

Library Computer and Network Security and Web Services

Introduction

- Library Security Principles
- User Security
- General Computer Security
- Workstation Security
- Server Security
- Network Security
- Web 2.0 and the Library

Library Security Principles

- Risk Assessment
- Creating a Security Policy
- Security Threats and Vulnerabilities
- Protection Strategies

User Security

- Network Passwords
- Smart Cards

General Computer Security

- OS Strengthening/Hardening
- Anti-Virus Software
- Registry Settings
- Other Alternative Software
- Operating System and Patches

Workstation Security

- Protecting BIOS
- Policy Setting
- Desktop Security Software
- Browser and Email Security
- Securing Office Applications
- Personal Firewalls

Server Security

- Email and Web Server Security
- Fault Tolerance
- Server Monitoring

Network Security

- Firewalls
- Basic Firewall Configuration
- Packets & Protocols
- Securing Wireless Networks
- Remote Access Security

Open Source Firewall

- PfSense
- Smoothwall
- IPCOP

IPCOP Open Source Firewall

- What is IPCOP?
 - IPCOP is a firewall.
 - Is a specialized LINUX Distribution; complete, configured, and ready to protect your network.
 - Is a community: where members help each other, all sharing to improve the project and each other.

IPCop Features

- A secure, stable and highly configurable Linux based firewall
- Easy administration through the built in web server
- A DHCP client that allows IPCop to, optionally, obtain its IP address from your ISP
- A DHCP server that can help configure machines on your internal network
- A caching DNS proxy, to help speed up Domain Name queries
- A web caching proxy, to speed up web access
- An intrusion detection system to detect external attacks on your network

IPCOP Features (cont..)

- A VPN facility that allows you to connect your internal network to another network across the Internet, forming a single logical network or to securely connect PCs on your BLUE, wireless, network to the wired GREEN network
- Traffic shaping capabilities to give highest priority to interactive services such as ssh and telnet, high priority to web browsing, and lower priority to bulk services such as FTP.
- A choice of four kernel configurations, allowing you to choose an optimum configuration for your circumstances.

System Requirements

- I386 Architecture
 - Intel x86 Based Processor
 - At least 32MB RAM
 - At least 300MB HDD
 - CDROM Drive (Optional)
 - At least one (1) Network Interface Card (NIC)

