Administrative Guide

IPCop

Chris Clancey

Harry Goldschmitt

John Kastner

Eric Oberlander

Peter Walker

Administrative Guide

by Chris Clancey, Harry Goldschmitt, John Kastner, Eric Oberlander, and Peter Walker

Published 20 September 2004

Revision History

Revision 0.1.0 (beta)	29 Dec 2001	Revised by: CW
Forward by Charles Williams		
Revision 1.2.0	10 Jan 2003	Revised by: RW
1.2.0 revisions		
Revision 1.3.0	4 May 2003	Revised by: HG
1.3.0 revisions		
Revision 1.4.0	30 August 2004	Revised by: CC, HG, JK, EO, PW
1.4.0 revisions		
Revision 1.4.10	13 December 2005	Revised by: HG, EO
1.4.10 revisions		

Table of Contents

Preface

Rights and Disclaimers

All programs and details contained within this document have been created to the best of our knowledge and tested carefully. However, errors cannot be completely ruled out. Therefore IPCop does not express or imply any guarantees for errors within this document or consequent damage arising from the availability, performance or use of this or related material.

The use of names in general use, names of firms, trade names, etc. in this document, even without special notation, does not imply that such names can be considered as "free" in terms of trademark legislation and that they can be used by anyone.

All trade names are used without a guarantee of free usage and might be registered trademarks. As a general rule, IPCop adheres to the notation of the manufacturer. Other products mentioned here could be trademarks of the respective manufacturer.

1st Edition - December 29, 2001

Editor Charles Williams

I would like to thank the folks that reviewed and corrected the document: Harry Goldschmitt, Mark Wormgoor, Eric S. Johansson and the rest of the IPCop Linux Group.

2nd Edition - January 10, 2003

Editors - Chris Clancey, James Brice, Harry Goldschmitt, and Rebecca Ward

3rd Edition - April 25, 2003

Editors - Chris Clancey, Harry Goldschmitt, and Rebecca Ward

4th Edition - September 25, 2004

Editors - Chris Clancey, Harry Goldschmitt, John Kastner, Eric Oberlander and Peter Walker

Forward

Hello. On behalf of our Project Leader, Jack Beglinger, the Documentation staff would like to welcome you to the IPCop Users Administration Document. We would like to take this opportunity to thank you for trying our firewall and we hope that it will serve your needs. The team would also like to thank the IPCop Linux Community for its continuing presence and the outstanding job it does helping new and experienced users alike. We would also like to thank the team at SmoothWall for bringing the IPCop Linux Community together.

Whether you are an existing user moving up the version chain or a new user getting ready for your first install, we hope you will find all you need to get up and running in this manual. If, for some reason, something is not covered here and you feel it should be, then by all means contact us and let us know. We always like to hear from our user base (actually some of us are just kinda lonely sitting on the computer all day and a little note is nice every once in a while) and hope to be able to accommodate their needs as much as possible. Now you can relax and enjoy the Internet without having to worry.

So, here is a bit of information for those of you that have the time to read this and are waiting for your IPCop Linux box to install. The initial release of IPCop was an interim release to assist us in finding problems in the IPCop Linux Distribution. We are now on our third full release. If you do happen to find problems, please check the IPCop FAQ first as we attempt to update the FAQ as soon as we find a problem and can provide solid information on either a work around or a direct fix.

If your problem is not referenced in the FAQ then you can either join us on IRC (server: irc.openprojects.net channel: #ipcop), contact the IPCop mailing list or send the IPCop Linux Group an email for direct support. Please be advised that you will more than likely receive a faster response and solution by using the first 3 methods listed above. Contacting the IPCop Linux Group directly could have a large delay, depending upon our development schedule.

You may find further information as well as the newest FAQ, mailing list information and IPCop Linux Group contact information on our web site: *IPCop Web Site* [2]

Notes

1. http://www.ipcop.org
2. http://www.ipcop.org

Chapter 1. Project Leader's Introduction

Welcome and thank-you for looking at and/or using IPCop.

What Is IPCop?

Now, what is IPCop?

1. IPCop is a firewall; first, last and always.
2. IPCop is a specialized Linux Distribution; complete, configured, and ready to protect your network. Further, it is distributed under the GNU General Public License[1], complete source ready to be downloaded, reviewed, or even be modified and/or recompiled by yourself for your personal needs or security reasons.
3. IPCop is a community; where members help each other, all sharing to improve the project and each other. This help goes from simple "Networking 101"type of instruction and direction, to helping members customize their IPCop to meet a specialized needs such as Net-Phones (VoIP) and multiple office integration.

This was a trick question. The correct answer is: All of the above.

Background:

IPCop grew out of many needs. The first of those needs was a need for secure protection of our personal and commercial networks. When IPCop started October 2001, there were other firewalls available. However, the team that started IPCop felt that the other two needs that IPCop fills were not addressed; GPL and a sense of community.

The IPCop founding group decided to do things differently and forked the base GPL code of an existing firewall and started out anew, looking to keep user community needs in the forefront. Among those needs is the need of the user to make IPCop their own, to install improvements, to just learn by seeing what others have done. Through these needs is where development gets some of improvements to IPCop, directly listening and seeing what has been done and why. This community makes IPCop grow and IPCop helps them grow.

Now, after almost two and a half years, the first major overhaul of IPCop has been released. With it, a lot of cool things have been added; quad network support, intrusion detection on all networks and a slick new interface, to name a few.

And so again, Welcome to IPCop!

Jack Beglinger
Project Leader

Partial List of Features

- IPTable network filters
- IDE, SCSI and CF (Disk on a Chip) drive support.
- Quad Network support:
  - GREEN — Internal Trusted Network
  - BLUE — Wireless Semi-Trusted Network (can be used as a second Green)
  - ORANGE — DMZ for Internet accessed servers
  - RED — The Internet connected via:
    - Dial modem
    - ISDN

  - NIC Connected:
    - DSL Modem
    - Cable Modem
  - USB Connected (w/ right driver):
    - DSL Modem
    - Cable Modem

- Multiple "Real" IP supported on RED when using a Static IP base.
- DHCP client support on RED to receive IP from ISP, also support for a dynamic DNS to be updated as this IP changes.
- DHCP server for GREEN and BLUE to simplify network setup and maintenance.
- NTP server and client for setting IPCop clock and supplying a common clock for internal GREEN and BLUE networks.
- Intrusion Detection for ALL networks (RED, ORANGE, BLUE and GREEN)
- Vitural Private Network (VPN) to allow multiple sites to act as single large network.
- Proxy Support for both Web Surfing and DNS support allow for "faster" connection response on and simplified network setup.
- Administration after initial load is via a secure Web Interface including:
  - Performance Graphics for CPU, Memory and Disk as well as Network throughput
  - Log viewing with autorotation.
  - Multiple language support.
- Use of older equipment. 386 or better. Version 1.4 has been tested on 486sx25 with 12M of RAM and 273M of hard drive. This was the oldest and smallest we could find at the time of test. It was loaded via the Net Install option and supported a full Cable Modem download speed of 3Mb/s.

Acknowledgements

IPCop software is both a collaborative project and built upon great prior works. These acknowledgements will cover many to help both directly and indirectly, but will never the less miss untold many who toiled to help develop this project but I failed to get them noted here. To those, I say many thanks and sorry for missing your name.

For the rest, thank you... For a more up to listing please see System⟶Credits in IPCop.

Core Team

- Mark Wormgoor — Lead Developer
- Alan Hourihane — SMP & SCSI Developer
- Giles Espinesse —
- Harry Goldschmitt — Lead Documentation
- Eric Oberlander — Developer & Translation Coordinator

Developers

Mark Wormgoor, Alan Hourihane, Eric S. Johansson, Darren Critchley, Robert Kerr, Gilles Espinasse, Steve Bootes, Graham Smith, Robert Wood, Eric Oberlander, Tim Butterfield and David Kilpatrick.

Documentors

Harry Goldschmitt, Chris Clancey, John Kastner, Eric Oberlander, Peter Walker

Translators

- *Brazilian Portuguese:* Edson-Empresa, Claudio Corrêa Porto, Adilson Oliveira, Mauricio Andrade, Wladimir Nunes
- *Chinese:* Vince Chu, Yuan-Chen Cheng, Sohoguard
- *Czech:* Petr Dvoracek, Jakub Moc
- *Danish:* Michael Rasmussen
- *Dutch:* Gerard Zwart, Berdt van der Lingen, Tony Vroon, Mark Wormgoor
- *Finnish:* Kai Käpölä
- *French:* Bertrand Sarthre, Michel Janssens, Erwann Simon, Patrick Bernaud, Marc Faid'herbe, Eric Legigan, Eric Berthomier, Stéphane Le Bourdon, Stéphane Thirion, Jan M. Dziewulski,spoutnik, Eric Darriak, Eric Boniface
- *German:* Dirk Loss, Ludwig Steininger, Helmet, Markus, Michael Knappe, Michael Linke, Richard Hartmann, Ufuk Altinkaynak, Gerhard Abrahams, Benjamin Kohberg, Samuel Wiktor
- *Greek:* Spyros Tsiolis, A. Papageorgiou, G. Xrysostomou
- *Hungarian:* Ádám Makovecz, Ferenc Mányi-Szabó
- *Italian:* Fabio Gava, Antonio Stano, Marco Spreafico
- *Latino Spanish:* Fernando Diaz
- *Norwegian:* Morten Grendal, Alexander Dawson, Mounir S. Chermiti, Runar Skraastad, Alf-Ivar Holm
- *Polish:* Jack Korzeniowski, Piotr, Andrzej Zolnierowicz
- *Portuguese:* Luis Santos, Renato Kenji Kano, Mark Peter, Wladimir Nunes, Daniela Cattarossi
- *Romanian:* Viorel Melinte
- *Russian/Ukranian:* Vladimir Grichina, Vitaly Tarasov
- *Spanish* Curtis Anderson, Diego Lombardia, Mark Peter, QuiQue Soriano, David Cabrera Lozano, Jose Sanchez, Santiago Cassina, Marcelo Zunino, Alfredo Matignon
- *Swedish:* Anders Sahlman, Christer Jonson
- *Turkish:* Ismail Murat Dilek, Emre Sumengen
- *Vietnamese:* Le Dinh Long

Other Projects and Companies:

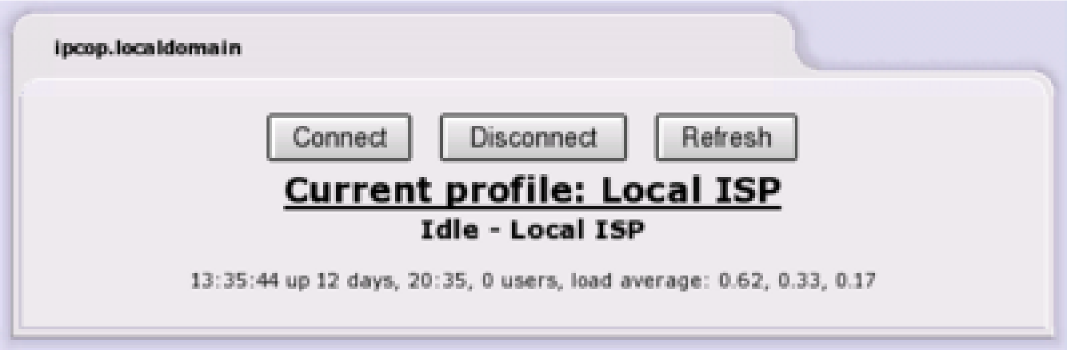
Traverse Technologies — Improved Dual ISDN and DOV support, Linux from Scratch (LFS) — Code Base for IPCop 1.4, FreeSwan and OpenFreeSwan — IPSec and VPN software, Smoothwall — Original foundation and inspiration, . . . and others too numerous to mention.

Notes

1. http://www.gnu.org/licenses/gpl.html

Chapter 2. Administration and Configuration

Home Administrative Window



Current profile: Local ISP

Idle - Local ISP

13:35:44 up 12 days, 20:35, 0 users, load average: 0.62, 0.33, 0.17

To access the IPCop GUI is as simple as starting your browser and entering the IP address (of the green IPCop interface) or hostname of your IPCop server along with a port director of either 445 (https/secure) or 81(redirected to 445): https://ipcop:445 or https://192.168.10.1:445 or http://ipcop:81 or http://192.168.10.1:81.

Note: Deprecation of HTTP Port 81 Connections: As of IPCop Release 1.4.0, http connections to port 81 will be redirected to https on port 445. Several years ago, when IPCop was originally designed, a small fraction of browsers could not handle the https protocol, so http on port 81 was made available. Most of these browsers have fallen out of use and sending IPCop passwords in the clear, over http is inherently dangerous, so http connections have been deprecated. For those in the habit of using port 81, the connection will be automatically redirected to https. If you are still using a browser that can not handle https, please download one of the many browsers that can and use it.

Changing the HTTPS Port: Some Users need to change the port used for secure connections to avoid a clash with port 445, which recent versions of Windows use for Directory Services (SMB over TCP/IP). Some ISPs routinely block port 445 as a security measure, to prevent the spread of viruses.

A commandline utility **setreservedports** was introduced in version 1.4.8 to allow Users to change the secure port.

```
$ /usr/local/bin/setreservedports 5445
```

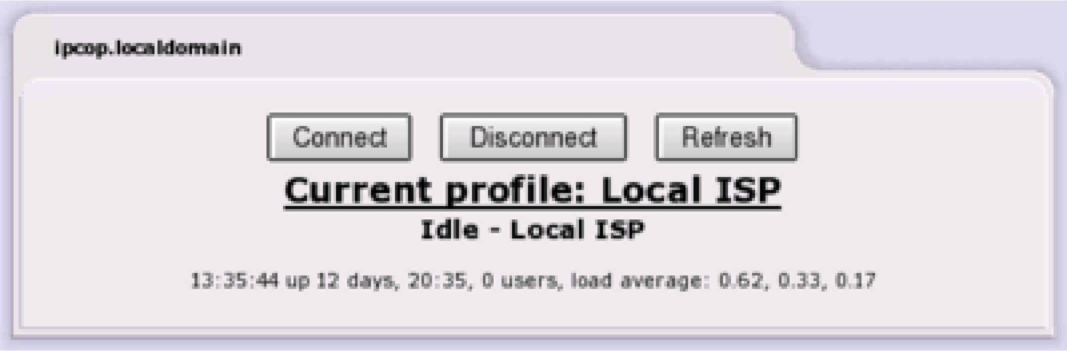
Although 5445 is suggested here as the alternative port, any port number between 445 and 65535 is allowed. If you forget which port you changed https to, use http and port 81 to be automatically redirected.

You should now be looking at the Home Page of your IPCop server's Administration GUI. You can immediately start exploring the different options and the information available to you through this interface. Below, we have listed the Main Configuration/Administration Options available through the GUI. When you have acquainted yourself sufficiently with the system, please continue with the next section.

IPCop's Administrative web pages or AWs are available via the tabs at the top of the screen.

- **System:** System configuration and utility functions associated with IPCop, itself.
- **Status** Displays detailed information on the status of various portions of your IPCop server.
- **Network** Used for the configuration/administration of your dial-up/PPP settings.
- **Services:** Configuration/Administration of your IPCop server's many Services options.
- **Firewall:** Configuration/Administration of IPCop's firewall options.
- **VPNs:** Configuration/Administration of your IPCop server's Virtual Private Network settings and options.
- **Logs:** View all your IPCop server's logs (firewall, IDS, etc.)

The Home web page is one of several web pages that will look differently depending on the way IPCop is configured. If your Internet connection is via an Ethernet RED interface the Home web page will only not show the current connection name, etc.



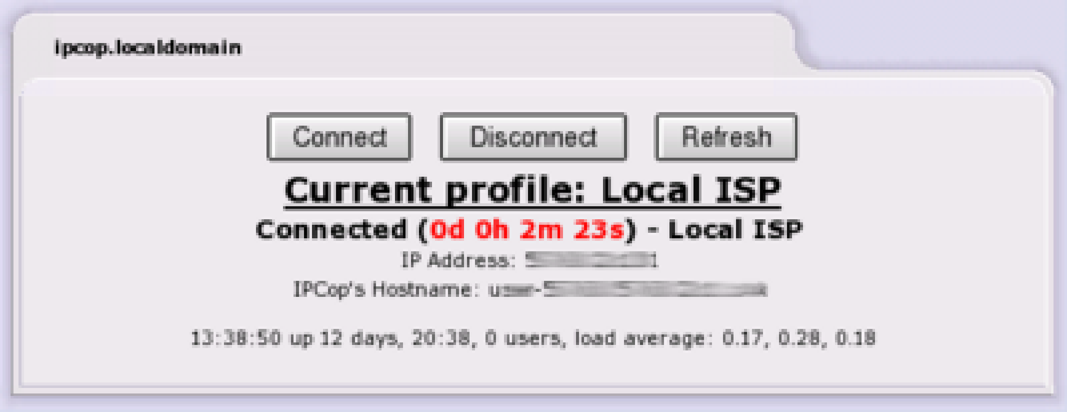
ipcop.localdomain

Current profile: Local ISP

Idle - Local ISP

13:35:44 up 12 days, 20:35, 0 users, load average: 0.62, 0.33, 0.17

If all went well during the configuration of your PPP connection and PPP is the connection type being used to connect to the Internet, then you will see 3 buttons on the IPCop GUI main page.



ipcop.localdomain

Current profile: Local ISP

Connected (0d 0h 2m 23s) - Local ISP

IP Address: [redacted]

IPCop's Hostname: [redacted]

13:38:50 up 12 days, 20:38, 0 users, load average: 0.17, 0.28, 0.18

> **Note:** You will not see an active connection until you have finished configuring your IPCop server.

At the top left corner of the folder you will see the fully qualified domain name of your IPCop machine.

Modem Connection Buttons

- **Connect** - This will force a connection attempt to the Internet.

- **Disconnect** - This will sever the connection to the Internet.
- **Refresh** - This will refresh the information on the main screen.

In addition to the above buttons you will see the “Current Profile” being used to connect to the Internet (Set in the Dialup AW). Below the “Current Profile” line, you will see your actual connection status. This will be one of the following:

- *Idle* - No connection to the Internet and not trying to connect.
- *Dialing* - Attempting to connect to the Internet.
- *Connected* - Currently connected to the Internet.
- *Dial on Demand waiting* - Currently not connected to the Internet. Waiting for activity from a Client on the network to initiate a connection.

If you are currently connected to the Internet you will see a Connection status line in the following format:

- Connected (#d #h #m #s)
- d=Days connected
- h=Hours connected
- m=Minutes connected
- s=Seconds connected

Below your connection status line you will see a line similar to the following:

```
7:07pm up 1 day, 7:21, 0 users, load average: 0.03, 0.01, 0.00
```

This line is basically the output of the Linux **uptime** command and displays the current time, the days/hours/minutes that IPCop has been running without a reboot, number of users logged in to the IPCop server, and the load average on the IPCop server. Additionally, if there are updates available for IPCop that you have not yet installed, you will be informed via this page.

IPCop has two web users, in addition to the root login user. The first is called “admin”. Authenticating as this user gives access to all Administrative Webpages. The other user, called “dial”, is able only to use the **Connect** or **Disconnect** buttons. By default, the “dial” user is disabled; to enable it you must set a password for that user. No password is required to view the Home or Credits webpages. All others require the “admin” password.

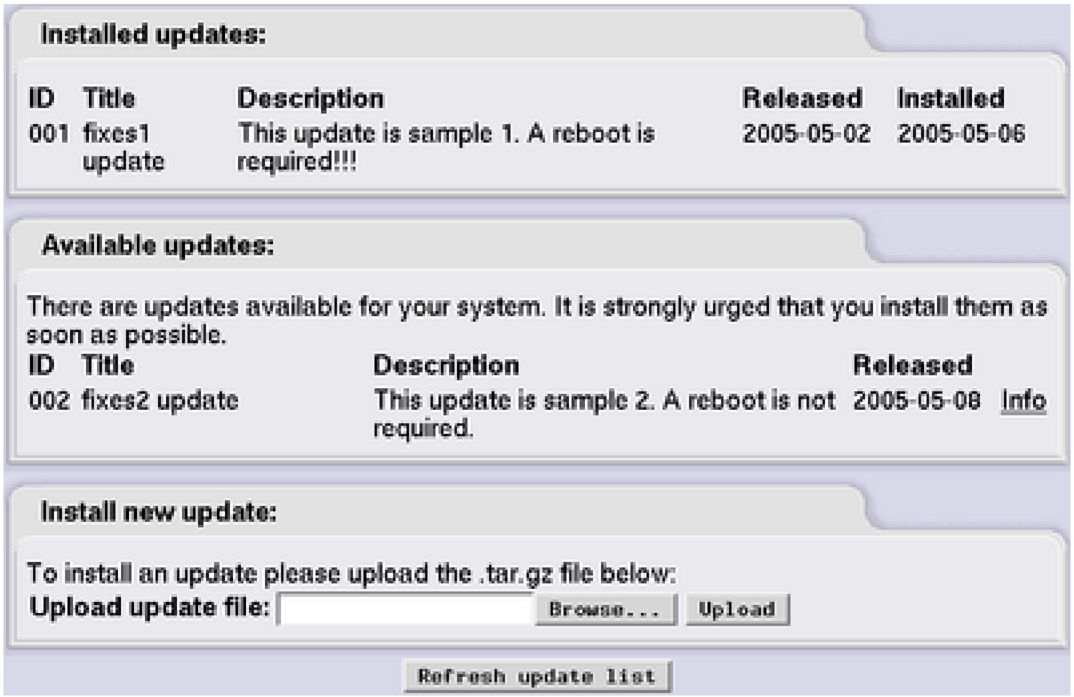
System Web Pages

This group of web pages is designed to help you administer and control the IPCop server itself. To get to these web pages, select **System** from the tab bar at the top of the screen. The following choices will appear in a dropdown:

- **Home** — Returns to the home page.
- **Updates** — Allows you to query and apply fixes to IPCop.
- **Passwords** — Allows you to set the admin and optionally, the dial password.
- **SSH Access** — Allows you to enable and configure Secure Shell, SSH, access to IPCop.
- **GUI Settings** — Enables or disables the use of JavaScript and allows you to set the language of the web display.
- **Backup** — Backs up your IPCop settings either to files or to a floppy disk. You can also restore your settings from this web page.

- **Shutdown** — Shutdown or restart your IPCop from this web page.
- **Credits**—This web page lists the many volunteers and other projects that make IPCop so great.

Updates AW



Installed updates:

ID	Title	Description	Released	Installed
001	fixes1 update	This update is sample 1. A reboot is required!!!	2005-05-02	2005-05-06

Available updates:

There are updates available for your system. It is strongly urged that you install them as soon as possible.

ID	Title	Description	Released	
002	fixes2 update	This update is sample 2. A reboot is not required.	2005-05-08	Info

Install new update:

To install an update please upload the .tar.gz file below:

Upload update file:

This section has 3 sections:

1. Shows your current patch level.
2. Informs you of new patches available.
3. Allows you to apply a given patch.

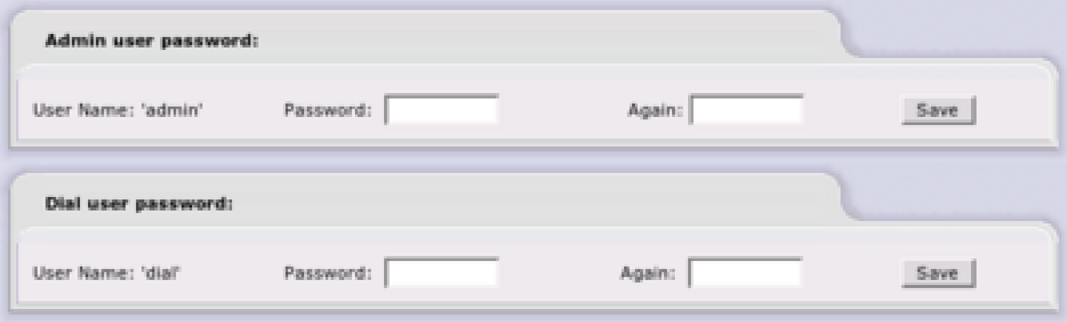
Every time you connect to the Internet IPCop will check for any new Updates that may be available. You may also manually check for updates by clicking the **Refresh update list**. When a new patch is available you will see the information on screen with the short description and a link for more information. Follow the “Info” link. When you have followed the link you will see a page with all relevant information about the patch including a download link.

Downloading the patch will place it on the machine you are running your web browser on, not the IPCop machine. Once you have downloaded the patch simply use the Update page to **Browse** to where you saved it and then **Upload** the patch to apply it to your IPCop server.

> **Note:** The Opera web browser does not handle uploads properly and thus should not be used for applying a patch to your IPCop server.

> **Note:** Only IPCop official patches will actually install on your IPCop server. Some patches may automatically reboot your IPCop server, so please read *all* patch information thoroughly before applying said patch.

Passwords



Admin user password:

User Name: 'admin' Password: Again:

Dial user password:

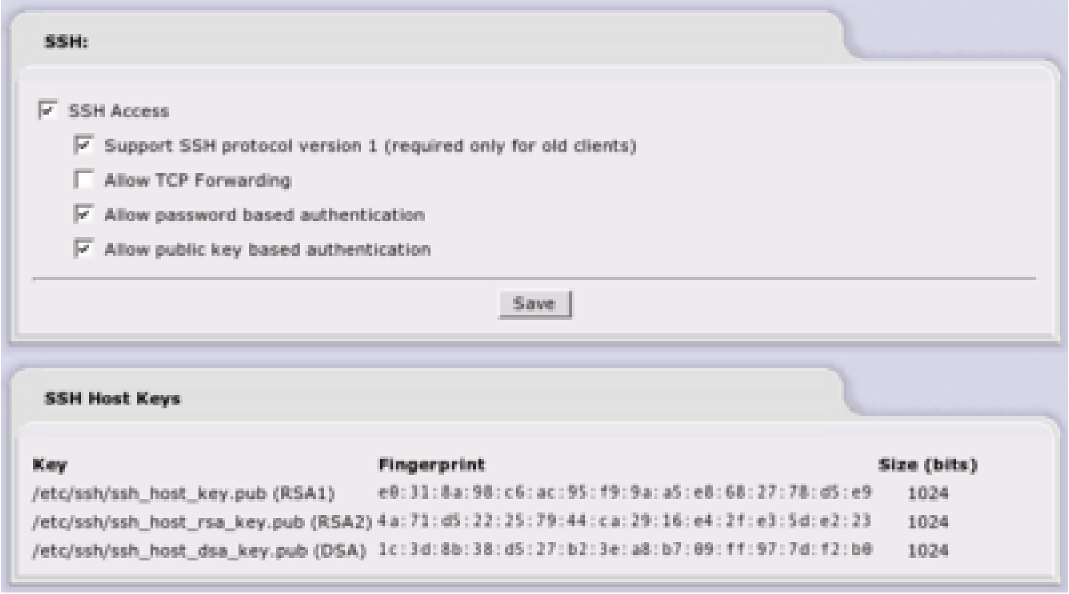
User Name: 'dial' Password: Again:

The *Passwords* subsection of this AW is present to allow you to change the Admin and/or Dial User passwords, as you deem necessary. Simply enter the desired password once in each field for the User you wish to update and click on **Save**.

Entering the Dial password activates the Dial user ID. This special user has the ability to use the buttons on the IPCop Home web page but cannot get to any other IPCop web pages. Use this facility if you have a dial up connection and want to allow users to connect to the Internet, but not have admin authority on the firewall.

SSH Access

The *SSH* subsection of this AW allows you to decide if remote SSH access is available on your IPCop server or not. By placing a checkmark in the box you will activate remote SSH access. It is also possible to configure several SSH daemon parameters from this web page. The SSH option is disabled by default and we would advise enabling it *only as needed and then disabling it afterwards*.



