iSentryIII Content Filtering Appliance

iSentry III Appliance
Administration Manual

REV 2.1

July 31, 2010

This guide is to be used for additional feature setup after the unit has been installed and proper operation has been confirmed. Begin this section by returning to the Webmin page previously used: **Webmin/Others/iSentryIII**

CAUTION: Under no circumstance should there be changes made to any of the pages which are accessible by clicking on the word Edit on the right side of this page. All changes made to any of the Editors below become active after clicking "Save" at the bottom of each page.

GROUP CONFIGURATION EDITOR

Create a new custom command. Create a new file editor.

Command	Description
iSentryII Group Configuration Editor	
Private Filter Editor	
Trusted Filter Editor	
Trusted Only Filter Editor	
Blocking Message Editor	
Proxy Bypass Configuration Editor	
Regular Expression Editor	
Content Filter Group 1 Proxy Log File	
Content Filter Group 2 Proxy Log File	
Content Filter Group 3 Proxy Log File	
Content Filter Group 4 Proxy Log File	
Content Filter Group 5 Proxy Log File	
Setup Script	
Setup Default Addresses	Only Run after editing the Setup script.
Transparent Proxy Bypass Editor	
Name Servers	
Group 5 Blocked Request by Time	
Group 5 Blocked Requests by Site Name	
Group 2 All User Report	
Group 2 blocked by name	
Group 5 All User Report	
DHCP Server Lease Address Range	
Local Startup File (enable dhcp. etc)	rc.local file editor
Firewall Editor	Port Forwarding, VPN's, etc. An error in editing this file can lock yo out of the system.
Restore factory defaults Following this command you must run the LILO command	
LILO ***Run this following the restore to factory defaults action. The system will not reboot if you fail to do this.	

Create a new custom command. Create a new file editor. Create a new SOL command.

Click once on the top line "**iSentryII Group Configuration Editor**". Scroll down to the bottom until you see a group of lines beginning with "Group5ads=No. There are 15 separate categories in each of the five available groups. At this point, all of your workstations should be operating in the transparent mode through the default Group 5. Changing each of these 15 categories is accomplished by making the last word on the line either "Yes" or "NO". Filtering will be immediately

accomplished for all URLs in any category set to “Yes” (turned ON) and will immediately cease for any set to “No” (turned OFF).

At this point **DO NOT** turn on the category “**Trustedonly**” but leave it set at **=No**. This category will be discussed later.

If your configuration includes more groups than the default Group 5 the above will be will be applicable for each of the groups you choose to implement.

PRIVATE FILTER EDITOR

Click once on the line: “**Private Filter Editor**”. This is where you can enter URLs that are to be blocked because of your Internet policy but are not included in the normal blocking list. An example shipped with the unit is: www.killfrog.com . If this URL is entered into a web browser the Blocked Site message will appear. If this entry is deleted, the page will be displayed as normal.

TRUSTED FILTER EDITOR

Click once on the line: “**Trusted Filter Editor**”. This is where URLs can be entered so that they are not ever blocked by the blocking list in any category. For instance, if the category “mail” is turned on (=Yes) but access was to always be allowed to Hotmail, then an entry would be made in this area: hotmail.com. Note: the www. prefix is not used for these entries.

TRUSTED ONLY FILTER EDITOR

Click once on the line: “**Trusted Only Filter Editor**”. This is a special category and must be used with care. This is a very useful tool where only specific, pre-defined sites can be accessed by the workstation users.
Some cautions for using this feature:

1. When “Trusted Only” is turned ON (set =Yes) all other categories must be turned OFF (set =No)
2. To be able to use a particular website with extensions beyond the “root” URL, the “root” URL must also be entered in the “Trusted Only” URLs.
   For example: to use the website www.bartleby.com/1004, the “root” URL of www.bartleby.com must also be entered.

BLOCKING MESSAGE EDITOR

Click once on the line: “Blocking Message Editor”. This is the message that is returned to a user’s screen in the event an attempt is made to access a blocked URL or Regular Expression entry. The message reads:

iSentryII has blocked this site. You can bypass this block if the feature has been turned on by your system administrator and you know the correct login id and password. Contact the help desk or system administrator for the current login id and password. iSentryII

This message is fixed and can only be modified by factory personnel.

This message and the Bypass feature are operational ONLY for users who are assigned to the default Group 5 transparent bridge mode. For others in Groups 1 through 4, the message reads: **[an error occurred while processing this directive].**

PROXY BYPASS CONFIGURATION EDITOR

Click once on the line: “Proxy Bypass Configuration Editor” The contents of this file as shipped are:
LAN_INTERFACE eth0 192.168.2.150 **(NOTE: these values will now be the entered during initial setup)**
WAN_INTERFACE eth1
TIMEOUT 600
PROXY_PORT 8086
AUTH bypass 1sentry2

TIMEOUT is a value in seconds that the bypass feature is available for any workstation in any group which has correctly entered a valid Login and Password. This can be modified by typing in a new timeout, in seconds.
Authorization control of the Bypass feature is done by the two fields after AUTH. The default Login is: **bypass** and the default password is: **1sentry2** . If changes are made to these entries they must be recorded by the administrator as Firewall Servers has **NO** way of extracting them if lost or forgotten.