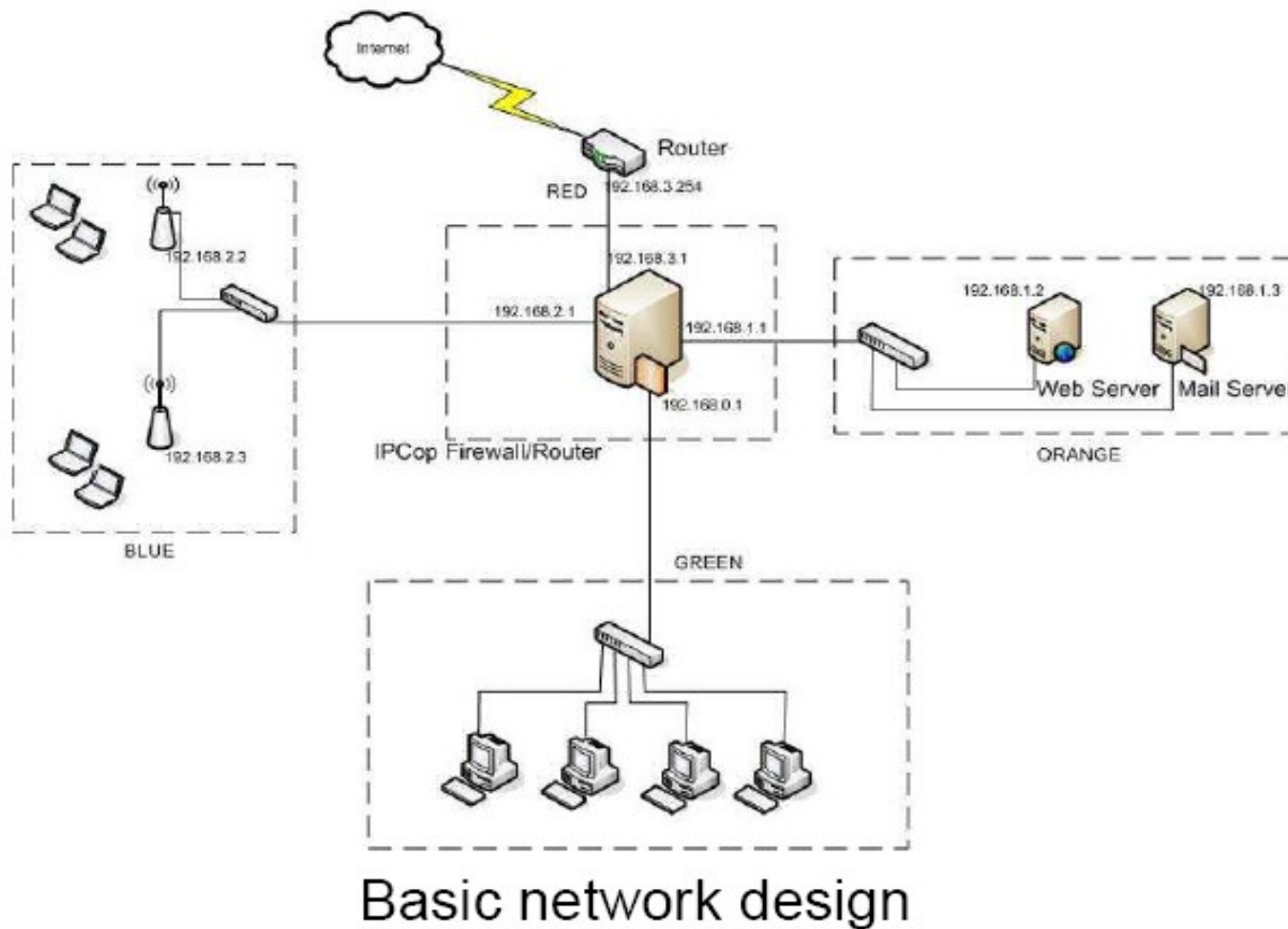
Installation Preparation

- Decide on your Configuration based on your network setup
- IPCOP defines upto four network interfaces: RED, GREEN, BLUE & ORANGE Networks
 - RED Network Interface: Internet (Untrusted Network)
 - GREEN Network Interface: Local Network (Network to be protected by IPCOP)
 - BLUE Network Interface: Optional Network (Wireless Network)
 - ORANGE Network Interface: Publicly accessible computers (servers)

IPCOP Network Interfaces

Connection	Modem	ISDN	USB DSL	Ethernet
RED, GREEN	1 NIC (G)	1 NIC (G)	1 NIC (G)	2 NIC (R, G)
RED, GREEN, BLUE	2 NIC (B, G)	2 NIC (B, G)	2 NIC (B, G)	3 NIC (R, B, G)
RED, ORANGE, GREEN	2 NIC (O, G)	2 NIC (O, G)	2 NIC (O, G)	3 NIC (R, O, G)
RED, ORANGE, BLUE, GREEN	3 NIC (O, B, G)	3 NIC (O, B, G)	3 NIC (O, B, G)	4 NIC (O, B, G, R)

Basic Network Design



Network Configuration Types

- GREEN (RED is modem/ISDN)
- GREEN + RED (RED is Ethernet)
- GREEN + ORANGE + RED (RED is Ethernet)
- GREEN + ORANGE (RED is modem/ISDN)
- GREEN + BLUE + RED (RED is Ethernet)
- GREEN + BLUE (RED is modem/ISDN)
- GREEN + BLUE + ORANGE + RED (RED is Ethernet)
- GREEN + BLUE + ORANGE (RED is modem/ISDN)

Installation

```
ISOLINUX 2.11 2004-08-16 Copyright (C) 1994-2004 H. Peter Anvin
```

```
Welcome to IPCop, Licensed under GNU GPL version 2.
```

```
PLEASE BEWARE! This installation process will kill all  
existing partitions on your PC or server. Please be aware  
of this before continuing this installation.
```

```
-----  
---- ALL YOUR EXISTING DATA WILL BE DESTROYED ----  
-----
```

```
Press RETURN to boot IPCop default installation.
```

```
Or, if you are having trouble you can try these options....
```

```
Type:  nopcmcia to disable PCMCIA detection  
       nousb to disable USB detection  
       nousborpcmcia to disable both PCMCIA & USB detection  
       dma to enable ide dma (SiS chipset workaround)
```

```
boot: _
```

Installation



- After a few seconds, the language selection screen will appear.



