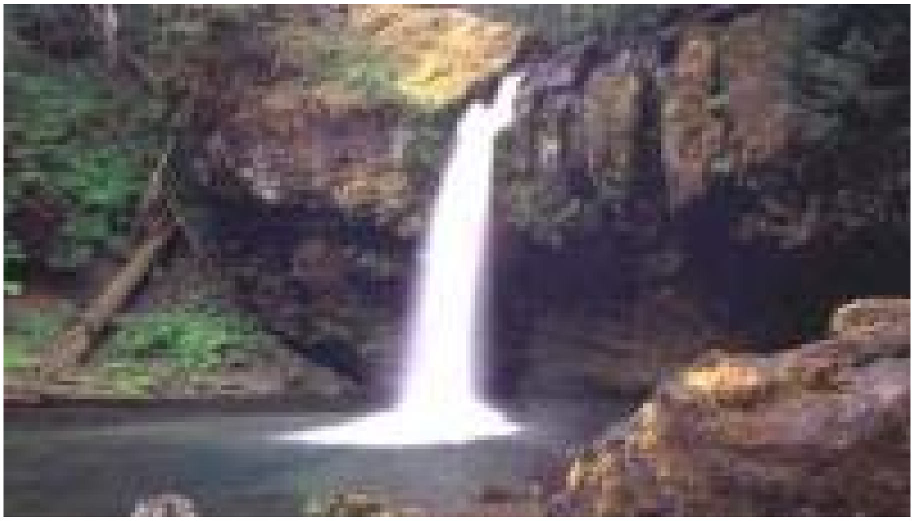


ComSifter

protect web users now!

User Guide

Model CS-1B

Version 1403 July 14, 2008

FCC STATEMENT

This product has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which is found by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

Reorient or relocate the receiving antenna

Increase the separation between the equipment or device

Connect the equipment to an outlet other than the receivers

Consult a dealer or an experienced radio/TV technician for assistance

Table of Contents

Chapter 1

Introduction and Getting Started

ComSifter® stops the pornography, the on-line gambling, the hate sites at the Internet gateway, before the offensive material reaches web users. You don't have to worry about web users surfing the Net. With ComSifter, if they accidentally misspell a word or use a search word that takes them to the "dark side," they will see a friendly message telling them the site has inappropriate content.

Features

ComSifter offers the following features:

- High performance destination based Port Blocker and content filter.
- Stops unauthorized programs from accessing the Internet.
- Stops access to pornography, hate and gambling sites.
- Blocks downloading of harmful and illegal files including mp3 music files.
- Filters networks with hundreds of computers.
- Intelligent filtering with CSphrase™ Filtering Technology is able to filter based on good words and bad words found on a web page.
- 800,000+ site Blacklist updated daily or weekly.
- Built in DHCP server, DNS Forwarding and Caching Proxy.
- Easy to install, no required maintenance.
- Unlimited licensing is standard.

How ComSifter Works

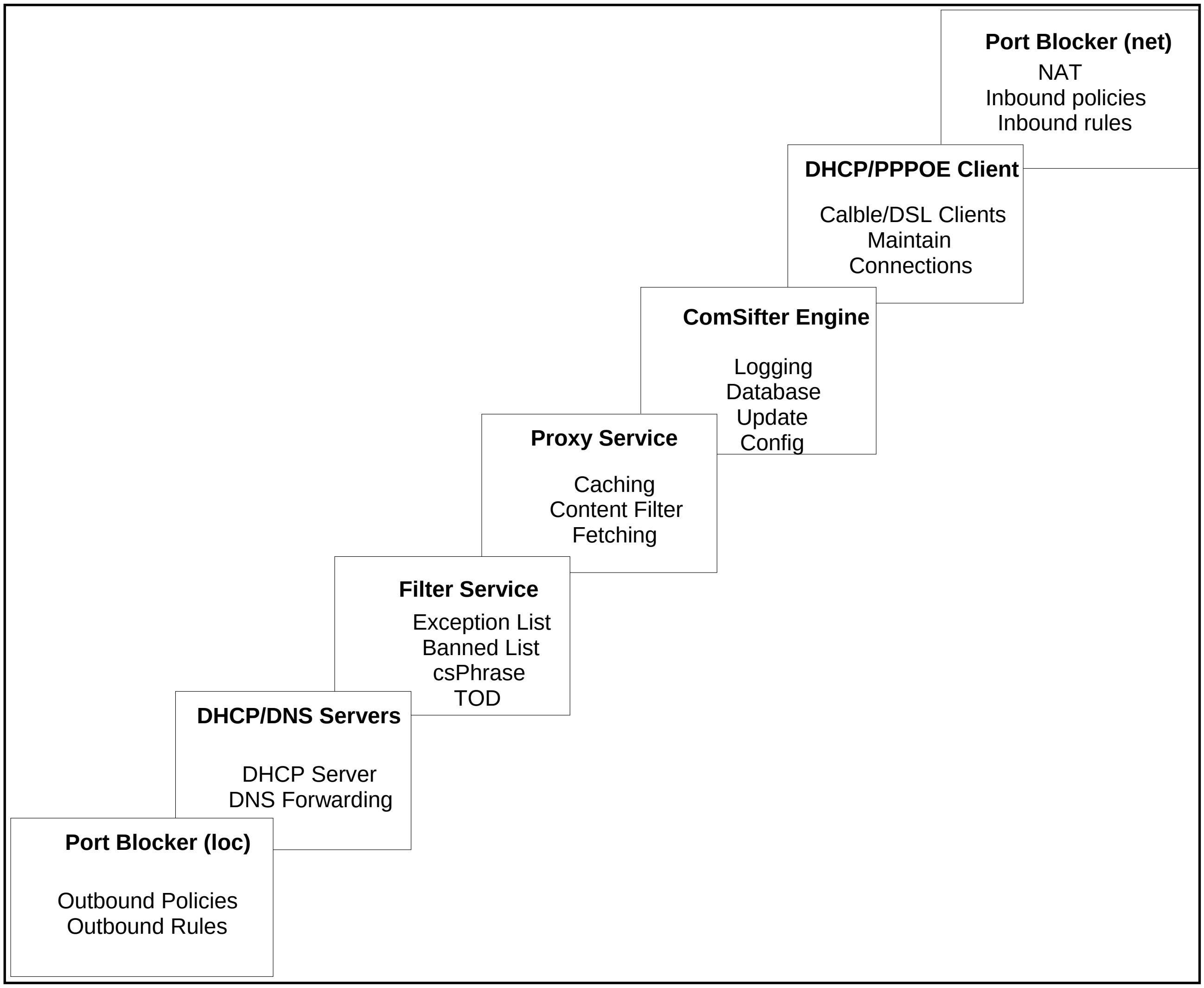


Figure 1-1: ComSifter Architecture

Overview

ComSifter is a Standalone appliance that connects to your internal LAN and offers content filtering and Port Blocking.

Operation

Filtering System

When the user computer accesses a web site, two types of filtering are performed:

First, ComSifter compares the requested site with its blacklist to determine if the address has already been deemed inappropriate. If the site is blacklisted the user will receive a Denied Access Page, and will not be able to view the site.

Second, if the site is not blacklisted, ComSifter will scan every word on the Internet page, using its CSphrase Filtering Technology, looking for words that indicate inappropriate content. The context of these words is then analyzed to determine if the page should be blocked. This greatly reduces the number of false positives while blocking those pages that are offensive. This feature accounts for ComSifter’s remarkable accuracy.

If the content passes through both types of filtering, ComSifter allows the page to be loaded on the user’s computer. If either of the filters disallow, a “Access Denied” page is sent to the user’s computer. All this is done in a fraction of a second, with no delay seen by the user.

Using This Guide

This User Guide is designed for the technical person that will be installing, configuring and operating the ComSifter network content filtering device.

The following list summarizes the chapters and appendixes that follow this chapter.

- Chapter 2, "Installing ComSifter" — describes how to install and physically connect ComSifter to your network.
- Chapter 3, "Configuring ComSifter" — describes how to configure ComSifter. This includes setting up administrators, configuring network and Port Blocker settings and describing maintenance items.
- Chapter 4, "Filter Setup" — describes how to configure the Master Filter and the filter profiles.
- Chapter 5, "Words/Phrases" — describes the configuration of ComSifters CSphrase filter.
- Chapter 6, "ComSifter Operation" — describes the operation of ComSifter.
- Appendix A, "Contact Information" —provides contact information including telephone numbers, address, email and hours of operation.
- Appendix B, "Specifications" — provides technical information about ComSifter.
- Appendix C, "Filter Defaults" — provides default information for the filter profiles.
- Appendix D, "License and Warranty" — provides information about ComSifter's Licensing and Warranty.

Navigating Through This User Guide

This User's Guide contains all the information you need to install, use, and troubleshoot ComSifter. To assist you in navigating through this document, we have added blue-colored hot links to the Table of Contents, index, chapters, and appendixes in this User's Guide. Clicking one of these hot links automatically moves you to that location in this User's Guide. For example, if you click one of the blue-colored chapter or appendix titles in the previous section, you automatically move to the first page in that chapter or appendix.

Conventions in This User's Guide

This User's Guide uses the following conventions:

- "Notes" are information requiring extra attention.
- "Tips" are helpful procedures or shortcuts for simplifying a task.
- "Important" is information that, if not followed, may affect the proper operation of the product.
- "Warning" is information that if not followed or understood, may affect the operation of the product, the operating system or the system configuration.
- "**Bold**" is used to denote an item that is to be clicked or selected.

Note: If you wish to print a hard copy of this guide it has been formatted to fit on standard 8.5 x 11 paper with margins appropriate for use in a three-ring notebook.

Getting Started

Comsift suggests that the following order of installation and configuration is followed.

Pre-install Preparation

1. Have the following information available when installing and configuring ComSifter.

IP ______________________________

(i.e. 192.168.1.9)

External subnet mask ______________________________

(i.e. 255.255.255.0)

Gateway ______________________________

(i.e. 192.168.1.1)

Primary DNS ______________________________

Secondary DNS ______________________________

Installation, Phase 1, Initial Connectivity

1. Physically Install and power up ComSifter as described in Chapter 2, Installing ComSifter. Estimated time, 5 minutes.
2. Configure ComSifter Network Settings using Network Wizards as described in Chapter 3, Configuring ComSifter, Network Wizard. Estimated time, 5 minutes.
3. Test if ComSifter can connect with the Internet by executing the Internet Connections Test described in Chapter 3, Configuring Comsifter, Internet Connection Test. Estimated time 2 minutes.
4. Perform an initial client connectivity test by visiting two or three well known web sites. Estimated time 2 minutes.
5. Change Admin password as described in Chapter 3, Configuring ComSifter, Admin, Comsift Admins, Setting Username and Password. Estimated time, 5 minutes.

Installation, Phase 2, Tuning the Filters

1. Adjust individual Filter Options for your installation as described in Chapter 4, Filter setup.
2. Adjust Words and Phrases for your installation as described in Chapter 5, Words/Phrases.

Installation, Phase 3, Finishing Up

1. Change the Access Denied Page to reflect your message by following the procedure outlined in Chapter 3, Maintenance, Denied Access Page.
2. Set System Time as described in Chapter 3, Maintenance, System Time.
3. Set System Name as described in Chapter 3, Maintenance, System Name.

Chapter 2

Installing ComSifter

In this chapter we will discuss the physical installation of ComSifter and how to connect a browser to ComSifter in preparation for configuration. ComSifter installs in your trusted network the in the same manner as your client computers, as shown in the diagram below.

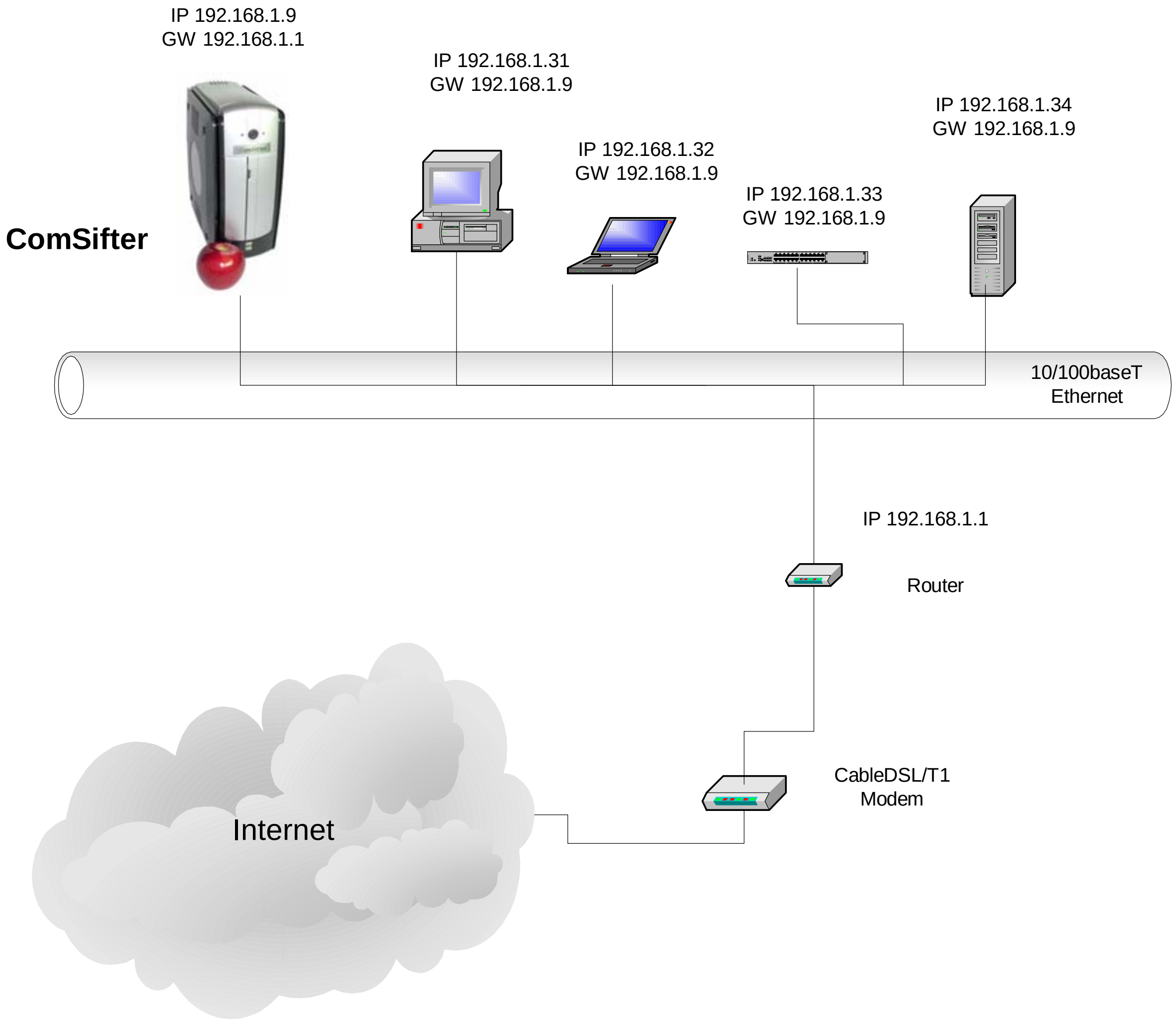


Figure 2-1: ComSifter in the Network

Installation

Security Considerations

ComSifter should be placed in a location that meets the security considerations of your organization.

Location

ComSifter should be installed in a clean, dry location located near your LAN switch or router. The location must be within the operating temperature range of ComSifter (10-35°C or 50-95°F). ComSifter may be placed in the horizontal or vertical position.

AC Power

Connect the supplied AC Power cord to the ComSifter power supply and a properly grounded 115VAC outlet. Connect the power supply output cable to the ComSifter. Although not required, best practices would suggest that ComSifter be placed on a UPS system. This will protect ComSifter from external power fluctuations and allow continued operation in the event of a momentary power outage.

Network Connections

ComSifter requires an Ethernet connection to a port on your internal LAN switch, hub or router.

Power On and Indicator Lights

After all connections are made, ComSifter may be powered on by pressing the power switch on the front of the unit. The green indicator light indicates that ComSifter is powered on and functioning normally. The yellow light indicates disk activity.

Note: After powering on, ComSifter will take approximately two minutes before it is ready for operation.

To power off ComSifter press the power button. All indicator lights will extinguish.

Connecting a browser to ComSifter

Configuration of ComSifter is done by way of TCP/IP using a Browser. Internet Explorer 4 or newer, Netscape 4 or newer, Opera, and Safari have been tested with ComSifter.

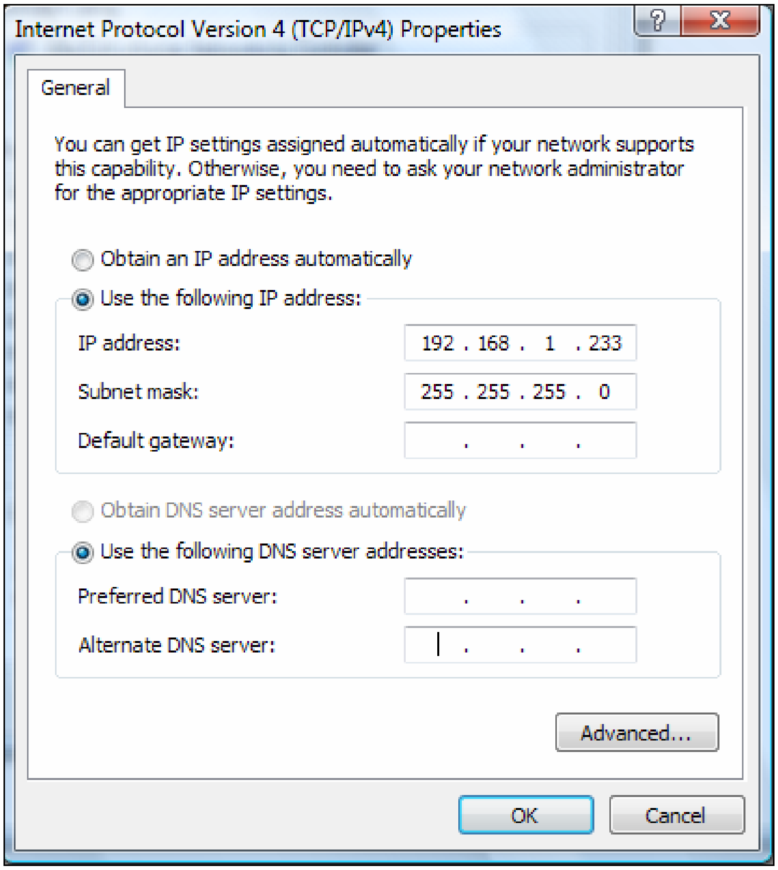
Note: Although ComSifter may be configured from a computer using Windows ME, Windows 2000, Windows XP, Windows Vista, MAC OS X or Linux as its operating system, the preferred arrangement is Windows 2000/XP/Vista using Internet Explorer 5 or above with a screen resolution of 1024 x 768 or greater. Additionally the File Manager and System Time modules require the use of Java™. If you need to obtain Java it is available for download courtesy of Sun Microsystems™ at www.sun.com .Windows 98 and Windows 95 should not be used to configure ComSifter. If you must use Windows 95 or Windows 98 to configure ComSifter please contact Comsift Technical Support. This warning does not apply to ComSifters ability to filter, only to its configuration.