SSH:

☑ SSH Access
- ☑ Support SSH protocol version 1 (required only for old clients)
- ☐ Allow TCP Forwarding
- ☑ Allow password based authentication
- ☑ Allow public key based authentication

SSH Host Keys

Key	Fingerprint	Size (bits)
/etc/ssh/ssh_host_key.pub (RSA1)	e0:31:8a:98:c6:ac:95:f9:9a:a5:e8:68:27:78:d5:e9	1024
/etc/ssh/ssh_host_rsa_key.pub (RSA2)	4a:71:d5:22:25:79:44:ca:29:16:e4:2f:e3:5d:e2:23	1024
/etc/ssh/ssh_host_dsa_key.pub (DSA)	1c:3d:8b:38:d5:27:b2:3e:a8:b7:09:ff:97:7d:f2:b0	1024

Figure 2-1. SSH Access and SSH Host Keys

Similar to the HTTP and HTTPS ports for the IPCop machine being switched to ports 81 and 445, the SSH port on the IPCop machine is switched to 222. If you are using a GUI based application to access your IPCop machine, remember to specify port 222. If you are using the ssh, scp or sftp commands, the syntax for specifying non-standard ports is different for each command, even though they are related. Assuming your IPCop machine is at IP address 192.168.254.1, the commands would be:

SSH

```
$ ssh -p 222 root@192.168.254.1
```

SCP

```
$ scp -P 222 some/file root@192.168.254.1:
```

SFTP

```
$ sftp -o port=222 root@192.168.254.1
```

Use your desktop machine's man pages to get a more complete explanation of these commands.

SSH Options

The following SSH options are available from the web page:

Enabled:

Checking this box enables SSH. Unless you use external access, SSH will only be available from the GREEN network. With SSH enabled it possible for anyone with the IPCop root password to log into your firewall at the command prompt.

Support SSH protocol version 1 (required only for old clients)

Checking this box enables support of SSH version 1 clients. Use of this option is strongly discouraged. There are known vulnerabilities with SSH version 1. Use this option only for temporary access, if you only have SSH version 1 clients and there is no way to upgrade to SSH version 2. Most, if not all, of the current SSH clients support version 2. Upgrade your clients if at all possible.

Allow TCP Forwarding

Checking this box, allows you to create SSH encrypted tunnels between machines inside your firewall and external users.

What use is this when IPCop already has a VPN?

You are on the road and something goes wrong with one of your servers. You haven't set up a road warrior VPN connection. If you know your IPCop root password you can use SSH port forwarding to get through your firewall and get access to a server on one of your protected networks. These next few paragraphs will discuss how to do this, assuming you have a Telnet server running on an internal computer at 10.0.0.20. It also assumes your remote machine is a Linux machine. The putty SSH command on Windows has the same capabilities, but they are accessed via dialog boxes. You may already have done one or more of the first two steps.

1. Enable or have someone else enable external access for port 445, the HTTPS port.
2. Use the IPCop web pages to enable SSH access, port forwarding and external access for port 222.
3. Create an SSH tunnel between your remote machine and the internal server running an SSH daemon by issuing the command:

   ```
   $ ssh -p 222 -N -f -L 12345:10.0.0.20:23 root@ipcop
   ```

   -p 222

   IPCop listens for SSH on port 222, not the normal 22.

   -N

   in conjunction with -f, tells SSH to run in the background without terminating. If you use this option, you will have to remember to use kill to terminate the SSH process. As an alternative, you may want to add the command **`sleep 100`** to the end of the command line, and not use the -N option. If you do this the SSH invoked by the ssh command will terminate after 100 seconds, but the telnet session and its tunnel will not terminate.

   -f

   option to run SSH in the background.

   -L

   tells SSH to build a port forwarding tunnel as specified by the next parameters.

   12345

   The local port that will be used to tunnel to the remote service. This should be greater than 1024, otherwise you must be running as root to bind to well known ports.

   10.0.0.20

   This is the GREEN address of the remote server.

   23

   This specifies the remote port number to be used, Telnet.

   root@ipcop.fqn

   Finally, this specifies you will be using your IPCop firewall as the port forwarding agent. You need a user ID to log in as, and the only one available on is root. You will be prompted for IPCop's root password.

4. Finally, log into the remote Telnet using the tunnel.

   ```
   $ telnet localhost 12345
   ```

localhost is the machine you are running on. The loopback address 127.0.0.1 is defined as localhost. 12345 is the local tunnel port specified on the previous command.

There is a tutorial on SSH port forwarding at Dev Shed[5].

Allow password based authentication

Allows users to log into the IPCop server using the root password. If you decide to turn this off, set up your SSH key files, first and then verify you can log in using your key files.

Allow public key based authentication

By checking this box, public key authentication can be used by SSH. This is the preferred method of securing IPCop using SSH. This article[6] has a discussion about using **SSH-keygen** to generate RSA keys and how to use them with SSH.

SSH Host Keys

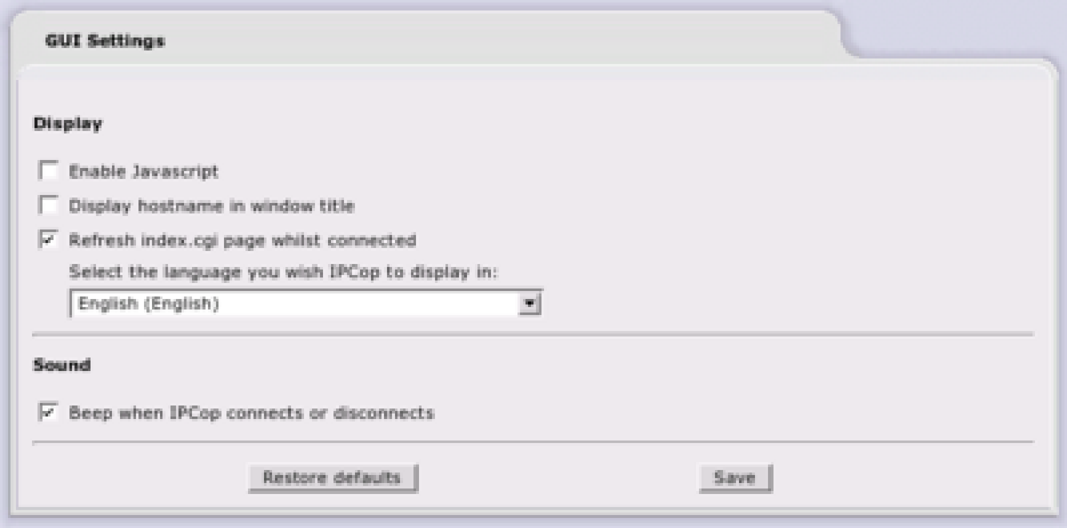
This section lists the host key fingerprints used by SSH on IPCop to verify you are opening a session with the right machine. The first time a session is opened, one of the fingerprints will be displayed by SSH and you will be asked to verify it’s correct. If you wish, you verify can it by looking at this web page.

GUI Settings

This web page governs how the IPCop web pages function and appear.

After making any changes, remember to press the **Save** button.

To restore the default settings, press the **Restore defaults** button, then press the **Save** button.



GUI Settings

Display

□ Enable Javascript

□ Display hostname in window title

☑ Refresh index.cgi page whilst connected

Select the language you wish IPCop to display in: English (English)

Sound

☑ Beep when IPCop connects or disconnects

Figure 2-2. GUI Settings

Display

Enable Javascript:

The 1.4.0 administrative web pages use JavaScript extensively to provide an improved look and feel. However, some browsers do not work properly wth JavaScript. If this button is not checked, the various drop down menus will be disabled and your choices on any page will appear across the top of the page.

Display hostname in window title:

This checkbox will turn on the display of an IPCop's hostname at the top of each web page. If you are maintaining more than one IPCop machine, this will be advantageous, since you will be able to tell which machine your browser is currently displaying.

Refresh index.cgi page whilst connected

By default, the Home page refreshes once when IPCop connects to the Internet, and a manual click on the "Refresh" button forces the Home page to update with the latest connection time.

Enabling this option forces the Home page to refresh every 30 seconds, so the connection time is regularly updated, and if the connection drops due to lack of demand, the "Dial on Demand waiting" status message will appear.

Select the language you wish IPCop to display in:

This drop down menu will let you choose which one of the 27 languages currently available for IPCop web pages, this IPCop will use for its display.

You can also select the language to be used by IPCop during installation. However, your desired language may not be available during installation. The IPCop translation group is planning on making more languages available as volunteers aid the translation effort. When new languages become available, these are added via the regular system updates.

Of course, you may wish to translate IPCop to another language yourself. If you do, we urge you to contact the IPCop Translation Coordinator, Eric Oberlander, `<eoberlander@users.sourceforge.net>`, first. He may be aware of ongoing translation projects for your language. Please check the IPCop How To Translate[7] web page for more details.

Sound

Beep when IPCop connects or disconnects

By default, IPCop will beep once when it connects, and twice when it disconnects.

Disable this option for silent operation.

This does not affect the chimes on startup and shutdown.

Backup Web Page

There are two ways to back up IPCop and three ways to restore it. One backup creates disk files and one puts its output on a floppy.

Creating a backup floppy limits the amount of data saved, since the result must fit onto a 1.44 MB floppy. It is, however, the backup used when restoring IPCop from scratch. During IPCop installation, you will be prompted for a floppy disk to restore. All settings saved on the floppy will be restored, and installation will complete.

When first creating backup files IPCop creates two files, a tar.gz file and a .dat file. It also creates a unique backup key that will be used to encrypt all the tar.gz files. The *Encrypted* and *Unencrypted* descriptions of the files are misnomers. While the .dat file is encrypted, the encryption is used to "sign" the .dat file, so it can't be accidentally restored on a different IPCop machine. Once a key has been created, only .dat files can be used for a restore.

For full backup/restore protection *all* methods and files should be used for backups, as explained in the following scenarios.

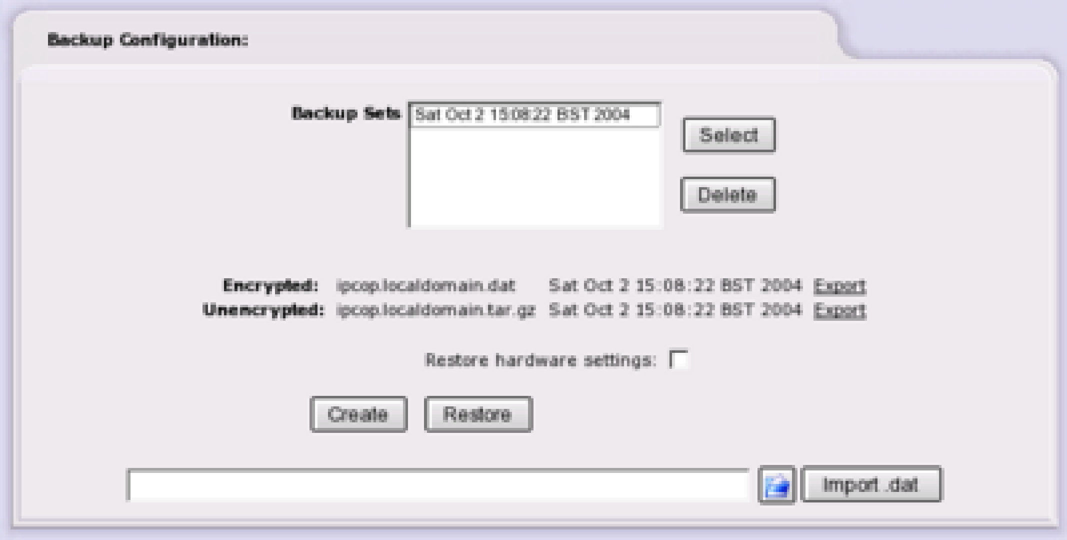
IPCop settings are damaged

Use an appropriate .dat file to restore saved settings.

You have to reinstall IPCop

Use a backup floppy, if you have one, during the installation process to restore your old settings. Then import the .tar.gz file to the new IPCop machine and restore all settings and logs.

Backup to Files



Backup Configuration:

Backup Sets: Sat Oct 2 15:08:22 BST 2004

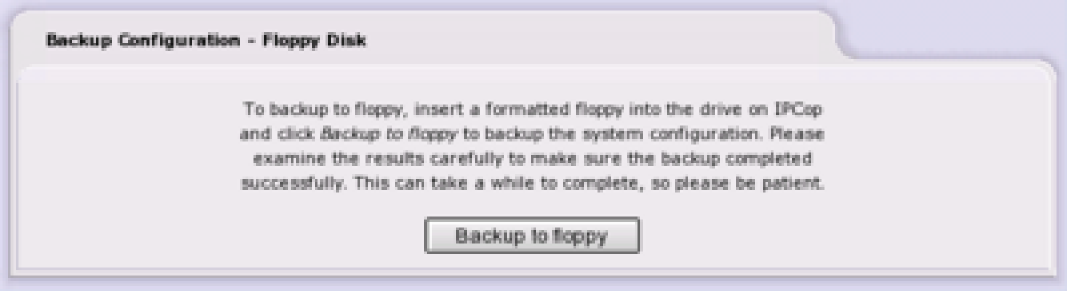
Encrypted: ipcop.localdomain.dat Sat Oct 2 15:08:22 BST 2004 Export
Unencrypted: ipcop.localdomain.tar.gz Sat Oct 2 15:08:22 BST 2004 Export

Restore hardware settings: □

This panel of the Backup web page manages the creation, export, import and restore of IPCop file backups. By clicking on the **create** button, IPCop will create a backup key, if one has not been created previously, and create the two backup files. If this is the first time you've created backup files, the text in the **Import .tar.gz** button will change to **Import .dat**. This indicates that in the future only .dat files may be imported. Next, export both files to the computer you are running your web browser on by clicking on their *Export* links.

If you wish to restore from a backup file, **select** one of the backup sets shown in the *Backup Sets* window. Or import a saved .dat file from another machine.

Backup to Floppy



Backup Configuration - Floppy Disk

To backup to floppy, insert a formatted floppy into the drive on IPCop and click *Backup to floppy* to backup the system configuration. Please examine the results carefully to make sure the backup completed successfully. This can take a while to complete, so please be patient.

This panel of the Backup Web Page will let you back up your IPCop configuration to a floppy disk. The easiest way to restore your configuration is to reinstall IPCop from CD-ROM or HTTP/FTP. Early in the installation process, you will be asked if you have a floppy with an IPCop system configuration on it. If you wish to restore your configuration from a backup floppy, place the floppy disk in the floppy drive and select the **Restore** button. Your configuration will be restored and installation will terminate.

After installation completes, you can use the Backup Web page to import an unsigned .tar.gz file and restore from it, regaining missing logs, etc.

Warning

At this time, IPCop will not overwrite DOS formatted floppy disks. To format a floppy disk for IPCop, you will need to format it for Linux. The command to do this is:

```
# fdformat /dev/fd0
```

If you have another Linux machine, you can format a floppy on that machine. Otherwise, use SSH or putty to log in to IPCop as root, and issue the command there. **fdformat** will not prompt for a floppy like DOS format will, so insert the floppy disk into the floppy disk drive before issuing **fdformat**.

Backup configuration

Place a floppy disk in the floppy disk drive and click the **Backup** button. Your configuration will be written to the floppy and verified.

Information

All messages generated during a backup will appear in this section of the page.

Shutdown Web Page

This page allows you to either **Shutdown** or **Reboot** the IPCop server. You can simply click the button for the option you want, or schedule a cronjob to reboot or shutdown IPCop at a particular time.

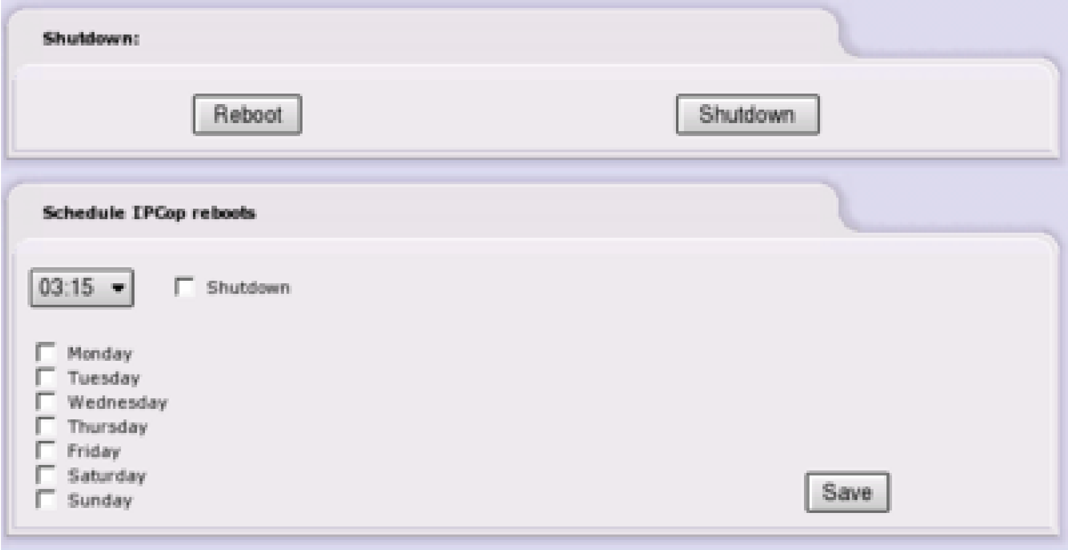


Figure 2-3. Shutdown and Schedule Reboots

Shutdown

Press one of the **Reboot** or **Shutdown** buttons to *immediately* reboot or halt the IPCop server.

Schedule IPCop reboots

The ability to schedule reboots or shutdowns was added in version 1.4.10. A cronjob is added to root's **crontab**. To schedule IPCop to reboot once a day on a regular schedule, select the time from the drop down menu; check the day (or days) you require; and press the **Save** button.

If you want to stop IPCop instead of restarting it, check the **Shutdown** checkbox as well.

To remove a schedule, clear (uncheck) all the checkboxes and press the **Save** button.

Status Menu

This group of web pages provides you with information and statistics from the IPCop server. To get to these web pages, select **Status** from the tab bar at the top of the screen. The following choices will appear in a dropdown:

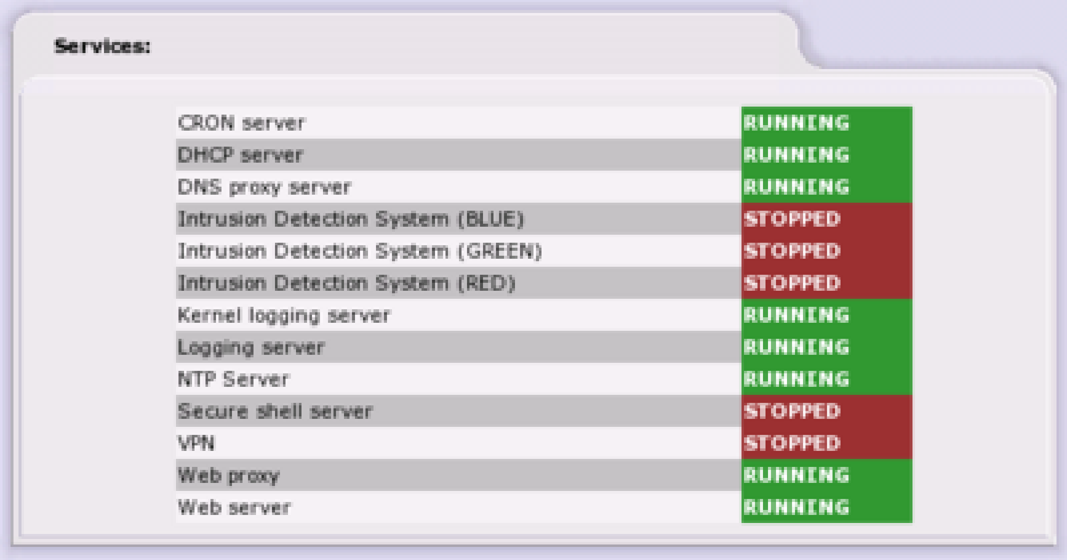
- **System Status**
- **Network Status**
- **System Graphs**
- **Traffic Graphs**
- **Proxy Graphs**
- **Connections**

System Status

The Status pages present you with a VERY thorough list of information regarding the current status of your IPCop server. The first subsection, *System Status*, displays the following in top-down order:

Services

Services - Displays which services are currently running.

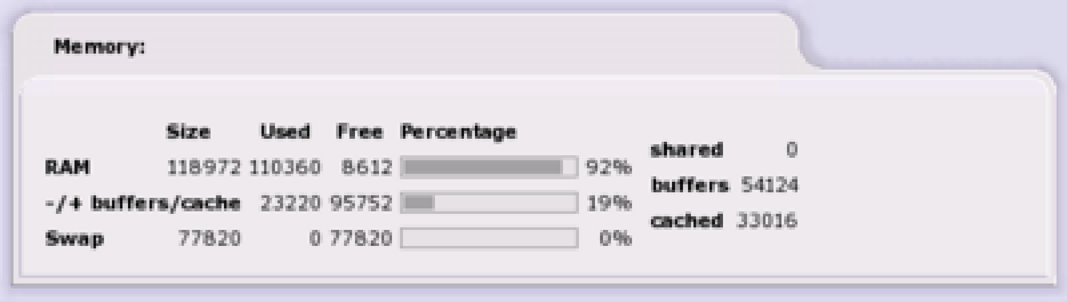


Services:

CRON server	RUNNING
DHCP server	RUNNING
DNS proxy server	RUNNING
Intrusion Detection System (BLUE)	STOPPED
Intrusion Detection System (GREEN)	STOPPED
Intrusion Detection System (RED)	STOPPED
Kernel logging server	RUNNING
Logging server	RUNNING
NTP Server	RUNNING
Secure shell server	STOPPED
VPN	STOPPED
Web proxy	RUNNING
Web server	RUNNING

Memory

Memory - Displays the memory/swapfile usage on your IPCop server.



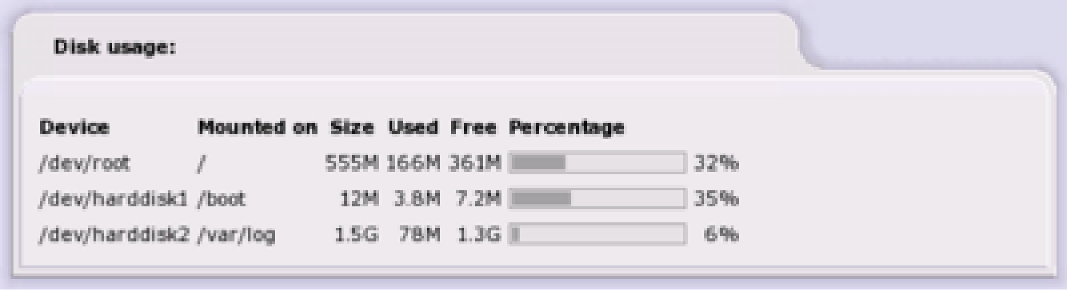
Memory:

	Size	Used	Free	Percentage	
RAM	118972	110360	8612		92%
-/+ buffers/cache		23220	95752		19%
Swap	77820	0	77820		0%

shared	0
buffers	54124
cached	33016

Disk Usage

Disk Usage - Displays the total/used amount of hard drive space on your IPCop server.

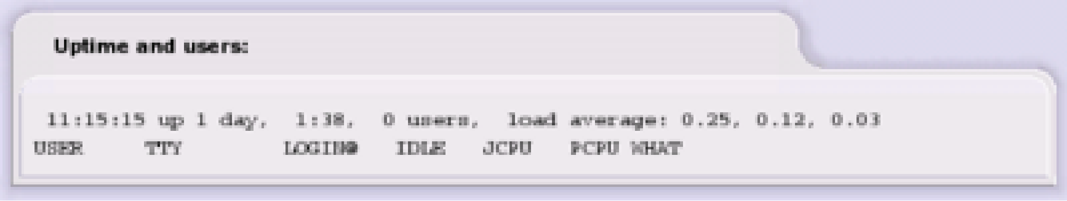


Disk usage:

Device	Mounted on	Size	Used	Free	Percentage
/dev/root	/	555M	166M	361M	32%
/dev/harddisk1	/boot	12M	3.8M	7.2M	35%
/dev/harddisk2	/var/log	1.5G	78M	1.3G	6%

Uptime and Users

Uptime and Users - Displays the output of the **uptime** command and information on users currently logged in on the IPCop server.

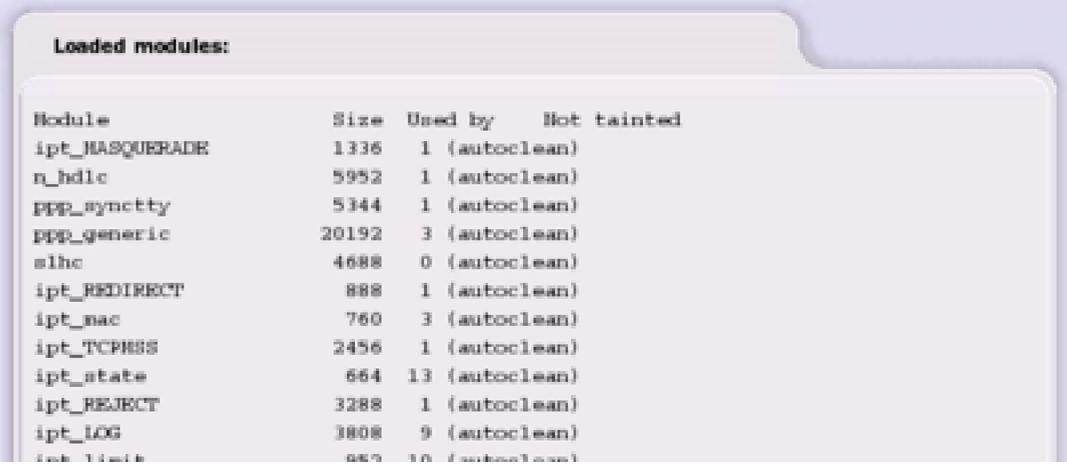


Uptime and users:

```
 11:15:15 up 1 day,  1:38,  0 users,  load average: 0.25, 0.12, 0.03
USER     TTY        LOGIN@   IDLE   JCPU   PCPU WHAT
```

Loaded Modules

Loaded Modules - This displays all modules currently loaded and in use by the kernel.

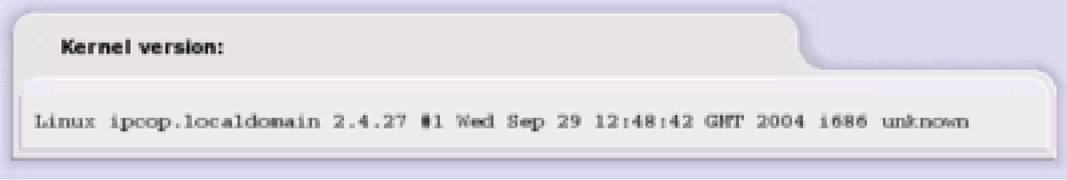


Loaded modules:

```
Module                  Size  Used by    Not tainted
ipt_MASQUERADE          1336   1 (autoclean)
n_hdlc                  5952   1 (autoclean)
ppp_synctty             5344   1 (autoclean)
ppp_generic            20192   3 (autoclean)
slhc                    4688   0 (autoclean)
ipt_REDIRECT             888   1 (autoclean)
ipt_mac                  760   3 (autoclean)
ipt_TCPMSS              2456   1 (autoclean)
ipt_state                664  13 (autoclean)
ipt_REJECT              3288   1 (autoclean)
ipt_LOG                 3808   9 (autoclean)
ipt_limit                952  10 (autoclean)
```

Kernel Version

Kernel Version - This displays information on the IPCop Kernel itself.



