

IPCop + Cop+ (DansGuardian)

Created October 12, 2006
by Bruce A. Westbrook

Revisions:

Introduction

This document describes the step by step process of installing and configuring IPCop firewall with Cop+ for proxying & URL filtering. Cop+ uses the DansGuardian and combines GUI controls for the DansGuardian with automatic blacklist updates and optional Squid authentication.

For the purposes of these procedures, we are installing IPCop to be used as a content filtering server for an internal network in conjunction with another firewall. IPCop will be placed between the inside network and the Internet firewall.

There is also a section detailing how to use IPCop as a proxy on the internal network and routing back to the internal firewall, without any network segmentation.

Useful Websites:

Home

<http://ipcop.org/index.php>

Install and Configure:

http://www.howtoforge.net/perfect_linux_firewall_ipcop

http://www.howtoforge.com/perfect_linux_firewall_ipcop_p2

Install Add-ons Server

<http://firewalladdons.sourceforge.net/index.html>

Install DansGuardian

<http://home.earthlink.net/~copplus/install.html>

Install IPCop

√	Description
Create ISO	Go to http://ipcop.org and download the ISO image for IPCop. For these installation and configuration procedures we are using version 1.4.10. Other versions may obviously have differences in their installation, configuration and use.
Boot with CD	Once you've downloaded and burned your CD, boot with it in the PC of your choice. Your PC MUST have at least 2 NICs to install and use IPCop properly.

	Install	<ol style="list-style-type: none">1. At the initial boot prompt, [ENTER]2. Select your Language, OK3. At the Welcome screen, OK4. For Installation Media, select CDROM5. Your CD is already in the drive (you booted off it), so just OK6. Partitioning explanation, OK7. When prompted to insert a floppy with an IPCop system configuration, select Skip8. You will now be prompted to Configure Networking for the GREEN interface. This interface is for your inside trusted network. Select Probe9. The installation will select the first NIC it finds as your GREEN interface, OK10. Set your inside IP address and mask for this NIC, OK11. The initial installation process will complete. Remove the CD and select OK12. Select your keyboard mapping, OK13. Select your timezone, OK14. Enter a hostname for your box, OK15. Enter a domain name for your box, OK16. ISDN should then be shown as currently disabled. Select Disable ISDN to continue17. You will now be at the Network configuration menu. Select Network configuration type18. Select GREEN + RED19. Back in the Network configuration menu select Drivers and card assignments20. You will be prompted to change the settings. Select OK21. At the next screen select Probe22. You will then receive a list of NICs available for the RED interface. If your box only had two NICs to start with, obviously you'll be given the only remaining NIC. Select it, then OK23. Card is assigned, OK24. Again, back at the Network configuration menu select Address settings25. Select the RED interface26. Set your static IP address and mask, then OK27. At the Address settings menu, select Done28. Once again, back at the Network configuration menu select DNS and Gateway settings29. Set your DNS and network gateway, then OK30. Finally back at the Network configuration menu select Done31. For the DHCP server configuration, leave it as disabled, then OK32. Set a root password (note that you will not see typing or even see the cursor move), OK33. Now set the admin user password, OK34. Setup is now complete! Select OK to reboot
--	----------------	--

Configure IPCop Basics

√	Description	
	Login	<p>Now that your systems is setup and running (did you hear the cool little beeps when it booted? :) you perform all of your administration from the web interface.</p> <ol style="list-style-type: none"> 1. To login, open a web browser on a machine located on the inside interface's network and go to https://ipcop_ip_address:445 2. You will be prompted about the SSL certificate since it's a self-signed cert. Accept it permanently (varies depending on your browser). 3. The IPCop interface will come up. Click Connect. The authentication is the username admin with the password you created during setup
	SSH	<p>We'll probably want to run this box headless, so for advanced features and functions, such as installing Cop+, we'll want SSH enabled</p> <ol style="list-style-type: none"> 1. Under system, select SSH Access 2. Click to select SSH Access 3. Click save
	Verify Routing	<p>If you did not have your RED interface patched in before you rebooted after setup, you'll need to patch it in now and reboot. To reboot, Under system select shutdown, then click Reboot</p> <p>Verify the box itself can route.</p> <ol style="list-style-type: none"> 1. SSH to your IPCop – note that the SSH port is set to 222 (not 22) by default 2. Login as root 3. Ping your gateway IP address 4. Ping something on the inside by name 5. Ping something on the Internet by name <p>If you have any networking problems, you'll obviously need to resolve these. To check things you can use basic linux commands like</p> <ul style="list-style-type: none"> • ifconfig – check interface IP addresses & masks • route – check the gateway <p>If you need to change any basic settings, like IP addresses, DNS, gateways, etc. you'll need to boot with the installation CD again and reconfigure those settings.</p> <p>Or if you think you know what you're doing ☺ you can edit the /var/ipcop/ethernet/settings file to change IP addresses, DNS, gateway, etc.</p>