- The WELCOME Screen

Installation



- The next screen simply informs you of how to abort the installation. “ Select the Cancel and press the Enter key. ”



- The next dialog box lets you choose the installation media. Since you are installing from CD-ROM, select it, tab to the Ok button and press the Enter key.

Installation

- Your final warning appears next
- After you select Ok and press Enter on this screen all of the data on your hard drive will be erased. To abort the installation, select Cancel and press the Enter key.
- Next IPCop will format and partition your hard drive. Then it will install all its files.



Installation



- At this point, you have the option of restoring files from an IPCop backup floppy.
- To do the restore, place the backup floppy in the floppy disk drive and select Restore and press the Enter key. Otherwise, select Skip and press the Enter key.



- Next IPCop will begin setting up your GREEN (local) network interface.

Installation

- If you specify Probe, above, the screen on the left will appear.



- IPCop will now configure its internal network address, the GREEN interface.

Installation



- All of IPCop has now been installed on your hard drive. The following screen will appear. Remove the IPCop CD from your CD drive and, if present, the bootable floppy from the floppy drive. Select Ok to continue.



- The first screen allows you to configure your keyboard.

Installation



- The next screen, above, asks for your time zone.



- You must then configure your IPCop machine's hostname.

Installation



- You must then configure your IPCop machine's domain name.



- Next you will configure your network interfaces. The Network Configuration Menu will take you through the steps necessary to configure them.

Installation



- As mentioned, there are four network interfaces supported by IPCop, RED, GREEN, BLUE and ORANGE.
- When you select Ok, you will be returned to the Network Configuration Menu . Tab to the Drivers and card assignments line,select it and press the Enter key.
- If you have ORANGE and/or BLUE networks, repeat the driver configuration steps you used to configure your GREEN interface. If your RED interface uses an Ethernet connection, configure it, too.



Configuration



The screenshot displays the IP Cop web interface. At the top left is the IP Cop logo with version 1.4.10. The navigation bar includes 'SYSTEM' (selected), 'HOME', 'SYSTEM', 'STATUS', 'NETWORK', 'SERVICES', 'FIREWALL', 'VPNS', and 'LOGS'. A banner reads 'The bad packets stop here.' with a cartoon character. The main content area shows a connection status for 'labproxy.usep.edu.ph' with 'Connect', 'Disconnect', and 'Refresh' buttons. It indicates a 'Connected' state for 2 days, 14 hours, 49 minutes, and 44 seconds, with IP address 172.16.0.2. A message states that updates are available. System statistics show the time as 14:51:32 up 2 days, 14:50, with 0 users and a load average of 0.24, 0.38, 0.32. At the bottom left is a cartoon penguin character. At the bottom right, it shows 'Connected (2d 14h 49m 50s)' and the same system statistics, along with the SOURCEFORGE.net logo.

IP Cop 1.4.10

SYSTEM HOME The bad packets stop here.

SYSTEM STATUS NETWORK SERVICES FIREWALL VPNS LOGS

labproxy.usep.edu.ph

Connect Disconnect Refresh

Connected (2d 14h 49m 44s)
IP Address: 172.16.0.2
IPCop's Hostname:

1. There are updates available for your system. Please go to the "Updates" section for more information.

14:51:32 up 2 days, 14:50, 0 users, load average: 0.24, 0.38, 0.32

Connected (2d 14h 49m 50s)
14:51:32 up 2 days, 14:50, 0 users, load average: 0.24, 0.38, 0.32

SOURCEFORGE.net

System Status



STATUS

SYSTEM STATUS

The bad packets stop here.

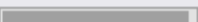

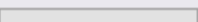


[Services:](#) | [Memory:](#) | [Disk usage:](#) | [Uptime and users:](#) | [Loaded modules:](#) | [Kernel version:](#)