Kernel version:

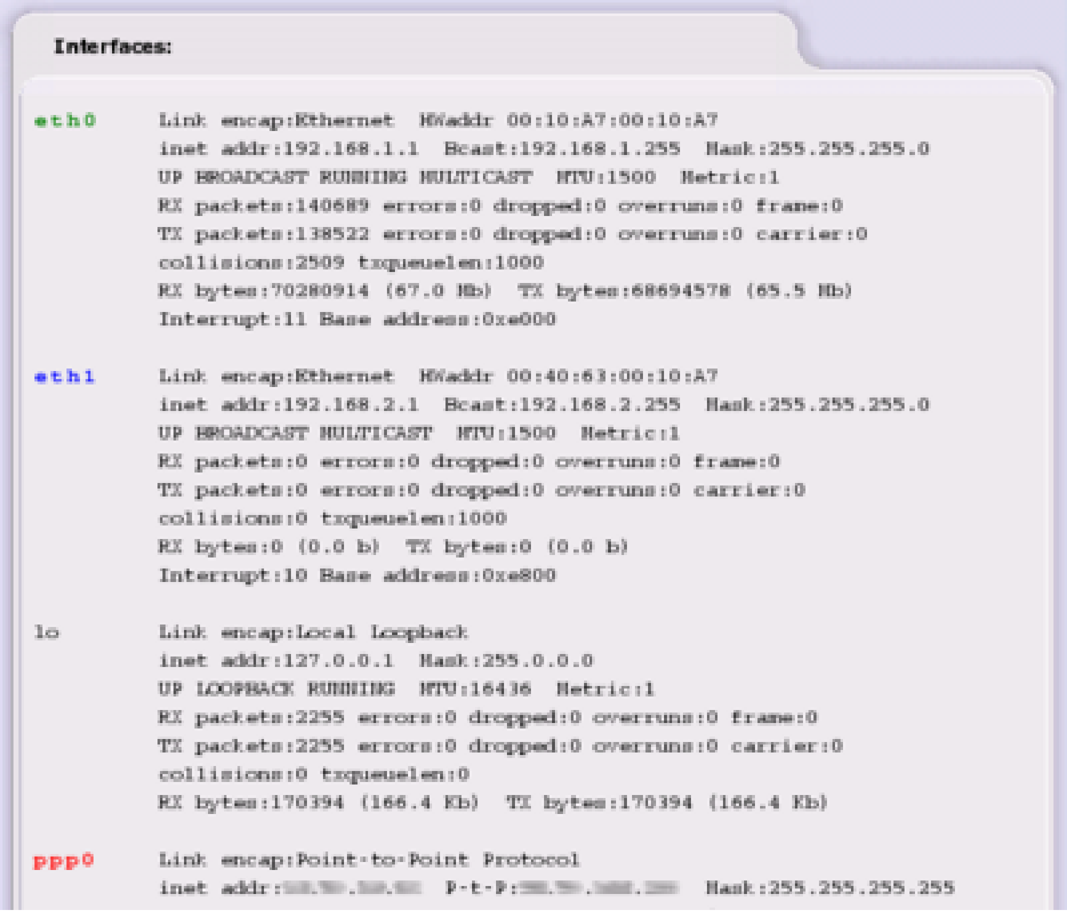
```
Linux ipcop.localdomain 2.4.27 #1 Wed Sep 29 12:48:42 GMT 2004 i686 unknown
```

Network Status

Content to be written...

Interfaces

Interfaces - This section displays information on *all* your network devices. This includes PPP, IPSec, Loopback, etc.



Interfaces:

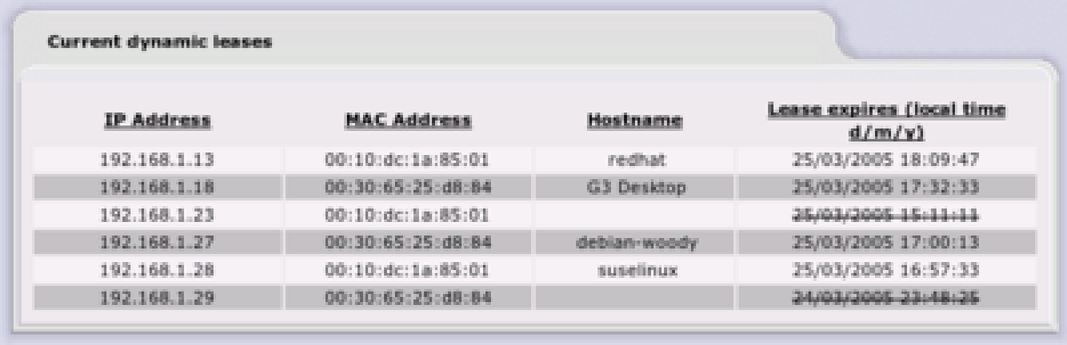
```
eth0      Link encap:Ethernet  HWaddr 00:10:A7:00:10:A7
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:140689 errors:0 dropped:0 overruns:0 frame:0
          TX packets:138522 errors:0 dropped:0 overruns:0 carrier:0
          collisions:2509 txqueuelen:1000
          RX bytes:70280914 (67.0 Mb)  TX bytes:68694578 (65.5 Mb)
          Interrupt:11 Base address:0xe000

eth1      Link encap:Ethernet  HWaddr 00:40:63:00:10:A7
          inet addr:192.168.2.1  Bcast:192.168.2.255  Mask:255.255.255.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:10 Base address:0xe800

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2255 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2255 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:170394 (166.4 Kb)  TX bytes:170394 (166.4 Kb)

ppp0      Link encap:Point-to-Point Protocol
          inet addr:[redacted]  P-t-P:[redacted]  Mask:255.255.255.255
```

Content to be checked...

Current Dynamic Leases

Displays the contents of the `/var/state/dhcp/dhcpd.leases` file if DHCP is enabled. The current dynamic leases are listed, with hostnames if available, and expiry dates.

Leases that have expired are scored through.



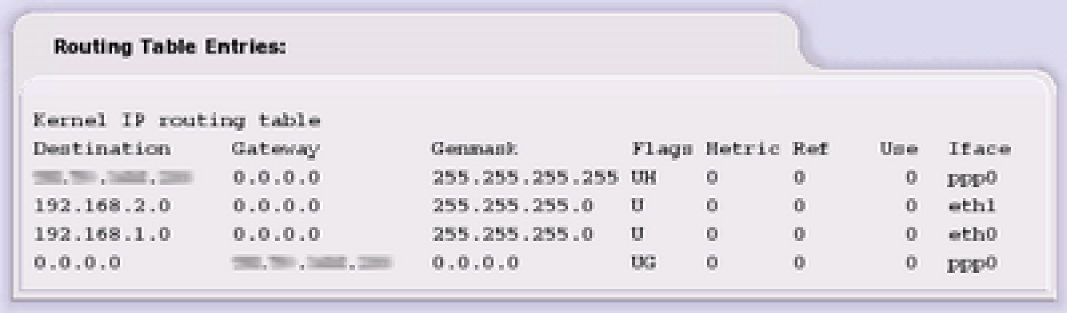
Current dynamic leases

IP Address	MAC Address	Hostname	Lease expires (local time d/m/y)
192.168.1.13	00:10:dc:1a:85:01	redhat	25/03/2005 18:09:47
192.168.1.18	00:30:65:25:d8:84	G3 Desktop	25/03/2005 17:32:33
192.168.1.23	00:10:dc:1a:85:01		~~25/03/2005 15:11:11~~
192.168.1.27	00:30:65:25:d8:84	debian-woody	25/03/2005 17:00:13
192.168.1.28	00:10:dc:1a:85:01	suselinux	25/03/2005 16:57:33
192.168.1.29	00:30:65:25:d8:84		~~24/03/2005 23:48:25~~

Note: This section will *only* be visible if DHCP is enabled. Refer to the section on the DHCP Server for details.

Routing Table Entries

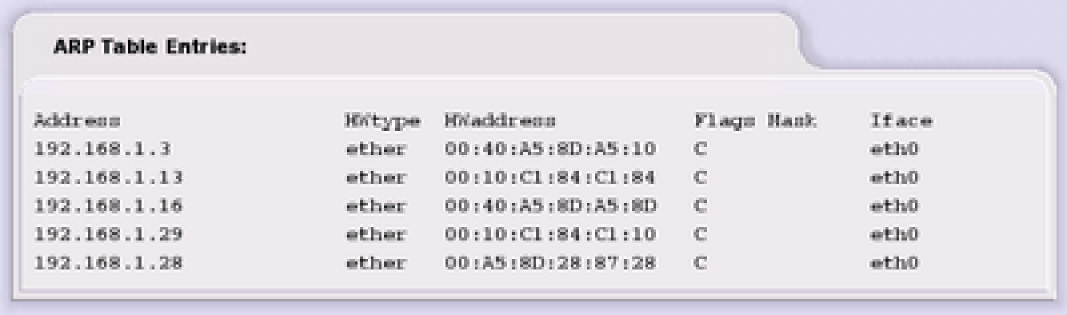
Content to be written...



Routing Table Entries:

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use  Iface
[redacted]      0.0.0.0         255.255.255.255 UH    0      0        0  ppp0
192.168.2.0     0.0.0.0         255.255.255.0   U     0      0        0  eth1
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0  eth0
0.0.0.0         [redacted]      0.0.0.0         UG    0      0        0  ppp0
```

ARP Table Entries



ARP Table Entries:

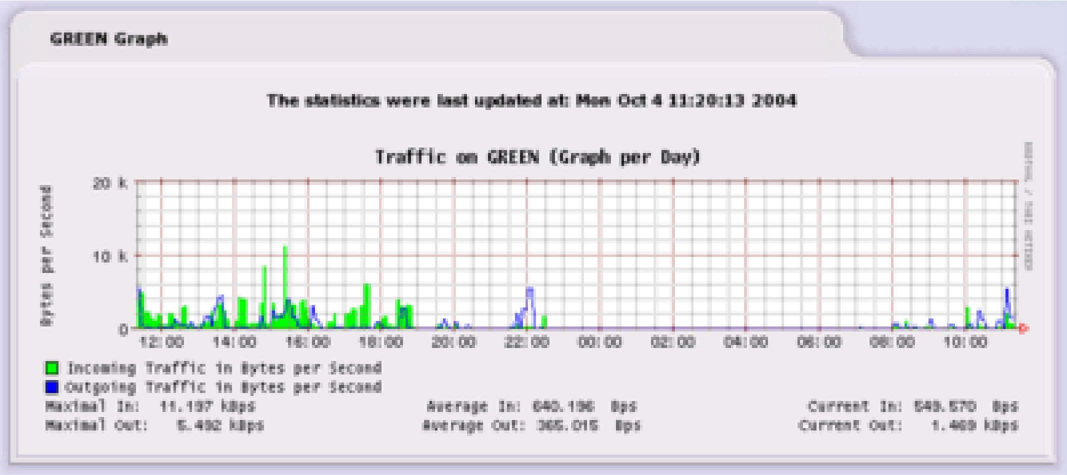
```
Address                  HWtype  HWaddress           Flags Mask     Iface
192.168.1.3              ether   00:40:A5:8D:A5:10   C              eth0
192.168.1.13             ether   00:10:C1:84:C1:84   C              eth0
192.168.1.16             ether   00:40:A5:8D:A5:8D   C              eth0
192.168.1.29             ether   00:10:C1:84:C1:10   C              eth0
192.168.1.28             ether   00:A5:8D:28:87:28   C              eth0
```

Content to be written...

System Graphs

Click on one of the four graphs (CPU Usage, Memory Usage, Swap Usage and Disk Access) to get graphs of the usage per Day, Week, Month and Year.

Traffic Graphs



GREEN Graph

The statistics were last updated at: Mon Oct 4 11:20:13 2004

Traffic on GREEN (Graph per Day)

🟩 Incoming Traffic in Bytes per Second
🟦 Outgoing Traffic in Bytes per Second