The Bypass feature is operational only in Group 5. All other groups DO NOT have the ability to Bypass a blocked page.

PROXY_PORT 8086 **should not** be modified without first consulting the factory.

REGULAR EXPRESSION EDITOR

Click one on the line: “Regular Expression Editor”. These are words or phrases that will block any site with the words or phrases in this list. As an example “kkk”. A search in Google for the subject “kkk” will bring up many sites. Those which have the exact phrase “kkk” in the text will be blocked. Any which are found by this search but use only “Klu Klux Klan” will not be blocked.
It is highly recommended that changes/additions to this list be made very judiciously and tested. Inadvertent blocking of acceptable sites can result from indiscriminate incorporation of words/phrases in this editor.

LOG FILES

Log files are kept for each group in their respective folder. These files are current as of the last inquiry. To see additional sites that are logged after opening the file, simply refresh the page.

All inquires which are NOT in Bypass mode are logged for a single group system in "**Content Filter Group 5 Proxy Log File**".
A typical line of data for someone trying to enter Playboy without bypass on would look like:

192.168.2.150 - - [16/Feb/2006:14:15:39 -0600] "GET http://www.playboy.com/ HTTP/1.1" **403** 877 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.0.1) Gecko/20060111 Firefox/1.5.0.1"

The number following HTTP/1.1" "**403**" indicates that this URL was blocked. Had it not been blocked that number would be "**200**"

Logging of URLs accessed by a workstation which has successfully entered into the Bypass mode will be logged in **"Content Filter Group 2 Proxy Log File".**
The URLs that result of being accessed after the Bypass feature is invoked would look like this:

192.168.2.150 - - [16/Feb/2006:14:41:02 -0600] "GET http://www.playboy.com/tools/css/homepage.css HTTP/1.1**" 200** 7591 "http://www.playboy.com/" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.0.1) Gecko/20060111 Firefox/1.5.0.1"

Note that the number **200** now appears in the header.

All subsequent URL requests for the workstation on Bypass will be logged in **Content Filter Group 2 Proxy Log File** until the Bypass Mode has timed out. Then it will return to the Group 5 log file.

Log file rotation is controlled by the size of the log file. The default setting is 10Mbytes. When the log file reaches this size it is automatically compressed and stored in: /var/log directory.

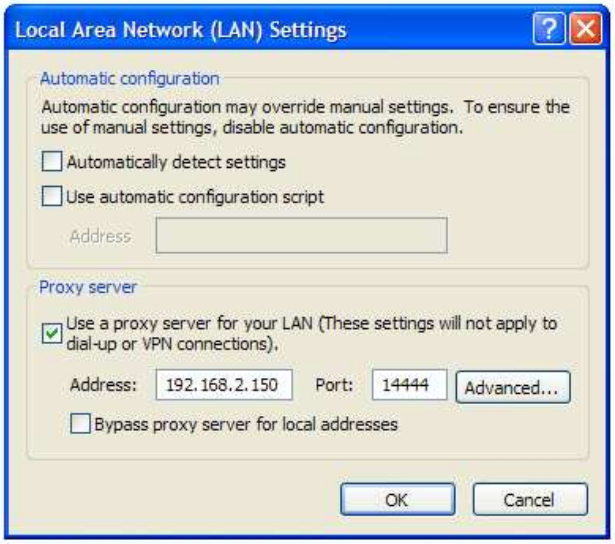
SETUP FOR ADDITIONAL GROUPS

As previously noted, the default for the iSentryIII appliance forces all users through Group 5. All workstations which will use any of the webmail programs i.e.: Hotmail, Yahoo, Gmail, etc and will be sending messages with attachments must be assigned to any group **OTHER** than Group 5. Failure to do so will result in messages hanging or being disconnected by the webmail program without transmission.

Four additional groups can be set up so that different filtering rules will be in affect for each of these groups. This is accomplished by re-routing the normal Port 80 traffic through a specific proxy port address as listed.