ComSifter is configured from the factory for the 192.168.1.9/255.255.255.0 subnet. If your network is already using this subnet then you are ready to configure ComSifter.

If your network is not using this subnet then you will need to configure the computer that will configure ComSifter to temporarily reflect a static IP on the 192.168.1.x network. This is done as follows:

Windows 2000/XP/Vista

1. Right click **My Network Places** (manage network connections in Vista)
2. Click **Properties** of the Local Area Network you are using.
3. Double click **Internet Protocol**.
4. Set the IP address as shown in Fig 2-2.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 233

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

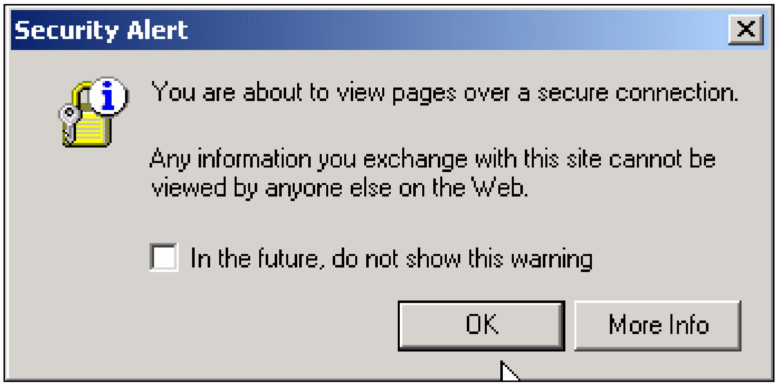
Alternate DNS server: . . .

Figure 2-2: Setting Windows2000/XP/Vista IP Address

Note:	After configuring ComSifter to your network subnet you may then set your computer back to its original network settings.

Making a secure connection

All configuration of ComSifter is done over a secure, encrypted channel. This channel is accessed by pointing your browser to https://192.168.1.9:10000 or the IP you have assigned to ComSifter. Upon a successful connection you will see:



You are about to view pages over a secure connection.

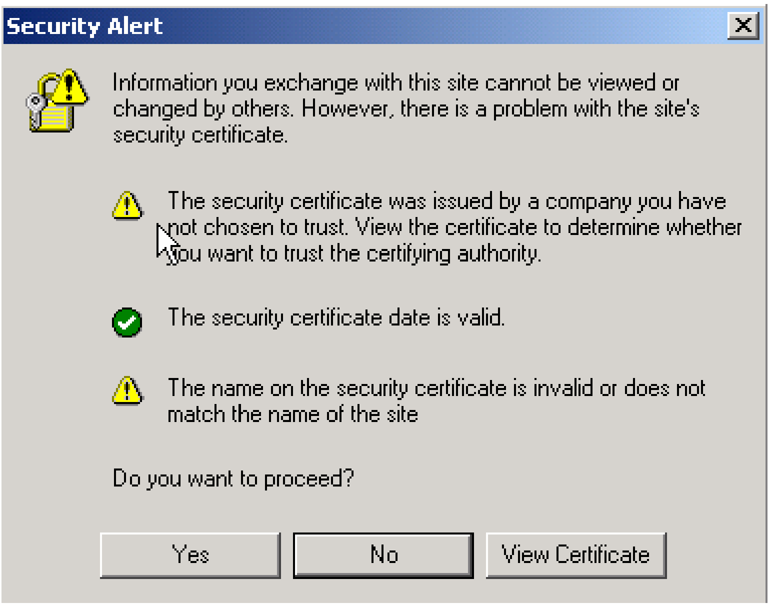
Any information you exchange with this site cannot be viewed by anyone else on the Web.

☐ In the future, do not show this warning

Figure 2-3: Security Alert

Accept this information by clicking **OK**

Upon clicking **OK** you will be presented with ComSifter's self-signed security certificate.



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate date is valid.

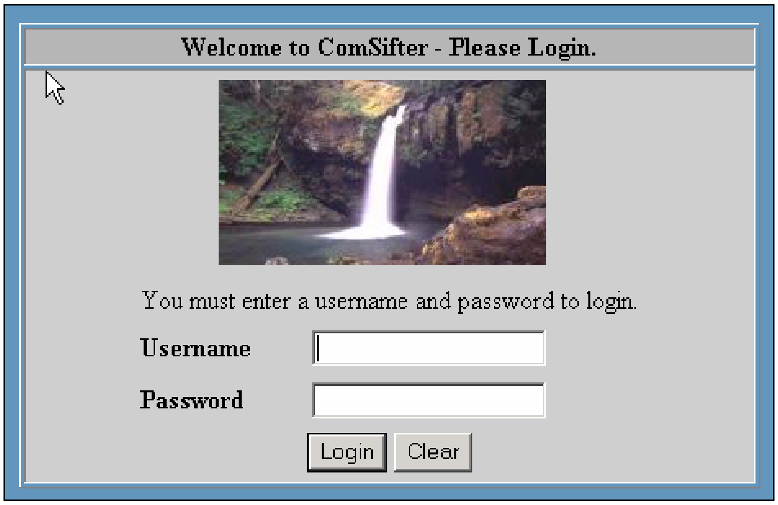
The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

Figure 2-4: Security Certificate

This certificate will allow the communication link to be encrypted. You may click **Yes** to continue or you may install the certificate by clicking **View Certificate** and follow the instructions for installing certificates for you browser.

After accepting the certificate you will be presented with ComSifter's login screen.



Welcome to ComSifter - Please Login.

You must enter a username and password to login.

Username

Password

Figure 2-5: ComSifter Login

You are now ready to configure ComSifter as described in the next chapter.

Chapter 3

Configuring ComSifter

Configuration Overview

ComSifter is designed to be flexible and secure. As an administrator you may define:

- Computer IP’s that may configure ComSifter.
- Admins that may configure ComSifter.
- Assign different responsibilities to each Admin
- Add/Delete users to the user database
- Assign a filter to each user.
- Configure the Filter Groups that are enabled in each filter.
- Perform Maintenance functions.

Admin

Understanding Modules and Categories

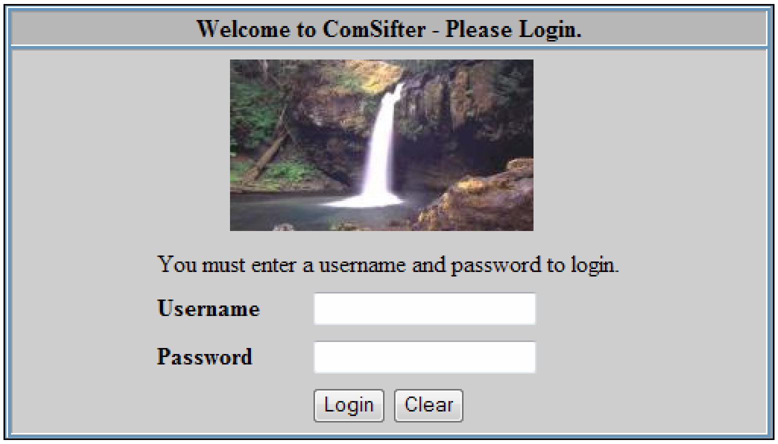
ComSifter uses a module concept to allow certain functions to be performed by different ComSifter Admins. A module may contain one or more “commands” that may be performed by the ComSifter Admin configuring the system. Modules are grouped within Categories. Categories are represented by Icons at the top of each page. There are six categories;

- Admin – this category includes two modules.
- Network – this category includes seven modules.
- Maintenance – this category includes ten modules.
- Filter Setup – this category includes six modules.
- Words/Phrases - this category includes fourteen modules.

Security Configuration

Login

Upon connection to ComSifter you will be presented with a login screen.



Welcome to ComSifter - Please Login.

You must enter a username and password to login.

Figure 3-1: ComSifter Login

The default Username is: admin

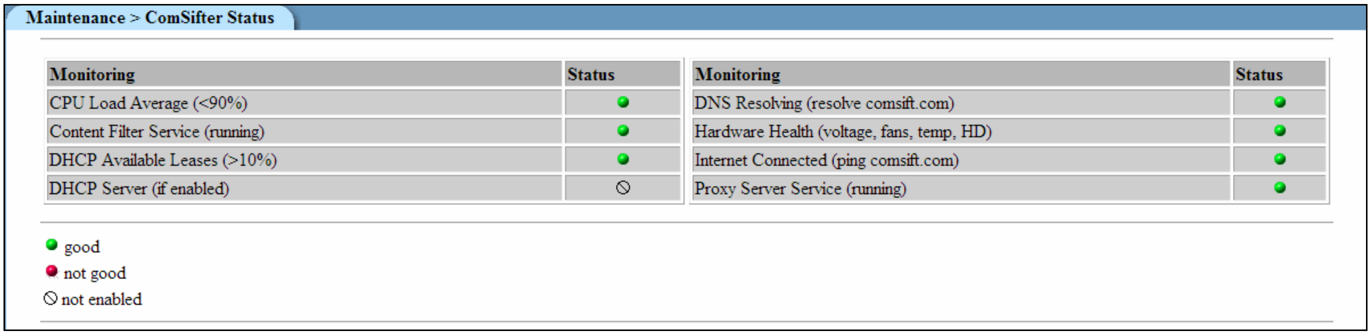
The default Password is: admin

Note: ComSifter will allow five failed login attempts and then will not allow further attempts for 10 minutes.

Note: It is recommended that you immediately change the default password to a password of your own choosing as described below.

Note: Administration of the ComSifter may be performed by only one user at a time. Any subsequent attempts to login to ComSifter by other users will be rejected. If the current user forgets to logout of ComSifter it may take up to 10 minutes for the inactivity timer to logout the previous user.

Upon successful login you will be presented with the initial ComSifter display. Refer to Maintenance > ComSifter Status for detailed information about this display.



Monitoring	Status	Monitoring	Status
CPU Load Average (<90%)	●	DNS Resolving (resolve comsift.com)	●
Content Filter Service (running)	●	Hardware Health (voltage, fans, temp, HD)	●
DHCP Available Leases (>10%)	●	Internet Connected (ping comsift.com)	●
DHCP Server (if enabled)	⦸	Proxy Server Service (running)	●

- ● good
- ● not good
- ⦸ not enabled

Figure 3-2: Initial Display After Login

By clicking on **Admin** you will be presented with the Admin Modules. Clicking on **ComSifter Admins** will bring up the ComSifter Admins menu.

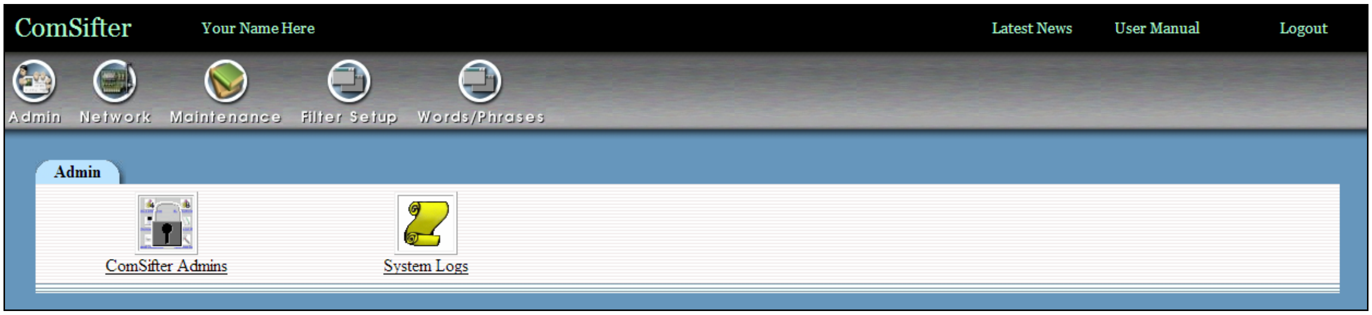
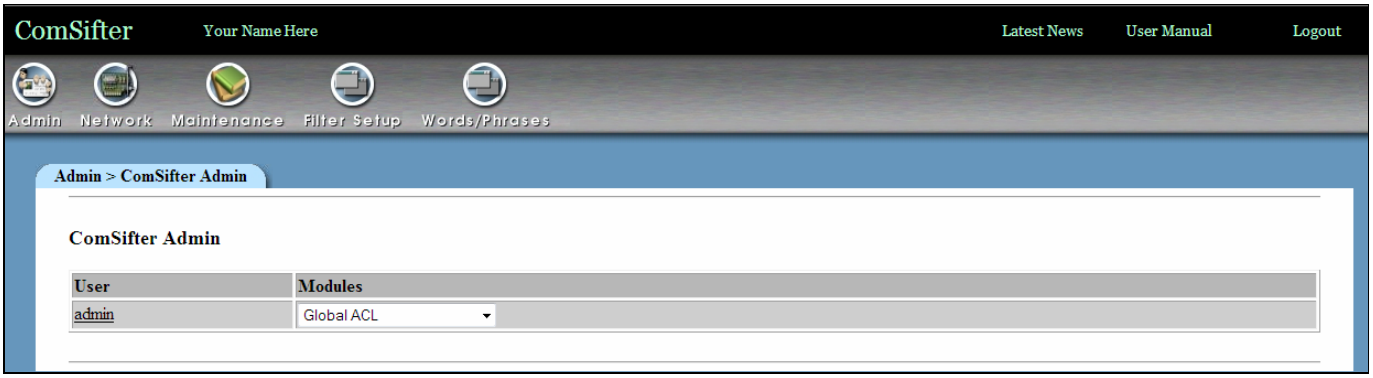


Figure 3-3: Select ComSifter Admins

ComSifter Admins

Overview

ComSifter Admins are personnel that will be configuring ComSifter. Ten ComSifter Admins have been pre-defined. A special ComSifter Admin, “Admin”, is designated as the System Administrator. Admin may edit the username and password of other ComSifter Admins and assign responsibilities to them by assigning Modules.



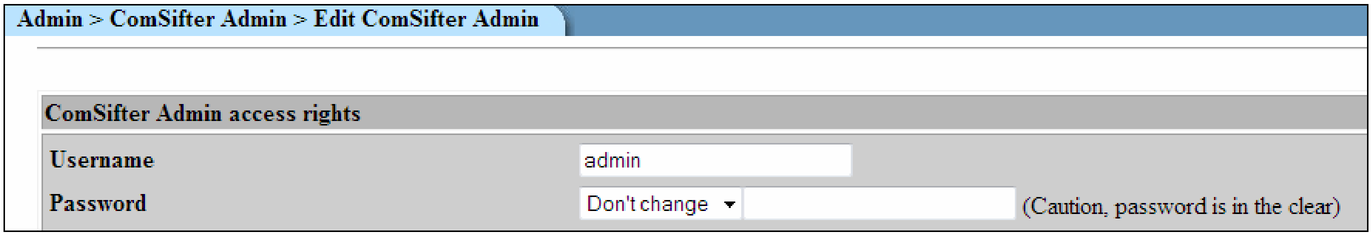
ComSifter Admin

User	Modules
admin	Global ACL

Figure 3-4: ComSifter Admin Screen

Setting the Username and Password

By clicking on **admin** you will be able to change the default password.



ComSifter Admin access rights

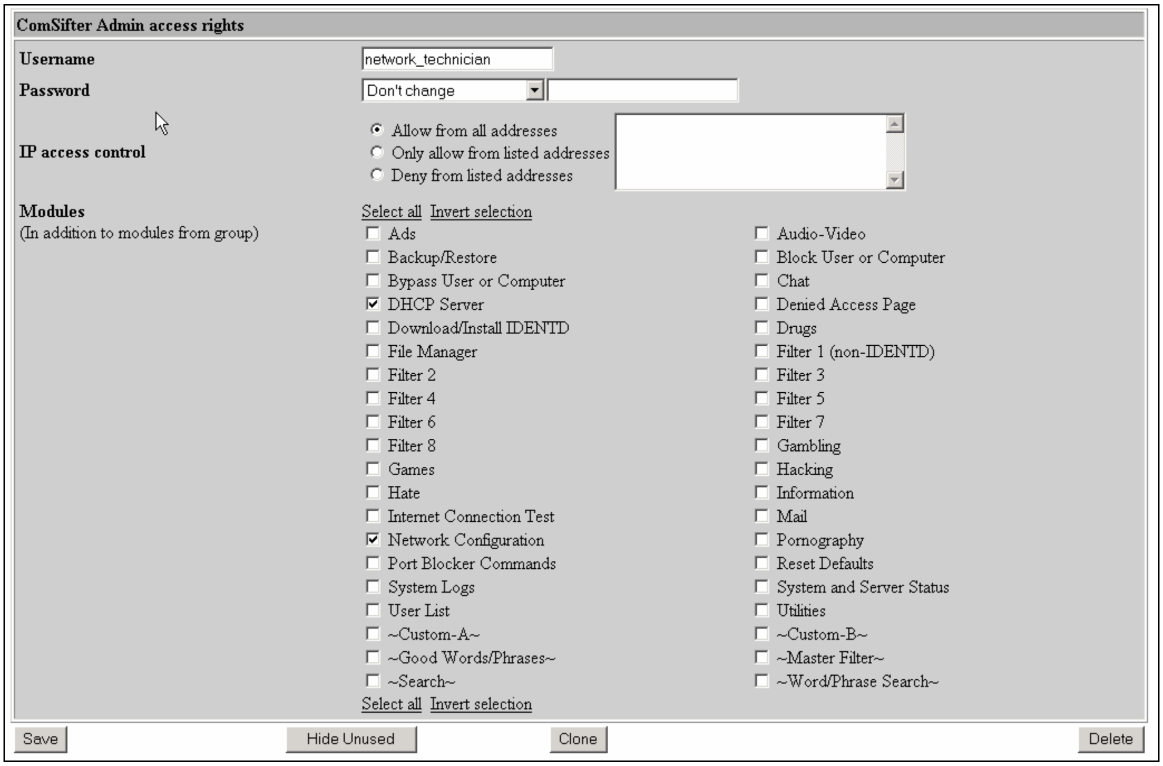
Username: admin

Password: Don't change ▾ (Caution, password is in the clear)

Figure 3-5: Changing Default Password

To change the default password enter the new password, change the Password drop down selection to **set to**, enter the new password, click on **Save.**

Warning: Do not forget your password. You will not be able to configure ComSifter if the password is forgotten. ComSifter does not have any "back-door" or hidden passwords.