```
Maximal In:   11.197 kBps       Average In:  640.196  Bps       Current In:  549.570  Bps
Maximal Out:   5.492 kBps       Average Out: 365.015  Bps       Current Out:   1.469 kBps
```

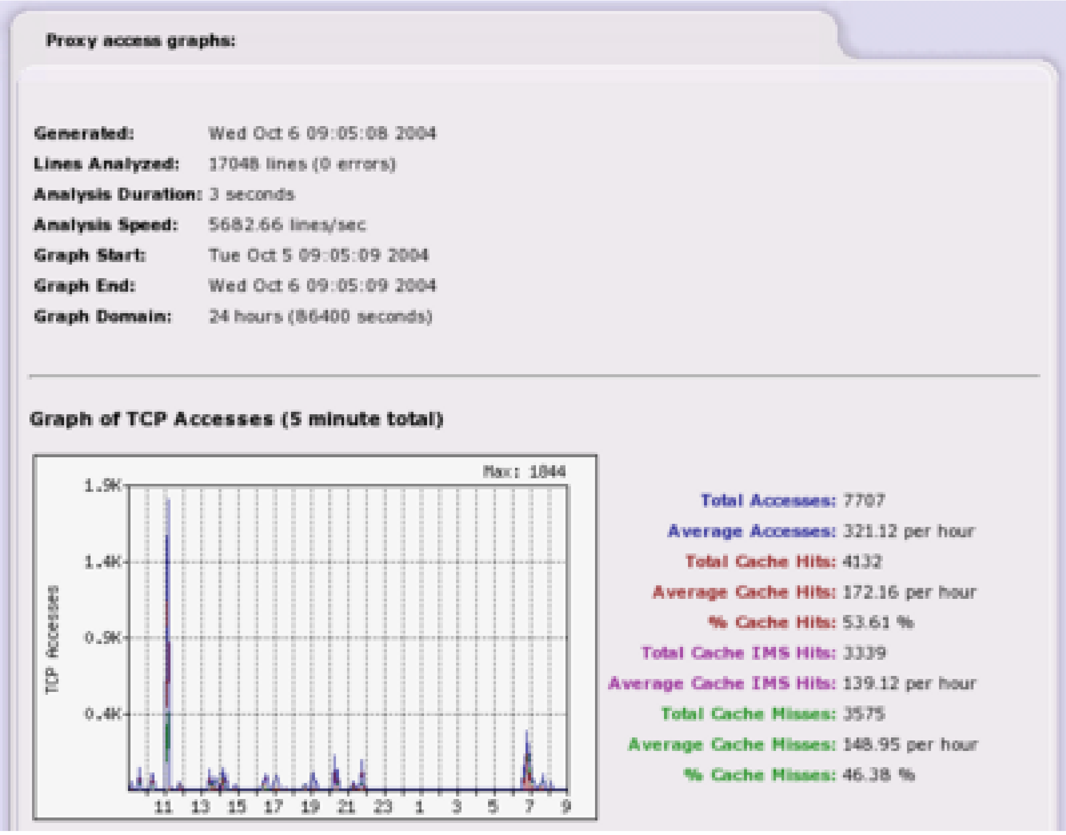
This page gives a graphic depiction of the traffic in and out of the IPCop box.

There are sections for each network interface, Green and Red, (and Blue and Orange if configured) which show graphs of incoming and outgoing traffic through that interface.

Click on one of the graphs to show more graphs of the traffic on that interface: per Day, Week, Month and Year.

> **Note:** When v1.4.0 was being developed, it was found that the `rrdtool` used to generate the graphs was unable to handle special characters, which particularly affects languages that rely on the UTF-8 character set. At the moment, the text on the graphs is forced to use English, until a solution can be found.

Proxy Graphs



Proxy access graphs:

Generated:	Wed Oct 6 09:05:08 2004
Lines Analyzed:	17048 lines (0 errors)
Analysis Duration:	3 seconds
Analysis Speed:	5682.66 lines/sec
Graph Start:	Tue Oct 5 09:05:09 2004
Graph End:	Wed Oct 6 09:05:09 2004
Graph Domain:	24 hours (86400 seconds)

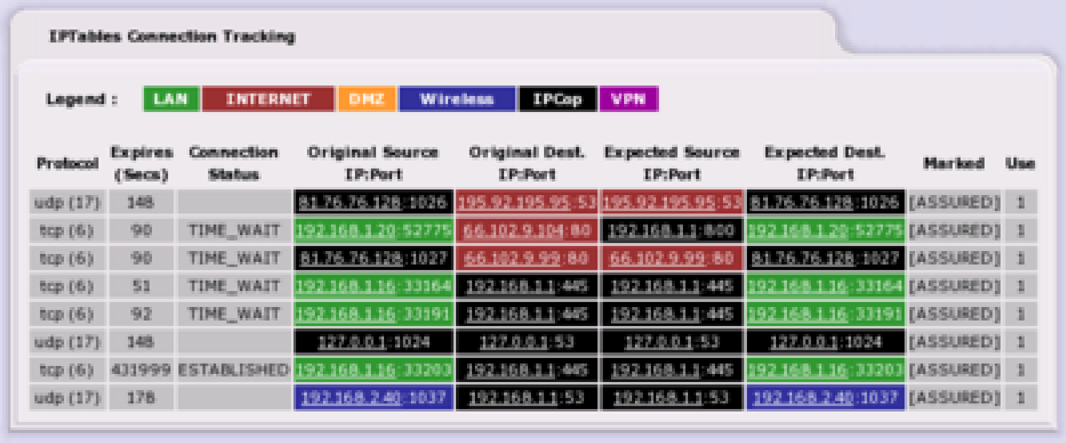
Graph of TCP Accesses (5 minute total)

Total Accesses:	7707
Average Accesses:	321.12 per hour
Total Cache Hits:	4132
Average Cache Hits:	172.16 per hour
% Cache Hits:	53.61 %
Total Cache IMS Hits:	3339
Average Cache IMS Hits:	139.12 per hour
Total Cache Misses:	3575
Average Cache Misses:	148.95 per hour
% Cache Misses:	46.38 %

This page shows traffic through the proxy service of the IPCop box. The first section gives the date and time the graph was created, the lines analyzed, the duration of the analysis, the speed (lines per second), the start and end date and time of the graph, and the domain (overall length of the graph in time).

This information is useful in seeing whether the proxy is the correct size for the load being experienced.

Connections



IPTables Connection Tracking

Legend : LAN INTERNET DMZ Wireless IPCop VPN

Protocol	Expires (Secs)	Connection Status	Original Source IP:Port	Original Dest. IP:Port	Expected Source IP:Port	Expected Dest. IP:Port	Marked	Use
udp (17)	148		81.76.76.128:1026	195.92.195.95:53	195.92.195.95:53	81.76.76.128:1026	[ASSURED]	1
tcp (6)	90	TIME_WAIT	192.168.1.20:52775	66.102.9.104:80	192.168.1.1:800	192.168.1.20:52775	[ASSURED]	1
tcp (6)	90	TIME_WAIT	81.76.76.128:1027	66.102.9.99:80	66.102.9.99:80	81.76.76.128:1027	[ASSURED]	1
tcp (6)	51	TIME_WAIT	192.168.1.16:33164	192.168.1.1:445	192.168.1.1:445	192.168.1.16:33164	[ASSURED]	1
tcp (6)	92	TIME_WAIT	192.168.1.16:33191	192.168.1.1:445	192.168.1.1:445	192.168.1.16:33191	[ASSURED]	1
udp (17)	148		127.0.0.1:1024	127.0.0.1:53	127.0.0.1:53	127.0.0.1:1024	[ASSURED]	1
tcp (6)	431999	ESTABLISHED	192.168.1.16:33203	192.168.1.1:445	192.168.1.1:445	192.168.1.16:33203	[ASSURED]	1
udp (17)	178		192.168.2.40:1037	192.168.1.1:53	192.168.1.1:53	192.168.2.40:1037	[ASSURED]	1

IPCop uses the Linux Netfilter or IPTables firewall facility to maintain a stateful firewall. Stateful firewalls keep track of connections to and from all GREEN, BLUE and ORANGE network IP addresses, based on both the source and destination IP addresses and ports, as well as the state of the connection itself. After a connection is established involving protected machines, only packets consistent with the current state of the connection are allowed through the IPCop firewall.

The *IPTables Connection Tracking* window shows the IPTables connections. Connection end points are color-coded based on their network location. The color-coding legend is displayed at the top of the page. Information on individual connections is displayed next. Each connection from or to your networks is shown.

Click on an IP Address to do a reverse DNS lookup.

Network Menu

Dialup

This subsection of the Dialup Administration Window (AW) is divided into 5 different editable sections and is only applicable if you are accessing the Internet using an analog modem, an ISDN device or a DSL connection.

Note that you cannot select or modify a profile while the IPCop server is online, or waiting to go online in "Dial on Demand" mode. Before using this page, go to the *Home* AW and if the status line reports *Connected* or *Dial on Demand waiting* then the click on the **Disconnect** button before returning to this Window. After setting up or selecting Profiles, remember to return to the *Home* AW and click the **Connect** button, if you want your IPCop server to go back online.

Profiles

This section of the Window provides the facilities to name and set up new Dialup Profiles (up to a total of five), or to rename existing Profiles and change their parameters.

Select a Profile to be created or modified from the drop-down list. Fill in or change the parameters for the profile (see below) and click on the **Save** button. To select the Profile to be used for future connections, use the drop-down list to make your choice and click the **Select** button at the bottom of the page. Use the **Restore** button while editing a Profile to reinstate the previous Profile settings.

Telephony

This section allows you to do the following:

1. Select the appropriate *Interface* for your Internet connection device. This will be either a Communications port (COM1 - COM4) used mostly for modems and ISDN cards, or PPPoE which is used mostly for DSL connections.
2. Select the appropriate *Computer to modem rate*. This will decide how quickly data is passed to and from your connection device. With older computer systems or modems, you may find it necessary to use one of the lower data rates to establish reliable computer/ modem communications.
3. Enter the correct *Number* to dial for your Internet connection. If connecting through the PPPoE interface then chances are you will probably be leaving this blank.
4. Select whether or not the *Modem speaker on*. Having the speaker on allows you to hear the connection taking place and can be a useful diagnostic aid when troubleshooting. This option is only likely to be useful if you are connecting via an analog modem.

5. Select your *Dialing mode* . Use Tone dialing unless your telephone connection only recognizes Pulse dialing. Pulse dialing is a lot slower than Tone dialing.
6. Enter your desired *Maximum retries*. This will decide how often IPCop attempts to connect to the Internet after a failed connection attempt.
7. Enter your *Idle timeout* . This will decide how IPCop handles your Internet connection when nothing is actually being sent or received via the Internet connection. The number you enter here indicates to IPCop how long it should wait after any Internet activity before it disconnects the modem link. If you set this parameter to *0* then IPCop, once connected, will not disconnect from the Internet of its own accord.
8. The *Persistent Connection* checkbox is used to instruct IPCop to maintain the modem connection at all times, even in the absence of Internet activity. In this mode it will attempt to reconnect the Internet connection whenever the link fails for any reason, such as a connection time-out at the ISP end of the modem link. Use this mode with caution. If you have metered connection charges you probably will not want to use this feature. However, if you have unlimited service time (often called "Flatrate") with your ISP, you may want to use this in order to keep the link connected as much as possible. Note that in *Persistent* mode, IPCop will cease reconnecting after more than the number of consecutive failed dial attempts set in *Maximum Retries* In this event, you have to use the **Dial** button on the *Home* AW.
9. *Dial on Demand* is available by clicking the checkbox. Note that after enabling Dial on Demand, you still have to click the **Connect** button on the *Home* AW before IPCop will start connecting automatically when it detects Internet activity. The *Dial on Demand* option is not available for PPPoE connections.
10. The *Dial on Demand for DNS* option determines whether IPCop will connect automatically when it detects DNS requests. This will be usually what you will want to happen.
11. *Connect on IPCop Restart* will make IPCop connect after booting, if *Dial on Demand* is not selected. You will probably want to set this option as active if you are also using *Dial on Demand*. This is because the combination of settings will automatically put the IPCop system into Dial on Demand waiting mode each time the IPCop server is switched on or rebooted.
12. *ISP Requires Carriage Return* Some ISPs require that the modem sends a carriage return to signal to indicate that it is finished sending data. If your ISP requires this, then leave it checked. If not then you can uncheck this box. The default is checked.

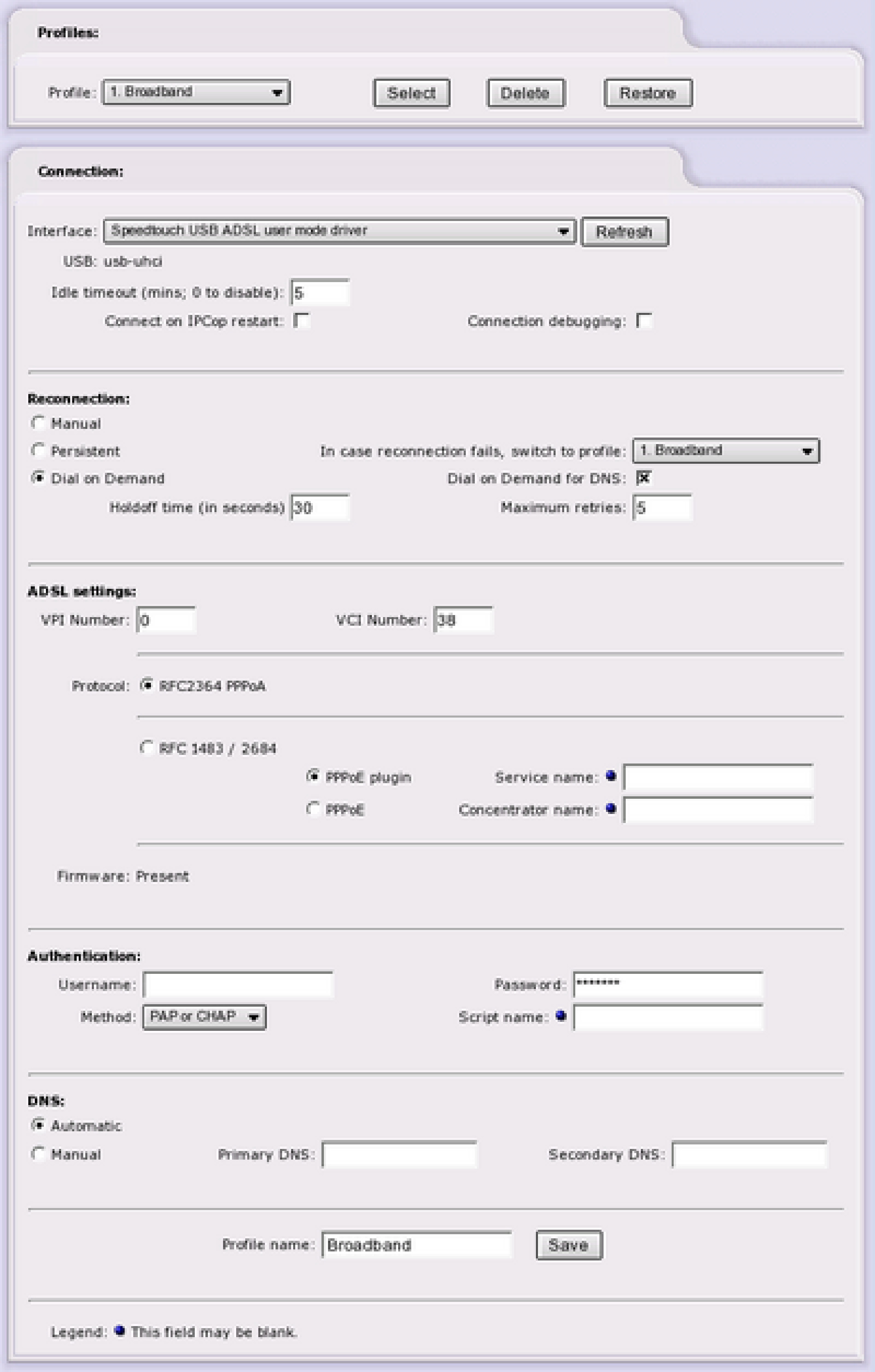
Additional PPPoE settings - If either PPPoE or USB ADSL is enabled, additional configuration options are available. Here you can enter two additional parameters, a service name, and a concentrator name, which some ISPs require. If your ISP does not require them, or does not give you any, then you may leave these two fields blank. Your ISP will give you two settings, VPI and VCI, which you must enter if you are using a USB ADSL connection.

Authentication

Username and *Password* are the username and password that your ISP should have supplied to you when you opened your account with them. There are several ways in which ISPs use this username and password to login to their systems. The most common methods are PAP or CHAP. Select this if your ISP uses either of those two. If your ISP uses a text-based login script, choose standard login script. For people in the UK who use Demon Internet as their ISP, a special script has been created for them to use. The "Other" login script option has been provided for people who have ISPs with special needs. If you need to do this, you will need to login to the IPCop box and create a file in /etc/ppp. This filename (without the /etc/ppp component) should be entered into the Script name box. The file contains 'expect send' pairs, separated by a tab. *`USERNAME`* will be substituted for the username and *`PASSWORD`* for the password. Examine the file demonloginscript in `/etc/ppp`, and use it as an example of what should be in this file.

DNS

Select *Automatic* if your ISP supports automatic DNS server configuration, as is now usually the case. The alternative is to leave *Automatic* unticked and put IP addresses in the *Primary DNS* and *Secondary DNS* boxes. These IP addresses will generally be provided where necessary by your ISP.



Profiles:

Profile: 1. Broadband

Connection:

Interface: Speedtouch USB ADSL user mode driver

USB: usb-uhci

Idle timeout (mins; 0 to disable): 5

Connect on IPCop restart: □ Connection debugging: □

Reconnection:

○ Manual

○ Persistent In case reconnection fails, switch to profile: 1. Broadband

● Dial on Demand Dial on Demand for DNS: ☒

Holdoff time (in seconds) 30 Maximum retries: 5

ADSL settings:

VPI Number: 0 VCI Number: 38

Protocol: ● RFC2364 PPPoA

○ RFC 1483 / 2684

● PPPoE plugin Service name: ●

○ PPPoE Concentrator name: ●

Firmware: Present

Authentication:

Username: Password: ********

Method: PAP or CHAP Script name: ●

DNS:

● Automatic

○ Manual Primary DNS: Secondary DNS:

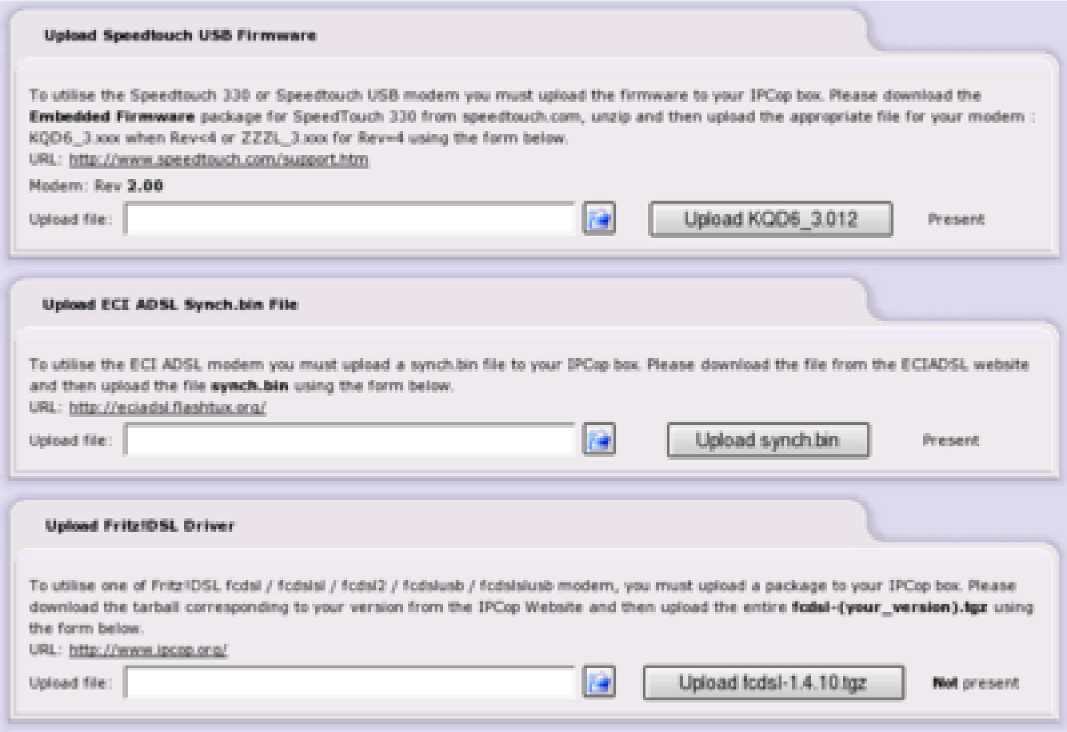
Profile name: Broadband

Legend: ● This field may be blank.

Figure 2-4. PPP Settings

Upload

Use this page to download the files necessary for supporting various modems to your desktop machine, and then upload it to your IPCop server.



Upload Speedtouch USB Firmware

To utilise the Speedtouch 330 or Speedtouch USB modem you must upload the firmware to your IPCop box. Please download the **Embedded Firmware** package for SpeedTouch 330 from speedtouch.com, unzip and then upload the appropriate file for your modem : KQD6_3.xxx when Rev<4 or ZZZL_3.xxx for Rev=4 using the form below.
URL: http://www.speedtouch.com/support.htm

Modem: Rev **2.00**

Upload file:

Upload ECI ADSL Synch.bin File

To utilise the ECI ADSL modem you must upload a synch.bin file to your IPCop box. Please download the file from the ECIADSL website and then upload the file **synch.bin** using the form below.
URL: http://eciadsl.flashtux.org/

Upload file:

Upload Fritz!DSL Driver

To utilise one of Fritz!DSL fcdsl / fcdslsl / fcdsl2 / fcdslusb / fcdslslusb modem, you must upload a package to your IPCop box. Please download the tarball corresponding to your version from the IPCop Website and then upload the entire **fcdsl-(your_version).tgz** using the form below.
URL: http://www.ipcop.org/

Upload file:

Figure 2-5. Upload Modem Drivers

Upload Speedtouch USB Firmware

Use this section to upload the file *mgmt.o* to the IPCop server - USB ADSL will not function before this has been done. Use the link specified to go to the web page, register and download the file to your desktop machine. Then choose the file on your desktop machine, and then press the **upload** button to transfer it to IPCop. Once this has been successfully uploaded, you can use USB ADSL.

Upload ECI ADSL Synch.bin File

Use this section to upload the file *sync.bin* to the IPCop server - ECI ADSL will not function before this has been done. Use the link specified to go to the web page and download the file to your desktop machine. Then choose the file on your desktop machine, and then press the **upload** button to transfer it to IPCop. Once this has been successfully uploaded, you can use ECI ADSL.

Upload Fritz!DSL Driver

Use this section to upload the file *fcdsl.o* to the IPCop server - Fritz!DSL will not function before this has been done. Use the link specified to go to the web page and download the file to your desktop machine. Then choose the file on your desktop machine, and then press the **upload** button to transfer it to IPCop. Once this has been successfully uploaded, you can use Fritz!DSL.

Modem

Modem Configuration

Is only applicable if you are attempting to connect to the Internet with a standard analog modem. The default settings that appear in this Administration Window are appropriate for most analog modems. However if you are experiencing problems connecting, then compare these settings with those suggested in the modem manual for use with your particular modem. Any or all of these settings may be left blank.

Init - The standard Initialization string used by most Hayes-compatible modems is already provided for you in this field. If, however, your modem requires a different setting then by all means change it.

Hangup - The standard Hang up string used by most Hayes-compatible modems is already provided for you in this field. If, however, your modem requires a different setting then by all means change it.

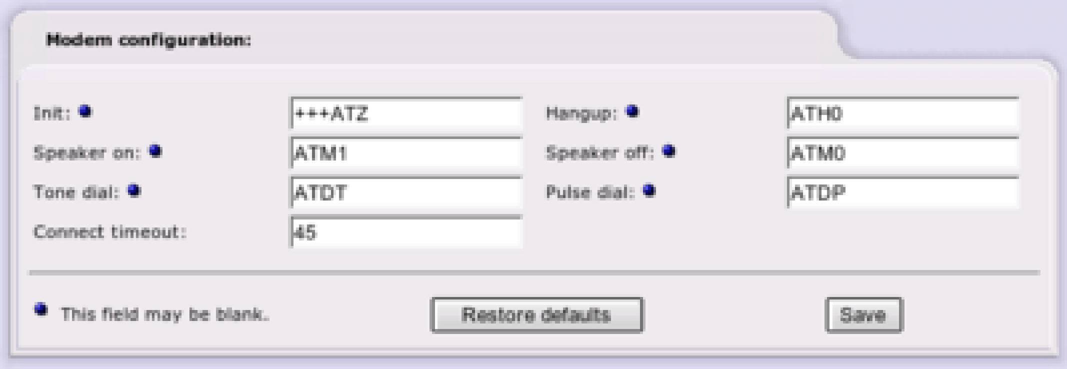
Speaker on - The standard Speaker on string used by most Hayes-compatible modems is already provided for you in this field. If, however, your modem requires a different setting then by all means change it.

Speaker off - The standard Speaker-off string used by most Hayes-compatible modems is already provided for you in this field. If, however, your modem requires a different setting then by all means change it.

Tone Dial - The standard Tone Dial string used by most Hayes-compatible modems is already provided for you in this field. If your modem and telephone line can support the Tone Dial feature and you are experiencing problems connecting then make sure that this string is appropriate for use with your modem.

