address>:81/`

For example, if your firewall is configured with the address 192.168.1.1, you could enter the address `http://192.168.1.1:81/` into your browser and you would see the configuration interface.

To get past the first page of the interface, you will need to know the "admin" account and password that you assigned during installation.

There is also a secure access to the configuration interface of IPCop - `https://192.168.1.1:445/` if you prefer to use an SSL connection, although IPCop generally will not have a valid certificate so you may get some warnings from your Web browser when you use this type of connection.

## Web Proxy

Probably IPCop's most important feature is the integration of the [Squid Web proxy server](#). This proxy service is disabled by default, but can be started from the configuration interface. Choose "Services" on the menu on the left-hand side of the interface, and then from the menu you see at the top of the page, select "Web proxy". The Web proxy is enabled by checking the box marked "Enabled". If your Web proxy is also your main gateway, then you may also want to select the "Transparent" option, which means your Web clients will not need to set up any proxy settings in their browsers, the proxy service will function automatically.

Most of the other settings in this area can be left blank.

## DHCP

IPCop contains a simple DHCP server, which is capable of serving dynamic IP addresses for a small LAN. Because I'm the sort of network guy that likes to know what address all of my workstations have, I prefer to use a different DHCP server that allows me to assign static IP addresses by MAC address.

If you want to use IPCop's DHCP server, however, it is very simple. Just go to the "dhcp" tab in the "Services" menu, and tick the "Enabled" box. You will also need to assign a start address and end address for the DHCP range, and enter some DNS details to be passed on to DHCP clients.

## **Intrusion Detection**

IPCop includes the [Snort](#) intrusion detection system, which is quite a powerful system for detecting various attacks on internal servers. If you are using IPCop to protect a server or two (either on your DMZ or your GREEN network) then you will find Snort quite useful.

IPCop makes setting up Snort very simple. Just go to the "IDS" tab on the IPCop menu, and tick the "Enabled" box. Remember to check your log files regularly if you are running Snort! These are accessible from the "IDS" tab as well.

An IDS such as Snort (or a firewall, for that matter) is in no way a substitute for the need to ensure that your Web servers are updated regularly with the appropriate service packs and security fixes as soon as they become available from your vendor, be that Debian, Red Hat, or Microsoft. Be aware of any vulnerabilities as soon as they are announced (the [BugTraq](#) mailing list is a good source of this information), because there only needs to be one cracker who discovers the vulnerability before you update your IDS, and you may very well be in trouble.

## **Port Forwarding and External Service Access**

The Port Forwarding and External Service Access tabs in the "Services" menu are used together to allow access to your internal servers from outside of your network (the Internet).

As a simple example, assume that we have a Web server and a mail server running on the DMZ. We have assigned the address range 192.168.200.x to our ORANGE network, and the Web server is at address 192.168.200.10 with the mail server at address 192.168.200.20.

Web services typically run on TCP port 80, while mail (SMTP) traffic happens on TCP port 25.

The entries that we would make are as follows:

- Under Port Forwarding:

| Protocol | Source Port | Destination IP | Destination Port |
|----------|-------------|----------------|------------------|
| TCP      | 80          | 192.168.200.10 | 80               |
| TCP      | 25          | 192.168.200.20 | 25               |

- Under External Service Access:

| Source IP Address | Destination Port |
|-------------------|------------------|
| ALL               | 80               |
| ALL               | 25               |

Note how the Source Port and Destination Port under port forwarding are usually the same (unless you wanted to redirect an external port to a different internal port), and how those same ports must also be enabled under external service access.

## DMZ Pinholes

DMZ Pinholes are only used in IPCop for allowing access from the ORANGE network to the GREEN network. Note that access from the GREEN network to the ORANGE network is enabled by default.

This type of access would normally only be used where a Web server on your DMZ needed to access a database server inside your network. You will need to find out the port number that the database server runs on (for example, for MySQL it is 3306, for other databases such as Oracle or Informix you will need to ask your vendor or consult the documentation).

Enabling the pinhole is a simple matter of selecting the "dmz pinholes" tab on the Services menu. As an example, to allow our Web server on the DMZ shown previously to access a MySQL server on our internal network at IP address 192.168.100.4, we would enter the following information:

| Source IP      | Destination IP | Destination Port |
|----------------|----------------|------------------|
| 192.168.200.10 | 192.168.100.4  | 3306             |

## On Line Documentation for IPCop

In addition to this article, there is a wealth of documentation on the [IPCop home page](#).

All of the IPCop documentation is maintained in a system called Twiki (a WikiWikiWeb engine written in Perl). This enables people from outside of the IPCop development team to freely contribute documentation for the project, after registering, and has meant that in a reasonably short space of time the documentation available for the system is comprehensive and complete.

The IPCop documentation can be accessed directly from the [IPCop v0.1 Documentation Page](#)

There is a full installation manual and an administration manual available via the above link.

### Setting up a VPN using IPCop

Setting up a VPN on Linux is a relatively complicated topic. This is primarily because the main VPN system available (FreeS/WAN), while being highly comprehensive and having many features, is also very complex to set up and understand.