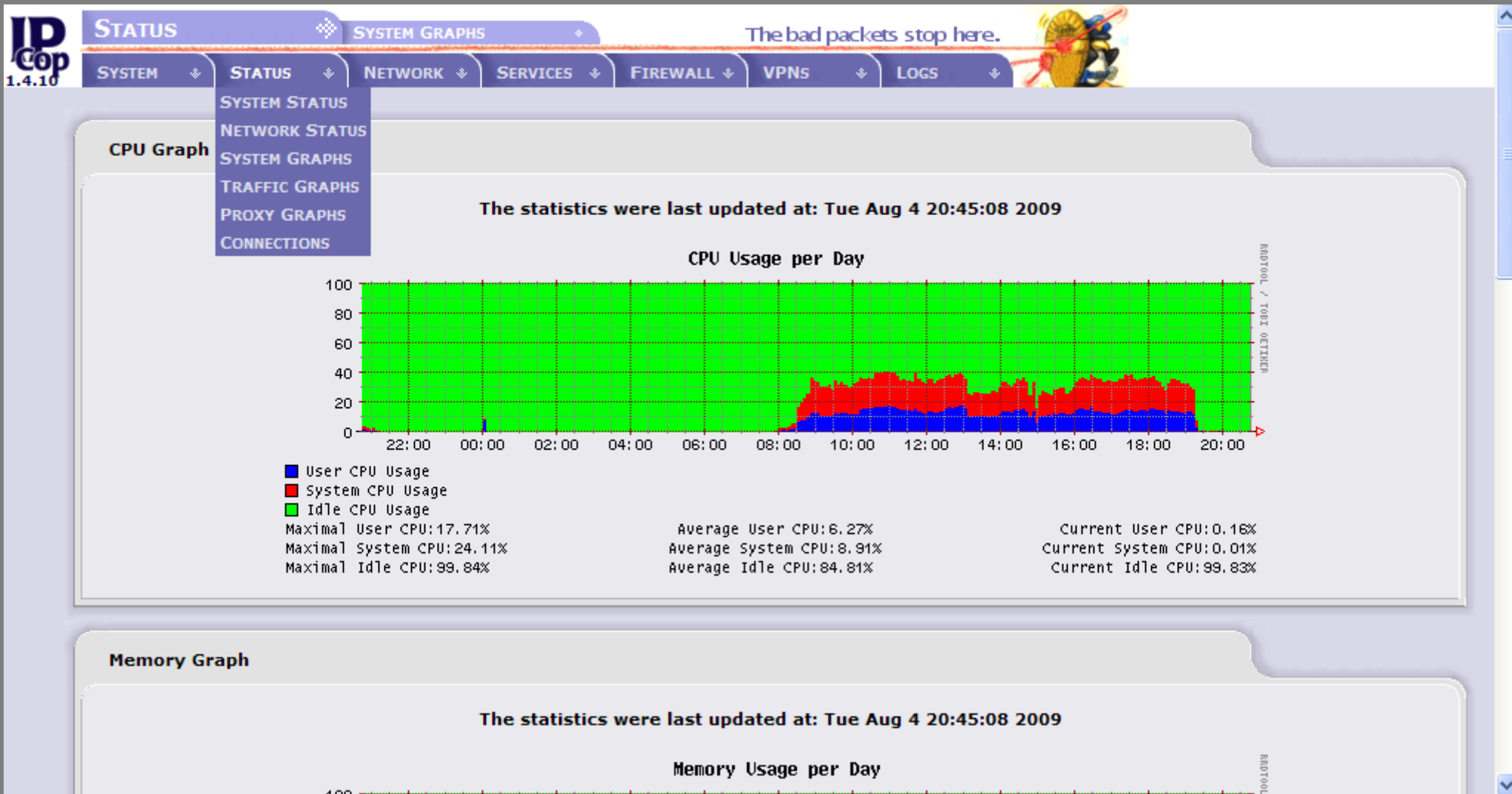
Services:

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

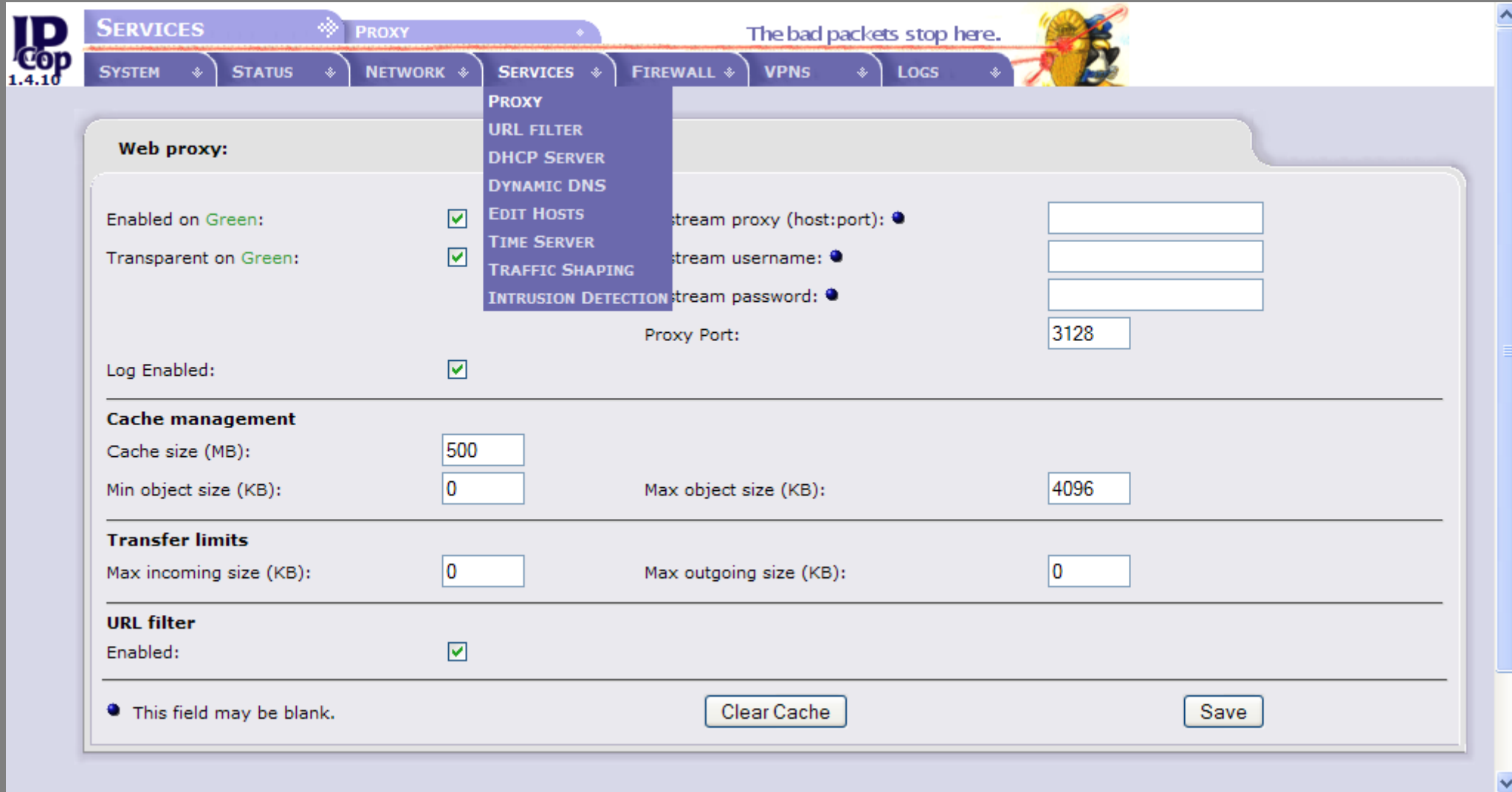
Memory:

	Size	Used	Free	Percentage		
RAM	256812	252896	3916	 98%	shared	0
-/+ buffers/cache	134792	122020		 52%	buffers	17848
Swap	32764	0	32764	 0%	cached	100256

System Status - Graph



Proxy Configuration



The screenshot shows the IP Cop 1.4.10 web interface for proxy configuration. The top navigation bar includes 'SERVICES', 'SYSTEM', 'STATUS', 'NETWORK', 'FIREWALL', 'VPNS', and 'LOGS'. The 'SERVICES' menu is open, showing options like 'PROXY', 'URL FILTER', 'DHCP SERVER', 'DYNAMIC DNS', 'EDIT HOSTS', 'TIME SERVER', 'TRAFFIC SHAPING', and 'INTRUSION DETECTION'. The 'PROXY' configuration page is active, featuring sections for 'Web proxy', 'Cache management', 'Transfer limits', and 'URL filter'. The 'Web proxy' section has checkboxes for 'Enabled on Green', 'Transparent on Green', and 'Log Enabled', all of which are checked. It also includes input fields for 'stream proxy (host:port)', 'stream username', 'stream password', and 'Proxy Port' (set to 3128). The 'Cache management' section has input fields for 'Cache size (MB)' (500), 'Min object size (KB)' (0), and 'Max object size (KB)' (4096). The 'Transfer limits' section has input fields for 'Max incoming size (KB)' (0) and 'Max outgoing size (KB)' (0). The 'URL filter' section has a checked 'Enabled' checkbox. At the bottom, there is a note 'This field may be blank.', a 'Clear Cache' button, and a 'Save' button.