	Create Backup of Configuration	<p>Now that we have our basic settings configured and verified, let's backup the configuration.</p> <ol style="list-style-type: none">1. Under system, select Backup2. You can choose to backup to a floppy or locally. For now, we'll just back up locally and then copy them off3. Under Backup Configuration, click Create4. You will now see a Backup Set with today's date & timestamp.5. You will also see both an Encrypted and Unencrypted file with an Export link next to each. Click the Export link for the Unencrypted file and save it to your workstation6. This is the same information that would go onto the backup floppy.
--	---------------------------------------	--

Install Cop+

√		Description
	Install Addons Server	<p>Cop+ uses the Addons Server mod, a mod that allows the easy installation of addons to IPCop.</p> <ol style="list-style-type: none">1. Go to http://firewalladdons.sourceforge.net/index.html and download the current version (these instructions are based on version 2.3). The easiest way I've found to do this is to download the file at your inside workstation, then use the Putty pscp.exe to copy the file to your IPCop box.2. Once you have the file downloaded, place it on your IPCop box in the <code>/root</code> directory3. Login to your IPCop box4. Change to your <code>/root</code> directory <code>cd /root</code>5. Issue the following commands to install the Addons Server v2.3b2: <code>tar -zxvf addons-2.3-CLI-b2.tar.gz -C /</code> <code>cd /addons</code> <code>./addoncfg -i</code>6. Now open your browser and go to your IPCop site (or refresh the page). You'll see a new tab called ADDONS

	Install Cop+	<p>Now that the Addons Server is installed, we can install the Cop+ package.</p> <ol style="list-style-type: none">1. Go to http://home.earthlink.net/~copplus/install.html and download the latest version of Cop+ (these instructions use are based on version 2.1 build 1)2. Again, once you have the file downloaded, place it on your IPCop box in the /root directory3. Login to your IPCop box4. Change to your /root directory <code>cd /root</code>5. Issue the following commands to install Cop+ v2.1 build 1: <code>mkdir /root/copplus</code> <line wrapped> <code>tar -zxvf Copplus-2.1-GUI-b1.tar.gz -C /root/copplus</code> <code>cd /root/copplus</code> <code>./setup</code>6. After the install completes (it will take a few minutes, be patient) refresh your IPCop browser window.7. Under Services, select Proxy8. You should see the that the proxy is both Enabled and Transparent9. Now under Services, select Content Filter10. Here you will see the DansGuardian settings and it should show the service as Running11. Let's download the latest blacklist. Click the Download blacklists now button12. Wait a few minutes and the refresh the browser and/or check the logs under Logs => System Logs13. If you want to track all visited websites, you'll also need to change the default setting that tracks only denied sites. Click the Advanced Settings button, then change the Log Level to 3 = all requests.14. Scroll down and click Save15. Click Return to Configuration16. Click BACK17. Click the button to Restart
	Setup Browsers	<p>You can now use IPCop to perform content filtering. Simply configure your workstation browsers to use the proxy server using the IP address (or name if you configured a host record in your internal DNS properly) and port 8080.</p>

IPCop with One NIC & Internal Routing

√	Description
Overview	<p>So, what if you'd like to use IPCop as a proxy for filtering on your internal network, but you still want to route all traffic out your normal firewall? And, you want to keep IPCop on your internal network without any segmentation – that is, you don't want to have to have GREEN (inside) NIC and a RED (outside) NIC?</p> <p>Well, here's the answer!</p>
Install	<p>During the install at the Network configuration type, you'll want to choose GREEN + Modem/ISDN</p> <p>You can then skip right by all the network settings by clicking Done.</p>
Routing	<p>After you have IPCop installed, you'll need to make a couple changes.</p> <ol style="list-style-type: none">1. First, add your inside gateway. At the command prompt type: <code>route add -net 0.0.0.0 netmask 0.0.0.0 gw IP eth0</code> ...where IP is the IP address of your internal router/firewall/gateway2. Second, configure your nameservers. <code>vim /etc/resolv.conf</code> Add your nameservers in the following format: <code>nameserver 207.169.53.69</code> <code>nameserver 207.169.53.70</code>3. Check your routing/resolution by issuing the command: <code>host www.google.com</code>4. If it resolve, then add your gateway route permanently by editing the /etc/rc.d/rc.local file: <code>vim /etc/rc.d/rc.local</code> Add the same route you entered at the command prompt here: <code>route add -net 0.0.0.0 netmask 0.0.0.0 gw IP eth0</code> ...where IP is the IP address of your internal5. Reboot IPCop and verify again that you can still route & resolve properly: <code>host www.cnn.com</code>
Client	<p>Your clients will be setup the same – just point them to the IPCop as their proxy on port 8080. Try one and see!</p>