ComSifter Admin access rights

Username: network_technician

Password: Don't change ▾

IP access control:
● Allow from all addresses
○ Only allow from listed addresses
○ Deny from listed addresses

Modules
(In addition to modules from group)

- ☐ Ads
- ☐ Audio-Video
- ☐ Backup/Restore
- ☐ Block User or Computer
- ☐ Bypass User or Computer
- ☐ Chat
- ☑ DHCP Server
- ☐ Denied Access Page
- ☐ Download/Install IDENTD
- ☐ Drugs
- ☐ File Manager
- ☐ Filter 1 (non-IDENTD)
- ☐ Filter 2
- ☐ Filter 3
- ☐ Filter 4
- ☐ Filter 5
- ☐ Filter 6
- ☐ Filter 7
- ☐ Filter 8
- ☐ Gambling
- ☐ Games
- ☐ Hacking
- ☐ Hate
- ☐ Information
- ☐ Internet Connection Test
- ☐ Mail
- ☑ Network Configuration
- ☐ Pornography
- ☐ Port Blocker Commands
- ☐ Reset Defaults
- ☐ System Logs
- ☐ System and Server Status
- ☐ User List
- ☐ Utilities
- ☐ ~Custom-A~
- ☐ ~Custom-B~
- ☐ ~Good Words/Phrases~
- ☐ ~Master Filter~
- ☐ ~Search~
- ☐ ~Word/Phrase Search~

Figure 3-6: Assign Module Rights

Access Log

The Access Log records each request to the Internet processed by the Content Filter. The log shows:

- Date - Date and time the event happened.
- User - Username of the user making the request.
- User IP - IP of the computer making the request.
- Status - The result of the request
- Domain/URL - The Domain/URL address requested.
- Bytes DL - Number of bytes downloaded.
- Location - Source of information (primary/secondary).

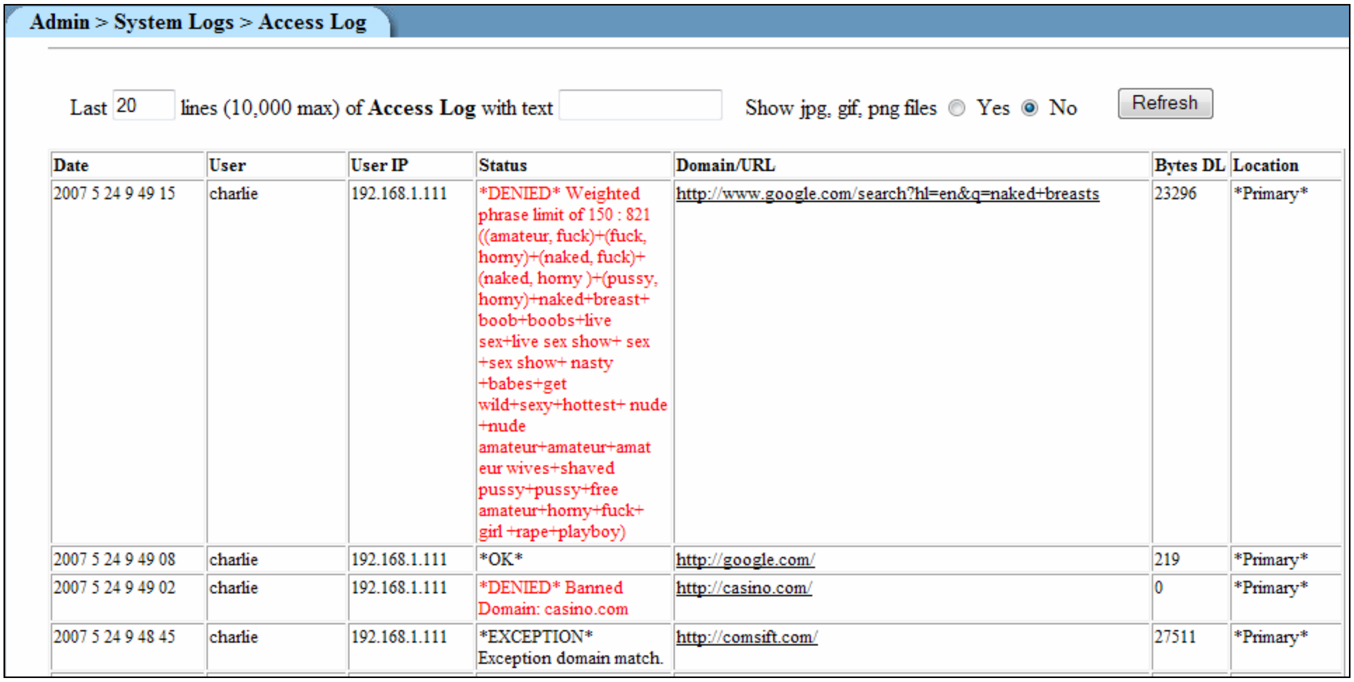
Status Messages

Possible Status Messages in the log are:

- *OK* - The Content Filter found the content acceptable.
- *DENIED* Banned Domain: - the domain is listed in one of the Blacklist Domain Filter Groups or is in the Banned Domain List.
- *DENIED* Banned URL - the URL is listed in one of the Blacklist URL Filter Groups or is in the Banned URL List.
- *DENIED* Banned Extension - the extension is listed in one of the Banned Extension Lists.
- *DENIED* Banned MIME type - the MIME type is listed in one of the Banned MIME Type Lists.
- *DENIED* Weighted phrase limit of xxx : yyy – the word/phrase is listed in one of the Weighted CSphrase Filter Groups.
- *DENIED* Per the Hours of Operation schedule the Internet is disabled – The filter the User is mapped to is not allowing Internet Access due to Hours of Operation scheduling.
- * EXCEPTION * Exception Word Match– the word is listed in one of the Good Words/Phrases CSphrase Filter Group
- * EXCEPTION * Exception Domain Match – The domain is listed in one of the Full Exception Domain Lists.
- *EXCEPTION* Exception URL Match - The URL is listed in one of the Full Exception URL Lists.

In the following example we see that user Charlie, at IP 192.168.1.111;

- Accessed “comsift.com”. This domain was in the Full Exception list of the filter he was connected to and thus allowed him full access to the site regardless of the content.
- Then he tried to access “casino.com”. This site was in the Blacklist of the filter he was connected to and thus he was *DENIED* from viewing the site.
- Next Charlie tried a Google search for “naked breasts”. This search exceeded the Sensitivity Level for his filter and he was *DENIED* from viewing the site. The entry in the log shows the Sensitivity Level for his filter was 150 and the actual calculated level was 821.



Admin > System Logs > Access Log

Last 20 lines (10,000 max) of **Access Log** with text Show jpg, gif, png files ○ Yes ● No

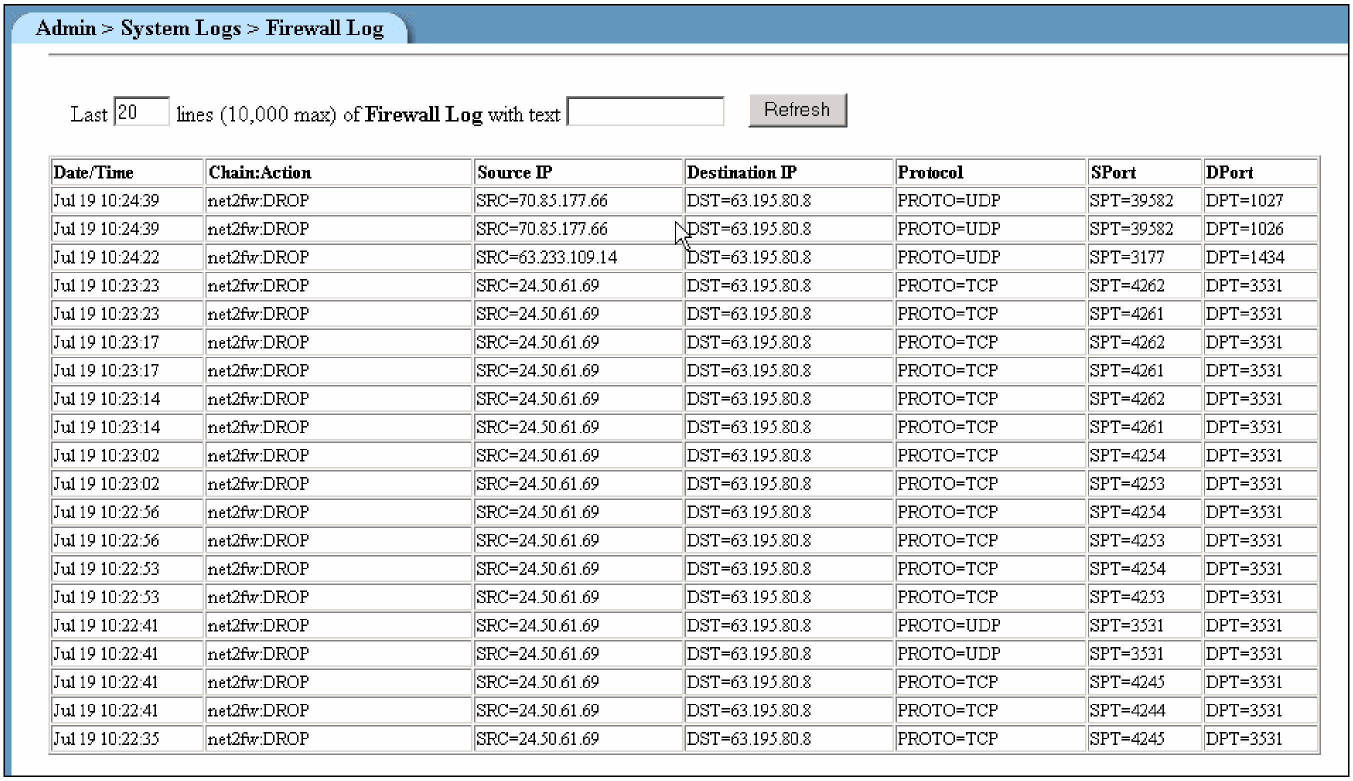
Date	User	User IP	Status	Domain/URL	Bytes DL	Location
2007 5 24 9 49 15	charlie	192.168.1.111	*DENIED* Weighted phrase limit of 150 : 821 ((amateur, fuck)+(fuck, horny)+(naked, fuck)+(naked, horny)+(pussy, horny)+naked+breast+boob+boobs+live sex+live sex show+ sex +sex show+ nasty +babes+get wild+sexy+hottest+ nude +nude amateur+amateur+amateur wives+shaved pussy+pussy+free amateur+horny+fuck+girl +rape+playboy)	http://www.google.com/search?hl=en&q=naked+breasts	23296	*Primary*
2007 5 24 9 49 08	charlie	192.168.1.111	*OK*	http://google.com/	219	*Primary*
2007 5 24 9 49 02	charlie	192.168.1.111	*DENIED* Banned Domain: casino.com	http://casino.com/	0	*Primary*
2007 5 24 9 48 45	charlie	192.168.1.111	*EXCEPTION* Exception domain match.	http://comsift.com/	27511	*Primary*

Figure 3-7: Access Log

Port Blocker

The Port Blocker Log shows all access to the Port Blocker from inside and outside of the local network and is dependent upon the logging settings that were defined when setting up the Port Blocker.

Note: The CS-1B only shows the Port Blocker entries for the local machine.


Admin > System Logs > Firewall Log
Last 20 lines (10,000 max) of **Firewall Log** with text
Refresh

Date/Time	Chain:Action	Source IP	Destination IP	Protocol	SPort	DPort
Jul 19 10:24:39	net2fw:DROP	SRC=70.85.177.66	DST=63.195.80.8	PROTO=UDP	SPT=39582	DPT=1027
Jul 19 10:24:39	net2fw:DROP	SRC=70.85.177.66	DST=63.195.80.8	PROTO=UDP	SPT=39582	DPT=1026
Jul 19 10:24:22	net2fw:DROP	SRC=63.233.109.14	DST=63.195.80.8	PROTO=UDP	SPT=3177	DPT=1434
Jul 19 10:23:23	net2fw:DROP	SRC=24.50.61.69	DST=63.195.80.8	PROTO=TCP	SPT=4262	DPT=3531
Jul 19 10:23:23	net2fw:DROP	SRC=24.50.61.69	DST=63.195.80.8	PROTO=TCP	SPT=4261	DPT=3531
Jul 19 10:23:17	net2fw:DROP	SRC=24.50.61.69	DST=63.195.80.8	PROTO=TCP	SPT=4262	DPT=3531
Jul 19 10:23:17	net2fw:DROP	SRC=24.50.61.69	DST=63.195.80.8	PROTO=TCP	SPT=4261	DPT=3531
Jul 19 10:23:14	net2fw:DROP	SRC=24.50.61.69	DST=63.195.80.8	PROTO=TCP	SPT=4262	DPT=3531
Jul 19 10:23:14	net2fw:DROP	SRC=24.50.61.69	DST=63.195.80.8	PROTO=TCP	SPT=4261	DPT=3531
Jul 19 10:23:02	net2fw:DROP	SRC=24.50.61.69	DST=63.195.80.8	PROTO=TCP	SPT=4254	DPT=3531
Jul 19 10:23:02	net2fw:DROP	SRC=24.50.61.69	DST=63.195.80.8	PROTO=TCP	SPT=4253	DPT=3531
Jul 19 10:22:56	net2fw:DROP	SRC=24.50.61.69	DST=63.195.80.8	PROTO=TCP	SPT=4254	DPT=3531
Jul 19 10:22:56	net2fw:DROP	SRC=24.50.61.69	DST=63.195.80.8	PROTO=TCP	SPT=4253	DPT=3531
Jul 19 10:22:53	net2fw:DROP	SRC=24.50.61.69	DST=63.195.80.8	PROTO=TCP	SPT=4254	DPT=3531
Jul 19 10:22:53	net2fw:DROP	SRC=24.50.61.69	DST=63.195.80.8	PROTO=TCP	SPT=4253	DPT=3531
Jul 19 10:22:41	net2fw:DROP	SRC=24.50.61.69	DST=63.195.80.8	PROTO=UDP	SPT=3531	DPT=3531
Jul 19 10:22:41	net2fw:DROP	SRC=24.50.61.69	DST=63.195.80.8	PROTO=UDP	SPT=3531	DPT=3531
Jul 19 10:22:41	net2fw:DROP	SRC=24.50.61.69	DST=63.195.80.8	PROTO=TCP	SPT=4245	DPT=3531
Jul 19 10:22:41	net2fw:DROP	SRC=24.50.61.69	DST=63.195.80.8	PROTO=TCP	SPT=4244	DPT=3531
Jul 19 10:22:35	net2fw:DROP	SRC=24.50.61.69	DST=63.195.80.8	PROTO=TCP	SPT=4245	DPT=3531

Figure 3-8: Port Blocker Log

The Port Blocker Log shows the following:

Date/Time - the Date/Time the event happened.

Chain/Action – shows the Chain (direction) of the event and what action was taken.

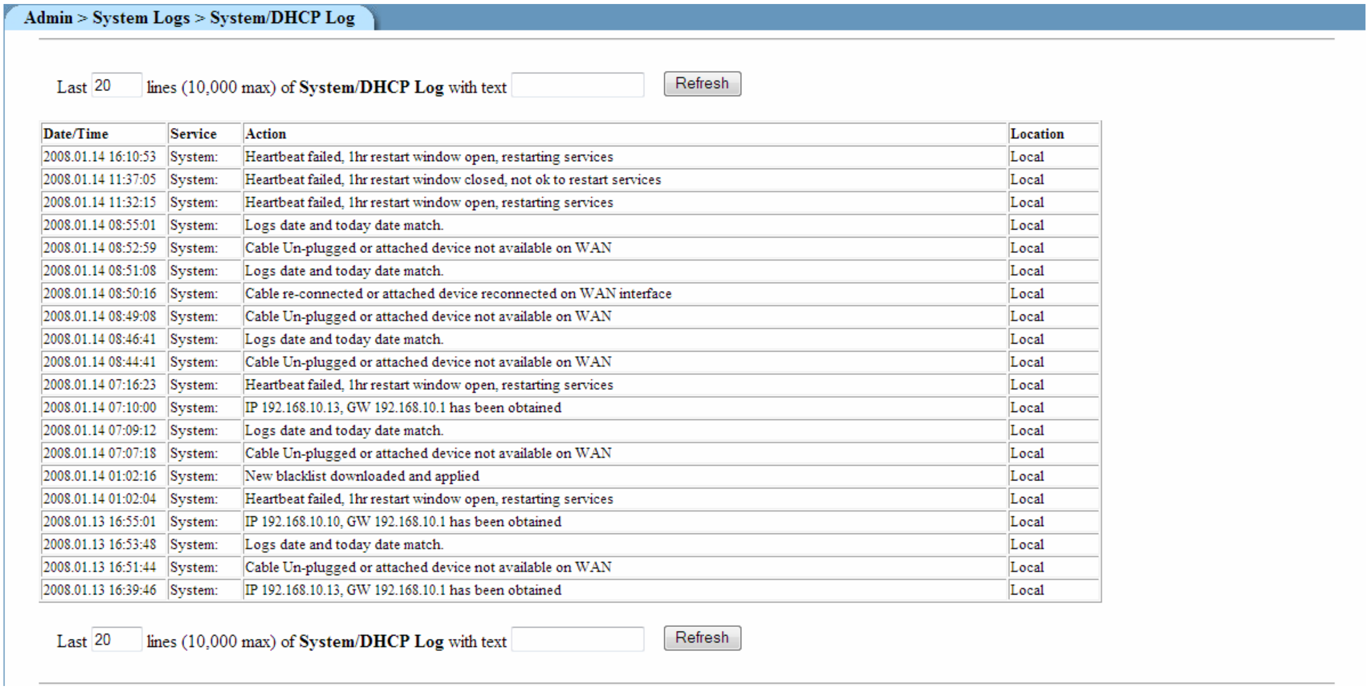
- Possible chains are;
- loc2fw – the packet was traversing from the internal LAN to the ComSifter. Typically these packets will be DHCP (port 66, 67) DNS (port 53) related, i.e. an internal computer is asking ComSifter for DNS or DHCP information
- loc2net – the packet was traversing from the internal LAN to the Internet.
- fw2lan – the packet was traversing from the ComSifter to the LAN
- fw2net – the packet was traversing from the ComSifter to the Internet
- net2fw – the packet was traversing from the Internet to the ComSifter.
- net2lan – the packet was traversing from the Internet to the LAN.
- Possible Actions are;

  a. Accept – a Port Blocker rule was matched and the packet was accepted.

- Drop – a Port Blocker rule was not found or an explicit rule to drop the packet was found. The packet is silently dropped.
- _redirect and _dnat – a matching rule was found to DNAT or Redirect the packet.
- Source IP – The IP the packet originated from.
- Destination IP – The IP the packet is destined for.
- Protocol – The protocol the packet is using.
- Sport – the port the packet originated from.
- DPort – the port the packet is destined for.

DHCP

All DHCP activity events are logged. Messages are self explanatory. In the following example, we see a number of DHCP messages and a number of messages. For debugging purposes you may select **“Show client DHCP messages**”. When selected **“yes”** all client DHCP request will be shown.