Pulse Dial - The standard Pulse Dial string used by most Hayes-compatible modems is already provided for you in this field. You should not need to change it, but if your telephone service does not support Tone Dialing then you may need to make sure this is the correct string for your modem.

The only section in this area that may not be blank is the Connect Timeout. This tells IPCop the amount of time to allow the modem to attempt to connect. After this number of seconds has elapsed without proper response on the receiving end, IPCop will give up and move on to the next connection attempt. The default should work fine for you but if you notice that the connection is being dropped in the middle of the negotiation sequence (turn on the modem speaker and listen to the attempted connection) then you may need to increase this parameter slightly until it connects successfully.



Modem configuration:

Init: ●	+++ATZ	Hangup: ●	ATH0
Speaker on: ●	ATM1	Speaker off: ●	ATM0
Tone dial: ●	ATDT	Pulse dial: ●	ATDP
Connect timeout:	45		

● This field may be blank.

Figure 2-6. Modem Settings

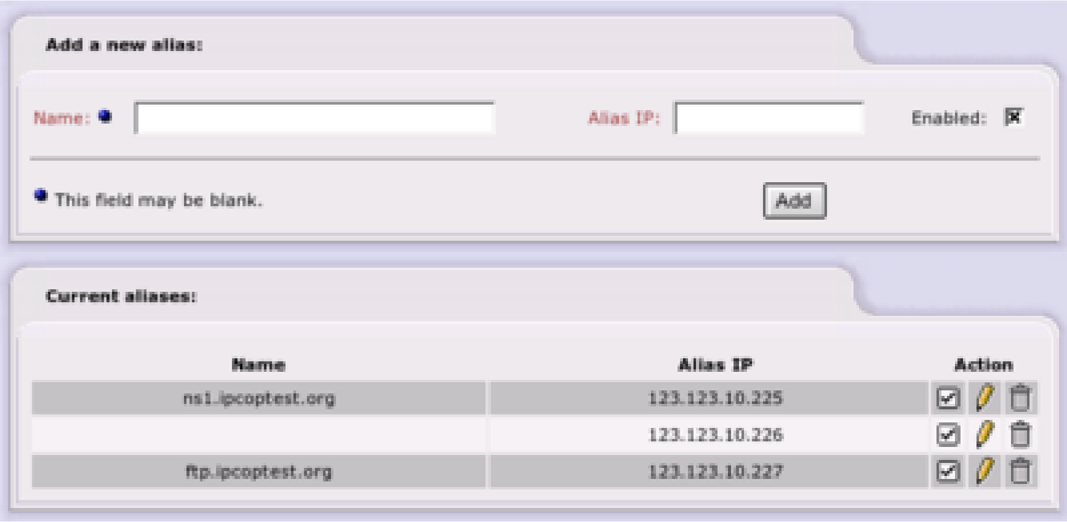
External Aliases Administrative Web Page

> **Note:** This Administrative Web Page will only appear as a menu item if your RED interface is STATIC.

In some cases, your ISP may assign you a range of IP addresses for your network.

If you have multiple IP addresses, only, so that you can connect multiple, non-server computers, to the Internet, you will no longer need the extra addresses. IPCop should connect directly to your modem or the Internet.

On the other hand, if you are providing a server on one of internal computers you may need to use multiple aliases on your RED interface. To use this facility effectively, you may have to adjust IPCop's routing tables by hand.



Add a new alias:

Name: ● Alias IP: Enabled: ☒

● This field may be blank.

Current aliases:

Name	Alias IP	Action
ns1.ipcoptest.org	123.123.10.225	☑ ✎ 🗑
	123.123.10.226	☑ ✎ 🗑
ftp.ipcoptest.org	123.123.10.227	☑ ✎ 🗑

Figure 2-7. External Aliases Settings

Add a new alias

Section to be written...

Once you have entered all the information, click the *Enabled* box and press **Add**. This will move the entry to the next section, and list it as an alias.

Current aliases

This section lists the aliases that are in effect. To remove one, click the “Trash Can” icon. To edit one, click the “Yellow Pencil” icon.

To enable or disable a rule - click on the “Enabled” icon (the checkbox on the left of the Action column) for the particular entry you want to enable or disable. The icon changes to an empty box when a rule is disabled. Click on the checkbox to enable it again.

Services Menu

As well as performing its core function of Internet firewall, IPCop can provide a number of other services that are useful in a small network.

These are:

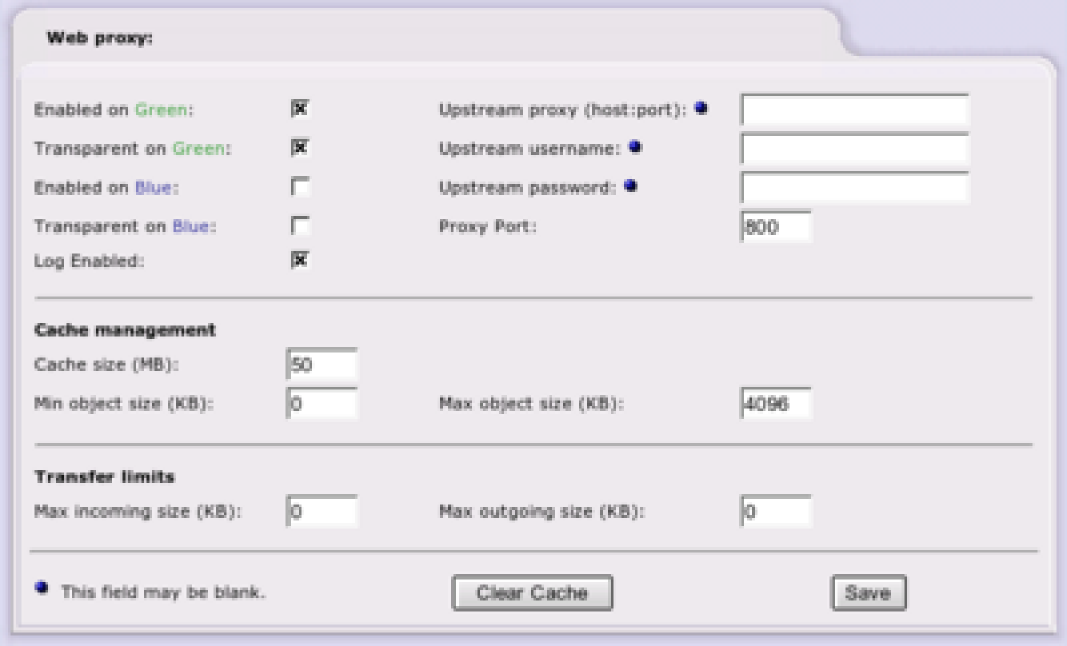
- Proxy (Web Proxy Server)
- DHCP Server
- Dynamic DNS Management
- Edit Hosts (Local DNS Server)
- Time Server
- Traffic Shaping
- Intrusion Detection System

In a larger network it is likely that these services will be provided by dedicated servers and should be disabled here.

Web Proxy Administrative Web Page

A web proxy server is a program that makes requests for web pages on behalf of all the other machines on your intranet. The proxy server will cache the pages it retrieves from the web so that if 3 machines request the same page only one transfer from the Internet is required. If your organization has a number of commonly used web sites this can save on Internet accesses.

Normally you must configure the web browsers used on your network to use the proxy server for Internet access. You should set the name/address of the proxy to that of the IPCop machine and the port to the one you have entered into the **Proxy Port** box, default 800. This configuration allows browsers to bypass the proxy if they wish. It is also possible to run the proxy in “transparent” mode. In this case the browsers need no special configuration and the firewall automatically redirects all traffic on port 80, the standard HTTP port, to the proxy server.



Web proxy:

Enabled on Green: ☒ Upstream proxy (host:port): ●

Transparent on Green: ☒ Upstream username: ●

Enabled on Blue: □ Upstream password: ●

Transparent on Blue: □ Proxy Port: 800

Log Enabled: ☒

Cache management

Cache size (MB): 50

Min object size (KB): 0 Max object size (KB): 4096

Transfer limits

Max incoming size (KB): 0 Max outgoing size (KB): 0

● This field may be blank.

You can choose if you want to proxy requests from your Green (private) network and/or your Blue (wireless) network. Just tick the relevant boxes.

If you choose to enable the proxy then you can also log web accesses by ticking the **Log Enabled** box. Accesses made through the proxy can be seen by clicking the Proxy Logs choice of the Logs menu.

If your ISP requires you to use their cache for web access then you should specify the hostname and port in the **Upstream proxy** text box. If your ISP's proxy requires a user name and password then enter them in the **Upstream username** and **Upstream password** boxes.

Cache Management

You can choose how much disk space should be used for caching web pages in the Cache Management section. You can also set the size of the smallest object to be cached, normally 0, and the largest, 4096KB. For privacy reasons, the proxy will not cache pages received via https, or other pages where a username and password are submitted via the URL.

Transfer limits

The web proxy can also be used to control how your users access the web. The only control accessible via the web interface is the maximum size of data received from and sent to the web. You can use this to prevent your users downloading large files and slowing Internet access for everyone else. Set these to 0,the default, to remove all restrictions.

To save any changes, press the **Save** button.

You can flush all pages out of the proxy cache at any time by clicking the **Clear Cache** button.

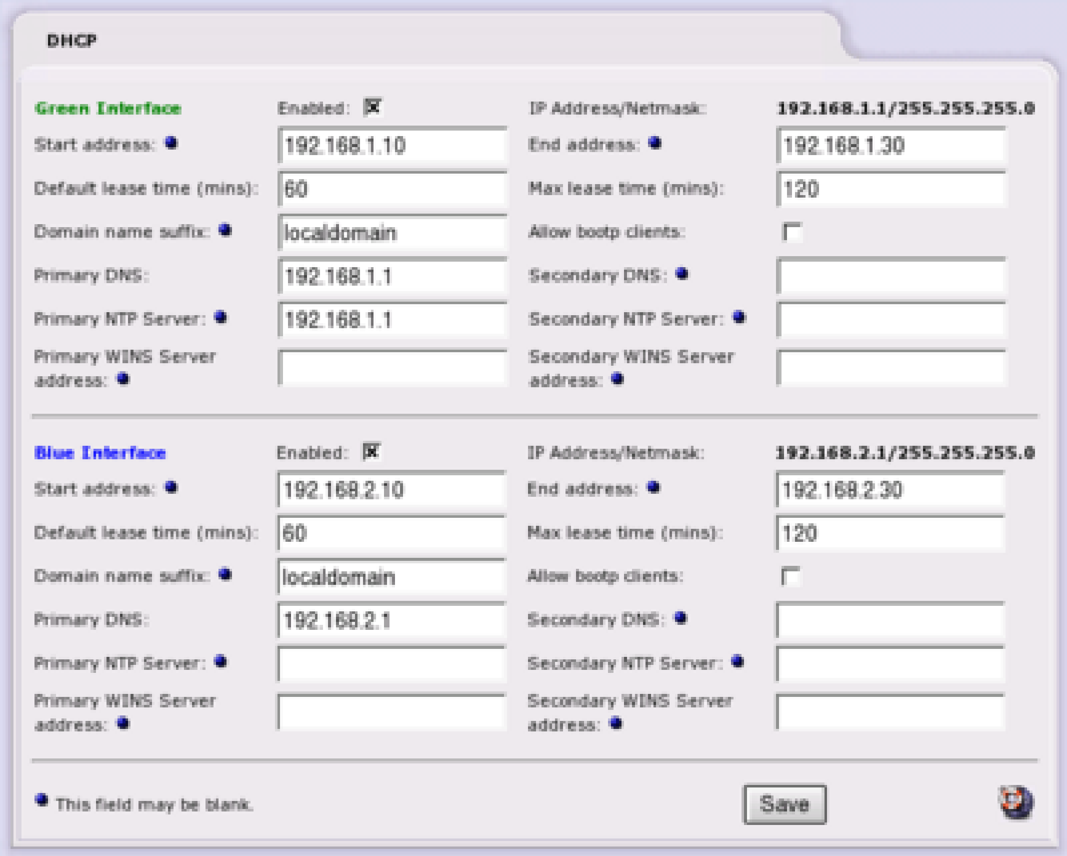
Warning

Caching can take up a lot of space on your hard drive. If you use a large cache, then the minimum size hard drive listed in the IPCop documentation will not be large enough.

The larger the cache you choose the more memory is required by the proxy server to manage the cache. If you are running IPCop on a machine with low memory do not choose a large cache.

DHCP Administrative Web Page

DHCP (Dynamic Host Configuration Protocol) allows you to control the network configuration of all your computers or devices from your IPCop machine. When a computer (or a device like a printer, pda, etc.) joins your network it will be given a valid IP address and its DNS and WINS configuration will be set from the IPCop machine. To use this feature new machines must be set to obtain their network configuration automatically.



DHCP

Green Interface	Enabled: ☒	IP Address/Netmask:	192.168.1.1/255.255.255.0
Start address: ●	192.168.1.10	End address: ●	192.168.1.30
Default lease time (mins):	60	Max lease time (mins):	120
Domain name suffix: ●	localdomain	Allow bootp clients:	☐
Primary DNS:	192.168.1.1	Secondary DNS: ●	
Primary NTP Server: ●	192.168.1.1	Secondary NTP Server: ●	
Primary WINS Server address: ●		Secondary WINS Server address: ●	
Blue Interface	Enabled: ☒	IP Address/Netmask:	192.168.2.1/255.255.255.0
Start address: ●	192.168.2.10	End address: ●	192.168.2.30
Default lease time (mins):	60	Max lease time (mins):	120
Domain name suffix: ●	localdomain	Allow bootp clients:	☐
Primary DNS:	192.168.2.1	Secondary DNS: ●	
Primary NTP Server: ●		Secondary NTP Server: ●	
Primary WINS Server address: ●		Secondary WINS Server address: ●	

● This field may be blank.

You can choose if you want to provide this service to your Green (private) network and/or your Blue (wireless) network. Just tick the relevant box.

For a full explanation of DHCP you may want to read Linux Magazine's " Network Nirvana - How to make Network Configuration as easy as DHCP " [8]

DHCP Server Parameters

The following DHCP parameters can be set from the web interface:

Enabled

Check this box to enable the DHCP server for this interface.

IP Address/Netmask

The IP Address of the network interface and it's Netmask are displayed here for reference.

Start Address (optional)

You can specify the lowest and highest addresses that the server will hand out to other requestors. The default is to hand out all the addresses within the subnet you set up when you installed IPCop. If you have machines on your network that do not use DHCP, and have their IP addresses set manually, you should set the start and end address so that the server will not hand out any of these manual IPs.

You should also make sure that any addresses listed in the fixed lease section (see below) are also outside this range.

End Address (optional)

Specify the highest address you will handout (see above).

> **Note:** To enable DHCP to provide fixed leases without handing out dynamic leases, leave both Start and End Address fields blank. However, if you provide a Start Address, you also have to provide an End Address, and vice versa.

Default lease time

This can be left at its default value unless you need to specify your own value. The default lease time is the time interval IP address leases are good for. Before, the lease time for an address expires your computers will request a renewal of their lease, specifying their current IP address. If DHCP parameters have been changed, when a lease renewal request is made the changes will be propagated. Generally, leases are renewed by the server.

Maximum lease time

This can be left at its default value unless you need to specify your own value. The maximum lease time is the time interval during which the DHCP server will always honor client renewal requests for their current IP addresses. After the maximum lease time, client IP addresses may be changed by the server. If the dynamic IP address range has changed, the server will hand out an IP address in the new dynamic range.

Domain name suffix (optional)

There should not be a leading period in this box. Sets the domain name that the DHCP server will pass to the clients. If any host name cannot be resolved, the client will try again after appending the specified name to the original host name. Many ISP's DHCP servers set the default domain name to their network and tell customers to get to the web by entering "www" as the default home page on their browser. "www" is not a fully qualified domain name. But the software in your computer will append the domain name suffix supplied by the ISP's DHCP server to it, creating a FQDN for the web server. If you do not want your users to have to unlearn addresses like www, set the Domain name suffix identically to your ISP's DHCP server specifies.

Allow bootp clients

Check this box to enable bootp Clients to obtain leases on this network interface. By default, IPCop's DHCP server ignores Bootstrap Protocol (BOOTP) request packets.

Primary DNS

Specifies what the DHCP server should tell its clients to use for their Primary DNS server. Because IPCop runs a DNS proxy, you will probably want to leave the default alone so the Primary DNS server is set to the IPCop box's IP address. If you have your own DNS server then specify it here.

Secondary DNS (optional)

You can also specify a second DNS server which will be used if the primary is unavailable. This could be another DNS server on your network or that of your ISP.

Primary NTP Server (optional)

If you are using IPCop as an NTP Server, or want to pass the address of another NTP Server to devices on your network, you can put its IP address in this box. The DHCP server will pass this address to all clients when they get their network parameters.

Secondary NTP Server (optional)

If you have a second NTP Server address, put it in this box. The DHCP server will pass this address to all clients when they get their network parameters.

Primary WINS server address (optional)

If you are running a Windows network and have a Windows Naming Service (WINS) server, you can put its IP address in this box. The DHCP server will pass this address to all hosts when they get their network parameters.

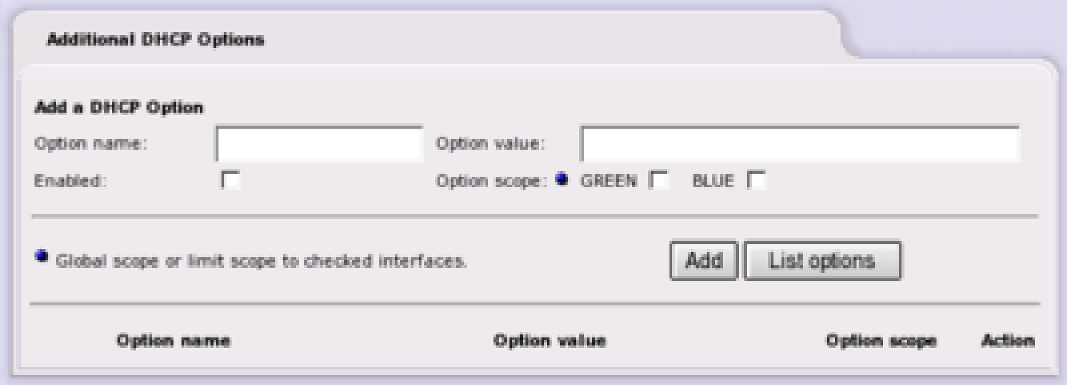
Secondary WINS server address (optional)

If you have a second WINS Server, you can put its IP address in this box. The DHCP server will pass this address to all hosts when they get their network parameters.

When you press **Save**, the change is acted upon.

Additional DHCP Options

If you have any special parameters you want to distribute to your network via the DHCP server, you add them here. (This functionality was added in v1.4.6).



● Global scope or limit scope to checked interfaces.

Figure 2-8. Additional DHCP Options

You can add additional DHCP Options here:

Option name

You specify the name of the DHCP option here, for example: `smtp-server` or `tcp-keepalive-interval`.

Option value

The value, appropriate to the option, goes here. It could be a string, an integer, an IP Address, or an on/off flag, depending on the option.

Option scope (optional)

The scope of the option will be Global, *unless* one of the interface checkboxes is checked, in which case it will only apply to that interface.

Enabled

Click on this check box to tell the DHCP server to hand out this option. If the entry is not enabled, it will be stored in IPCop's files, but the DHCP server will not issue the option.

Add

Click on this button to add the option.

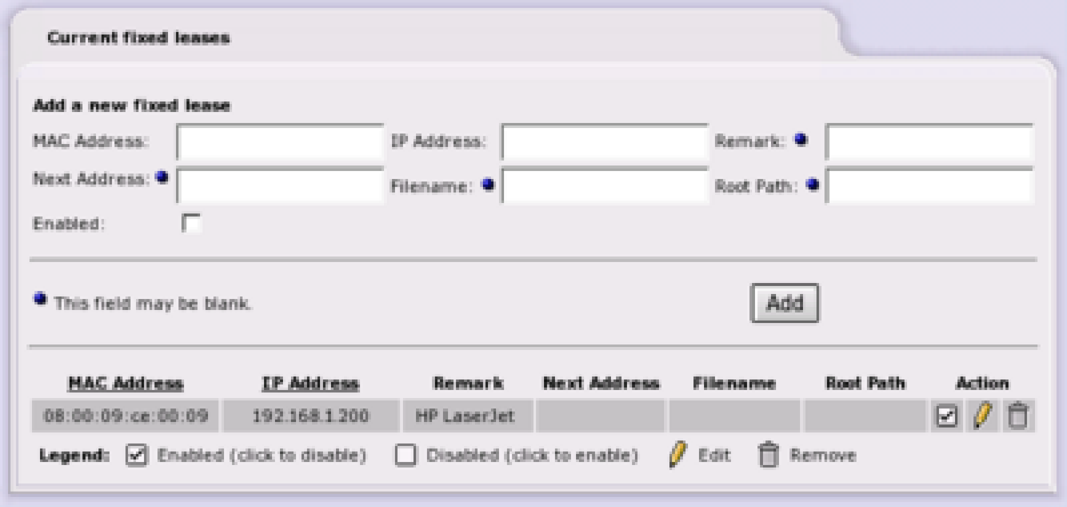
List options

Click on this button to display a list of options with possible values.

Fixed Leases

If you have machines whose IP addresses you would like to manage centrally but require that they always get the same fixed IP address you can tell the DHCP server to assign a fixed IP based on the MAC address of the network card in the machine.

This is different to using manual addresses as these machines will still contact the DHCP server to ask for their IP address and will take whatever we have configured for them.



Current fixed leases

Add a new fixed lease

MAC Address:		IP Address:		Remark: ●	
Next Address: ●		Filename: ●		Root Path: ●	
Enabled:	□				

● This field may be blank.

MAC Address	IP Address	Remark	Next Address	Filename	Root Path	Action
08:00:09:ce:00:09	192.168.1.200	HP LaserJet				☑ ✎ 🗑

Legend: ☑ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit 🗑 Remove

Figure 2-9. Add a new fixed lease

You can specify the following fixed lease parameters:

MAC Address

The six octet/byte colon separated MAC address of the machine that will be given the fixed lease.

> **Warning**
>
> The format of the MAC address is xx:xx:xx:xx:xx:xx, not xx-xx-xx-xx-xx-xx, as some machines show, i.e. 00:e5:b0:00:02:d2.

IP Address

The static lease IP address that the DHCP server will always hand out for the associated MAC address. Do not use an address in the server's dynamic address range.

Remark (optional)

If you want, you can include a string of text to identify the device using the fixed lease. (This field was added in v1.4.4).

Next Address (optional)

Some machines on your network may be thin clients that need to load a boot file from a network server. You can specify the server here if needed.

File Name (optional)

Specify the boot file for this machine.

Root Path (optional)

If the boot file is not in the default directory then specify the full path to it here.

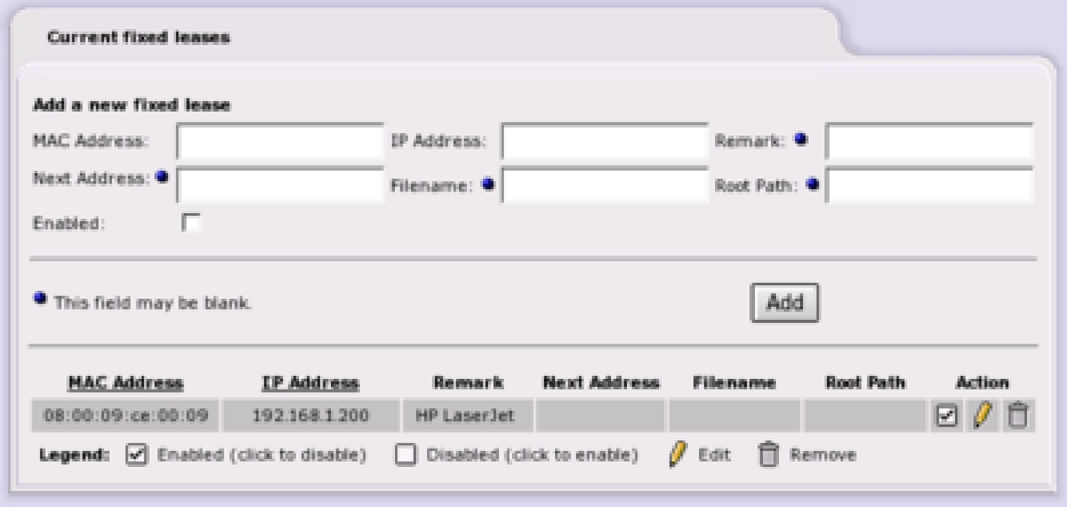
Enabled