SERVICES **PROXY** The bad packets stop here.

SYSTEM STATUS NETWORK SERVICES FIREWALL VPNS LOGS

Web proxy:

Enabled on Green:

Transparent on Green:

Log Enabled:

stream proxy (host:port):

stream username:

stream password:

Proxy Port:

Cache management

Cache size (MB):

Min object size (KB):

Max object size (KB):

Transfer limits

Max incoming size (KB):

Max outgoing size (KB):

URL filter

Enabled:

This field may be blank.

URL/Content Filtering

The screenshot displays the IP Cop 1.4.10 web interface. At the top, a navigation bar includes 'SERVICES' (selected), 'SYSTEM', 'STATUS', 'NETWORK', 'FIREWALL', 'VPNS', and 'LOGS'. A dropdown menu is open under 'SERVICES', listing options: PROXY, URL FILTER (selected), DHCP SERVER, DYNAMIC DNS, EDIT HOSTS, TIME SERVER, TRAFFIC SHAPING, and INTRUSION DETECTION. The main content area is titled 'URL filter settings:' and features a 'Block categories' section with a grid of checkboxes for various content types. Below this are sections for 'Custom blacklist' and 'Custom whitelist', each with text input fields for domains and URLs. The interface also includes a top banner with the slogan 'The bad packets stop here.' and a small graphic of a robot.

Block categories

ads:	<input checked="" type="checkbox"/>	aggressive:	<input checked="" type="checkbox"/>	audio-video:	<input type="checkbox"/>	drugs:	<input checked="" type="checkbox"/>
gambling:	<input checked="" type="checkbox"/>	hacking:	<input checked="" type="checkbox"/>	mail:	<input type="checkbox"/>	porn:	<input checked="" type="checkbox"/>
proxy:	<input type="checkbox"/>	violence:	<input checked="" type="checkbox"/>	warez:	<input checked="" type="checkbox"/>		

Custom blacklist

Blocked domains (one per line) ●

```
friendster.com
youtube.com
pornstar.com
rapidshare.com
facebook.com
```

Blocked URLs (one per line) ●

Enable custom blacklist:

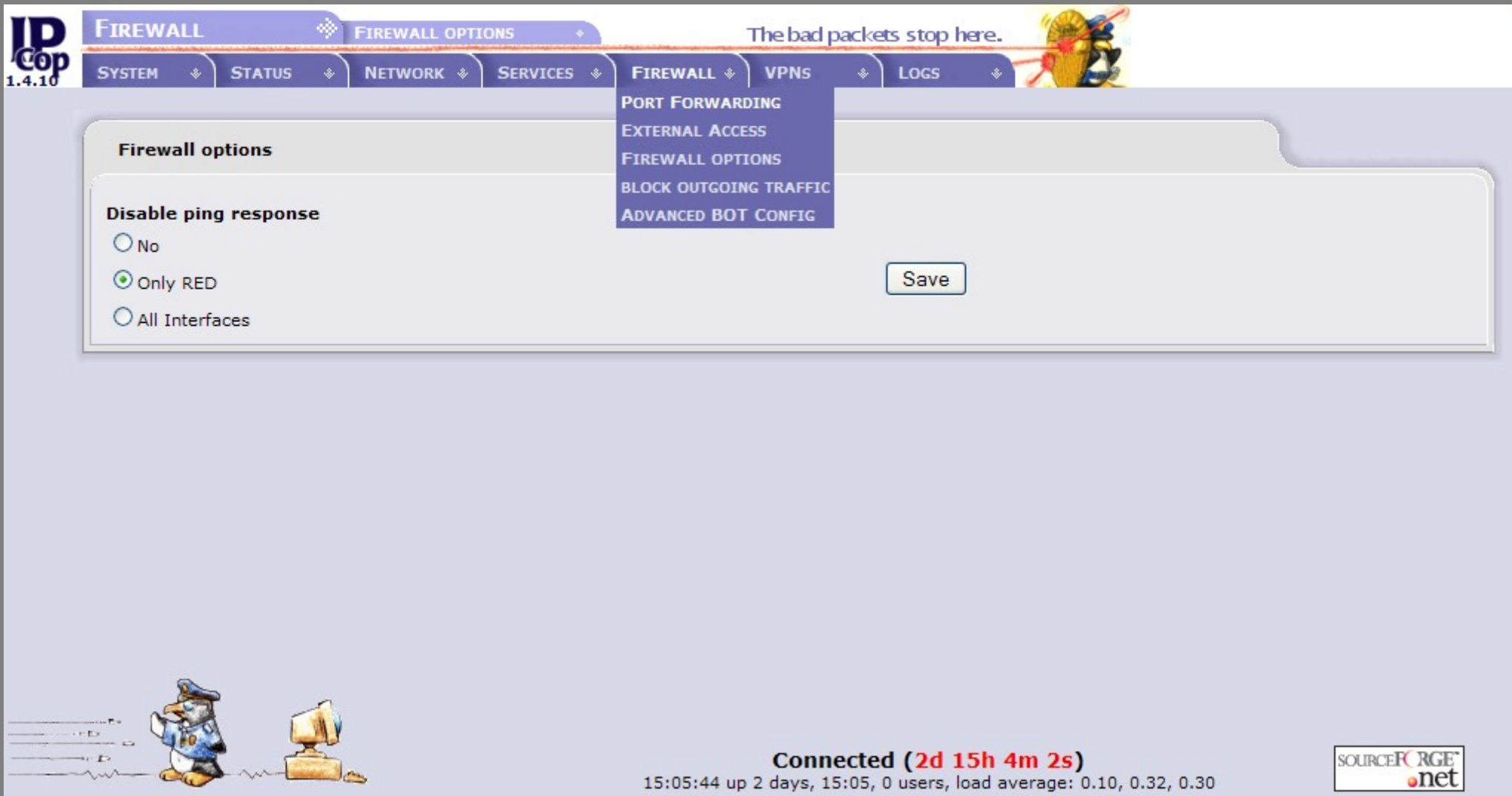
Custom whitelist

Allowed domains (one per line) ●

```
google.com
yahoo.com
```

Allowed URLs (one per line) ●

Firewall Settings



The screenshot shows the IP Cop 1.4.10 web interface. The top navigation bar includes 'FIREWALL', 'SYSTEM', 'STATUS', 'NETWORK', 'SERVICES', 'FIREWALL', 'VPNS', and 'LOGS'. The 'FIREWALL' menu is expanded, showing options: 'PORT FORWARDING', 'EXTERNAL ACCESS', 'FIREWALL OPTIONS', 'BLOCK OUTGOING TRAFFIC', and 'ADVANCED BOT CONFIG'. The 'FIREWALL OPTIONS' sub-page is active, displaying the 'Firewall options' section. Under 'Disable ping response', there are three radio buttons: 'No', 'Only RED' (which is selected), and 'All Interfaces'. A 'Save' button is located to the right of these options. The page header features the slogan 'The bad packets stop here.' and a cartoon character. At the bottom, there is a status bar showing 'Connected (2d 15h 4m 2s)', system uptime '15:05:44 up 2 days, 15:05, 0 users, load average: 0.10, 0.32, 0.30', and the SourceForge.net logo. A cartoon character is also present in the bottom left corner.

Web 2.0 and the Library

- Web 2.0 in a Nutshell
 - "**Web 2.0**" refers to the second generation of web development and web design that facilitates information sharing and collaboration on the World Wide Web.
- Web 2.0 in the Library
 - Wordpress and **Scriblio**
 - MARC module in Drupal
 - Others (Blogger, Joomla, etc.)

Open Source and the Library

- Koha
- Emilda
- PHPMyLibrary
- OpenBiblio
- MARC in Drupal
- Scriblio in Wordpress

Why Open Source?

- Open Source grants FREEDOM
 - Use, Study, Modify, Distribute
- Evolved from Free Software
- COST ???

Wordpress - Scriblio

- **WordPress** is a state-of-the-art publishing platform with a focus on aesthetics, web standards, and usability. WordPress is both free and priceless at the same time. (<http://www.wordpress.org>)
- **Scriblio** (formerly WPopac) is an award winning, free, open source CMS and OPAC with faceted searching and browsing features based on WordPress. Scriblio is a project of Plymouth State University, supported in part by the Andrew W. Mellon Foundation.

Who are using WP-Scriblio?

- Lamson Library, of Plymouth State University
- Cook Memorial Library, in Tamworth New Hampshire (our public library development partner)
- Beyond Brown Paper, an archive of photos from the Brown Manufacturing Company in northern New Hampshire
- Boston University School of Theology's History of Missiology collection
- Hong Kong University of Science and Technology

Now, let's get our hands dirty...