Last 20 lines (10,000 max) of **System/DHCP Log** with text

Date/Time	Service	Action	Location
2008.01.14 16:10:53	System:	Heartbeat failed, 1hr restart window open, restarting services	Local
2008.01.14 11:37:05	System:	Heartbeat failed, 1hr restart window closed, not ok to restart services	Local
2008.01.14 11:32:15	System:	Heartbeat failed, 1hr restart window open, restarting services	Local
2008.01.14 08:55:01	System:	Logs date and today date match.	Local
2008.01.14 08:52:59	System:	Cable Un-plugged or attached device not available on WAN	Local
2008.01.14 08:51:08	System:	Logs date and today date match.	Local
2008.01.14 08:50:16	System:	Cable re-connected or attached device reconnected on WAN interface	Local
2008.01.14 08:49:08	System:	Cable Un-plugged or attached device not available on WAN	Local
2008.01.14 08:46:41	System:	Logs date and today date match.	Local
2008.01.14 08:44:41	System:	Cable Un-plugged or attached device not available on WAN	Local
2008.01.14 07:16:23	System:	Heartbeat failed, 1hr restart window open, restarting services	Local
2008.01.14 07:10:00	System:	IP 192.168.10.13, GW 192.168.10.1 has been obtained	Local
2008.01.14 07:09:12	System:	Logs date and today date match.	Local
2008.01.14 07:07:18	System:	Cable Un-plugged or attached device not available on WAN	Local
2008.01.14 01:02:16	System:	New blacklist downloaded and applied	Local
2008.01.14 01:02:04	System:	Heartbeat failed, 1hr restart window open, restarting services	Local
2008.01.13 16:55:01	System:	IP 192.168.10.10, GW 192.168.10.1 has been obtained	Local
2008.01.13 16:53:48	System:	Logs date and today date match.	Local
2008.01.13 16:51:44	System:	Cable Un-plugged or attached device not available on WAN	Local
2008.01.13 16:39:46	System:	IP 192.168.10.13, GW 192.168.10.1 has been obtained	Local

Last 20 lines (10,000 max) of **System/DHCP Log** with text

Figure 3-17: DHCP Log

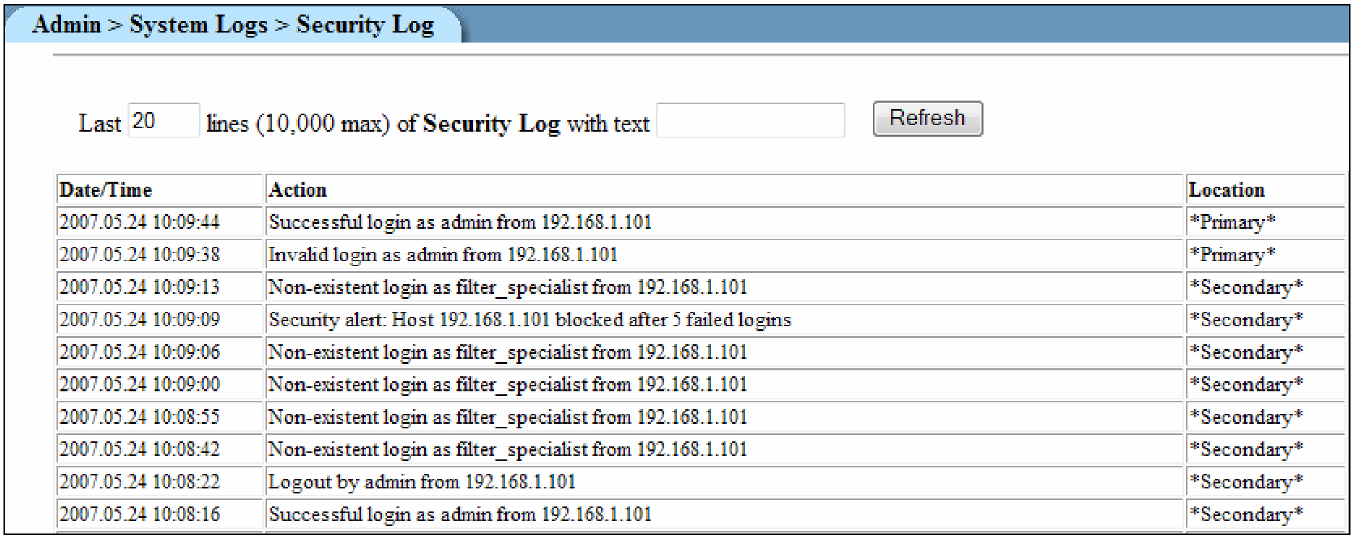
Security Log

Any access by a ComSifter Admin, or any other attempted login to ComSifter, will be logged. In the following example we see that;

- ComSifter Admin “admin” logged into the *Secondary* successfully at 10:08:16.
- Non-existent ComSifter Admin “filter_specialist” tried to login 5 times into the *Secondary* and was locked out on the fifth try.

Note: A lock out lasts for 10 minutes. The lock out is by IP Address. In this example, IP 192.168.1.101 will be locked out for 10 minutes.

- At 10:09:44 ComSifter Admin “admin” tried to log into the *Primary* but forgot their password.

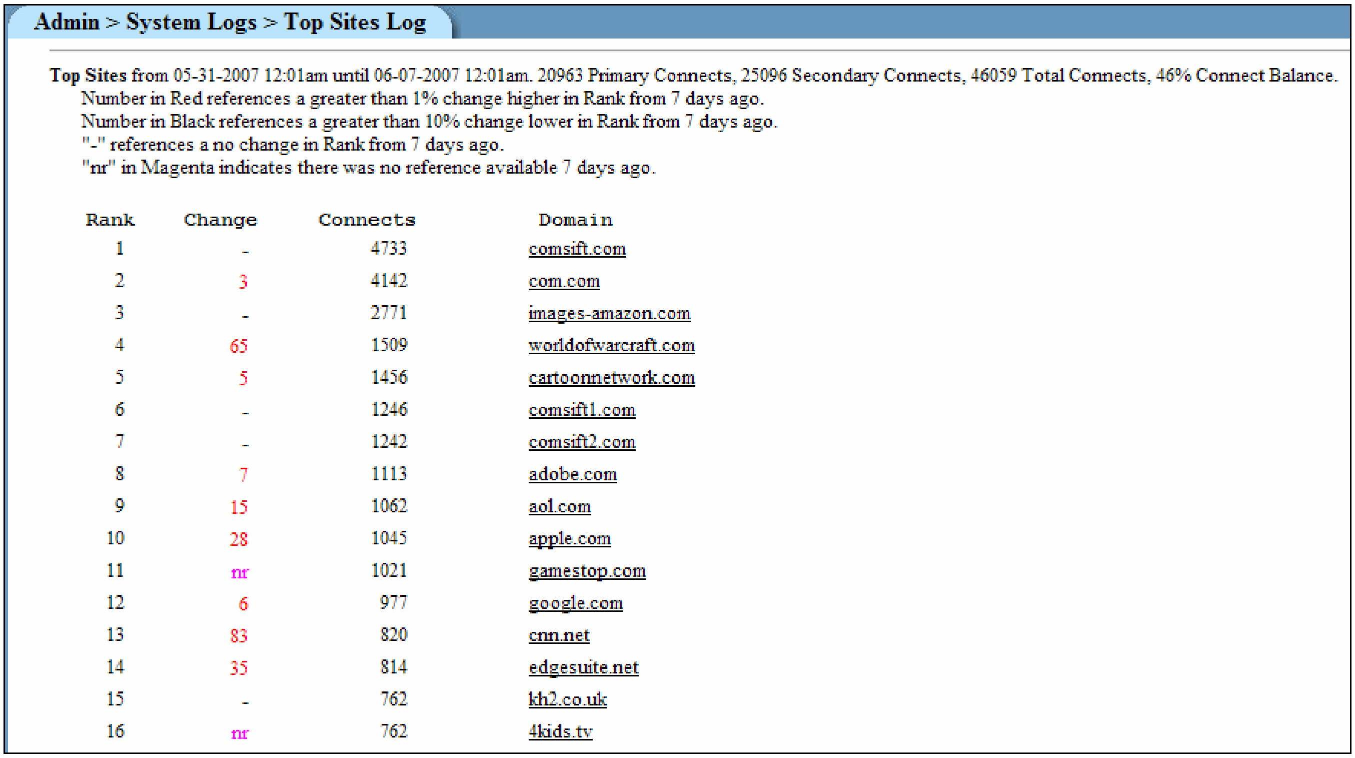


Last 20 lines (10,000 max) of **Security Log** with text

Date/Time	Action	Location
2007.05.24 10:09:44	Successful login as admin from 192.168.1.101	*Primary*
2007.05.24 10:09:38	Invalid login as admin from 192.168.1.101	*Primary*
2007.05.24 10:09:13	Non-existent login as filter_specialist from 192.168.1.101	*Secondary*
2007.05.24 10:09:09	Security alert: Host 192.168.1.101 blocked after 5 failed logins	*Secondary*
2007.05.24 10:09:06	Non-existent login as filter_specialist from 192.168.1.101	*Secondary*
2007.05.24 10:09:00	Non-existent login as filter_specialist from 192.168.1.101	*Secondary*
2007.05.24 10:08:55	Non-existent login as filter_specialist from 192.168.1.101	*Secondary*
2007.05.24 10:08:42	Non-existent login as filter_specialist from 192.168.1.101	*Secondary*
2007.05.24 10:08:22	Logout by admin from 192.168.1.101	*Secondary*
2007.05.24 10:08:16	Successful login as admin from 192.168.1.101	*Secondary*

Figure 3-9: Security Log

Top Sites Log



Top Sites from 05-31-2007 12:01am until 06-07-2007 12:01am. 20963 Primary Connects, 25096 Secondary Connects, 46059 Total Connects, 46% Connect Balance.
Number in Red references a greater than 1% change higher in Rank from 7 days ago.
Number in Black references a greater than 10% change lower in Rank from 7 days ago.
"-" references a no change in Rank from 7 days ago.
"nr" in Magenta indicates there was no reference available 7 days ago.

Rank	Change	Connects	Domain
1	-	4733	comsift.com
2	3	4142	com.com
3	-	2771	images-amazon.com
4	65	1509	worldofwarcraft.com
5	5	1456	cartoonnetwork.com
6	-	1246	comsift1.com
7	-	1242	comsift2.com
8	7	1113	adobe.com
9	15	1062	aol.com
10	28	1045	apple.com
11	nr	1021	gamestop.com
12	6	977	google.com
13	83	820	cnn.net
14	35	814	edgesuite.net
15	-	762	kh2.co.uk
16	nr	762	4kids.tv

Figure 3-10: Top Sites Log

Top Sites shows the most frequently visited domains. Due to the large number of entries the top sites report is created at 12:05AM every morning. It is static until it is recreated the following morning. When the log is created ComSifter converts every entry in its Access to the root Domain, then totals the number of accesses to individual domains.

This log can quickly show the domains that are most frequented by your users. In the above example we see sites that are used for on-line purchasing and children's games being accessed frequently. If accessing these sites is not suitable for your environment then you can take steps to ban these sites.

The Top Site Report shows the following information:

- Rank - Sites with the most connects are shown in descending order. A site must have at least 10 connects to be shown on the Top Site Log.
- Change - Change shows the relative change referenced to 7 days ago. Possible conditions are:
- Number in Red references a greater than 1% change higher in Rank from 7 days ago.
- Number in Black references a greater than 10% change lower in Rank from 7 days ago.
- "-" references a no change in Rank from 7 days ago.
- "nr" in Magenta indicates there was no reference available 7 days ago.
- Connects - This is the total number of connects between the primary and secondary ComSifter's for the listed domain.
- Domain – All connects are stripped to their top level domain. For instance, if you went to "http://comsift.com/servicesintro.htm" it would be stripped to "comsift.com".

In the above example we see a popular game sites ranking has risen 65 places to the number 4 position in the past 7 days. We also see another popular game site has risen to the number 11 position. It has done this in one week as 7 days ago there was no reference. A popular news organization has risen 83 places in the past week to number 13. The rapid rise in use of these sites would signal that maybe a closer look is warranted.

Network

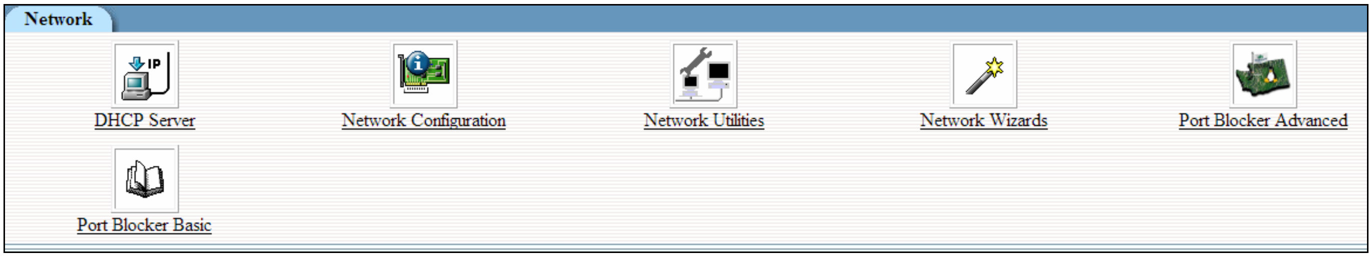


Figure 3-11: Network Category

Network allows configuration of all the parameters in ComSifter that relate to networking. This includes:

- ADSL Client - Allows setting up an ADSL Client (PPPOE). This includes setting login names and password for the account.
- Port Blocker Advanced - Configures, Checks, Starts/Stops, Backup, Restores the Port Blocker.
- Port Blocker Basic - Includes easy to use Templates to configure the Port Blocker.
- Network Configuration - Allows setting the ComSifters IP, Gateway and DNS settings.
- Network Wizard - An easy to use wizard that allows you to easily set up your ComSifter.

Note: It is suggested that you start with the Network Wizard. The Wizard can configure your ComSifter to your proper IP, DNS, set a basic Port Blocker configuration, and optionally enable the DHCP Server.

- DHCP Server - Allows configuration of ComSifters DHCP Server. This includes setting peer relationships, parameters, starting/stopping the DHCP server, DHCP scopes, Client DNS, and Gateway settings.
- QOS – Quality of Services allows certain outbound IPs and port to be prioritized.

Port Blocker Advanced

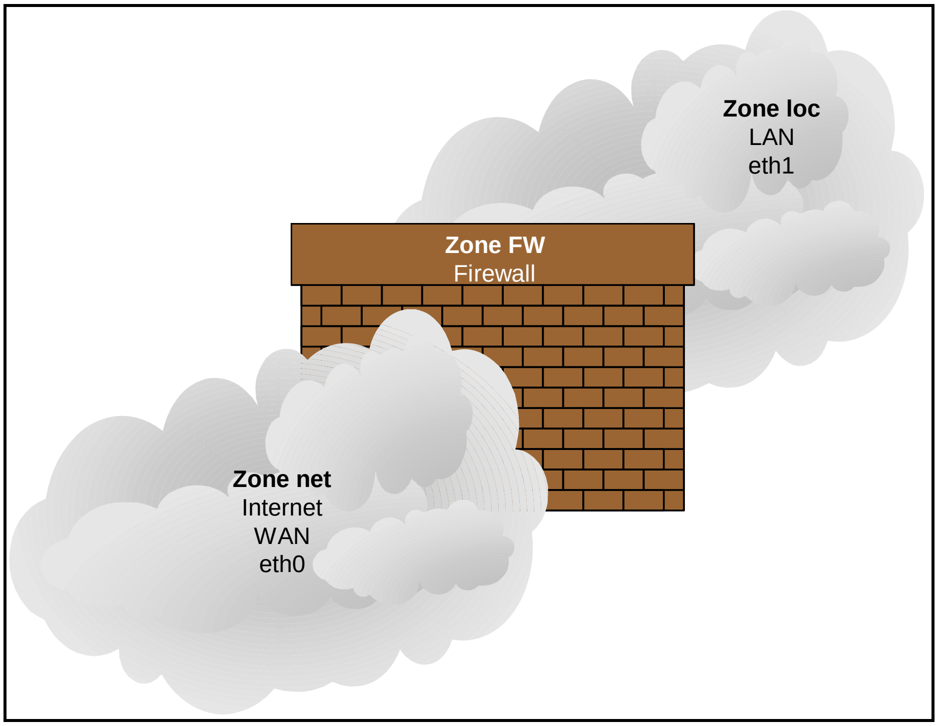


Figure 3-12: Port Blocker Zones

Overview

ComSifters Port Blocker is based on a zone concept. There are three zones.

Loc – addresses on your network (ie 192.168.1.0) or LAN

Net – addresses not on your network .

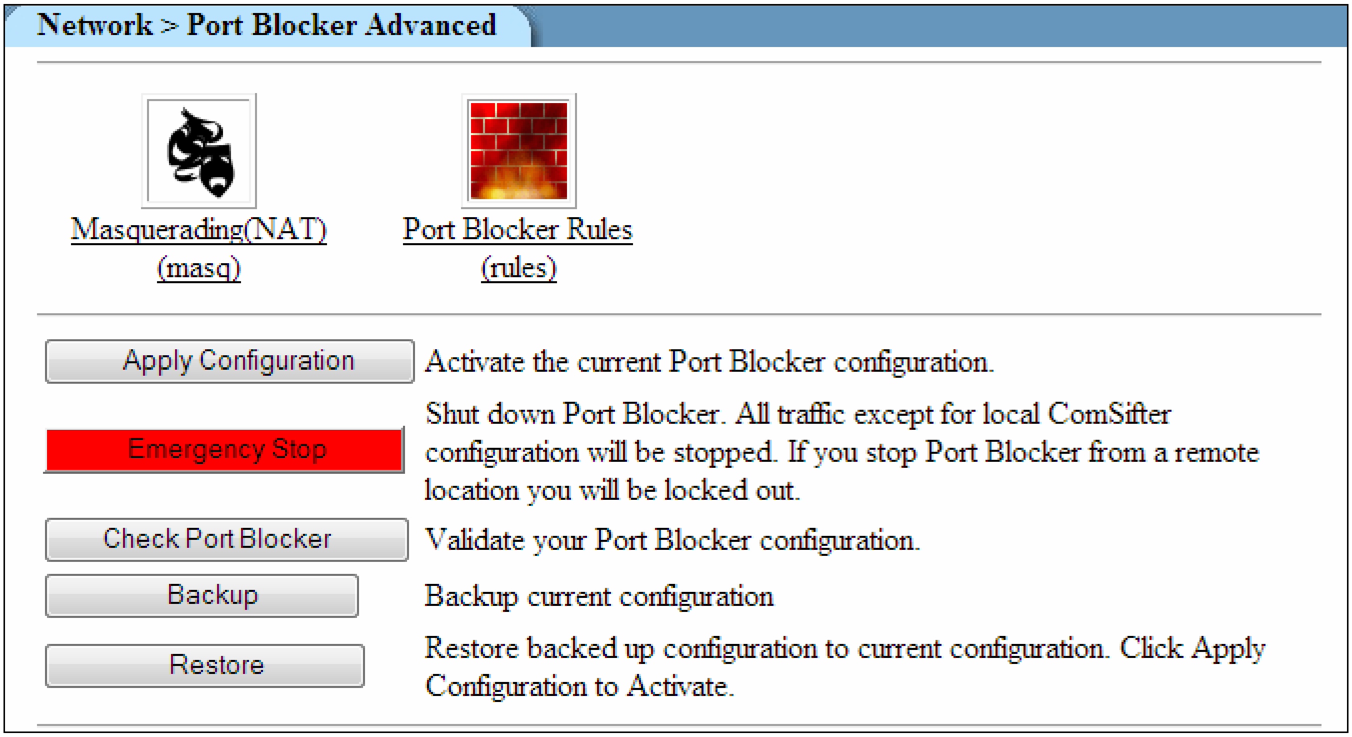
FW - is the Port Blocker itself.