Click on this check box to tell the DHCP server to hand out this static lease. If the entry is not enabled, it will be stored in IPCop's files, but the DHCP server will not issue this lease.

Current fixed leases

The current fixed leases are displayed at the foot of this section, and they can be enabled/disabled, edited or deleted.

You can sort the display of the fixed leases by clicking on the underlined headings *MAC Address* or *IP Address*. Another click on the heading will reverse the sort order.



Current fixed leases

Add a new fixed lease

MAC Address: IP Address: Remark: ●

Next Address: ● Filename: ● Root Path: ●

Enabled: □

● This field may be blank.

MAC Address	IP Address	Remark	Next Address	Filename	Root Path	Action
08:00:09:ce:00:09	192.168.1.200	HP LaserJet				☑ ✎ 🗑

Legend: ☑ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit 🗑 Remove

Figure 2-10. List of fixed leases

To edit an existing lease, click on its **pencil** icon. The fixed leases values will be displayed in the *Edit an existing lease* section of the page. The fixed lease being edited will be highlighted in yellow. Click the *Update* button to save any changes.

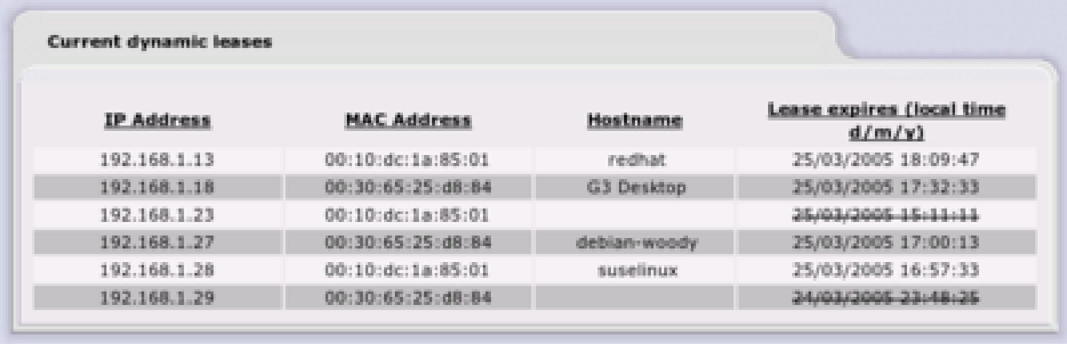
To remove an existing profile, click on its **trash can** icon. The lease will be removed.

Current dynamic leases

If DHCP is enabled, this section lists the dynamic leases contained in the `/var/state/dhcp/dhcpd.leases` file. The IP Address, MAC Address, hostname (if available) and lease expiry time of each record are shown, sorted by IP Address.

You can re-sort the display of dynamic leases by clicking on any of the four underlined column headings. A further click will reverse the sort order.

It is easy to cut and paste a MAC Address from here into the fixed lease section, if needed.



Current dynamic leases

IP Address	MAC Address	Hostname	Lease expires (local time d/m/y)
192.168.1.13	00:10:dc:1a:85:01	redhat	25/03/2005 18:09:47
192.168.1.18	00:30:65:25:d8:84	G3 Desktop	25/03/2005 17:32:33
192.168.1.23	00:10:dc:1a:85:01		~~25/03/2005 15:11:11~~
192.168.1.27	00:30:65:25:d8:84	debian-woody	25/03/2005 17:00:13
192.168.1.28	00:10:dc:1a:85:01	suselinux	25/03/2005 16:57:33
192.168.1.29	00:30:65:25:d8:84		~~24/03/2005 23:48:25~~

Figure 2-11. Current dynamic leases

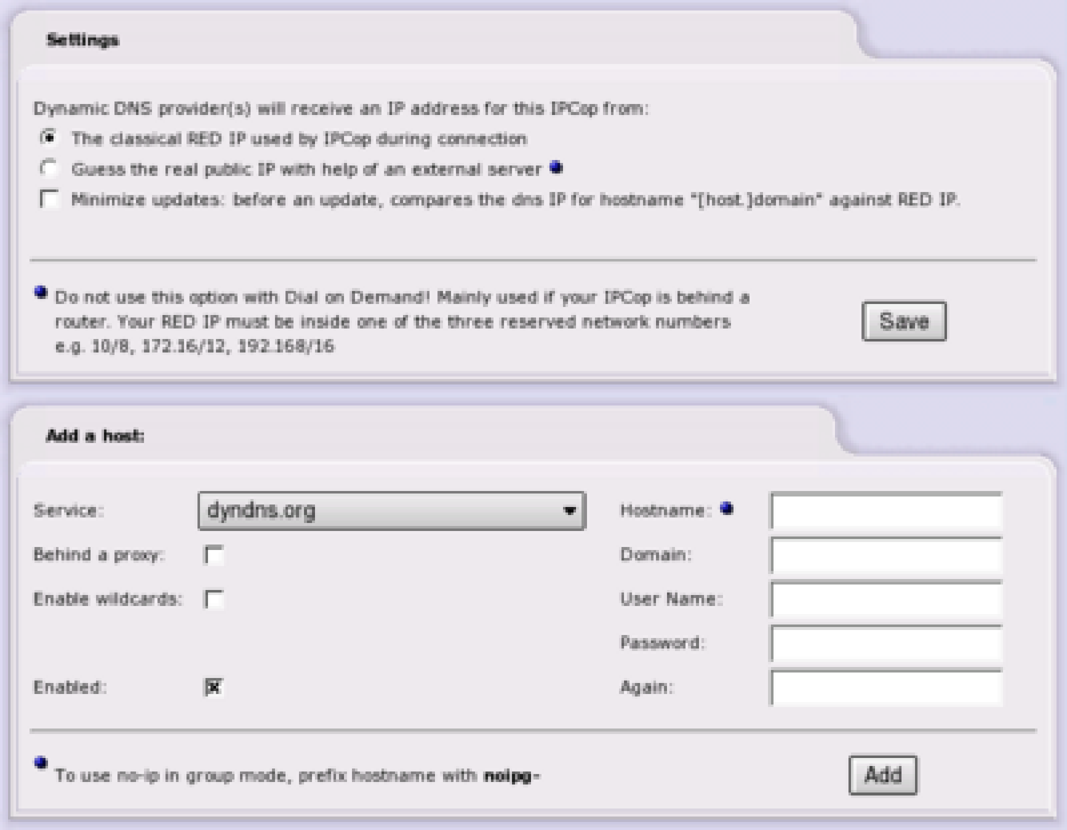
Lease times that have already expired are “struck through”.

Error messages

An error message will appear at the top of the page if a mistake is found in the input data, after you press the **Save** button.

Dynamic DNS Administrative Web Page

Dynamic DNS (DYNDNS) allows you to make your server available to the Internet even though it does not have a static IP address. To use DYNDNS you must first register a subdomain with a DYNDNS provider. Then whenever your server connects to the Internet and is given an IP address by your ISP it must inform the DYNDNS server of that IP address. When a client machine wishes to connect to your server it will resolve the address by going to the DYNDNS server, which will give it the latest value. If this is up to date then the client will be able to contact your server (assuming your firewall rules allow this). IPCop makes the process of keeping your DYNDNS address up to date easier by providing automatic updates for many of the DYNDNS providers.



Settings

Dynamic DNS provider(s) will receive an IP address for this IPCop from:

◉ The classical RED IP used by IPCop during connection

○ Guess the real public IP with help of an external server ●

□ Minimize updates: before an update, compares the dns IP for hostname "[host.]domain" against RED IP.

● Do not use this option with Dial on Demand! Mainly used if your IPCop is behind a router. Your RED IP must be inside one of the three reserved network numbers e.g. 10/8, 172.16/12, 192.168/16

Save

Add a host:

Service:	dyndns.org	Hostname: ●	
Behind a proxy:	□	Domain:	
Enable wildcards:	□	User Name:	
		Password:	
Enabled:	☒	Again:	

● To use no-ip in group mode, prefix hostname with **noipg-**

Add

Figure 2-12. Dynamic DNS Settings

Add a host

The following DYNDNS parameters can be set from the web interface:

Service

Choose a DYNDNS provider from the dropdown. You should have already registered with that provider.

Behind a proxy

This tick box should be ticked only if you are using the no-ip.com service and your IPCop is behind a proxy. This tick box is ignored by other services.

Enable wildcards

Enable Wildcards will allow you to have all the subdomains of your dynamic DNS hostname pointing to the same IP as your hostname (e.g. with this tick box enabled, www.ipcop.dyndns.org will point to the same IP as ipcop.dyndns.org). This tick box is useless with no-ip.com service, as they only allow this to be activated or deactivated directly on their website.

Hostname

Enter the hostname you registered with your DYNDNS provider.

Domain

Enter the domain name you registered with your DYNDNS provider.

Username

Enter the username you registered with your DYNDNS provider.

Password

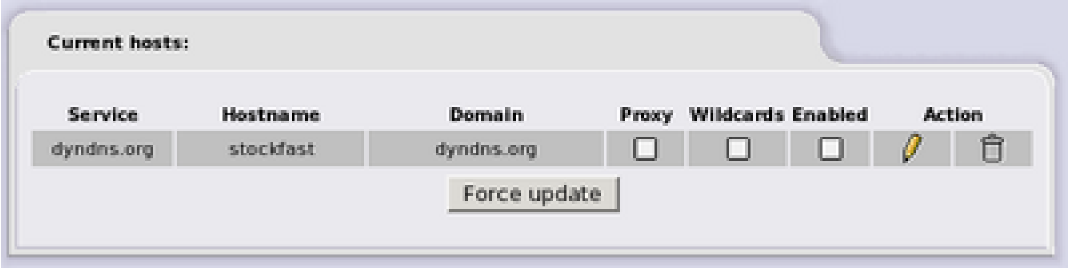
Enter the password for your username.

Enabled

If this is not ticked then IPCop will not update the information on the DYNDNS server. It will retain the information so you can re-enable DYNDNS updates without reentering the data.

Current hosts

This section shows the DYNDNS entries you have currently configured.



Current hosts:

Service	Hostname	Domain	Proxy	Wildcards	Enabled	Action	
dyndns.org	stockfast	dyndns.org	□	□	□	✎	🗑

To edit an entry click on its **pencil** icon. The entry's data will be displayed in the form above. Make your changes and click the **Save** button on the form.

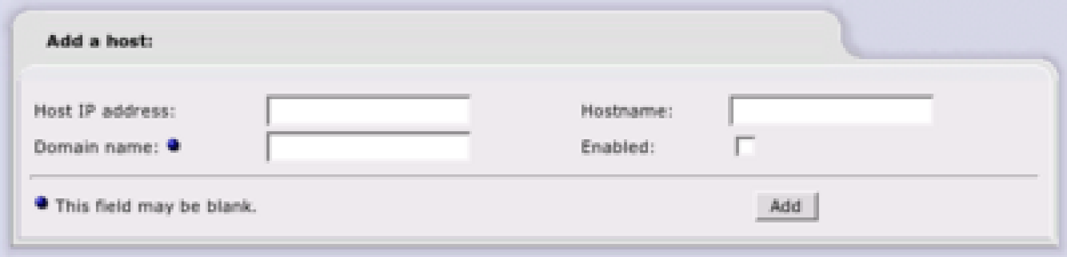
You can also update the *Behind a proxy*, *Use wildcards* and *Enabled* tick boxes directly from the current hosts list entry.

Forcing a Manual Update

You can force IPCop to refresh the information manually by pressing **Force Update**, however, it is best to only update when the IP address has actually changed, as dynamic DNS service providers don't like to handle updates that make no changes. Once the host entries have been enabled your IP will automatically be updated each time your IP changes.

Edit Hosts Administrative Web Page

As well as caching DNS information from the Internet, the DNS proxy on IPCop allows you to manually enter hosts whose address you want to maintain locally. These could be addresses of local machines or machines on the Internet whose address you might want to override.



Add a host:

Host IP address:		Hostname:	
Domain name: ●		Enabled:	□

● This field may be blank.

Figure 2-13. Add a Host Input Screen

Add a host

The following parameters can be set from the web interface:

Host IP Address

Enter the IP address here.

Hostname

Enter the host name here.

Domain name (optional)

If the host is in another domain then enter it here.

Hostname

Enter the host name here.

Enabled

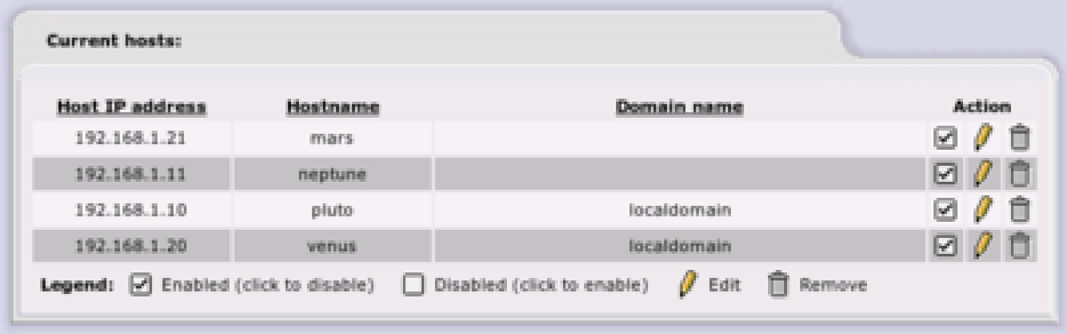
Check this box to enable the entry.

When you press **Add**, the details will be saved.

Current hosts

This section shows the local DNS entries you have currently configured.

You can re-sort the display by clicking on any of the three underlined column headings. A further click will reverse the sort order.



Current hosts:

Host IP address	Hostname	Domain name	Action
192.168.1.21	mars		☑ ✏ 🗑
192.168.1.11	neptune		☑ ✏ 🗑
192.168.1.10	pluto	localdomain	☑ ✏ 🗑
192.168.1.20	venus	localdomain	☑ ✏ 🗑

Legend: ☑ Enabled (click to disable) □ Disabled (click to enable) ✏ Edit 🗑 Remove

Figure 2-14. List of current hosts

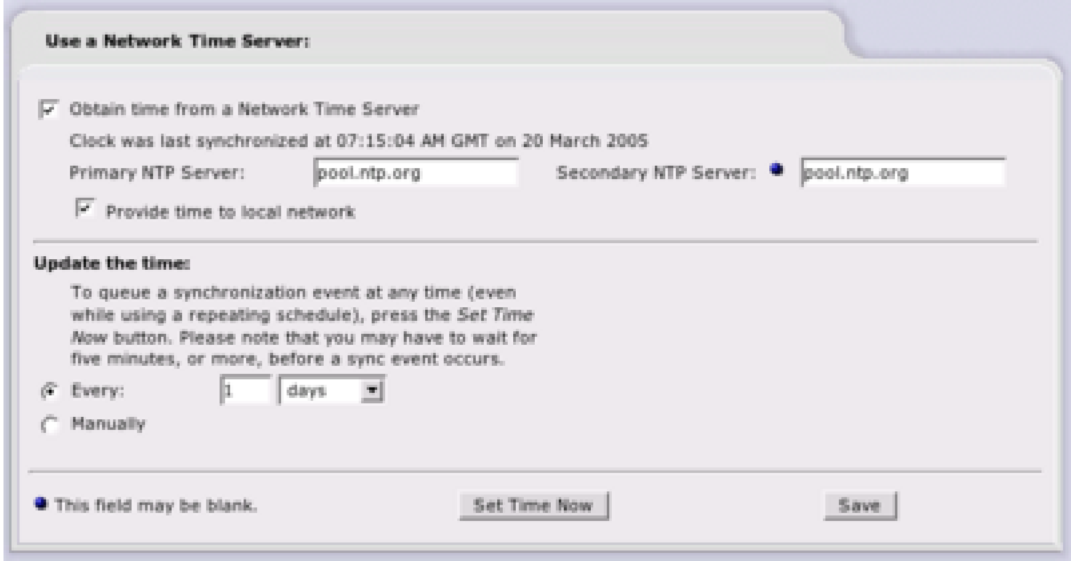
To enable or disable an entry - click on the “Enabled” icon (the checkbox in the Action column) for the particular item you want to enable or disable. The icon changes to an empty box when a rule is disabled. Click on the checkbox to enable it again.

To edit an entry click on its **Pencil** icon. The entry’s data will be displayed in the form above. Make your changes and click the **Update** button on the form.

To delete an entry click on its **Trash Can** icon.

Time Server Administrative Web Page

IPCop can be configured to obtain the time from a known accurate timeserver on the Internet. In addition to this it can also provide this time to other machines on your network.



Use a Network Time Server:

☑ Obtain time from a Network Time Server

Clock was last synchronized at 07:15:04 AM GMT on 20 March 2005

Primary NTP Server: pool.ntp.org   Secondary NTP Server: ● pool.ntp.org

☑ Provide time to local network

Update the time:

To queue a synchronization event at any time (even while using a repeating schedule), press the *Set Time Now* button. Please note that you may have to wait for five minutes, or more, before a sync event occurs.

◉ Every: 1 days

○ Manually

● This field may be blank.

Figure 2-15. Network Time Server Settings

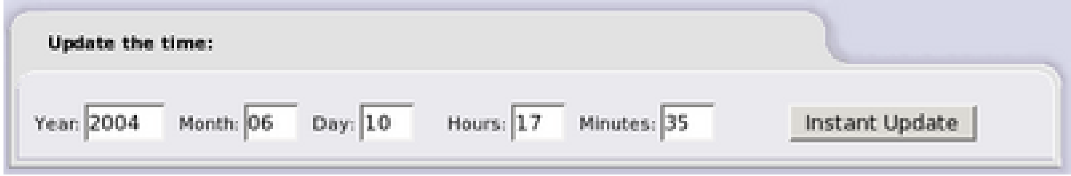
To configure the time system, make sure that the *Enabled* box is ticked and enter the full name of the timeserver you want to use in the *Primary NTP Server* box. You can also enter an optional *Secondary NTP Server* if you want.

If you want to provide a time service to the rest of your network then tick the *Provide time to local network* checkbox.

You can choose to update the time on IPCop on a periodic basis, for instance every hour, or to update it when you wish from this web page (just click *Set Time Now*).

To save your configuration click the *Save* button.

> **Note:** Although IPCop can act as a timeserver for your network, it uses the ntpdate program to update its time on a periodic basis instead of allowing the more accurate ntpd server to maintain the time continuously. This means that the IPCop clock is more likely to drift out of synchronisation with the real time but does not require that IPCop is permanently connected to the Internet.



Update the time:

Year: 2004 Month: 06 Day: 10 Hours: 17 Minutes: 35

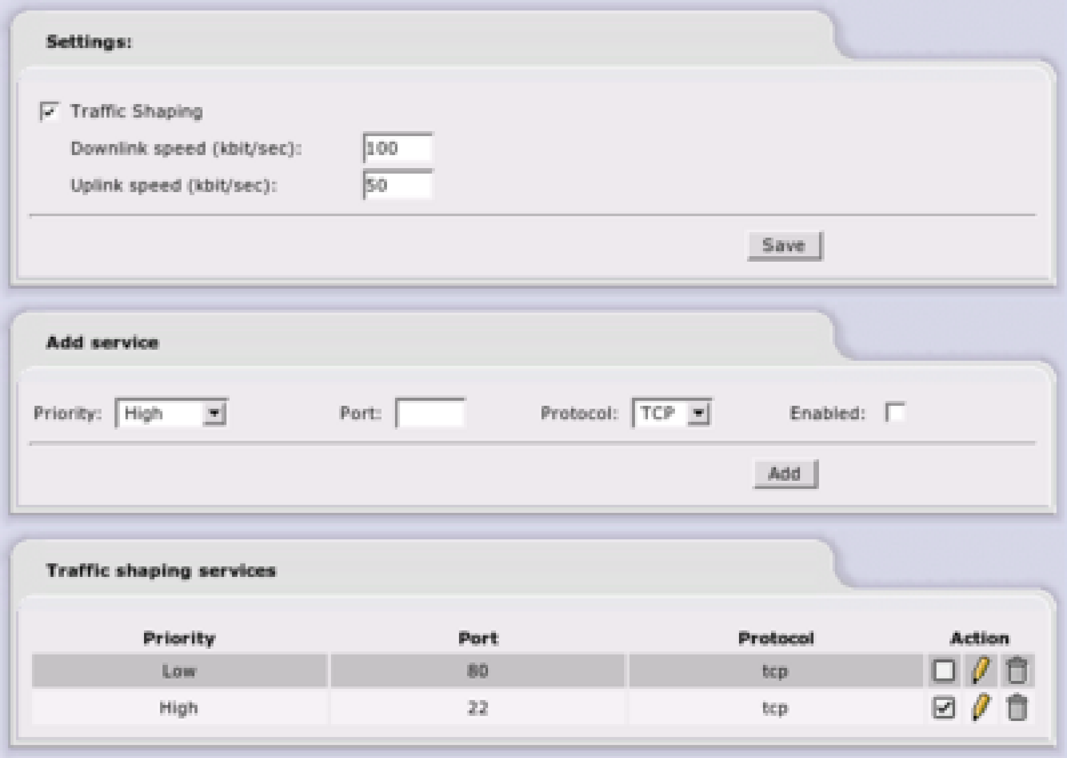
Figure 2-16. Update the time manually

If you do not want to use an Internet timeserver you can enter the time manually and click the **Instant Update** button.

> **Warning**
>
> If you correct the time by a large amount, and offset the clock ahead of itself, the fcron server that runs regular cron jobs can appear to stop while it waits for the time to catch up. This can affect graph generation and other regular tasks that run in the background.
>
> If this happens, try running the command **fcrontab -z** in a terminal to reset the fcron server.

Traffic Shaping Administrative Web Page

Traffic Shaping allows you to prioritize IP traffic moving through your firewall. IPCop uses WonderShaper to accomplish this. WonderShaper was designed to minimize ping latency, ensure that interactive traffic like SSH is responsive all while downloading or uploading bulk traffic.



Settings:

☑ Traffic Shaping

Downlink speed (kbit/sec): 100

Uplink speed (kbit/sec): 50

Add service

Priority: High Port: Protocol: TCP Enabled: □

Traffic shaping services

Priority	Port	Protocol	Action
Low	80	tcp	□ ✎ 🗑
High	22	tcp	☑ ✎ 🗑

Figure 2-17. Traffic Shaping Settings

Many ISPs sell speed as download rates, not as latency. To maximize download speeds, they configure their equipment to hold large queues of your traffic. When interactive traffic is mixed into these large queues, their latency shoots way up, as ACK packets must wait in line before they reach you. IPCop takes matters into its own hands and prioritizes your traffic the way you want it. This is done by setting traffic into High, Medium and Low priority categories. Ping traffic always has the highest priority — to let you show off how fast your connection is while doing massive downloads.

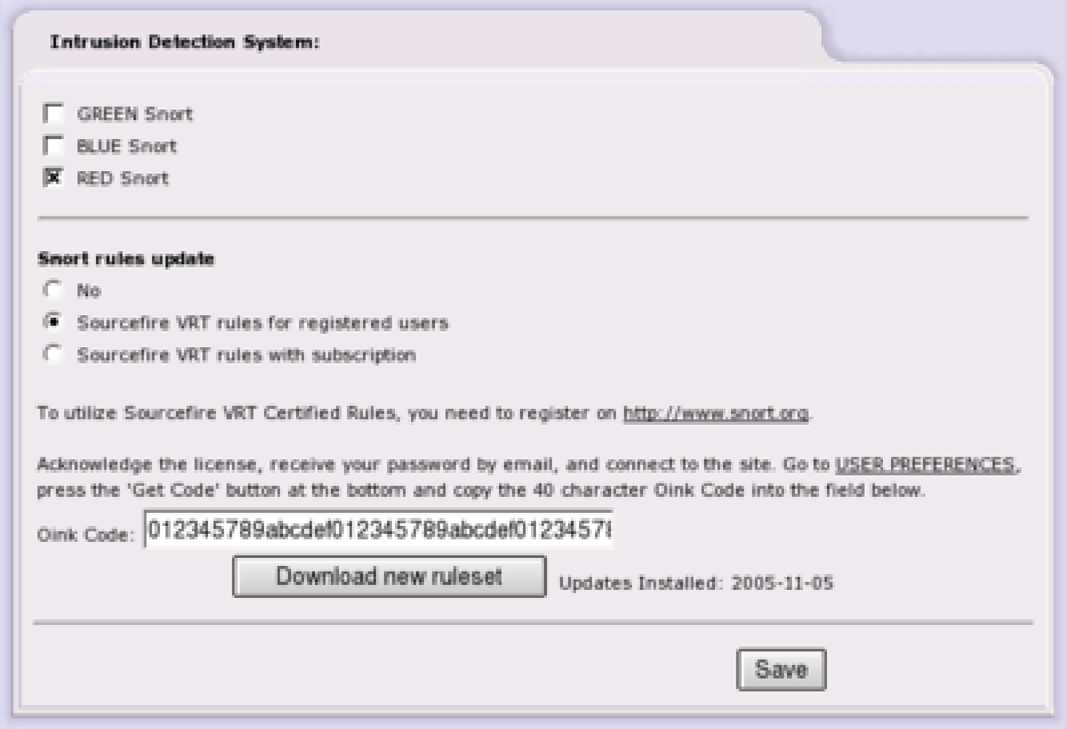
To use Traffic Shaping in IPCop:

1. Use well known fast sites to estimate your maximum upload and download speeds. Fill in the speeds in the corresponding boxes of the *Settings* portion of the web page.
2. Enable traffic shaping by checking the *Enable* box.
3. Identify what services are used behind your firewall.
4. Then sort these into your 3 priority levels. For example:
    a. Interactive traffic such as SSH (port 22) and VOIP (voice over IP) go into the high priority group.
    b. Your normal surfing and communicating traffic like the web (port 80) and streaming video/audio to into the medium priority group.
    c. Put your bulk traffic such as P2P file sharing into the low traffic group.
5. Create a list of services and priorities using the *Add service* portion of the web page.

The services, above, are only examples of the potential Traffic Shaping configuration. Depending on your usage, you will undoubtedly want to rearrange your choices of high, medium and low priority traffic.

Intrusion Detection System Administrative Web Page

IPCop contains a powerful intrusion detection system, Snort, which analyses the contents of packets received by the firewall and searches for known signatures of malicious activity.



Intrusion Detection System:

□ GREEN Snort
□ BLUE Snort
☒ RED Snort

Snort rules update

○ No
● Sourcefire VRT rules for registered users
○ Sourcefire VRT rules with subscription

To utilize Sourcefire VRT Certified Rules, you need to register on http://www.snort.org.

Acknowledge the license, receive your password by email, and connect to the site. Go to USER PREFERENCES, press the 'Get Code' button at the bottom and copy the 40 character Oink Code into the field below.

Oink Code: 012345789abcdef012345789abcdef01234578

Updates Installed: 2005-11-05

Figure 2-18. Intrusion Detection Settings

IPCop can monitor packets on the Green, Blue, Orange and Red interfaces. Just tick the relevant boxes and click the *Save* button.

Snort rules update

Follow the instructions to obtain an Oink Code from www.snort.org[9] if you intend to use Sourcefire VRT Certified rules.

Select the correct radio button, add your Oink Code (if appropriate), and click the *Save* button *before* your first attempt to download a ruleset.

As more attacks are discovered the rules Snort uses to recognize them will be updated. To download the latest version, click the *Download new ruleset* button.

Firewall Menu

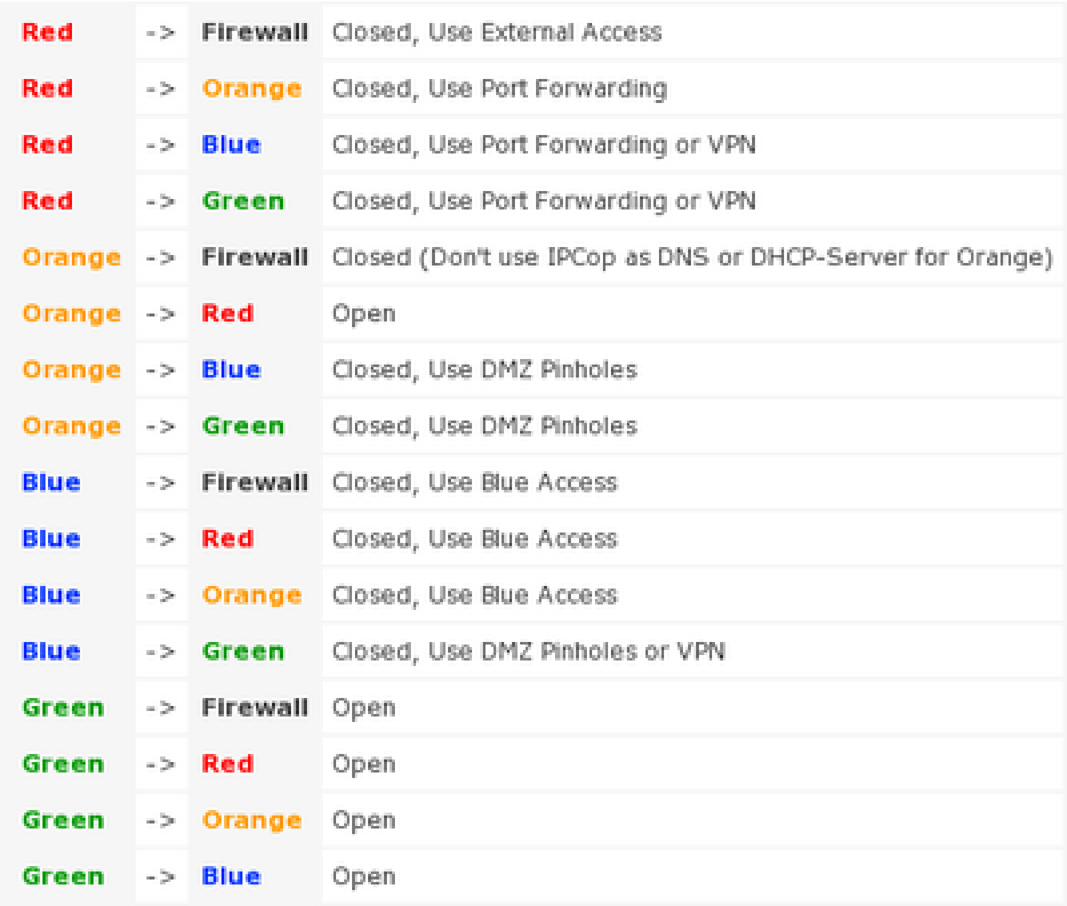
Grouped together in the Firewall Menu are some of the core functions of IPCop which controls how traffic flows through the firewall.

These are:

- Port Forwarding
- External Access (Controls remote administration of IPCop from the Internet)
- DMZ Pinholes
- Blue Access (Connecting a Wireless Access Point to IPCop)
- Firewall Options

What traffic is allowed between Interfaces?

The table below summarizes the default firewall settings and the steps required to open or control access between them.



Red	->	Firewall	Closed, Use External Access
Red	->	Orange	Closed, Use Port Forwarding
Red	->	Blue	Closed, Use Port Forwarding or VPN
Red	->	Green	Closed, Use Port Forwarding or VPN
Orange	->	Firewall	Closed (Don't use IPCop as DNS or DHCP-Server for Orange)
Orange	->	Red	Open
Orange	->	Blue	Closed, Use DMZ Pinholes
Orange	->	Green	Closed, Use DMZ Pinholes
Blue	->	Firewall	Closed, Use Blue Access
Blue	->	Red	Closed, Use Blue Access
Blue	->	Orange	Closed, Use Blue Access
Blue	->	Green	Closed, Use DMZ Pinholes or VPN
Green	->	Firewall	Open
Green	->	Red	Open
Green	->	Orange	Open
Green	->	Blue	Open

Figure 2-19. IP Traffic Flow

User Customization

In v1.4 there is a new file for users to make their own changes to firewall rules. Have a look inside the file `/etc/rc.d/rc.firewall.local`

It is called by `/etc/rc.d/rc.firewall`, and for manual use, the usage is:

```
$ /etc/rc.d/rc.firewall.local {start|stop|reload}
```

> **Note:** The **reload** option was added in v1.4.2, and further modified in v1.4.6, but changes were not included in Official Updates, to avoid overwriting Users' existing modifications.

There are also specific chains for Users' use, called `CUSTOMINPUT`, `CUSTOMFORWARD` etc. as per version 1.3.

Introduced in version 1.3, there is also the file `/etc/rc.d/rc.local` which is run when IPCop boots, and can contain your own specific commands to run at boot time, for instance to setup an internal modem.

Neither of these files will be affected by Official Updates, and are included in the set of files saved when you backup the system files.

Port Forwarding Administrative Web Page

This subsection allows you to configure the Port Forwarding settings for IPCop. This is 100% optional, so you may safely ignore this section if you do not wish to make use of this feature.

Port Forwarding Overview

Firewalls prevent externally initiated requests from accessing the protected system. However, sometimes, this is too strict a situation. For example, if one is running a web server, then any requests to that web server by users outside the protected network will be blocked by default. This means that only other users on the same internal network can use the web server. This is not the normal situation for web servers. Most people *want* outsiders to be able to access the server. This is where Port Forwarding comes in.

Port Forwarding is a service that allows limited access to the internal LANs from outside. When you set up your server, you can choose the receiving or "listening" ports on the internal network machines. This is done differently depending on which software is being used. Please refer to the documentation that came with your servers to set up the ports on those servers.

Once those receiving ports are ready, you are ready to enter information into the AW on IPCop. The *TCP/UDP* drop down list allows you to choose which protocol this rule will follow. Most regular servers use TCP. Some game servers and chat servers use UDP. If the protocol is not specified in the server documentation, then it is usually TCP. *Source port* is the port to which the outsiders will connect. In most cases, this will be the standard port for the service being offered (80 for web servers, 20 for FTP servers, 25 for mail servers, etc.) If you wish, you may specify a range of ports to forward. To specify a range use the ":" character between two port numbers, lowest number first. *Destination IP* is the internal IP address of the server (for example, you may have your web server on 192.168.0.3). *Destination Port* is the port that you chose when you set up your server in the first paragraph. The *SourceIP* dropdown menu allows you to choose which Red IP this rule will affect. IPCop has the capability of handling more than one Red IP. If you only have one Red IP set up, then choose *Default IP*.

Port Forwarding and External Access

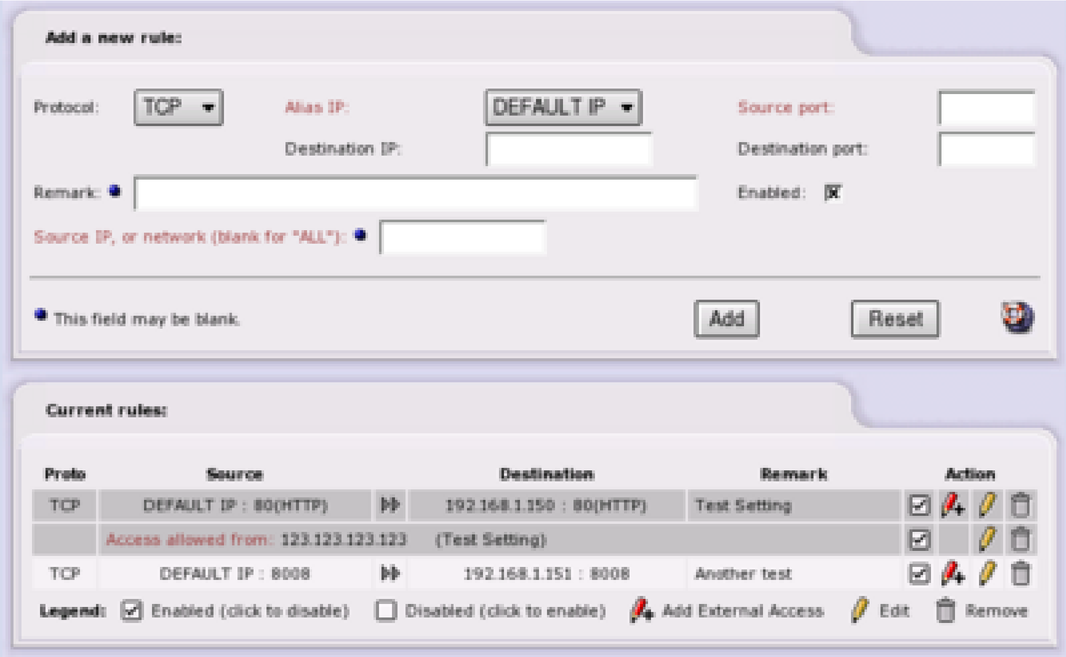
The Port Forwarding interface was re-written for version 1.3.0. It is quite different from earlier versions. However, please note that the port numbers used for a particular service have not changed, and you should still refer to these above.

The External Access page has *NO* affect on the GREEN or ORANGE networks. It is there to allow you to open ports to the IPCop box itself and not the GREEN or ORANGE networks.

How do you open up external access then? It is combined into the Port Forward page - there is a field on the page labeled:

’Source IP, or network (blank for "ALL"):’

This is the field that controls external access - if you leave it BLANK, your port forward will be open to *ALL INTERNET ADDRESSES*. Alternatively if you put an address or network in there, it will be restricted to that network or Internet address.



Add a new rule:

Protocol:	TCP	Alias IP:	DEFAULT IP	Source port:	
		Destination IP:		Destination port:	
Remark: ●				Enabled:	☒
Source IP, or network (blank for "ALL"): ●					

● This field may be blank.

Current rules:

Proto	Source		Destination	Remark	Action
TCP	DEFAULT IP : 80(HTTP)	⏩	192.168.1.150 : 80(HTTP)	Test Setting	☑ ✚ ✎ 🗑
	Access allowed from: 123.123.123.123		(Test Setting)		☑ ✎ 🗑
TCP	DEFAULT IP : 8008	⏩	192.168.1.151 : 8008	Another test	☑ ✚ ✎ 🗑

Legend: ☑ Enabled (click to disable) □ Disabled (click to enable) ✚ Add External Access ✎ Edit 🗑 Remove

Figure 2-20. Port Forwarding Settings

You can have more than one external address - after you have created the port forward entry, it will appear in the table. If you wish to add another external address, click the Red Pencil with the Plus sign next to the entry, the entry screen at the top of the page will change (it will load values from the port forward) and allow you to enter an external IP address or network.

When added you will now notice that there is a new entry under the port forward in the table.

Other things to note:

- We support the GRE protocol.
- You can have port ranges and wildcards. Valid wildcards are:
- * which translates to 1-65535

- 85-* which translates into 85-65535
- *-500 which translates into 1-500

Valid characters to separate a port range are “:” or “-”. Note that - will be modified to a “:” even though it will be displayed as a “-” on the screen.

You only need to enter the first source port, the destination will be filled in for you.

You can edit a record by clicking on the Yellow Pencil icon in the Action column, and until you hit the update button, nothing changes and nothing is lost.

When you are editing a record, you will see the record highlighted in yellow.

To delete a record, click on the Trash Can icon on the right hand side of the Action column.

Ports ranges cannot overlap each other.

Individual ports cannot be placed in the middle of a range i.e. if you have 2000-3000 already set up and then try to forward port 2500, it will give you an error. You cannot forward the same port to several machines.

Reserved ports - on the main Red Address (DEFAULT IP) some ports are reserved for IPCop to do its business, they are 67, 68, 81, 222, and 445.

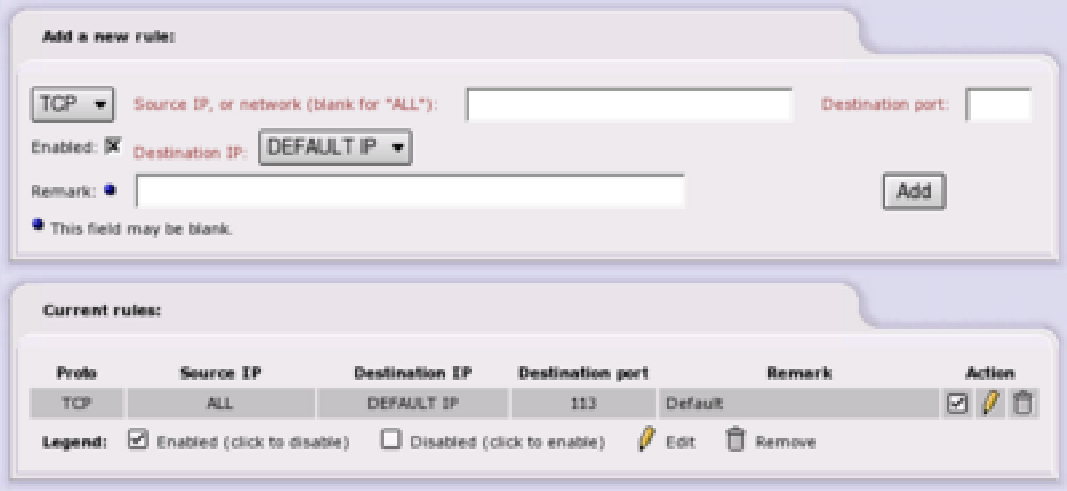
When you edit a port forward, there will be an extra check box labeled ’Override external access to ALL’. This is used as a quick and dirty way to open a port to ALL Internet addresses for testing or whatever your reasons. This was a user request.

If you have a port forward with multiple external accesses, when you delete all of the external accesses, the port becomes open to ALL addresses, be careful of this one.

There is a Shortcut to enable or disable a port forward or external access - click on the “Enabled” icon (the checkbox in the Action column) for the particular entry you want to enable or disable. The icon changes to an empty box when a rule is disabled. Click on the checkbox to enable it again. *Note:* when you disable the port forward, all associated external accesses are disabled, and when you enable the port forward, all associated external accesses are enabled.

External Access Administrative Web Page

This subsection allows you to configure the External Access settings for IPCop machine itself. This is 100% optional, so you may safely ignore this section if you do not wish to make use of this feature.



Add a new rule:

TCP ▾ Source IP, or network (blank for "ALL"): Destination port:

Enabled: ☒ Destination IP: DEFAULT IP ▾

Remark: ●

● This field may be blank.

Current rules:

Proto	Source IP	Destination IP	Destination port	Remark	Action
TCP	ALL	DEFAULT IP	113	Default	☑ ✎ 🗑

Legend: ☑ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit 🗑 Remove

Figure 2-21. External Access Settings

From v1.3.0 onwards, External Access only controls access to the IPCop box. It has no affect on the Green, Blue or Orange network access. That is now controlled in the Port Forwarding section, see above.

If you wish to maintain your IPCop machine remotely, you should specify TCP port 445, https. If you have enabled ssh access, you can also enable TCP port 222, ssh.

The *TCP/UDP* drop down list allows you to choose which protocol this rule will follow. Most regular servers use TCP. If the protocol is not specified in the server documentation, then it is usually TCP. *Source IP* is the IP address of an external machine you give permission to access your firewall. You may leave this blank, which allows any IP address to connect. Although dangerous, this is useful if you want to maintain your machine from anywhere in the world. However, if you can limit the IP addresses for remote maintenance, the IP addresses of those machines or networks that are allowed access, should be listed in this box. *Destination Port* is the external port that they are allowed to access, i.e. 445. The *Destination IP* dropdown menu allows you to choose which Red IP this rule will affect. IPCop has the capability of handling more than one Red IP. If you only have one Red IP set up, then choose *Default IP*.

Once you have entered all the information, click the *Enabled* box and press **Add**. This will move the rule to the next section, and list it as an active rule.

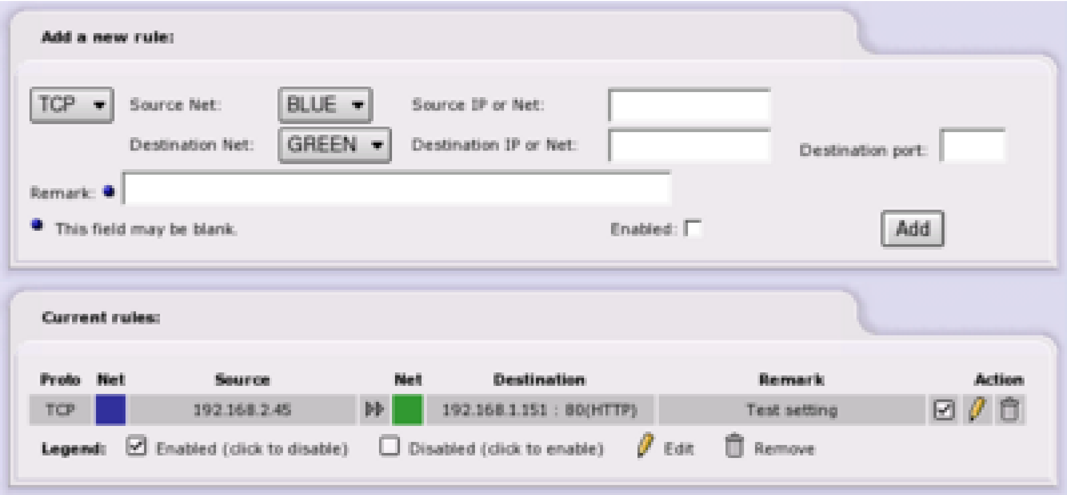
Current rules lists the rules that are in effect. To remove one, click the "Trash Can" icon. To edit one, click the "Yellow Pencil" icon.

To enable or disable a rule - click on the "Enabled" icon (the checkbox in the Action column) for the particular entry you want to enable or disable. The icon changes to an empty box when a rule is disabled. Click on the checkbox to enable it again.

DMZ Pinholes Administrative Web Page

This subsection allows you to configure the DMZ Pinholes settings for IPCop. This is 100% optional, so you may safely ignore this section if you do not wish to make use of this feature.

This page will *only* be visible if you have installed and configured an Orange or a Blue network interface card.



Add a new rule:

TCP ▾ Source Net: BLUE ▾ Source IP or Net:

Destination Net: GREEN ▾ Destination IP or Net: Destination port:

Remark: ●

● This field may be blank. Enabled: □

Current rules:

Proto	Net	Source		Net	Destination	Remark	Action
TCP	🟦	192.168.2.45	▶▶	🟩	192.168.1.151 : 80(HTTP)	Test setting	☑ ✎ 🗑

Legend: ☑ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit 🗑 Remove

Figure 2-22. Pinhole Settings

A DMZ or Demilitarized Zone (Orange zone) is used as a semi-safe interchange point between the external Red Zone and the internal Green zone. The Green zone has all your internal machines. The Red zone is the Internet at large. The DMZ allows them to share servers without allowing undue access to the internal LAN by those in the Red Zone.

For example, suppose that your business has a web server. Certainly, you want your customers (those in the Red zone) to be able to access it. But suppose you also want your web server to be able to send customer orders to employees in the Green Zone? In a traditional firewall setup, this wouldn't work, because the request for access to the Green zone would be initiating from outside the Green zone. You certainly do not want to give all your customers direct access to the machines on the Green side, so how can this work? By using the DMZ and DMZ pinholes.

DMZ pinholes give machines in the Orange (DMZ) zone limited access to certain ports on Green machines. Because servers (the machines in the Orange zone) have to have relaxed rules with respect to the Red zone, they are more susceptible to hacking attacks. By only allowing limited access from Orange to Green, this will help to prevent unauthorized access to restricted areas should your server be compromised.

The *TCP/UDP* drop down list allows you to choose which protocol this rule will follow. Most regular servers use TCP. Some game servers and chat servers use UDP. If the protocol is not specified in the server documentation, then it is usually TCP. Use the protocol specified on the Port Forwarding page.

Source Net is a drop down menu that shows the available source networks on the machine.

Source IP is the IP address of the machine that you wish to give permission to access your internal servers.

Destination Net is a drop down menu that shows the available networks on the machine.

The *Destination IP* is the machine in the Green or Blue zone that will receive the request.

Destination Port is the port on the machine that will be listening for the request.

Once you have entered all the information, click the *Enabled* box and press **Add**. This will move the rule to the next section, and list it as an active rule.

Current rules lists the rules that are in effect. To remove one, click the "Trash Can" icon. To edit one, click the "Yellow Pencil" icon.

To enable or disable a rule - click on the “Enabled” icon (the checkbox in the Action column) for the particular entry you want to enable or disable. The icon changes to an empty box when a rule is disabled. Click on the checkbox to enable it again.

Blue Access Administrative Web Page

This subsection allows you to configure which Wireless Access Points on the Blue network can connect to IPCop. This is 100% optional, so you may safely ignore this section if you do not wish to make use of this feature.

> **Note:** This page will *only* be visible if you have installed and configured a Blue network interface card.

To setup Blue Access do the following:

1. Use a supported Ethernet card to setup the Blue interface.
2. Connect an Access Point to that Ethernet card. (Use the LAN Ethernet port on the AP, if you have a choice of ports).
3. You can use DHCP to serve dynamic or static addresses on Blue, although static is preferred for security of MAC addresses. Refer to the DHCP Server section for more information on configuring static leases.

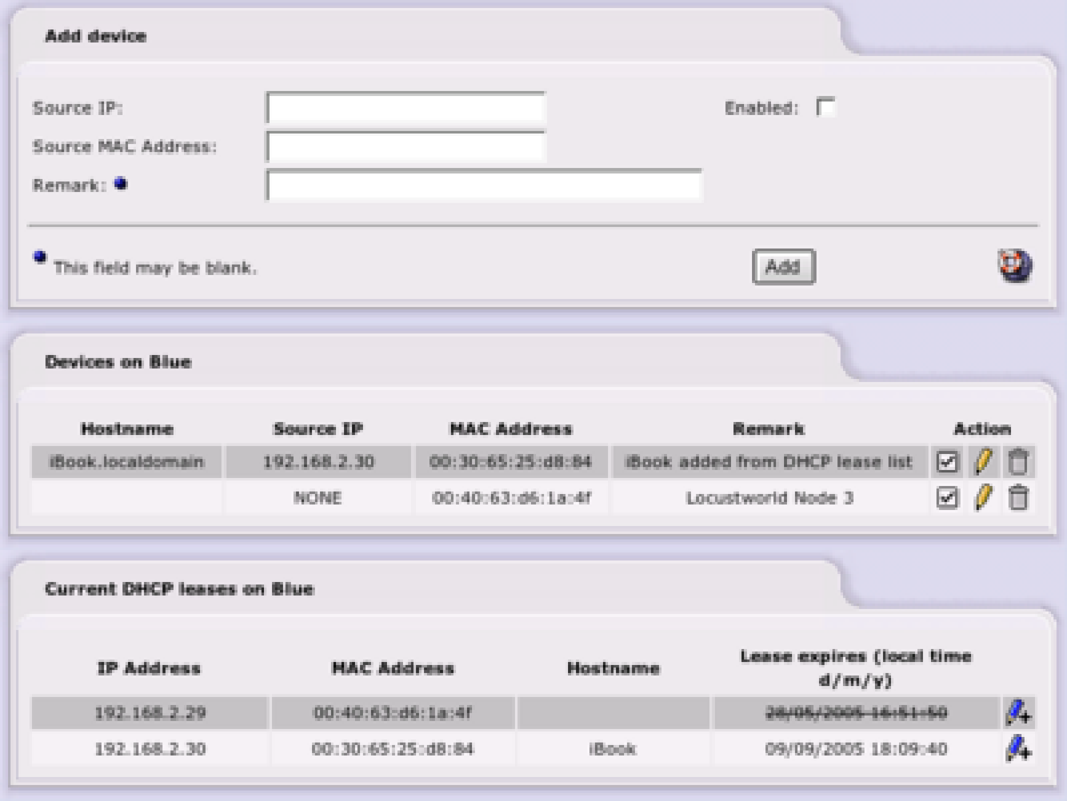
If you only need to provide access for http traffic on the Blue network to the Internet (Red network), just add the IP Address or the MAC Address of the Wireless Router, or the individual wireless connected devices if you are using an Access Point, via the web page shown below.

An Access Point behaves like an Ethernet hub, and IPCop serves out DHCP leases through it to wireless devices. A Wireless Router does NAT, serves out DHCP on it’s own subnet, and has it’s own access controls.

You will be able to view IPCop’s web interface from a computer on the Blue network, but you will not be able to connect to the Green network without some additional work.

To connect to the Green network from the Blue network, you have to either:

1. Use the DMZ Pinholes page and shoot bullet holes through the Blue interface for your services, or:
2. Setup a VPN for your road-warriors on Blue to provide access.



Add device

Source IP:		Enabled:	□
Source MAC Address:			
Remark: ●			

● This field may be blank.

Devices on Blue

Hostname	Source IP	MAC Address	Remark	Action
iBook.localdomain	192.168.2.30	00:30:65:25:d8:84	iBook added from DHCP lease list	☑ ✎ 🗑
	NONE	00:40:63:d6:1a:4f	Locustworld Node 3	☑ ✎ 🗑

Current DHCP leases on Blue

IP Address	MAC Address	Hostname	Lease expires (local time d/m/y)	
192.168.2.29	00:40:63:d6:1a:4f		~~28/05/2005 16:51:50~~	✎
192.168.2.30	00:30:65:25:d8:84	iBook	09/09/2005 18:09:40	✎

Figure 2-23. Blue Access Settings

In the *Add Device* section you input the IP Address or the MAC Address of a wireless Access Point, or any device on the Blue network that you want to connect to the Internet through IPCop.

Once you have entered all the information, click the *Enabled* box and press **Add**. This will move the entry to the next section, and list it as enabled.

The *Devices on Blue* section lists the current entries. To remove one, click the “Trash Can” icon. To edit one, click the “Yellow Pencil” icon.

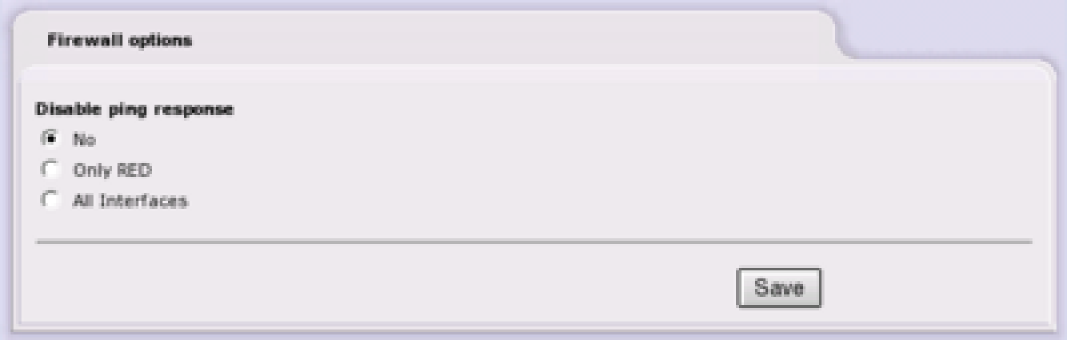
To enable or disable an entry, click on the “Enabled” icon (to the left of the Yellow Pencil) for the particular entry you want to enable or disable. The icon changes to an empty box when a device is disabled. Click the checkbox to enable it again.

If DHCP is enabled for the Blue network, the *Current DHCP leases on Blue* section will be displayed.

This provides a quick way of adding wireless devices to the list. You just have to click on the “Blue Pencil” icon for a device to be added to the list of enabled devices. You can then edit the entry, if necessary, by clicking on the “Yellow Pencil” icon, as before.

Firewall Options Administrative Web Page

This subsection allows you to configure some firewall behaviour. This is 100% optional, so you may safely ignore this section if you do not wish to make use of this feature.



Disable ping response

● No
○ Only RED
○ All Interfaces

Figure 2-24. Firewall Options

Disable ping response

- **No** - IPCop responds to **ping** requests on any interface. This is the default behaviour.
- **Only RED** - IPCop does not respond to **ping** requests on the Red Interface.
- **All Interfaces** - IPCop does not respond to any **ping** requests on any interface.

To save changes, press the **Save** button.

VPNs Menu

Virtual Private Networks (VPNs)

Virtual Private Networks or VPNs allow two networks to connect directly to each other over another network such as the Internet. All data is transmitted securely over an encrypted tunnel, hidden from prying eyes. Similarly, a single computer can also connect to another network using the same facilities. One of the protocols used to create VPNs is known as IPSec.

IPCop can easily establish VPNs between other IPCop servers. IPCop can also interoperate with just about any VPN product that supports IPSec and standard encryption technologies such as 3DES. VPN connections in IPCop are defined as Net-to-Net or Host-to-Net. This is 100% optional, so you may safely ignore this section if you do not wish to make use of this feature.

Most modern operating systems have support for IPSec. This includes Windows, Macintosh OSX, Linux and most Unix variants. Unfortunately, the tools needed to provide this support vary greatly and may be difficult to set up.

Net-to-Net

Net-to-net VPNs link two or more private networks across the Internet, by creating an IPSec “tunnel”. In a net-to-net VPN, at least one of the networks involved must be connected to the Internet with an IPCop firewall. The other network can be connected to an IPCop firewall, or another IPSec enabled router or firewall. These router/firewalls have public IP addresses assigned by an ISP and are most likely to be using Network Address Translation, hence the term Net-to-Net.

If desired, a VPN can be created between wireless machines on your BLUE network and an IPCop firewall. This ensures that traffic on your BLUE network cannot be intercepted with wireless sniffers.

Host-to-Net

A Host-to-Net connection is where IPCop is at one end of the VPN tunnel and a remote or mobile user is on the other end. The mobile user is most likely to be a laptop user with a dynamic public IP address assigned by an ISP, hence the terms Host-to-Net or Roadwarrior.

Methods of Authentication

It is necessary to have a pre-shared key/password/pass phrase or an X.509 certificate before trying to configure a Roadwarrior or Net-to-Net VPN connection. These are methods of authentication, which identify the user trying to access the VPN. They will be required in the VPN configuration stage.

Pre-shared Key

The pre-shared key authentication method or PSK is a very simple method that allows VPN connections to be set up quickly. For this method, you enter an authentication phrase. This can be any character string — similar to a password. This phrase must be available for authentication on IPCop and to the VPN client.

The PSK method involves fewer steps than certificate authentication. It can be used to test connectivity of a VPN and to become familiar with the procedure of establishing a VPN connection. Experienced users may wish to progress straight to generating a certificate of authority before trying to configure a roadwarrior or a net-to-net VPN connection.

The pre-shared key method should not be used with Roadwarrior connections as all roadwarriors must use the same pre-shared key.

> **Note:** The *clocks* on either end of the IPCop VPN tunnel should be *up to date* before configuring a VPN.

X.509 Certificates

X.509 certificates are a very secure way of connecting VPN servers. To implement X.509 certificates you must either generate or setup up the certificates on IPCop or use another certification authority on your network.

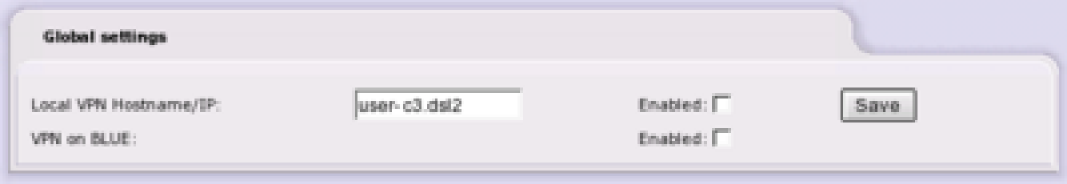
> **X.509 Terminology:** X.509 certificates on IPCop and many other implementations are manipulated and controlled by OpenSSL. SSL, or the Secure Sockets Layer, has its own terminology.
>
> X.509 certificates, depending on their type, may contain public and private encryption keys, pass phrases and information about the entity they refer to. These certificates are meant to be validated by Certification Authorities (Certificate Authorities) or CAs. When used by web browsers, the CA certificates of major, pay for, CAs are compiled into the browsers. To validate a host certificate, the certificate is passed to the appropriate CA to perform validation. On private networks or unique hosts, the CA may reside on a local host. In IPCop's case, this is the IPCop firewall, itself.
>
> Certification requests are requests for X.509 certificates that are passed to CAs. The CAs in turn generate an X.509 certificate by signing the request. These are returned to

> the requesting entity as X.509 certificates. This certificate will be known to the CA, since it signed it.
>
> You will see that X.509 certificates and requests can be stored on your hard drive in three different formats, usually identified by their extensions. PEM format is the default for OpenSSL. It can contain all the information associated with certificates in printable format. DER format contains just the key information and not any extra X.509 information. This is the default format for most browsers. PEM format wraps headers around DER format keys. PKCS#12, PFK or P12 certificates contain the same information as PEM files in binary format. Using the **openssl** command, PEM and PKCS#12 files can be transformed into their opposite number.

To use a certificate, you must import it into the other side's CA, too. The IPSec implementation on IPCop contains its own built in CA. CAs may run on roadwarrior's machines, also.

If the roadwarrior's IPSec implementation does not have CA capabilities, you can generate a certificate request, import it into IPCop so that IPCop's CA can sign it, export the resulting certificate and import it into the originating road warrior's IPSec software.

Global Settings



Global settings

Local VPN Hostname/IP: user-c3.dsl2 Enabled: □ Save

VPN on BLUE: Enabled: □

Figure 2-25. VPN Global Settings

Enter the VPN server details, either its fully qualified domain name or the public IP address of the red interface. If you are using a dynamic DNS service, you should use your dynamic DNS name here.

> **VPNs and Dynamic DNS:** If your ISP changes your IP address, be aware that Net-to-Net VPNs may have to be restarted from both ends of the tunnel. Roadwarriors will also have to restart their connections in this case.

Enable the VPN on IPCop by selecting *Local VPN Hostname/IP* and click on the **Save** button. The *VPN on Blue* option will only be visible if you have configured a BLUE network interface card. To enable a VPN over your BLUE wireless connection click on the *VPN on BLUE* **Enabled:** check box and then click on the **Save** button.

Connection Status and Control

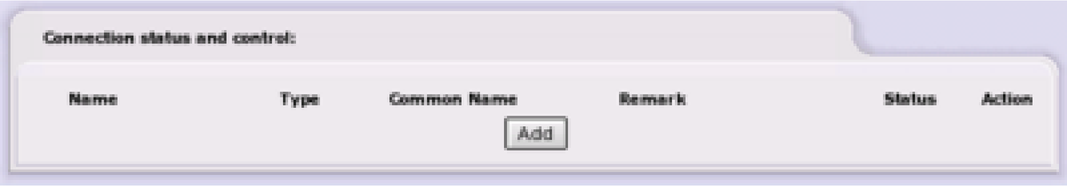
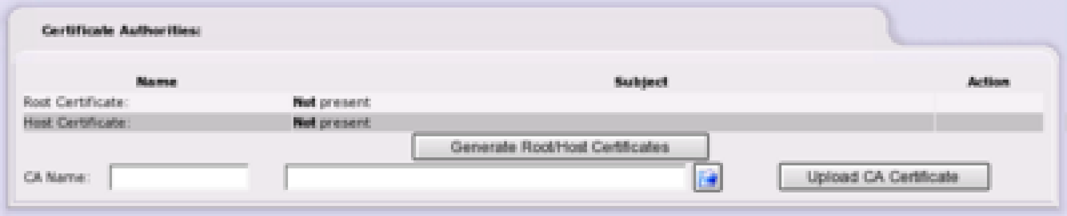


Figure 2-26. VPN Connection status and control window: Initial View

To create a VPN connection use the **Add** button. The VPN connection type page will appear.

Creating IPCop's Certificates



Name	Subject	Action
Root Certificate:	**Not** present	
Host Certificate:	**Not** present	

Figure 2-27. VPN Certificate Authorities window: Initial View

To create an IPCop's Certificate Authority or CA, enter your CA's name in the *CA Name* box. The name should be different than the IPCop machine's host name to avoid confusion. For example, **`ipcopca`** for the CA and **`ipcop`** for the hostname. Then click on the **Generate Root/Host Certificates** button.

The *Generate Root/Host Certificates* will appear. Fill out the form and both a X.509 root and host certificate will be generated.

Organization Name

The organization name you want used in the certificate. For example, if your VPN is tying together schools in a school district, you may want to use something like "Some School District."

IPCop's Hostname

This should be the fully qualified domain name of your IPCop. If you are using a dynamic DNS service, use it.

Your E-mail Address

Your E-mail address, so that folks can get hold of you.

The next three fields; department, city and state or province. You can leave them out if you wish.

Your Department

This is the department or suborganization name. Continuing the school district example, this could be `XX Elementary School.`

City

The city or mailing address for your machine.

State or Province

The state or province associated with the mailing address.

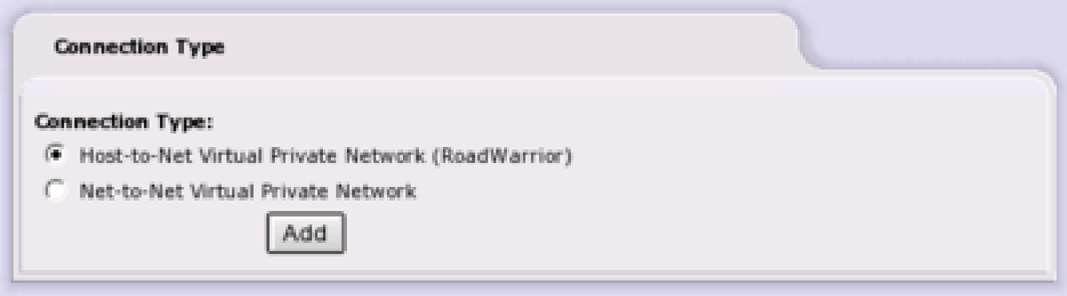
Country

This pull down selection menu contains every ISO recognized country name. Use it to select the country associated with the certificate.

After completing the form, click on the **Generate Root/Host Certificates** button to generate the certificates.

If desired, you can generate several root and host certificates on a single IPCop, and then export them to PKCS12 format files, encrypted with a password. You can then email them as attachments to your other sites. Using the *Upload PKCS12 file* portion of this web page, you can upload and decrypt the certificates on a local IPCop machine.

Connection Type



Connection Type

Connection Type:

● Host-to-Net Virtual Private Network (RoadWarrior)

○ Net-to-Net Virtual Private Network

Figure 2-28. VPN Connection Type Selection

Select either *Host-to-Net (Roadwarrior)* for mobile users who need access to the GREEN network or *Net-to-Net* to allow users on another network access to your GREEN network and to allow users on your GREEN network access to the other network.

Choose the connection type you wish to create and click on the **Add** button.

The next web page that appears contains two sections. The *Connection* section will be different depending on the connection type you are adding. The *Authentication* section will be the same.

Host-to-Net Connection

Name

Choose a simple name (lower case only with no spaces) to identify this connection.

Interface

Then select the IPCop network interface the road warrior will be connecting on, either RED or BLUE. Selecting the RED interface will allow the roadwarrior to connect from the Internet. Selecting the BLUE interface will allow the roadwarrior to connect to the GREEN network from a local wireless network.

Local Subnet

Local Subnet defaults to your GREEN network. If desired, you can create a subnet of your GREEN network to limit roadwarrior access to your GREEN network.

Remark

Remark allows you to add an optional remark that will appear in the IPCop VPNs connection window for this connection.

Enable

Click on the **Enable** check box to enable this connection.

Edit advanced settings when done.

Click on the **Edit advanced settings when done** check box if you need to modify IPCop's default settings for IPSec.

Net-to-Net Connection

Name

Choose a simple name (lower case only with no spaces) to identify this connection.

IPCop side

Choose an *IPCop side, right* or *left*, that will be used in the IPSec configuration files to identify this IPCop's side of the connection on this machine. Remember, the side makes no difference.

Local Subnet

Local Subnet defaults to your GREEN network. If desired, you can create a subnet of your GREEN network to limit roadwarrior access to your GREEN network.

Remote Host/IP

Enter the static Internet IP address of the remote network's IPSec server. You can also enter the fully qualified domain name of the remote server. If the remote server is using a dynamic DNS service, you may have to restart the VPN if its IP address changes. There are several scripts available on the IPCop news groups that will do this for you.

Remote subnet

Enter the remote network's network address and subnet mask in the same format as the *Local Subnet* field. This network must be different from the *Local Subnet* since IPSec sets up routing table entries to send IP packets to the correct remote network.

Remark

The *Remark* field allows you to add an optional comment that will appear in the IPCop VPNs connection window for this connection.

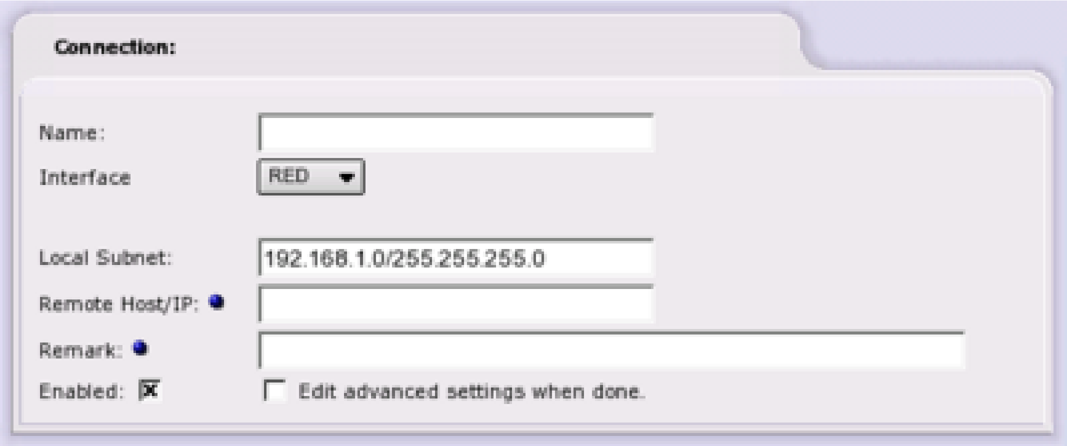
Enable

Click on the **Enable** check box to enable this connection.

Edit advanced settings when done.

Click on the **Edit advanced settings when done.** check box if you need to modify IPCop's default settings for IPSec.

Host-to-Net Connection



Connection:

Name:

Interface RED

Local Subnet: 192.168.1.0/255.255.255.0

Remote Host/IP: ●

Remark: ●

Enabled: ☒ □ Edit advanced settings when done.

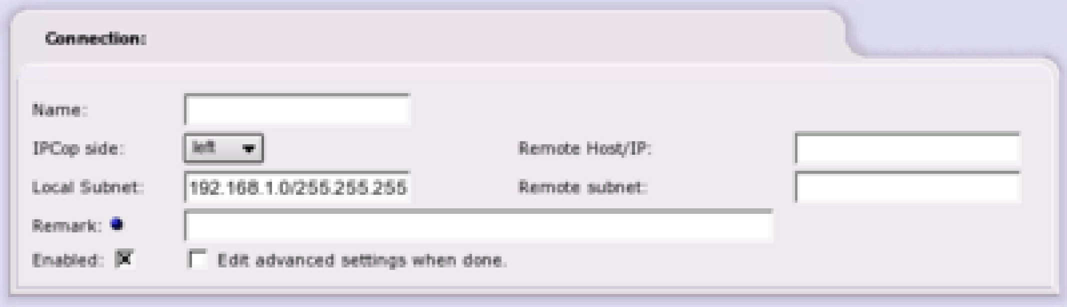
Figure 2-29. VPN Host-to-Net Connection Input

Name

A simple name (lowercase only, with no spaces) to identify this connection.

Section to be written...

Net-to-Net Connection



Connection:

Name:

IPCop side: left

Remote Host/IP:

Local Subnet: 192.168.1.0/255.255.255

Remote subnet:

Remark: ●

Enabled: ☒ □ Edit advanced settings when done.

Figure 2-30. VPN Net-to-Net Connection Input

> **Note on IPSec Terminology:** IPSec uses the terms *right* and *left* for the two sides of a connection or tunnel. These terms have no real meaning. IPSec will orient itself based on network addresses and routes. Once it determines which network connection, left or right, to use to get to the other side of a connection, all other right or left parameters follow. Many folks use left for the local side of a connection and right for the remote side. This is not necessary. It is best to think of the terms as “side 1” and “side A” of an old LP record.

Name

A simple name (lowercase only, with no spaces) to identify this connection.

IPCop side

Section to be written...

Section to be written...

Authentication

The second section of the web page deals with authentication. In other words, this is how this IPCop will make sure the tunnel established by both sides of the interface is talking to its opposite number. IPCop has made every effort to support both PSKs and X.509 certificates. There are four mutually exclusive choices that can be used to authenticate a connection.

Use a Pre-Shared Key

Enter a pass phrase to be used to authenticate the other side of the tunnel. Chose this if you wish a simple Net-to-Net VPN. You can also use PSKs while experimenting in setting up a VPN. *Do not use PSKs to authenticate tunnels to roadwarriors.*

Upload certificate request

Some roadwarrior IPSec implementations do not have their own CA. If they wish to use IPSec’s built in CA, they can generate what is called a certificate request. This is a partial X.509 certificate that must be signed by CA to be a complete certificate. During certificate request upload, the request is signed and the new certificate will become available on the VPNs main web page.

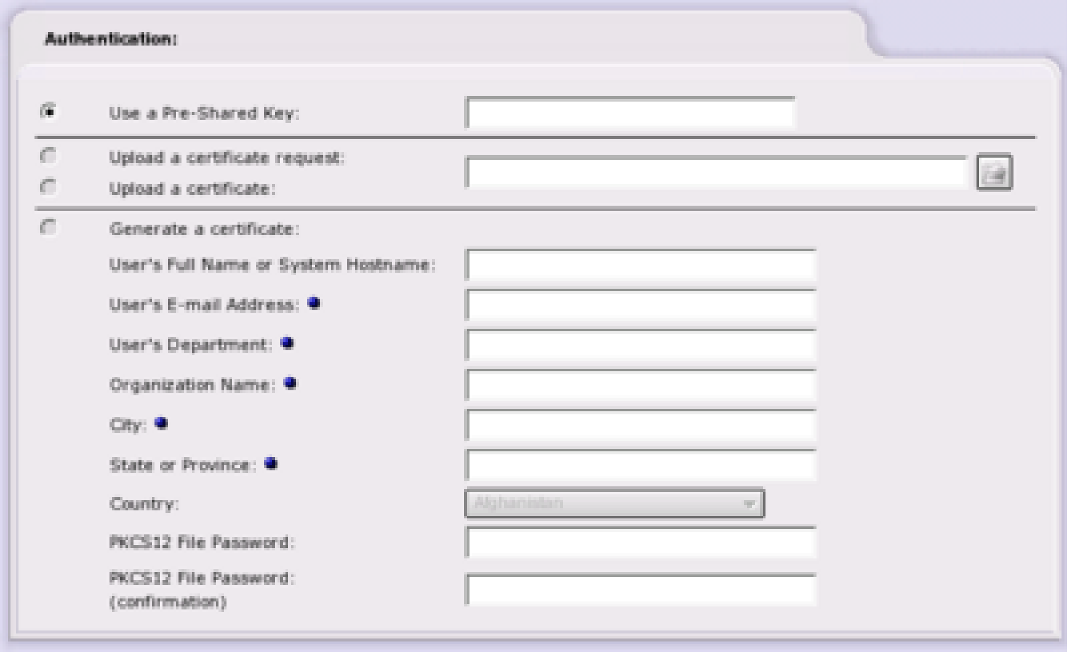
Upload a certificate

In this case, the peer IPSec has a CA available for use. Both the peer’s CA certificate and host certificate must be uploaded.

Generate a certificate

In this case, the IPSec peer will be able to provide an X.509 certificate, but lacks the capacity to even generate a certificate request. In this case, complete the required fields. Optional fields are indicated by blue dots. If this certificate is for a Net-to-Net connection, the *User’s Full Name or System Hostname* field may need to be the Internet fully qualified domain name of the peer. The optional organization name is meant to isolate different portions of an organization from access to IPCop’s full GREEN network by subnetting the *Local Subnet* in the connection definition portion of this web page. The *PKCS12 File Password* fields ensure that the host certificates generated cannot be intercepted and compromised while being transmitted to the IPSec peer.

Authentication



Authentication:

● Use a Pre-Shared Key:

○ Upload a certificate request:
○ Upload a certificate:

○ Generate a certificate:
User's Full Name or System Hostname:
User's E-mail Address: ●
User's Department: ●
Organization Name: ●
City: ●
State or Province: ●
Country: Afghanistan
PKCS12 File Password:
PKCS12 File Password: (confirmation)

Figure 2-31. VPN Authentication Input

Section to be written...

Logs Menu

Introduction

The Logs AW Consists of five or six sub-pages - Log Settings, Log Summary, Proxy Logs, Firewall Logs, IDS Logs (if enabled) and System Logs. These share a common set of interface features to select the log information to be displayed, and to export that information to your local machine. Dropdown *Month:* and *Day:* lists in the *Settings:* area of the AW are provided to allow you to select Logs information for preceding days and months. Each time that you select a new combination of *Month:* and *Day:*, you must also click the **Update** button before the Logs information will be updated. When you first select a sub-page, the Logs information displayed will be that for the current date.

The << button lets you quickly jump back a day, and the >> button moves a day forward.

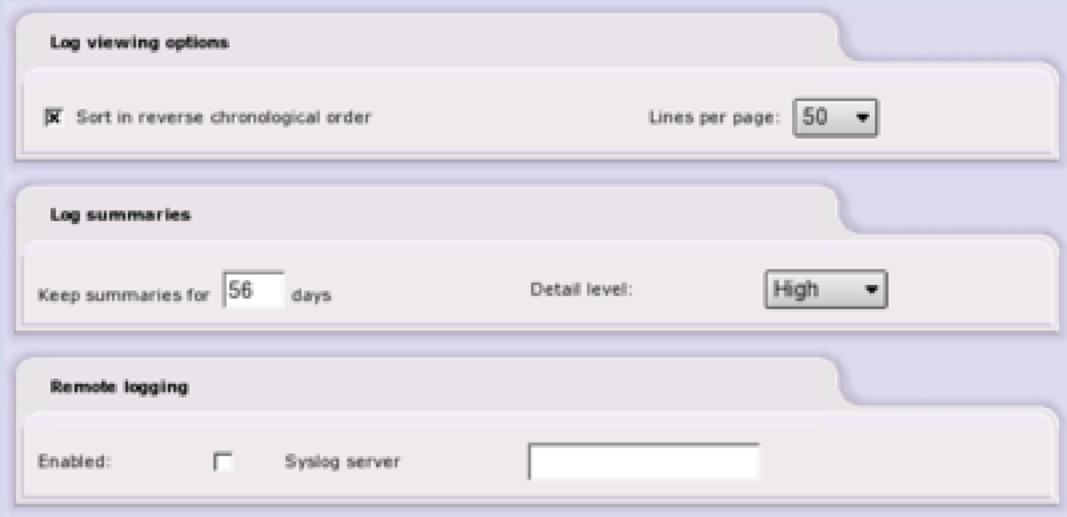
The Logs information appears as a list in the main section of the window (usually labeled *Log:*). If that list is too long to fit into a reasonably sized window, only the latest Logs information is displayed. In that situation, the *Older* and *Newer* links at the top and bottom of this section of the window become active and you may use these to page through the list of Logs data.

Pressing the **Export** button downloads a text-format file (`log.dat`), containing the information from the current Logs AW page, from the IPCop server to your computer.

Depending on how your computer is set up, pressing the **Export** button will initiate a file download dialogue on your computer, show the contents of `log.dat` in your web browser window, or open the file in a text editor. In the latter cases, you can save `log.dat` as a text-format file if required.

Log Settings Administrative Web Page

Section to be written...



Log viewing options

☒ Sort in reverse chronological order

Lines per page: 50

Log summaries

Keep summaries for 56 days

Detail level: High

Remote logging

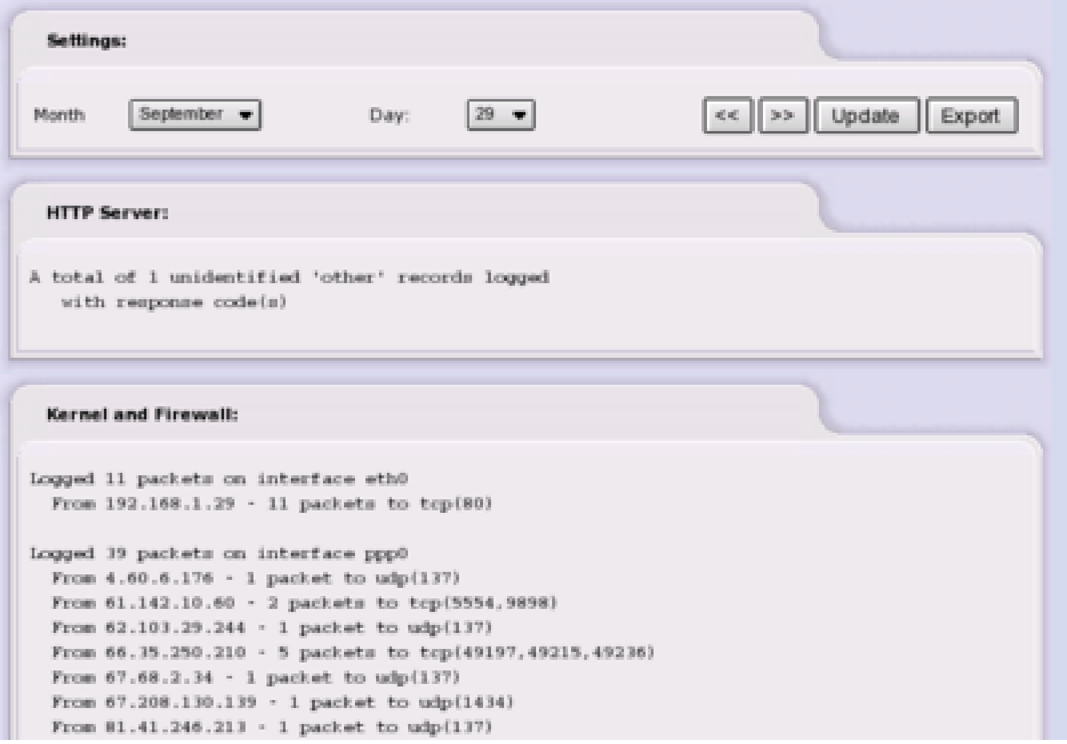
Enabled: □

Syslog server

Figure 2-32. Log Settings

Log Summary Page

Section to be written...



Settings:

Month: September

Day: 29

HTTP Server:

```
A total of 1 unidentified 'other' records logged
   with response code(s)
```

Kernel and Firewall:

```
Logged 11 packets on interface eth0
  From 192.168.1.29 - 11 packets to tcp(80)

Logged 39 packets on interface ppp0
  From 4.60.6.176 - 1 packet to udp(137)
  From 61.142.10.60 - 2 packets to tcp(5554,9898)
  From 62.103.29.244 - 1 packet to udp(137)
  From 66.35.250.210 - 5 packets to tcp(49197,49215,49236)
  From 67.68.2.34 - 1 packet to udp(137)
  From 67.208.130.139 - 1 packet to udp(1434)
  From 81.41.246.213 - 1 packet to udp(137)
```

Figure 2-33. Log Summary Output

Proxy Logs Page

This page provides you with the facility to see the files that have been cached by the web proxy server within IPCop. The web proxy is inactive after first installation of IPCop, and may be activated (and deactivated) through a specific administration page (**Services** > **Proxy**).

> **Note:** The Proxy Log menu item will *only* appear if you have enabled logging on the **Services** > **Proxy** page.
>
> Due to the large amount of information that has to be processed, the *Web Proxy* page can take an appreciable time to appear after its initial selection or an *Update*.

There are several controls on this page in addition to the *Month:*, *Day:*, and **Update** controls described at the beginning of this Section:

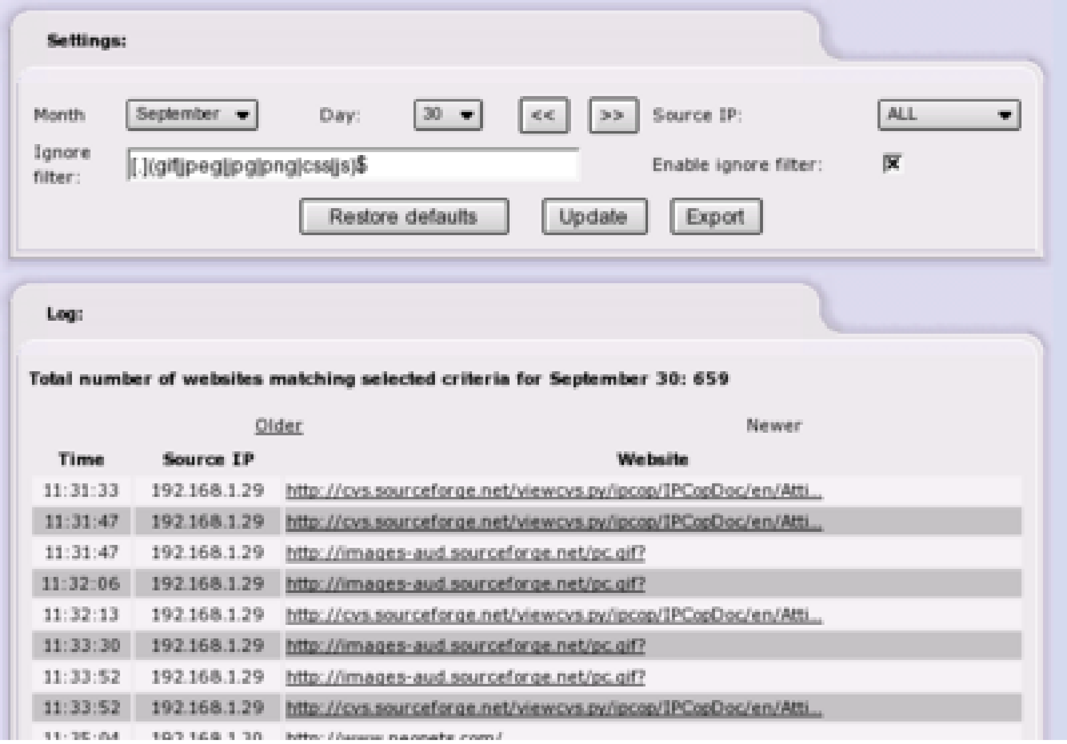
- The *Source IP:* dropdown box allows you selectively look at web proxy activity related to individual IP addresses on the local network, or the activity related to *ALL* machines that have used the proxy.
- The *Ignore filter:* box allows you type in a regular expressions text string to define which file types should be omitted from the web proxy Logs. The default string hides image files (.gif, .jpeg, .png & .png), stylesheet files (.css) and JavaScript files (.js).
- The *Enable ignore filter:* tick box allows you to control whether the *Ignore filter:* is active or not.

- The *Restore defaults* button allows you to return the above controls and filters to their defaults.

For this page, the Logs information appearing in the *Log:* section of the window consists of:

- The *Time* the file was requested and cached.
- The *Source IP* address of the local system requesting the file.
- The *Website* - or more precisely the URL for each file requested and cached.

> **Note:** The *Website* URL entries in these Logs are also hyperlinks to the referenced web pages or files.



Month: September
Day: 30
Source IP: ALL
Ignore filter: [.](gif|jpeg|jpg|png|css|js)$
Enable ignore filter: ☒

Total number of websites matching selected criteria for September 30: 659

Time	Source IP	Website
11:31:33	192.168.1.29	http://cvs.sourceforge.net/viewcvs.py/ipcop/IPCopDoc/en/Atti...
11:31:47	192.168.1.29	http://cvs.sourceforge.net/viewcvs.py/ipcop/IPCopDoc/en/Atti...
11:31:47	192.168.1.29	http://images-aud.sourceforge.net/pc.gif?
11:32:06	192.168.1.29	http://images-aud.sourceforge.net/pc.gif?
11:32:13	192.168.1.29	http://cvs.sourceforge.net/viewcvs.py/ipcop/IPCopDoc/en/Atti...
11:33:30	192.168.1.29	http://images-aud.sourceforge.net/pc.gif?
11:33:52	192.168.1.29	http://images-aud.sourceforge.net/pc.gif?
11:33:52	192.168.1.29	http://cvs.sourceforge.net/viewcvs.py/ipcop/IPCopDoc/en/Atti...
11:35:04	192.168.1.30	http://www.neopets.com/

Figure 2-34. Proxy Log Output

Firewall Logs Page

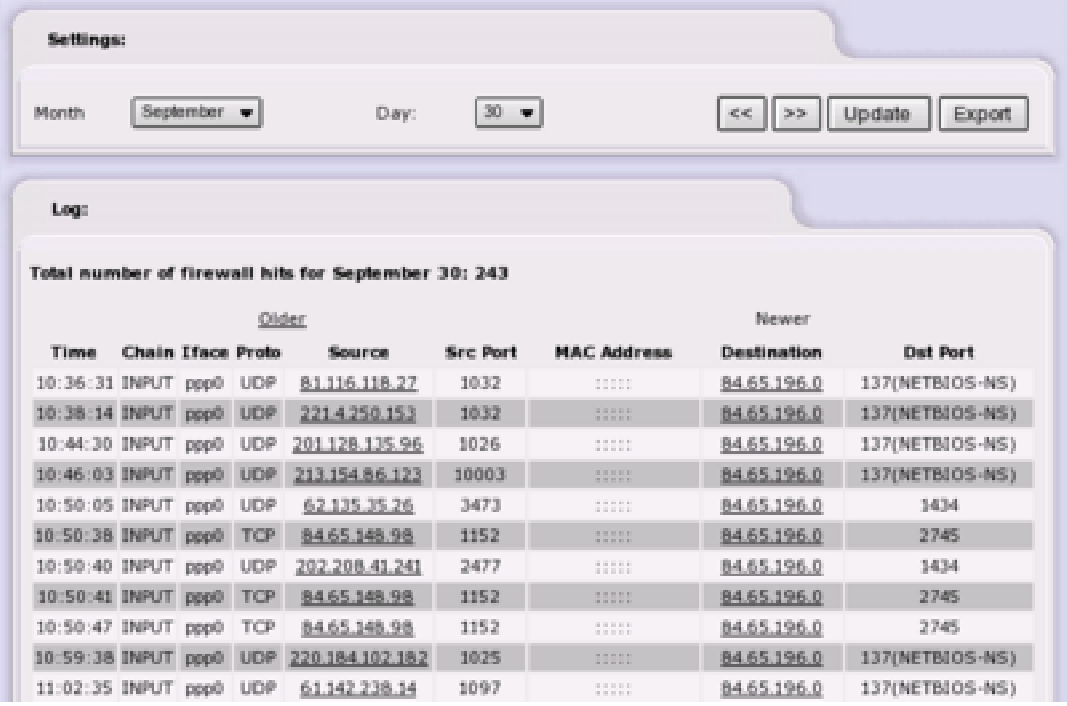
This page shows data packets that have been blocked by the IPCop firewall.

> **Note:** Not all denied packets are hostile attempts by crackers to gain access to your machine. Blocked packets commonly occur for a number of harmless reasons and many can be safely ignored. Among these may be attempted connections to the "ident/auth" port (113), which are blocked by default in IPCop.

The controls on this page are the basic *Month*, *Day*, << (Day before), >> (Day after), **Update** and **Export** buttons that are described in detail at the beginning of this Section.

The *Log:* section of this page contains an entry for each of the packets that were "dropped" by the firewall. Included is the time of the event, the Source and Destination IP addresses and ports for the dropped packet, the protocol used for that packet, and the IPCop Chain and Interface involved.

You can obtain information about the listed IP addresses by clicking on an IP Address. IPCop performs a DNS lookup and reports any available information about its registration and ownership.



Settings:

Month: September Day: 30

Log:

Total number of firewall hits for September 30: 243

Time	Chain	Iface	Proto	Source	Src Port	MAC Address	Destination	Dst Port
10:36:31	INPUT	ppp0	UDP	81.116.118.27	1032	:::::	84.65.196.0	137(NETBIOS-NS)
10:38:14	INPUT	ppp0	UDP	221.4.250.153	1032	:::::	84.65.196.0	137(NETBIOS-NS)
10:44:30	INPUT	ppp0	UDP	201.128.135.96	1026	:::::	84.65.196.0	137(NETBIOS-NS)
10:46:03	INPUT	ppp0	UDP	213.154.86.123	10003	:::::	84.65.196.0	137(NETBIOS-NS)
10:50:05	INPUT	ppp0	UDP	62.135.35.26	3473	:::::	84.65.196.0	1434
10:50:38	INPUT	ppp0	TCP	84.65.148.98	1152	:::::	84.65.196.0	2745
10:50:40	INPUT	ppp0	UDP	202.208.41.241	2477	:::::	84.65.196.0	1434
10:50:41	INPUT	ppp0	TCP	84.65.148.98	1152	:::::	84.65.196.0	2745
10:50:47	INPUT	ppp0	TCP	84.65.148.98	1152	:::::	84.65.196.0	2745
10:59:38	INPUT	ppp0	UDP	220.184.102.182	1025	:::::	84.65.196.0	137(NETBIOS-NS)
11:02:35	INPUT	ppp0	UDP	61.142.238.14	1097	:::::	84.65.196.0	137(NETBIOS-NS)

Figure 2-35. Firewall Log Output

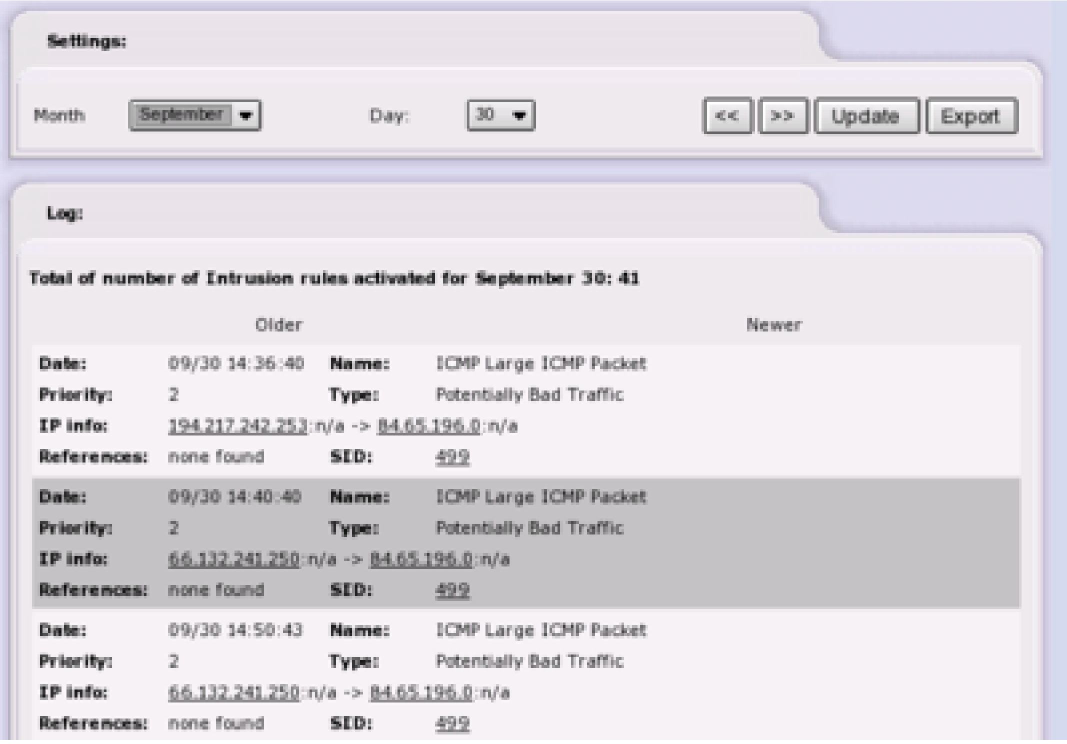
Intrusion Detection System Log Page

This page shows incidents detected by the IPCop Intrusion Detection System (IDS). The IDS system is inactive after first installation of IPCop, and may be activated (and deactivated) through a specific administration page (**Services** > **Intrusion Detection**).

The controls on this page are the basic *Month*, *Day*, << (Day before), >> (Day after), **Update** and **Export** buttons that are described in detail at the beginning of this Section. These allow you to examine the IDS Logs for a specific day. These Logs consist of a number of items for each detected incident:

- The *Date:* and time of the incident.
- *Name:* - a description of the incident.
- *Priority:* (if available). This is the severity of the incident, graded as 1 ("bad"), 2 ("not too bad"), & 3 ("possibly bad").

- *Type:* - a general description of the incident (if available).
- *IP Info:* - the IP identities (address & port) of the source and target involved in the incident. Each IP address is a hyperlink, which you can use to perform a DNS lookup for that IP address and obtain any available information about its registration and ownership.
- *References:* - hyperlinked URLs to any available sources of information for this type of incident.
- *SID:* - the Snort ID number (if available). "Snort" is the software module used by IPCop to provide the IDS function, and SID is the ID code used by the Snort module to identify a particular pattern of attack. This parameter is hyperlinked to a web page carrying the relevant entry on the Snort database of intrusion signatures.



Month: September Day: 30

```
Total of number of Intrusion rules activated for September 30: 41

Date:         09/30 14:36:40   Name:   ICMP Large ICMP Packet
Priority:     2                Type:   Potentially Bad Traffic
IP info:      194.217.242.253:n/a -> 84.65.196.0:n/a
References:   none found       SID:    499

Date:         09/30 14:40:40   Name:   ICMP Large ICMP Packet
Priority:     2                Type:   Potentially Bad Traffic
IP info:      66.132.241.250:n/a -> 84.65.196.0:n/a
References:   none found       SID:    499

Date:         09/30 14:50:43   Name:   ICMP Large ICMP Packet
Priority:     2                Type:   Potentially Bad Traffic
IP info:      66.132.241.250:n/a -> 84.65.196.0:n/a
References:   none found       SID:    499
```

Figure 2-36. IDS Log Output

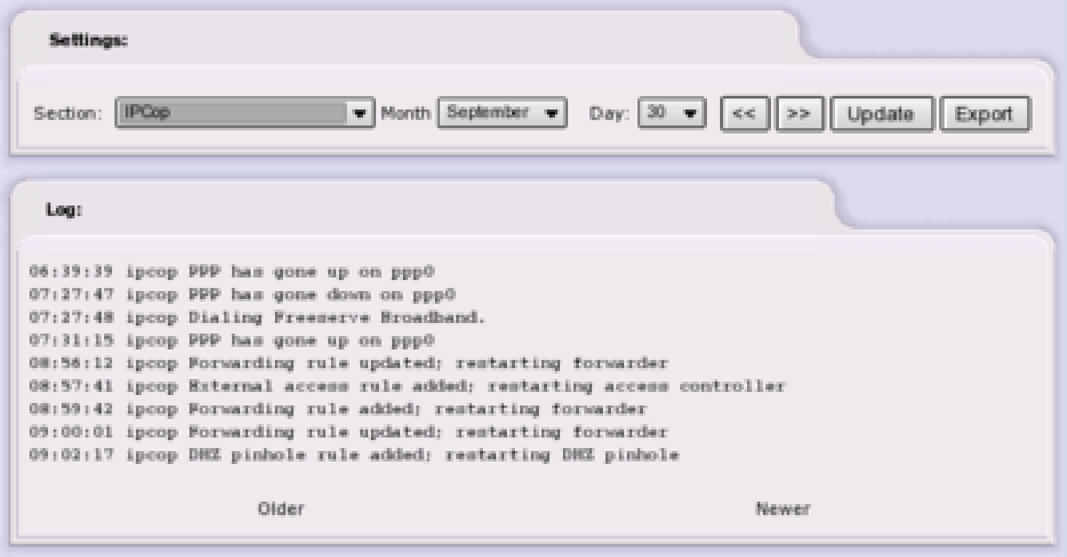
System Log Page

This page allows you to view the system and other miscellaneous Logs. (See the beginning of this Section on how to use the *Month*, *Day*, << (Day before), >> (Day after) and **Update** controls). There are eleven different categories, selected via the *Section* dropdown list:

- *IPCop* (default) - general IPCop events like PPP profile saving and connection ("`PPP has gone up on ppp0` ") and disconnection ("`PPP has gone down on ppp0` ") of dialup modem links.
- *RED* - traffic sent over the interface that is providing the PPP interface for IPCOP. This includes the data strings sent to, and received from modems and other net-

work interfaces. This can be a very useful resource in troubleshooting "failure to connect" situations.

- *DNS* - shows a log of activity for dnsmasq, the domain name service utility.
- *DHCP server* - shows a log of activity for the DHCP Server function within IPCop.
- *SSH* - provides a record of users who have logged in to, and out of the IPCop server over a network via the SSH interface.
- *NTP* - shows a log of activity for the ntpd Server function.
- *Cron* - provides a record of activity of the cron daemon.
- *Login/Logout*- provides a record of users who have logged in to, and out of the IPCop server. This includes both local log-ins and logins over a network via the SSH interface.
- *Kernel* - is a record of kernel activity in the IPCop server.
- *IPSec* - is a record of activity of IPSec - the VPN software module used by IPCop.
- *Update transcript* - is a log of the results of any updates applied to the IPCop software via the **System** > **Update** window.
- *Snort* - shows a log of activity for Snort, the Intrusion Detection System.



Section: IPCop
Month: September
Day: 30

```
06:39:39 ipcop PPP has gone up on ppp0
07:27:47 ipcop PPP has gone down on ppp0
07:27:48 ipcop Dialing Freeserve Broadband.
07:31:15 ipcop PPP has gone up on ppp0
08:56:12 ipcop Forwarding rule updated; restarting forwarder
08:57:41 ipcop External access rule added; restarting access controller
08:59:42 ipcop Forwarding rule added; restarting forwarder
09:00:01 ipcop Forwarding rule updated; restarting forwarder
09:02:17 ipcop DMZ pinhole rule added; restarting DMZ pinhole
```

Figure 2-37. System Log Output

Notes

1. https://ipcop:445
2. https://192.168.10.1:445
3. http://ipcop:81
4. http://192.168.10.1:81
5. http://www.devshed.com/c/a/Administration/Secure-Tunnelling-with-SSH/
6. http://security.itworld.com/4360/LWD010410SSHtips/page_1.html
7. http://www.ipcop.org/modules.php?op=modload&name=phpWiki&file=index&pagename=HowTo

8. http://www.linux-mag.com/2000-04/networknirvana_01.html
9. http://www.snort.org/

Appendix A. GNU Free Documentation License

0. Preamble

The purpose of this License is to make a manual, textbook, or other functional and useful document “free” in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of “copyleft”, which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. Applicability and Definitions

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The “Document”, below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as “you”. You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A “Modified Version” of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A “Secondary Section” is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document’s overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The “Invariant Sections” are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The “Cover Texts” are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A “Transparent” copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not “Transparent” is called “Opaque”.

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include PostScript, PDF, proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The “Title Page” means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, “Title Page” means the text near the most prominent appearance of the work’s title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. Verbatim Copying

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. Copying In Quantity

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document’s license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover

Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. Modifications

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled “History” in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the “History” section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. In any section Entitled “Acknowledgements” or “Dedications”, Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled “Endorsements”. Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled “Endorsements” or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version’s license notice. These titles must be distinct from any other section titles.

You may add a section Entitled “Endorsements”, provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made ’by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. Combining Documents

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled “History” in the various original documents, forming one section Entitled “History”; likewise combine any sections Entitled “Acknowledgements”, and any sections Entitled “Dedications”. You must delete all sections Entitled “Endorsements.”

6. Collections of Documents

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. Aggregation With Independent Works

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an “aggregate” if the copyright resulting from the compilation is not used to limit the legal rights of the compilation’s users beyond what the individual works permit. When the Document is included an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document’s Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. Translation

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warrany Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled “Acknowledgements”, “Dedications”, or “History”, the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. Termination

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. Future Revisions of This License

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See the GNU Free Documentation License [1] web site.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

Notes

1. http://www.gnu.org/licenses/licenses.html#FDL