Fortunately, the IPCop system simplifies the process somewhat, and makes setting up a VPN between two IPCop systems much more straightforward.

### Documentation

There is some documentation in the IPCop documentation tree on setting up a VPN, including a VPN how-to. This is a fairly comprehensive document, which can be obtained by following the links from the IPCop home, or directly via the [IPCop VPN How-To page](#)

Another useful document for understanding IPSec based VPNs and FreeS/WAN in particular can be obtained via the [FreeS/WAN home page](#).

## Configuration of the VPN

Configuring a VPN between two IPCop machines involves the following steps:

- Ensuring that the machines are connected to the Internet and can view each other.
- Deciding on a Left and Right interface, and gather information.
- Enabling the VPN settings on each IPCop machine.
- Setting up the VPN connection on each IPCop machine, and rebooting.

### Ensure The Machines Are Connected

This is the first important step - ensure that both VPN machines are connected to the Internet and are switched on and running. You will also need to ensure that they can ping each other.

Also ensure that a machine behind each firewall can ping the external IP address of the opposite firewall. So, if your firewalls are at addresses A and B, make sure a machine behind firewall A can ping B, and a machine behind firewall B can ping A.

Most VPN problems are caused by a problem with this basic connectivity.

### Decide On A Left and Right Interface

One of your IPCop firewalls must be designated as "Left" and one must be designated as "Right". This designation does not change through any of the next steps.

You need to establish the following information:

- The external, or RED IP address of each firewall. Ideally these should be fixed IP addresses. For our example, I have a LEFT firewall with an external address of 203.99.88.77 and a RIGHT firewall with an external address of 210.55.44.33.
- The networks and addresses behind each firewall, in "slash" notation. For example, I will set up a VPN between a network behind my LEFT firewall which is 192.168.100.0 netmask 255.255.255.0 and a network behind my RIGHT firewall which is 192.168.150.0 netmask 255.255.255.0
- The "next hop" address of each firewall. Normally this will be the gateway address of each firewall, which would be the next router between your firewall and the Internet. For example, my LEFT firewall may be connected to a router at 203.99.88.254, and my

RIGHT firewall to a router at 210.55.44.254.

Although it might sound strange (from a network administrator's point of view) to have to do so, you must provide this "next hop" information. The KLIPS (Kernel IP Security) component of FreeS/WAN bypasses the normal routing machinery, so you must give KLIPS the information even though the routing tables already know it.

## Enable the VPN settings

Enabling the VPN settings on each machine is simply a matter of going to the "VPNs" menu on the IPCop administration page, and selecting the "control" tab. Enter the external (RED) address of each firewall into its own "Local VPN IP" entry box, check the "Enabled" box, and press the "Save" button.

## Set Up the VPN Connections

After enabling the VPN settings, click on the "connections" tab in the VPN menu.

You will now need to enter the LEFT and RIGHT interface information that you gathered earlier. In addition, you will need to enter:

- A name for the connection. For example "sydney-newyork" to designate the left and right endpoints of the connection.
- A secret key. IPCop does not currently support dynamic keying of IPSec interfaces, and so you will need to generate a key for the connection. I suggest creating some random data, and passing this through the "md5sum" program on the nearest Linux box, or perhaps taking the output of "ps auxwww" and passing this through md5sum. For example, use the following command: `ps auxwww | md5sum`. You need to add this same key into both ends of the connection, and of course I don't need to remind you that passing this key across the Internet in plain text would probably be a very silly idea.

When you are entering the LEFT and RIGHT information, remember that the LEFT machine remains LEFT at both ends. Don't make the common (but understandable) mistake of entering firewall A's information as LEFT at one end and RIGHT at the other.

## Test

Once your connection details are entered, you will need to return to the control tab and Restart the VPN settings at both ends. It may be that the VPN takes a little while to become established, but once it has you should be able to ping any machine on the A network from any machine on the B network.

If you cannot ping between the A and B networks (LEFT and RIGHT) once the VPN is established, then go back and check your connection details. Make sure that the same information is entered at both ends of the connection, and read carefully through any error messages in the log (on the connections page) for messages that may indicate the cause of the problem.

### **Connecting a VPN From IPCop to Other Systems**

Another popular Linux-based firewall is the commercial product, Watchguard Firebox II. This is sold as an integrated hardware and software device, and also supports IPSec-based VPNs. Because both the Firebox II and IPCop use the industry standard IPSec protocol for VPN connections, it is possible to set up a VPN between a Firebox II and a machine running IPCop. There is even a special how-to on this at the IPCop Web site: <http://ipcop.sourceforge.net/cgi-bin/twiki/view/IPCop/IPCopWatchguardVPNHowto>

Or follow the links from the IPCop home page to the IPCop documentation tree, and select the Watchguard VPN HOWTO under "Other Documentation"

It is also possible to set up a VPN between an IPCop system and a Check Point VPN-1 firewall, although how to do that is beyond the scope of this article. However, keep your eyes open for an upcoming article on Linux and IPSec, in which Check Point and IPCop will be discussed.

[Privacy Statement](#)

Copyright 2006, SecurityFocus