The Port Blockers responsibility is to block all traffic from the Internet to your LAN and vice-versa, unless a rule explicitly allows the traffic to pass.

In this section we will discuss how these rules are created and what rules to use to allow different applications to access the Internet or the LAN.

Upon selecting the **Network** Icon you will be presented with the Port Blocker Advanced screen. From this menu you will be able to:

- Enable/disable Masquerading (NAT).
- Create Port Blocker rules.
- Apply the Port Blocker Configuration.
- Stop the Port Blocker.
- Check a new Port Blocker configuration.
- Backup the existing Port Blocker.
- Restore a previously backed up configuration.

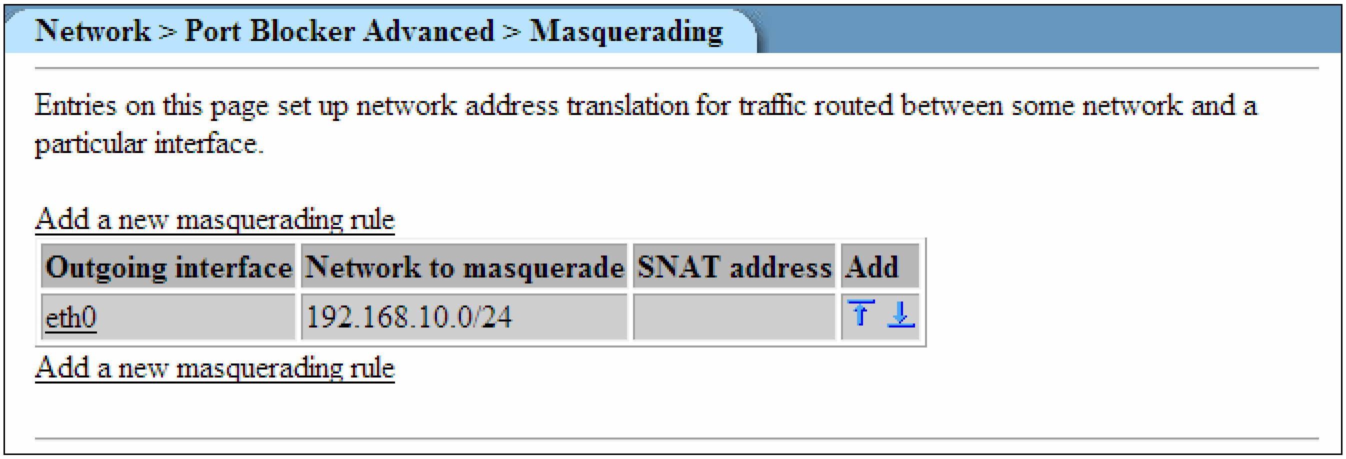


Network > Port Blocker Advanced

Apply Configuration	Activate the current Port Blocker configuration.
Emergency Stop	Shut down Port Blocker. All traffic except for local ComSifter configuration will be stopped. If you stop Port Blocker from a remote location you will be locked out.
Check Port Blocker	Validate your Port Blocker configuration.
Backup	Backup current configuration
Restore	Restore backed up configuration to current configuration. Click Apply Configuration to Activate.

Figure 3-13: Port Blocker Advanced

Masquerading (SNAT)



Network > Port Blocker Advanced > Masquerading

Entries on this page set up network address translation for traffic routed between some network and a particular interface.

Add a new masquerading rule

Outgoing interface	Network to masquerade	SNAT address	Add
eth0	192.168.10.0/24		⤒ ⤓

Add a new masquerading rule

Figure 3-14: Masquerading

Masquerading, or Network Address Translation (NAT), allows the internal network to use a non-routable IP range i.e. 192.168.1.0 and removes the complexity of obtaining and maintaining a public Class A, B or C network.

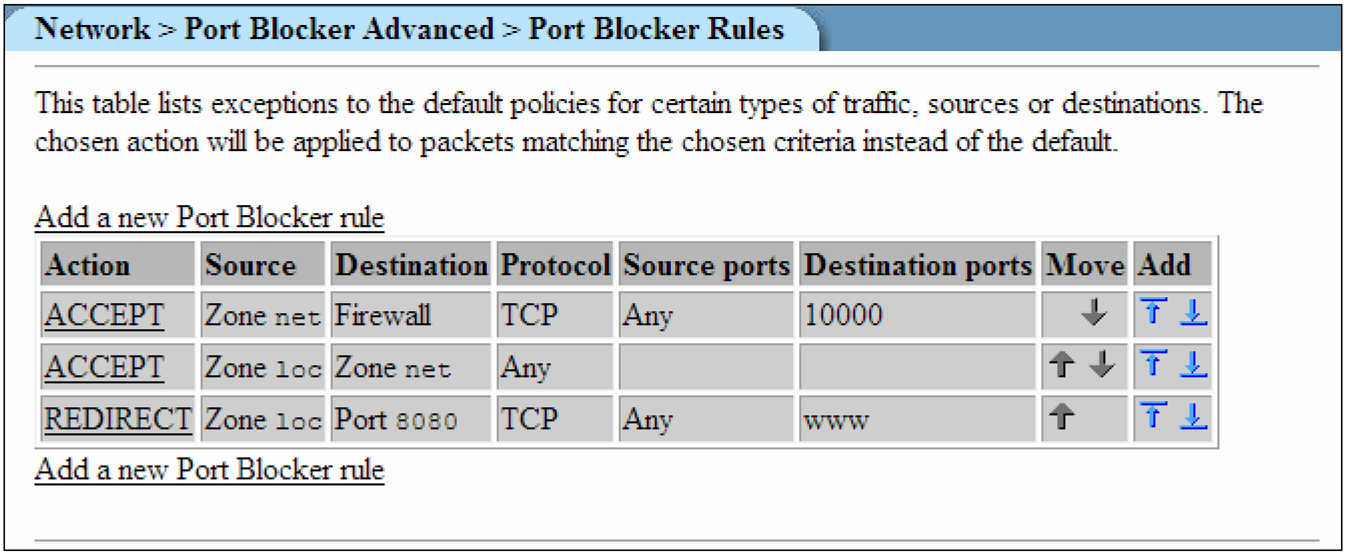
The non-routable range is translated to the external (public) IP. Traffic from the LAN appears to be coming only from the public IP. This is a very secure way of hiding your internal LAN from the Internet (thus the name masquerading). All traffic into and out of the LAN is by way of the public IP.

The above example is default for the ComSifter and should not be changed unless you are using a public Class A, B, or C network. If so you may disable Masquerading by selecting each of the interfaces and deleting the masquerading rule for that interface.

Port Blocker Rules

Port Blocker rules allow ports to be opened or closed. This allows various user applications to either be allowed to communicate over the Internet or be denied access to the Internet. By default ComSifter does not allow any access from the Internet to the Local Area Network (LAN). By default ComSifter will allow access from anywhere on the LAN to the Internet.

Each packet that reaches the Port Blocker will be examined in order by the Port Blocker Rules. If a match is found then the packet will be acted on according to the rule. If a rule is not found the packet will be dropped.



Network > Port Blocker Advanced > Port Blocker Rules

This table lists exceptions to the default policies for certain types of traffic, sources or destinations. The chosen action will be applied to packets matching the chosen criteria instead of the default.

Add a new Port Blocker rule

Action	Source	Destination	Protocol	Source ports	Destination ports	Move	Add
ACCEPT	Zone net	Firewall	TCP	Any	10000	↓	⤒ ⤓
ACCEPT	Zone loc	Zone net	Any			↑ ↓	⤒ ⤓
REDIRECT	Zone loc	Port 8080	TCP	Any	www	↑	⤒ ⤓

Add a new Port Blocker rule

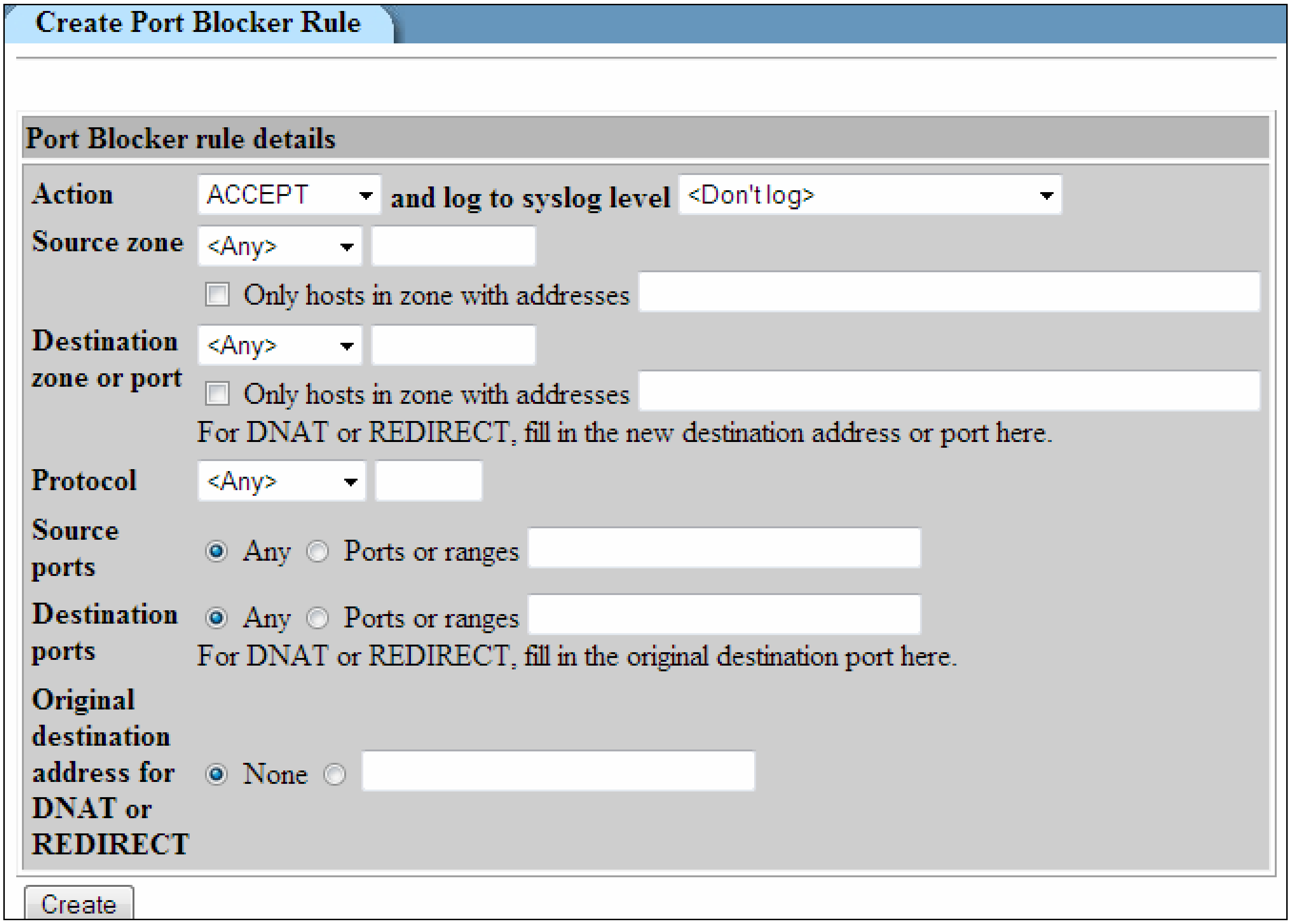
Figure 3-15: Port Blocker Rules

ComSifter includes templates located in Basic Port Blocker that can dramatically limit access from the LAN to the Internet. These templates may be used as a starting point and then modified as needed for your network.

In the preceding example we have a group of rules that:

- The first rule, a REDIRECT, takes any TCP packet from the Local Zone destined for Port 80 and redirects it to Port 8080. This rule is used to intercept LAN traffic that is destined for web sites (port 80) and redirect that traffic to port 8080. ComSifter filtering service is listening on port 8080.
- The next rule, a DNAT, takes any TCP packet from the Internet destined for port 80, and forwards it to an internal IP 192.169.1.11 port 80. A web server is installed at this IP. This may also be called Port Forwarding.
- The next rule, an ACCEPT, allows any traffic from the LAN, not matching the rules above, to access the Internet.
- The next two rules, DNAT, allow traffic from the Internet to access an internal PPTP server located at 192.168.1.7. The first of these rules allows the TCP protocol to connect, the second allows the specialized protocol used by PPTP, type 47 (GRE).
- The last rule, an ACCEPT, allows ping and traceroute requests from the Internet to the ComSifter Port Blocker to be answered.

Create Port Blocker Rules



Create Port Blocker Rule

Port Blocker rule details

Action: ACCEPT and log to syslog level <Don't log>

Source zone: <Any>

☐ Only hosts in zone with addresses

Destination zone or port: <Any>

☐ Only hosts in zone with addresses

For DNAT or REDIRECT, fill in the new destination address or port here.

Protocol: <Any>

Source ports: ● Any ○ Ports or ranges

Destination ports: ● Any ○ Ports or ranges

For DNAT or REDIRECT, fill in the original destination port here.

Original destination address for DNAT or REDIRECT: ● None ○

Figure 3-16: Create Port Blocker Rule

Action

Actions determine what ComSifter will do with a packet that matches a rule. Possible actions are:

Accept – Accept is used when processing a rule from the LAN (loc) to the Internet (net). It may be used to allow packets to traverse ports that have been accepted.

Drop – Drop is used when processing a packet in either direction. The packet will be silently dropped. This is the normal action of all traffic from the Internet (net) to the LAN (loc).

Reject – Reject is used when processing a packet in either direction. A “port closed” response to the packet will be sent. Do not use reject unless you specifically need it.

DNAT – or Port Forwarding, is used to dynamically route packets from the Internet (net) to specific IP’s on the LAN (loc). This action is typically used to allow access to servers running on the LAN.

DNAT- TBD

Redirect – Redirect is used to redirect packets from the LAN to the Internet to another port. An example of this is redirecting all port 80 requests on the ComSifter to port 8080 where filtering takes place.

Continue - TBD

Logging

This setting determines if ComSifter will log the action to the Port Blocker Log. It is suggested that logging be on for any action from the Internet (net) to the LAN (loc) as these actions may point to your Port Blocker being scanned.

It is further suggested that normal port 80 traffic (redirected to 8080) not be logged due to the large volume of data that will be logged from outbound traffic.

Note:	By default, for each log rule, ComSifter limits logging to 300 entries per minute. This is to reduce the chance that a Denial of Service (DOS) attack from the Internet to the Port Blocker will overload the ComSifter, thus denying legitimate traffic.

Source Zone

Source Zone is the zone that the packet will originate from.

This may be further refined by selecting **only hosts in zone with address**. IP’s may be entered in this field. Multiple IP’s may be entered by separating the IP’s by a space. A “not” function may be entered by using the “!” character in front of the 1st IP.

Destination Zone

Destination Zone is the zone that the packet is destined for.

This may be further refined by selecting **only hosts in zone with address**. IP’s may be entered in this field. Multiple IP’s may be entered by separating the IP’s by a space. A “not” function may be entered by using the “!” character in front of the 1st IP.

Protocol

Protocol is the protocol that the packet will use. Valid Protocols are:

- Any
- TCP
- UDP
- ICMP
- 47 (GRE)

Source Ports

Source Port is the port that the packet will originate from.

Destination Ports

Destination Port is the port that the packet is destined for.

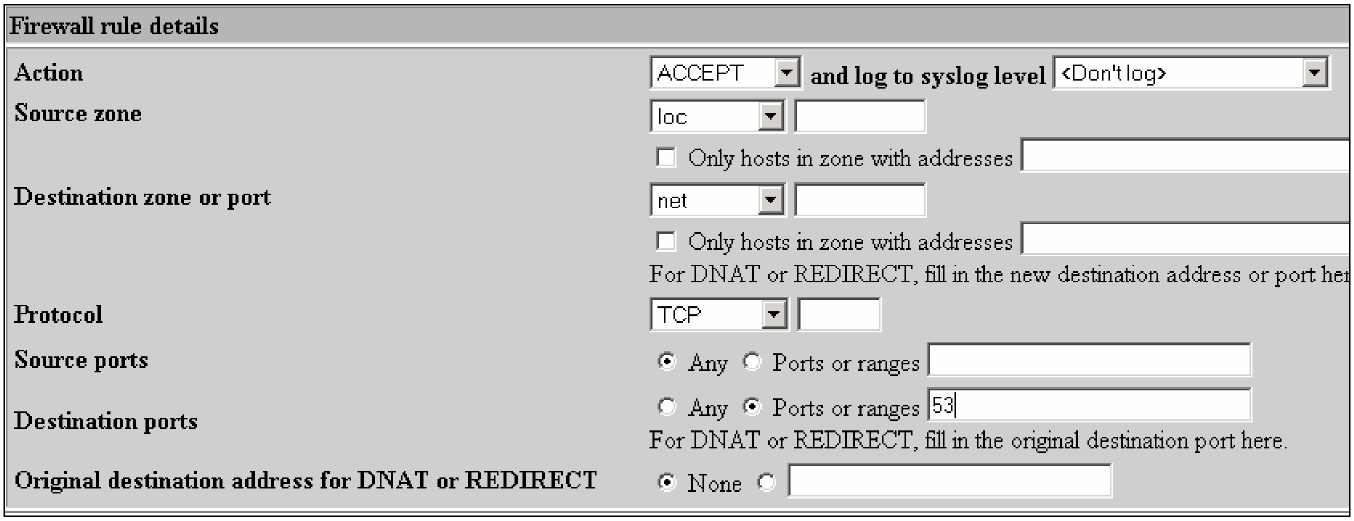
Common Rules

The following rules are examples of how to configure the Port Blocker for some of the most common applications that access the Internet. If your application is not listed then you will need to consult the documentation for the application to determine what ports are required.