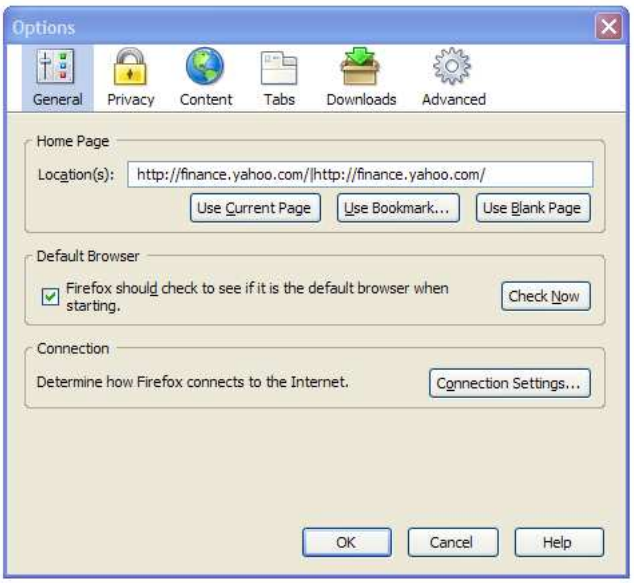
GROUP	PORT ADDRESS
1	14444
2	14446 (do not use if bypass mode in Group5 is in use)
3	14448
4	14450

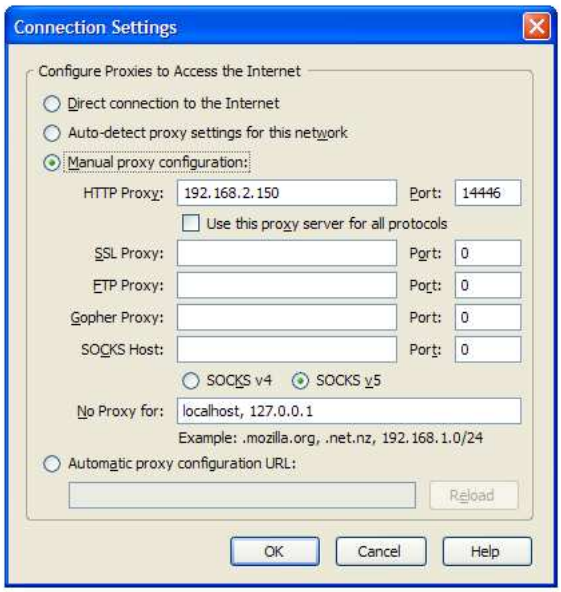
To assign a workstation to one of these groups, information must be entered into the workstation's browser configuration. This example is for workstations using Windows XP. Internet Explorer has a configuration parameter which must be changed by clicking on "**TOOLS**" on the main toolbar. Then open the tab "**Connections**" and then "**LAN Settings**"



Now check the "**Use a proxy server for your LAN**". Now enter the IP Address of the LAN interface of the iSentryIII Appliance in the Address box (for this example it would be 192.168.2.150), and the Port (14444, 14446, 14448 or 14450). The internet traffic for this workstation will be filtered by whatever group settings you have chosen.

The Firefox browser is very similar.





From “**TOOLS**” on the task bar, choose “**General**” and then click once on “**Connection Settings**”. Choose “**Manual proxy configuration**” and input the address you previously chose in the initial setup. For this example it is: 192.168.2.150. Input the port number from the above table corresponding to the group you want the particular workstation to be part of. Click OK and exit back to the main page of the browser.

Other browsers will have similar setup configuration screens.

DHCP Server Lease Address Range

The iSentryIII appliance has its own DHCP server for establishing proper IP addresses for the workstations operating through it. This was also shown in the Quik Start Manual.