DNS

Port 53 (TCP UDP)

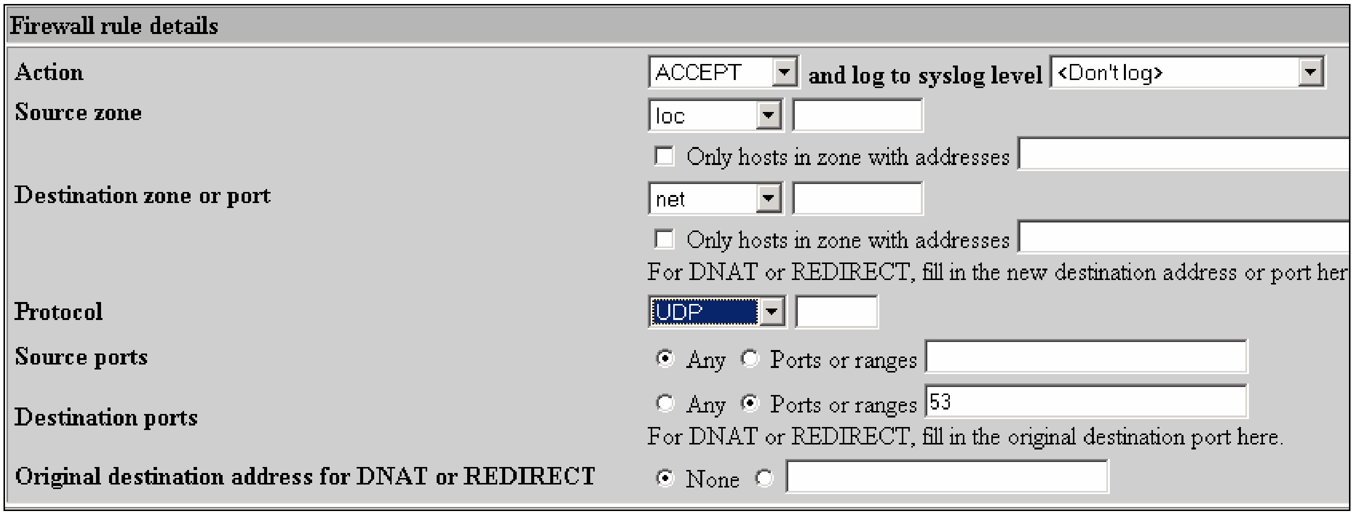
To allow client access from the LAN to the Internet use the following two rules:



Firewall rule details

Action	ACCEPT and log to syslog level <Don't log>
Source zone	loc ☐ Only hosts in zone with addresses
Destination zone or port	net ☐ Only hosts in zone with addresses For DNAT or REDIRECT, fill in the new destination address or port her
Protocol	TCP
Source ports	● Any ○ Ports or ranges
Destination ports	○ Any ● Ports or ranges 53 For DNAT or REDIRECT, fill in the original destination port here.
Original destination address for DNAT or REDIRECT	● None ○

Figure 3-17: Client Access to DNS (TCP)



Firewall rule details

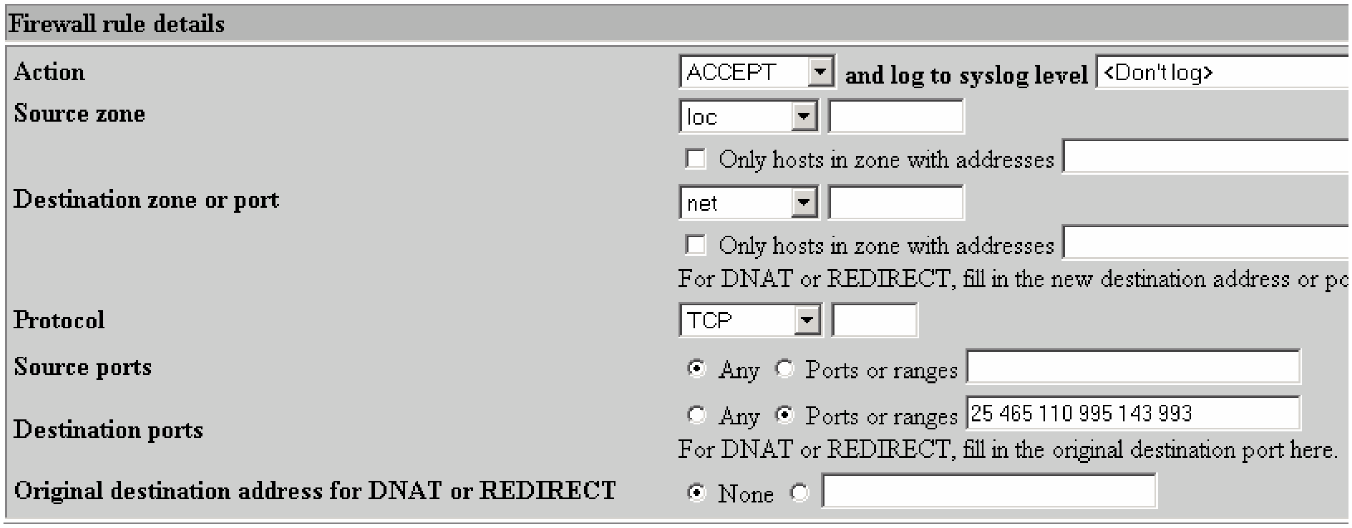
Action	ACCEPT and log to syslog level <Don't log>
Source zone	loc ☐ Only hosts in zone with addresses
Destination zone or port	net ☐ Only hosts in zone with addresses For DNAT or REDIRECT, fill in the new destination address or port her
Protocol	UDP
Source ports	● Any ○ Ports or ranges
Destination ports	○ Any ● Ports or ranges 53 For DNAT or REDIRECT, fill in the original destination port here.
Original destination address for DNAT or REDIRECT	● None ○

Figure 3-18: Client Access to DNS (UDP)

Client Email (POP3, IMAP, SMTP)

Ports – POP3 unsecure 110 (TCP), POP3 Secure 995 (TCP), IMAP unsecure 143 (TCP), IMAP secure 993 (TCP), SMTP 125 (TCP).

To allow client access from the LAN to the Internet use the following rule:

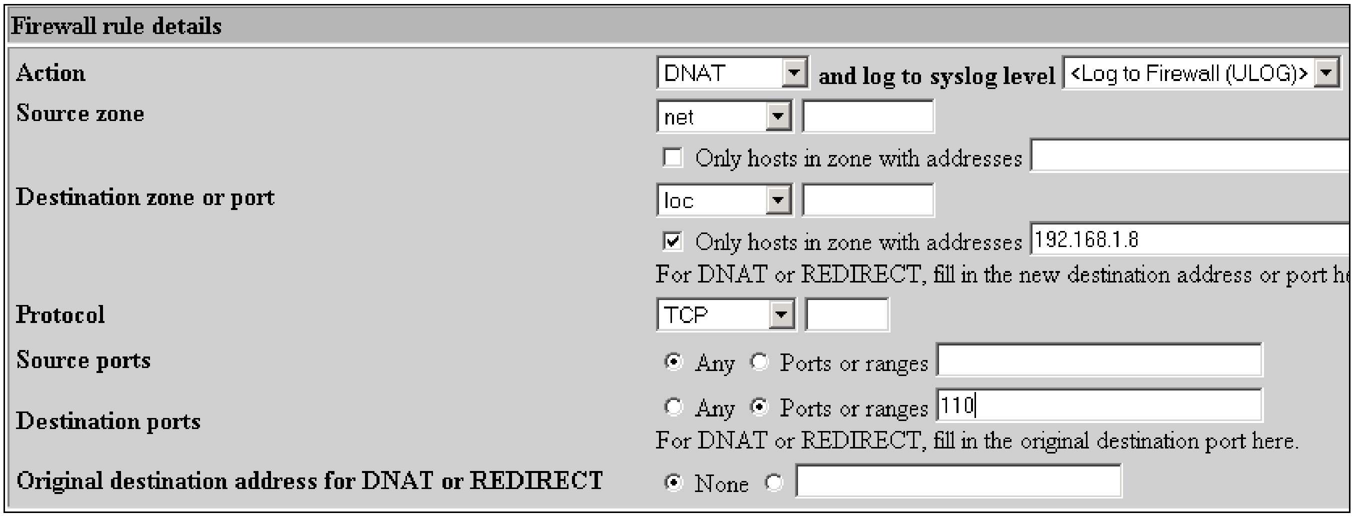


Firewall rule details

Action: ACCEPT **and log to syslog level** <Don't log>
Source zone: loc
☐ Only hosts in zone with addresses
Destination zone or port: net
☐ Only hosts in zone with addresses
For DNAT or REDIRECT, fill in the new destination address or po
Protocol: TCP
Source ports: ● Any ○ Ports or ranges
Destination ports: ○ Any ● Ports or ranges 25 465 110 995 143 993
For DNAT or REDIRECT, fill in the original destination port here.
Original destination address for DNAT or REDIRECT: ● None ○

Figure 3-19: Client Email

If you have an internal mail server and you wish to allow client access from the Internet to the LAN use the following rule:



Firewall rule details

Action: DNAT **and log to syslog level** <Log to Firewall (ULOG)>
Source zone: net
☐ Only hosts in zone with addresses
Destination zone or port: loc
☑ Only hosts in zone with addresses 192.168.1.8
For DNAT or REDIRECT, fill in the new destination address or port h
Protocol: TCP
Source ports: ● Any ○ Ports or ranges
Destination ports: ○ Any ● Ports or ranges 110
For DNAT or REDIRECT, fill in the original destination port here.
Original destination address for DNAT or REDIRECT: ● None ○

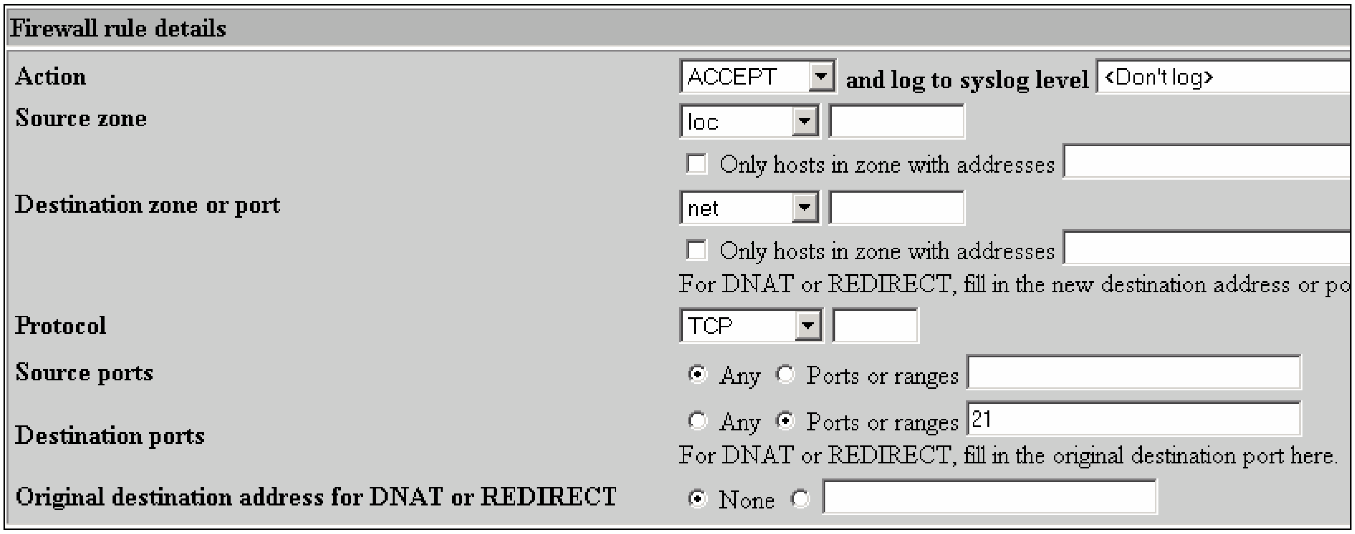
Figure 3-20: Internet Access to Email Server

In this example we have a POP3 email server at 192.168.1.8 port 110.

FTP

Port 21 (TCP)

To allow client access from the LAN to the Internet use the following rule:

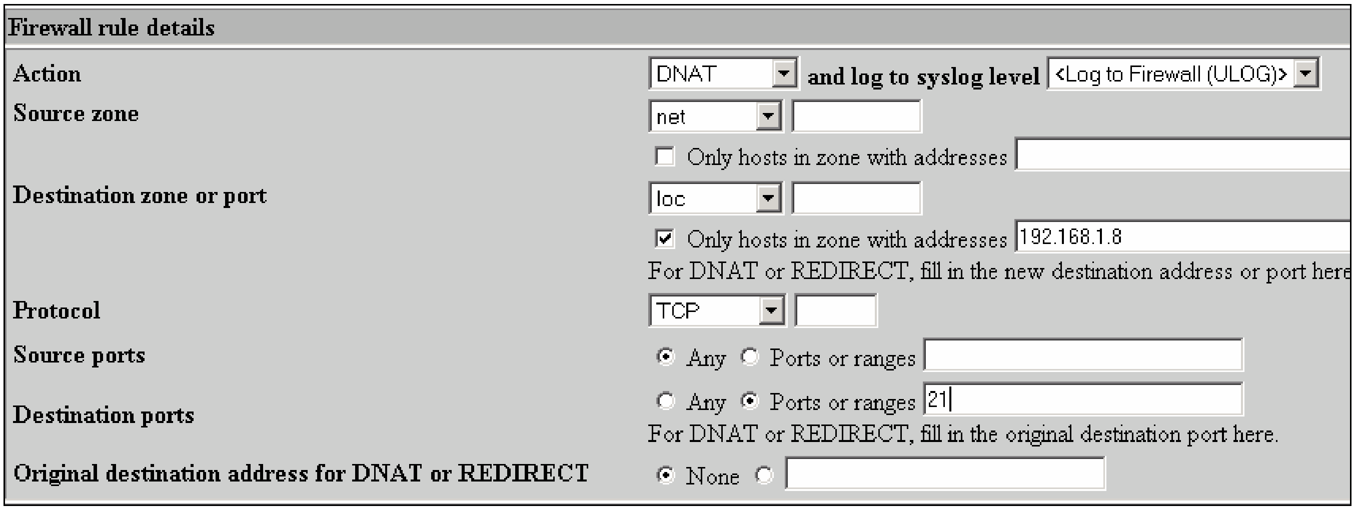


Firewall rule details

Action	ACCEPT **and log to syslog level** <Don't log>
Source zone	loc ☐ Only hosts in zone with addresses
Destination zone or port	net ☐ Only hosts in zone with addresses For DNAT or REDIRECT, fill in the new destination address or po
Protocol	TCP
Source ports	● Any ○ Ports or ranges
Destination ports	○ Any ● Ports or ranges 21 For DNAT or REDIRECT, fill in the original destination port here.
Original destination address for DNAT or REDIRECT	● None ○

Figure 3-21: Client FTP Access

If you have an internal FTP server and you wish to allow client access from the Internet to the LAN use the following rule:



Firewall rule details

Action	DNAT **and log to syslog level** <Log to Firewall (ULOG)>
Source zone	net ☐ Only hosts in zone with addresses
Destination zone or port	loc ☑ Only hosts in zone with addresses 192.168.1.8 For DNAT or REDIRECT, fill in the new destination address or port her
Protocol	TCP
Source ports	● Any ○ Ports or ranges
Destination ports	○ Any ● Ports or ranges 21 For DNAT or REDIRECT, fill in the original destination port here.
Original destination address for DNAT or REDIRECT	● None ○

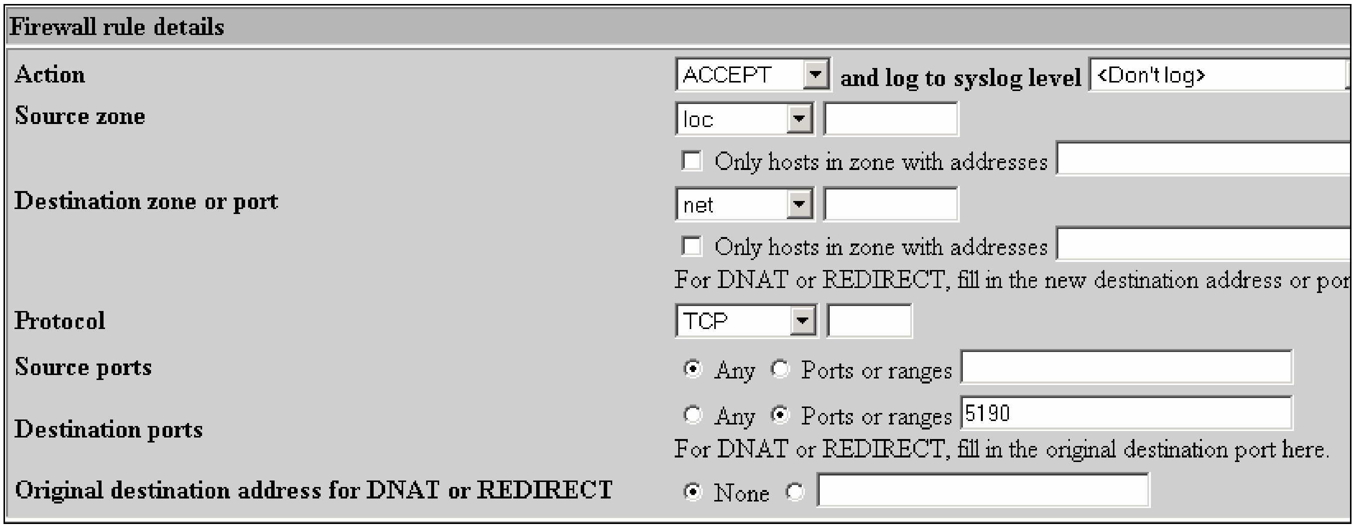
Figure 3-22: Access to Internal FTP Server

In this rule any packet from the Internet destined for port 21 will be routed to the FTP server located at 192.168.1.8.