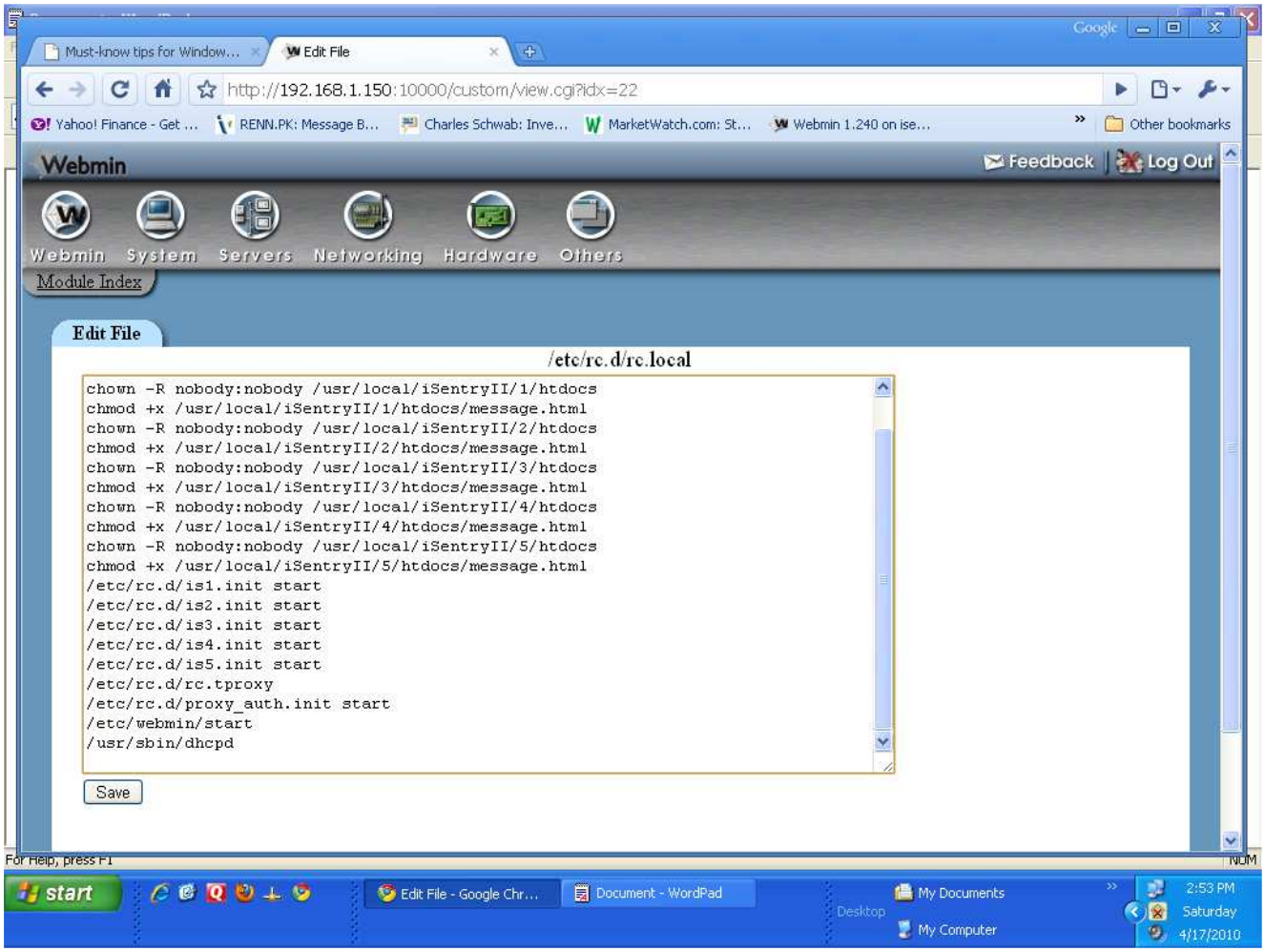
Define DHCP Server Lease Range

Click once on “**DHCP Server Lease Address Range** to open the following page:

Notice that there is a space between the two addresses for “range dynamic-bootp”.
The “default–lease time” is expressed in seconds. The example of 3600 would therefore result in a lease time of 60 minutes.
When completed, click only once on the “Save” Button.

All network devices with fixed or static addresses, such as network printers or network servers, etc, should NOT be operating through the iSentry III appliance but should be attached directly to the LAN.

Local Startup File (enable DHCP etc)



The only editing action required for this item is to be sure that the letter “x” is NOT in front of the last line such as:

x/usr/sbin/dhcpd.

If the letter “x” is present, delete it so that the last line appears as shown above and click the “Save” button once.

Firewall Editor

The iSentryIII appliance has a fully operational IP Tables firewall installed and is operational upon booting the unit. It is designed to provide maximum protection to the workstations operating through the appliance. It is designed to reject all attempts to enter the portion of the LAN occupied behind the iSentryIII appliance.
Modification of the rules for both the firewall and port forwarding must be done only by someone well versed in Linux and IP Tables.

Restore Factory Defaults and LILO

These commands are for resetting the unit to the original factory settings, including all network addresses. The time required for the software to complete the reset is approximately 3 to 5 minutes. No entries should be made from the iSentryIII’s console keyboard nor should the power to the unit be turned off until this operation is complete. Upon completion of the reset, **BEFORE** any other actions are taken, the last entry in the Command page must be clicked, on the work LILO. Failure to do this will result in a corrupted boot file and the unit will be inoperable. To fix this problem, the unit must be returned to the factory and a charge of $150 will be required for repair.

Configuration of the iSentryIII Content Filtering Appliance is now complete. Your unit should perform flawlessly for many years to come.

The unit is bundled with a minimum of one year of bi-weekly updates. To activate this service, email the IP address that is providing internet connection to the iSentry III appliance to: techsupport@firewall-servers.com . If you are not positive what this IP address is, go to any of the workstations attached to the appliance and type in the browser:

http://www.whatismyip.com/ This will return the proper IP address.

For free techsupport during the first 30 days after shipment, please email: techsupport@firewall-servers.com