ICQ/IM

Port 5190 (TCP)

To allow client access from the LAN to the Internet use the following rule:



Firewall rule details

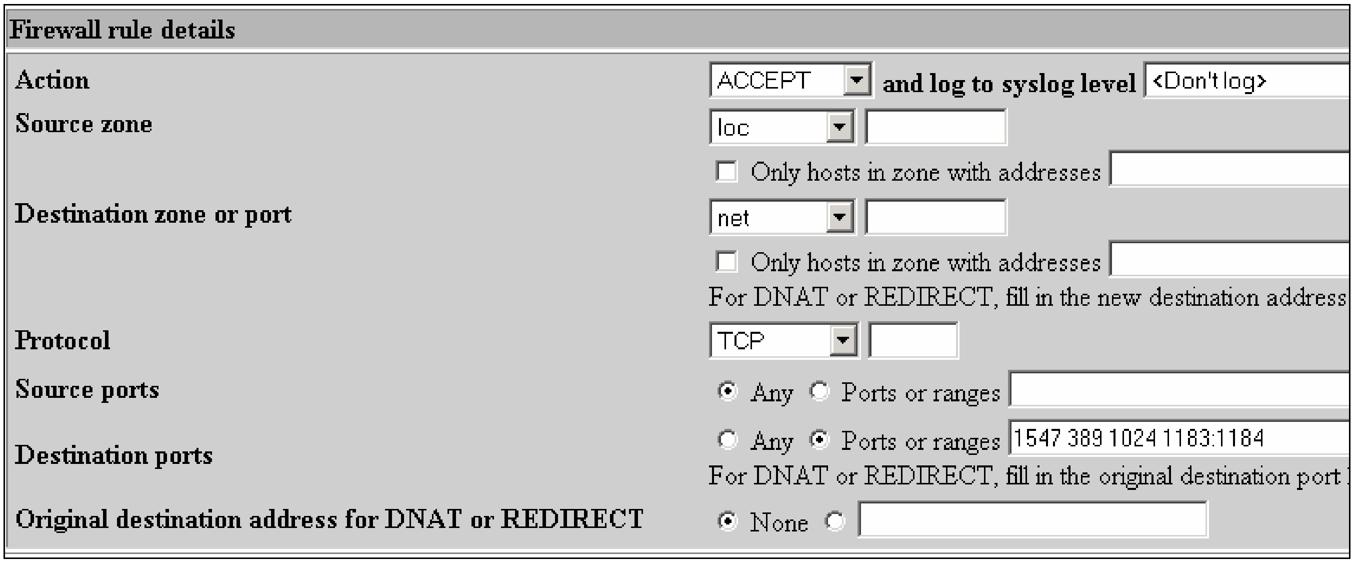
Action	ACCEPT **and log to syslog level** <Don't log>
Source zone	loc
	☐ Only hosts in zone with addresses
Destination zone or port	net
	☐ Only hosts in zone with addresses
	For DNAT or REDIRECT, fill in the new destination address or por
Protocol	TCP
Source ports	● Any ○ Ports or ranges
Destination ports	○ Any ● Ports or ranges 5190
	For DNAT or REDIRECT, fill in the original destination port here.
Original destination address for DNAT or REDIRECT	● None ○

Figure 3-23: ICQ/AOL Client Access

Laplink™

Ports 1547 (TCP), 389 (TCP), 1024 (TCP), 1183 (TCP), 1184 (TCP)

To allow client access from the LAN to the Internet use the following rule:

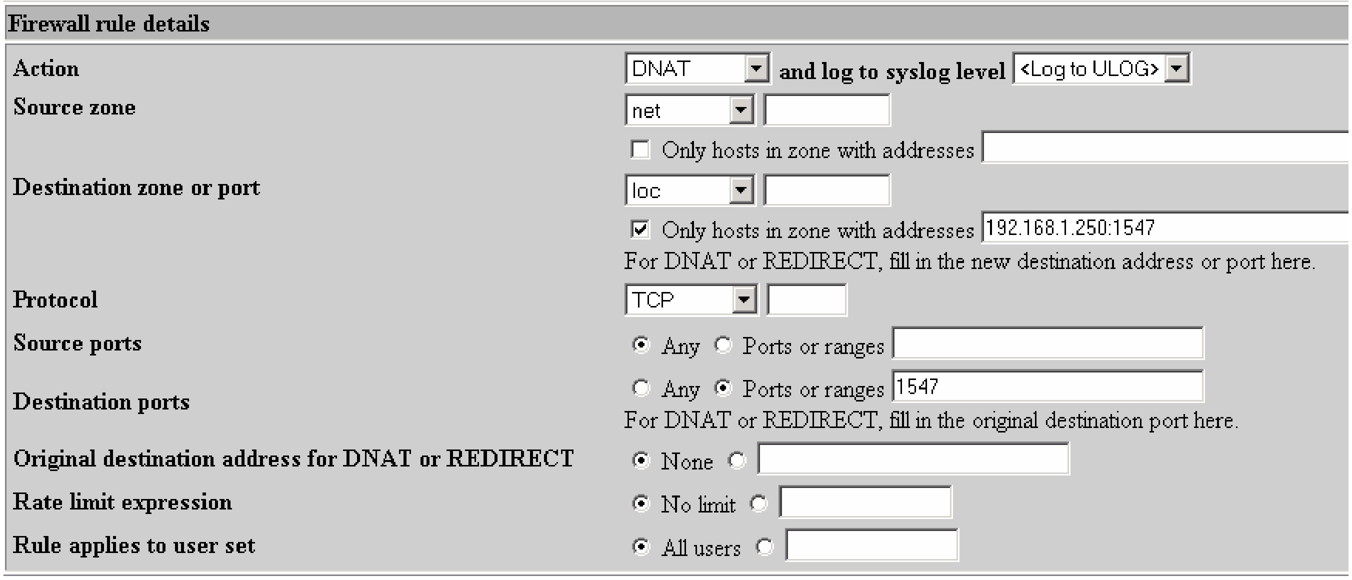


Firewall rule details

Action	ACCEPT and log to syslog level <Don't log>
Source zone	loc ☐ Only hosts in zone with addresses
Destination zone or port	net ☐ Only hosts in zone with addresses For DNAT or REDIRECT, fill in the new destination address
Protocol	TCP
Source ports	● Any ○ Ports or ranges
Destination ports	○ Any ● Ports or ranges 1547 389 1024 1183:1184 For DNAT or REDIRECT, fill in the original destination port
Original destination address for DNAT or REDIRECT	● None ○

Figure 3-24: Client Access to Laplink

If you have an internal Laplink server and you wish to allow access from the Internet to the server add the following rule:



Firewall rule details

Action	DNAT and log to syslog level <Log to ULOG>
Source zone	net ☐ Only hosts in zone with addresses
Destination zone or port	loc ☑ Only hosts in zone with addresses 192.168.1.250:1547 For DNAT or REDIRECT, fill in the new destination address or port here.
Protocol	TCP
Source ports	● Any ○ Ports or ranges
Destination ports	○ Any ● Ports or ranges 1547 For DNAT or REDIRECT, fill in the original destination port here.
Original destination address for DNAT or REDIRECT	● None ○
Rate limit expression	● No limit ○
Rule applies to user set	● All users ○

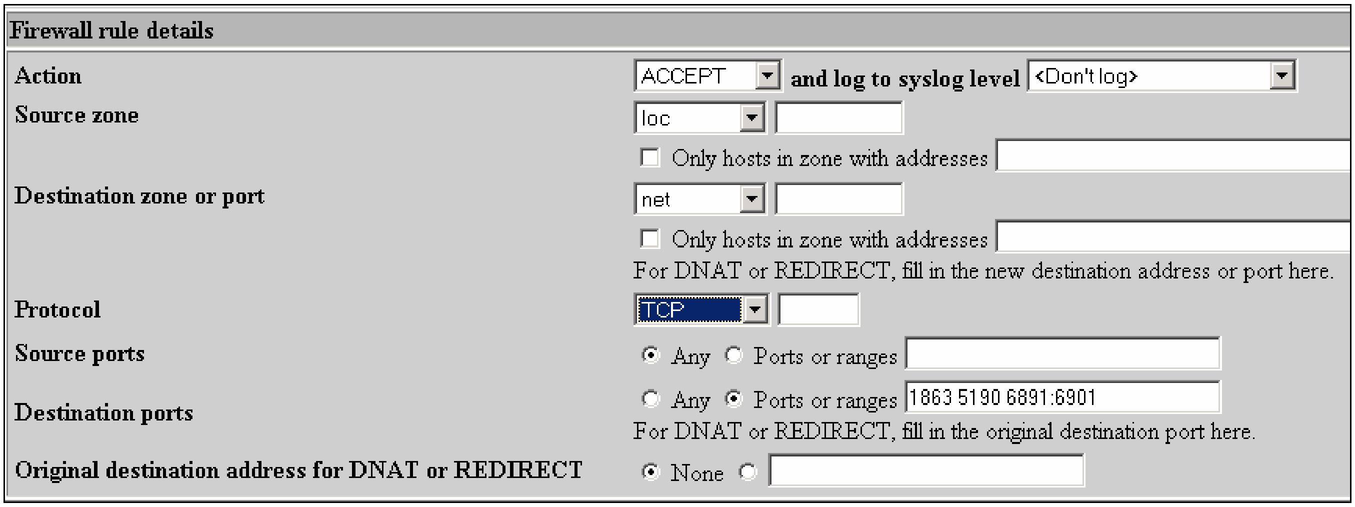
Figure 3-25: Accessing an Internal Laplink Server

In this rule packets from the Internet destined for port 1547 are forwarded to 192.168.1.250 port 1547.

MSN™ Messenger

Ports 1863 (TCP), 5190 (TCP), 6891-6901 (TCP)

To allow client access from the LAN to the Internet use the following rule:



Firewall rule details

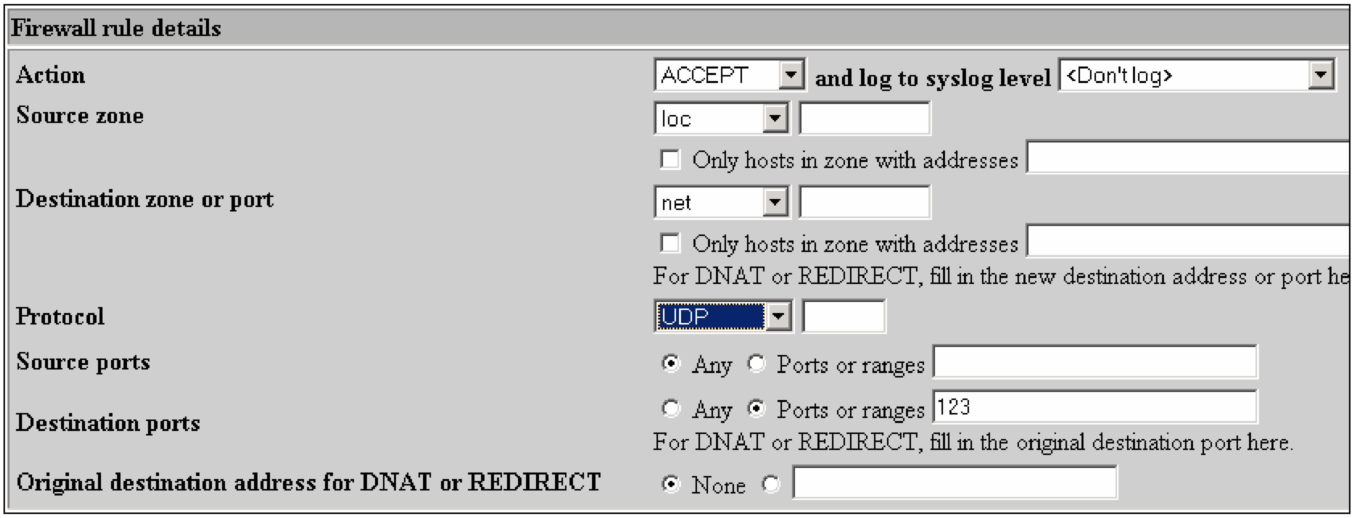
Action	ACCEPT and log to syslog level <Don't log>
Source zone	loc ☐ Only hosts in zone with addresses
Destination zone or port	net ☐ Only hosts in zone with addresses For DNAT or REDIRECT, fill in the new destination address or port here.
Protocol	TCP
Source ports	● Any ○ Ports or ranges
Destination ports	○ Any ● Ports or ranges 1863 5190 6891:6901 For DNAT or REDIRECT, fill in the original destination port here.
Original destination address for DNAT or REDIRECT	● None ○

Figure 3-26: Client Access to MSN Messenger

NTP (Network Time Protocol)

Port 123 UDP

To allow client access from the LAN to the Internet use the following rule:



Firewall rule details

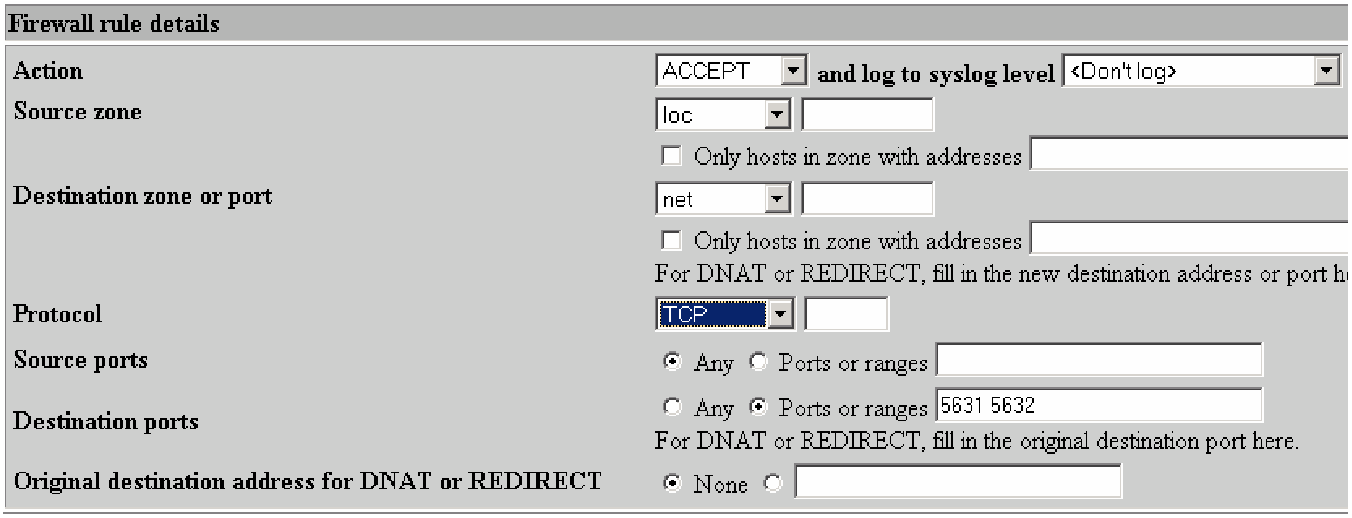
Action	ACCEPT **and log to syslog level** <Don't log>
Source zone	loc ☐ Only hosts in zone with addresses
Destination zone or port	net ☐ Only hosts in zone with addresses For DNAT or REDIRECT, fill in the new destination address or port he
Protocol	UDP
Source ports	● Any ○ Ports or ranges
Destination ports	○ Any ● Ports or ranges 123 For DNAT or REDIRECT, fill in the original destination port here.
Original destination address for DNAT or REDIRECT	● None ○

Figure 3-27: Client Access to NTP

PCAnywhere™

Ports 5631 (TCP), 5632 (TCP)

To allow client access from the LAN to the Internet use the following rule:

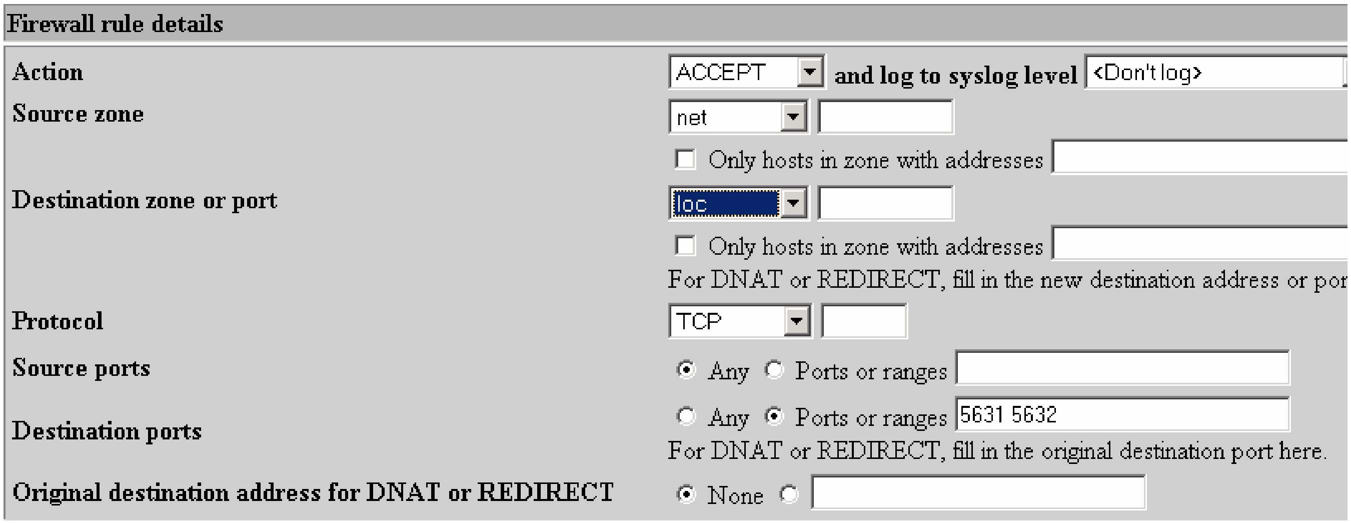


Firewall rule details

Action	ACCEPT **and log to syslog level** <Don't log>
Source zone	loc
	☐ Only hosts in zone with addresses
Destination zone or port	net
	☐ Only hosts in zone with addresses
	For DNAT or REDIRECT, fill in the new destination address or port h
Protocol	TCP
Source ports	● Any ○ Ports or ranges
Destination ports	○ Any ● Ports or ranges 5631 5632
	For DNAT or REDIRECT, fill in the original destination port here.
Original destination address for DNAT or REDIRECT	● None ○

Figure 3-28: Client Access to PCAnywhere

If you have an internal PCAnywhere server and you wish to allow access from the Internet to the server add the following rule:



Firewall rule details

Action	ACCEPT **and log to syslog level** <Don't log>
Source zone	net
	☐ Only hosts in zone with addresses
Destination zone or port	loc
	☐ Only hosts in zone with addresses
	For DNAT or REDIRECT, fill in the new destination address or por
Protocol	TCP
Source ports	● Any ○ Ports or ranges
Destination ports	○ Any ● Ports or ranges 5631 5632
	For DNAT or REDIRECT, fill in the original destination port here.
Original destination address for DNAT or REDIRECT	● None ○

Figure 3-29: Accessing an Internal PCAnywhere Server

Ping & Traceroute

Port 8 (ICMP)

By default:

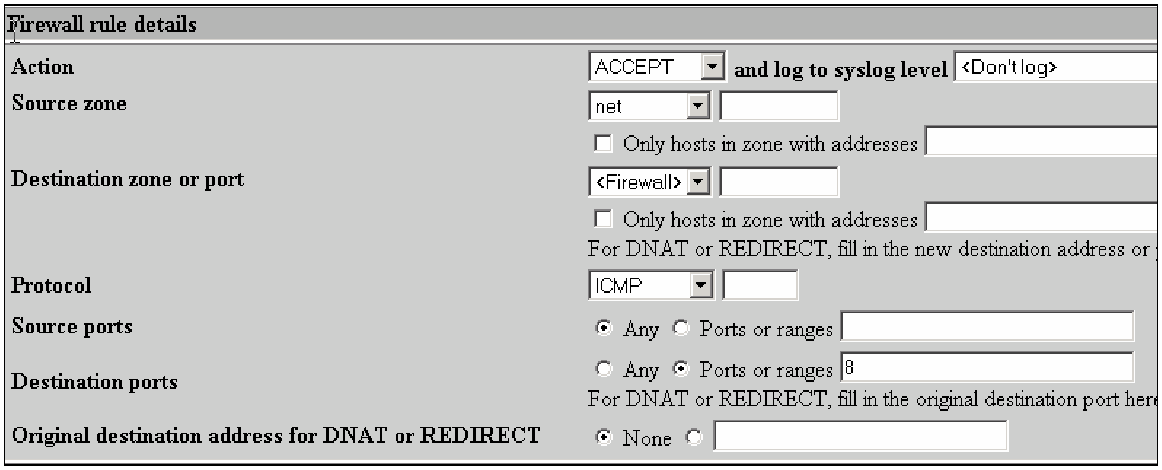
ComSifter is configured to allow all ICMP requests from the LAN to the Port Blocker. This allows ComSifter to always reply to pings and traceroute commands from inside the LAN. This may not be changed.

ComSifter will not reply to a Ping request from the Internet. This allows ComSifters Port Blocker to operate in a Stealth Mode i.e. it does not exist. Using the rule shown below ComSifter can be configured to reply to a ping from the Internet.

Warning: Allowing a Ping from the Internet will confirm the existence of your location to potential hackers. Best practices would suggest that this only be allowed for testing purposes.

ComSifter will not allow ping requests from the LAN to the Internet. Using the rule shown below ComSifter can be configured to allow ping from the LAN to the Internet.

To allow a ComSifter to reply to a Ping request from the Internet apply the following rule.

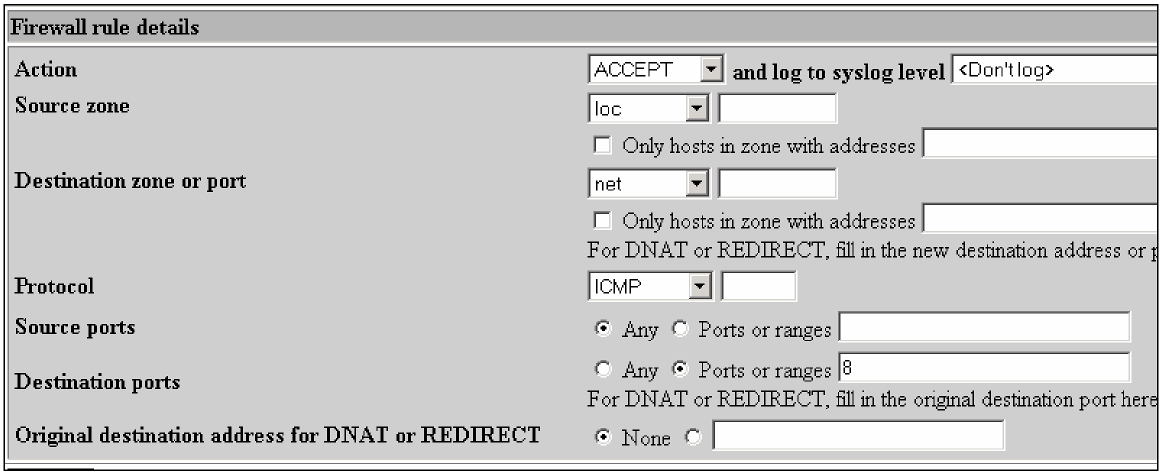


Firewall rule details

Action	ACCEPT **and log to syslog level** <Don't log>
Source zone	net
	☐ Only hosts in zone with addresses
Destination zone or port	<Firewall>
	☐ Only hosts in zone with addresses
	For DNAT or REDIRECT, fill in the new destination address or
Protocol	ICMP
Source ports	● Any ○ Ports or ranges
Destination ports	○ Any ● Ports or ranges 8
	For DNAT or REDIRECT, fill in the original destination port her
Original destination address for DNAT or REDIRECT	● None ○

Figure 3-30: Allow Ping from the Internet

To allow a client on the LAN to ping addresses on the Internet apply the following rule.



Firewall rule details

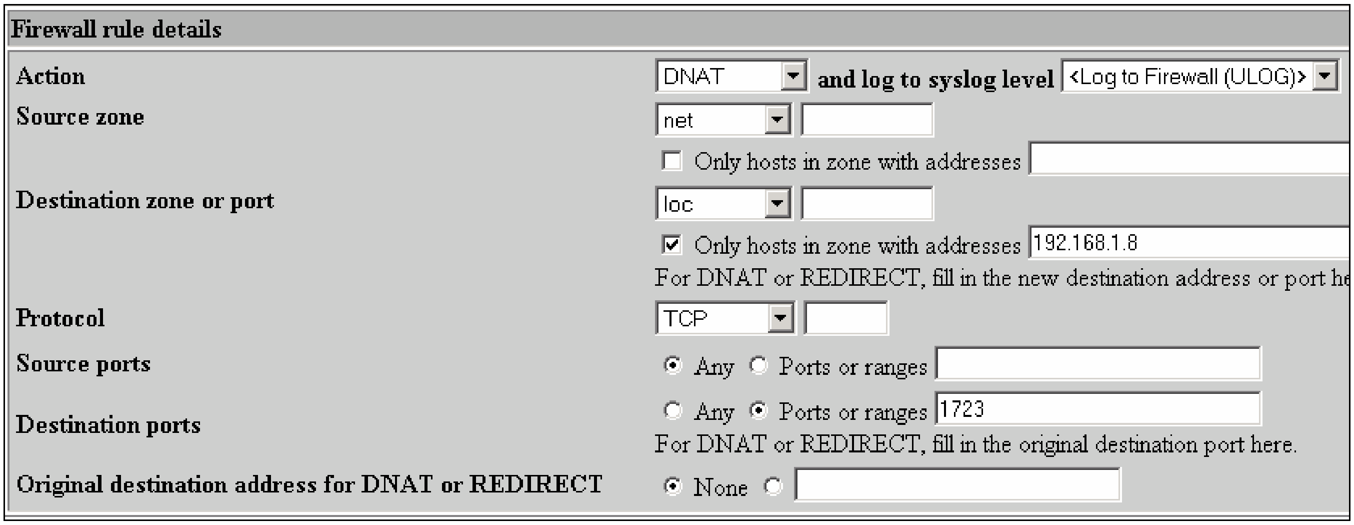
Action	ACCEPT **and log to syslog level** <Don't log>
Source zone	loc
	☐ Only hosts in zone with addresses
Destination zone or port	net
	☐ Only hosts in zone with addresses
	For DNAT or REDIRECT, fill in the new destination address or
Protocol	ICMP
Source ports	● Any ○ Ports or ranges
Destination ports	○ Any ● Ports or ranges 8
	For DNAT or REDIRECT, fill in the original destination port here
Original destination address for DNAT or REDIRECT	● None ○

Figure 3-31: Client Access to Ping

PPTP

Port 1723 (TCP) (GRE)

To allow client access from the LAN to the Internet use the following rule:



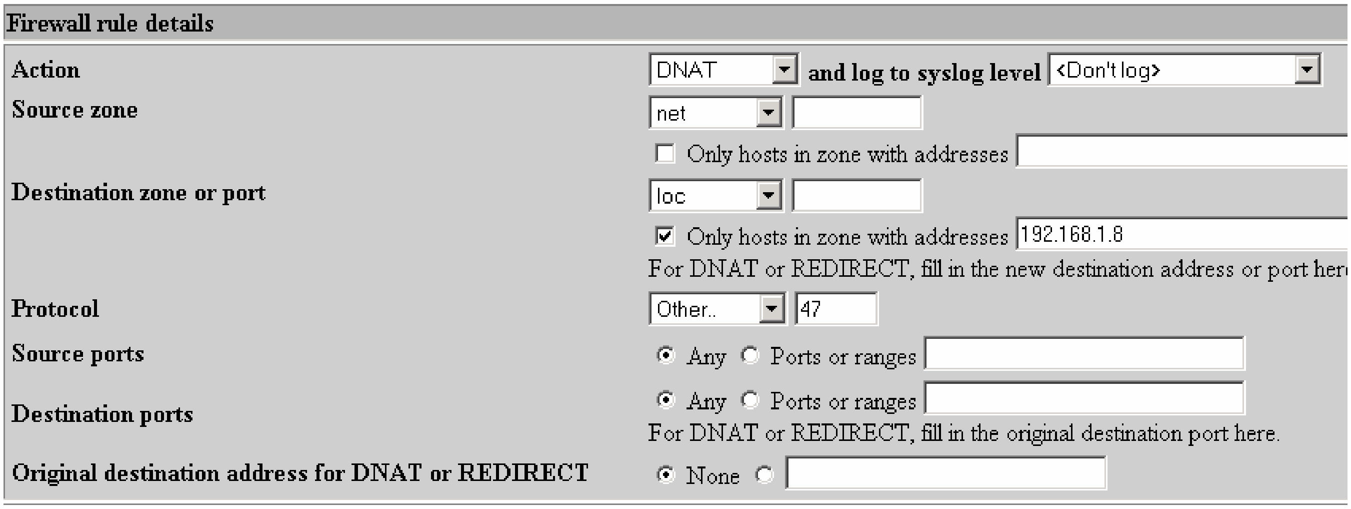
Firewall rule details

Action	DNAT and log to syslog level <Log to Firewall (ULOG)>
Source zone	net ☐ Only hosts in zone with addresses
Destination zone or port	loc ☑ Only hosts in zone with addresses 192.168.1.8 For DNAT or REDIRECT, fill in the new destination address or port he
Protocol	TCP
Source ports	● Any ○ Ports or ranges
Destination ports	○ Any ● Ports or ranges 1723 For DNAT or REDIRECT, fill in the original destination port here.
Original destination address for DNAT or REDIRECT	● None ○

Figure 3-32: Client Access to PPTP

To allow client access from the Internet to the LAN use the following rule:

First enable Protocol 47 (GRE).

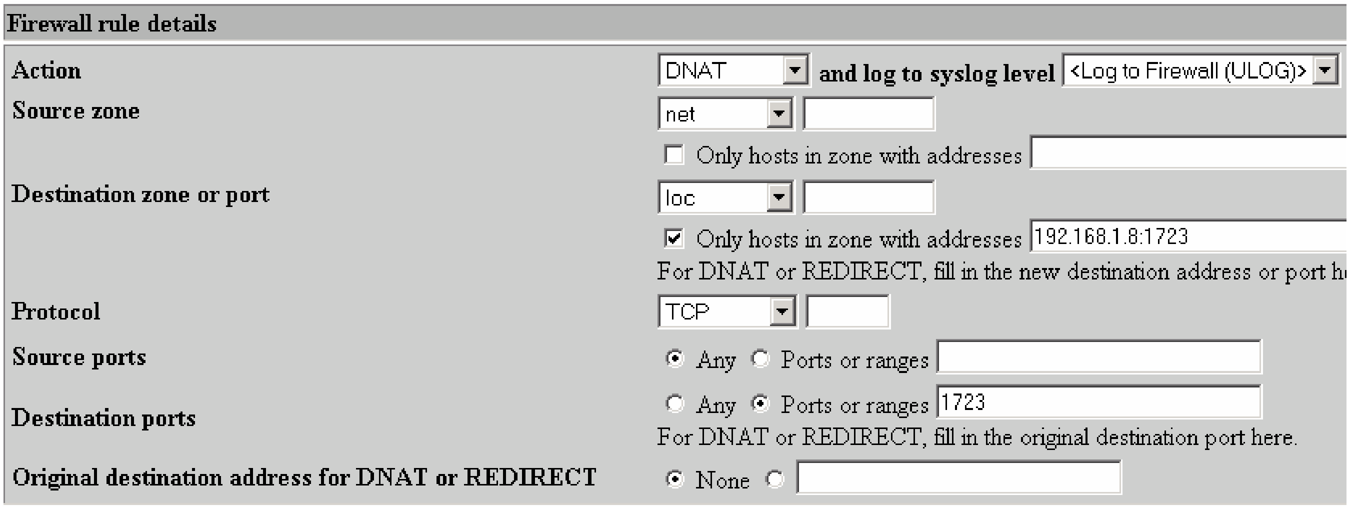


Firewall rule details

Action	DNAT and log to syslog level <Don't log>
Source zone	net ☐ Only hosts in zone with addresses
Destination zone or port	loc ☑ Only hosts in zone with addresses 192.168.1.8 For DNAT or REDIRECT, fill in the new destination address or port her
Protocol	Other.. 47
Source ports	● Any ○ Ports or ranges
Destination ports	● Any ○ Ports or ranges For DNAT or REDIRECT, fill in the original destination port here.
Original destination address for DNAT or REDIRECT	● None ○

Figure 3-33: Client Access to PPTP (protocol)

Then add a rule that connects TCP to the PPTP server.



Firewall rule details

Action DNAT **and log to syslog level** <Log to Firewall (ULOG)>

Source zone net

☐ Only hosts in zone with addresses

Destination zone or port loc

☑ Only hosts in zone with addresses 192.168.1.8:1723

For DNAT or REDIRECT, fill in the new destination address or port h

Protocol TCP

Source ports ● Any ○ Ports or ranges

Destination ports ○ Any ● Ports or ranges 1723

For DNAT or REDIRECT, fill in the original destination port here.

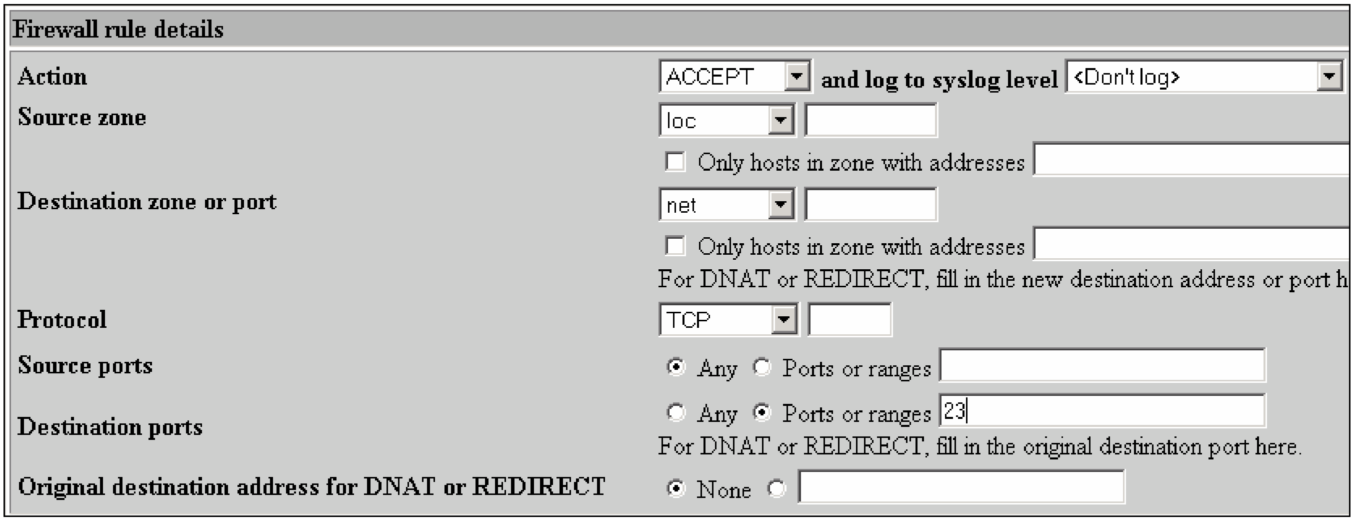
Original destination address for DNAT or REDIRECT ● None ○

Figure 3-34: Client Access to PPTP

Telnet

Port 21 (TCP)

To allow client access from the LAN to the Internet use the following rule:



Firewall rule details

Action ACCEPT **and log to syslog level** <Don't log>

Source zone loc

☐ Only hosts in zone with addresses

Destination zone or port net

☐ Only hosts in zone with addresses

For DNAT or REDIRECT, fill in the new destination address or port h

Protocol TCP

Source ports ● Any ○ Ports or ranges

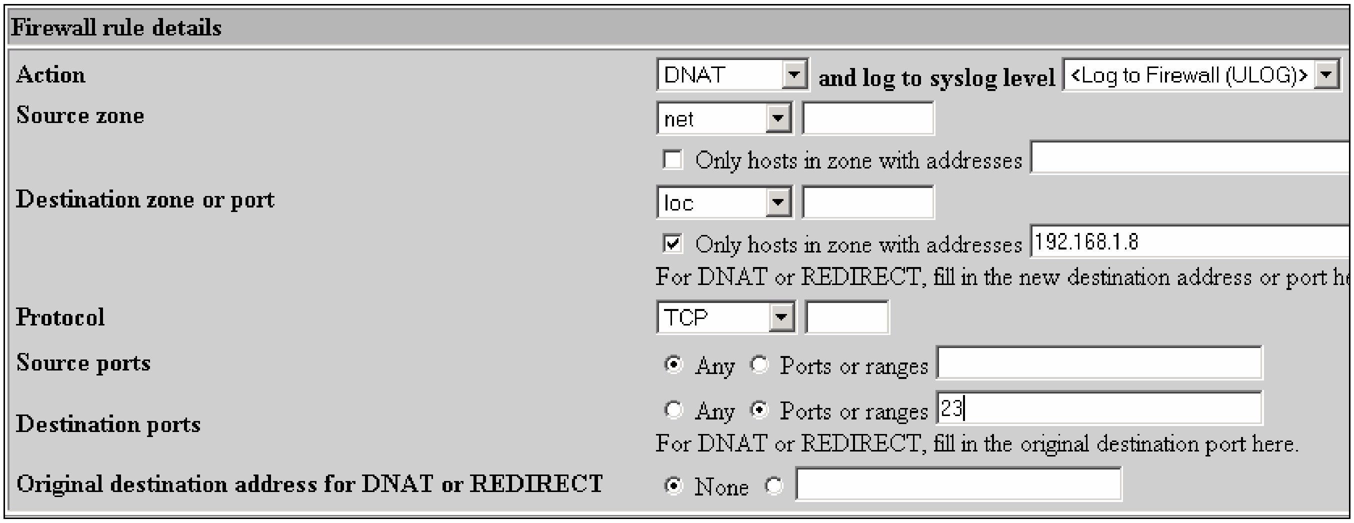
Destination ports ○ Any ● Ports or ranges 23

For DNAT or REDIRECT, fill in the original destination port here.

Original destination address for DNAT or REDIRECT ● None ○

Figure 3-35: Client Access to Telnet

If you have an internal Telnet server and you wish to allow access from the Internet to the server add the following rule:



Firewall rule details

Action DNAT **and log to syslog level** <Log to Firewall (ULOG)>

Source zone net

☐ Only hosts in zone with addresses

Destination zone or port loc

☑ Only hosts in zone with addresses 192.168.1.8

For DNAT or REDIRECT, fill in the new destination address or port h

Protocol TCP

Source ports ● Any ○ Ports or ranges

Destination ports ○ Any ● Ports or ranges 23

For DNAT or REDIRECT, fill in the original destination port here.

Original destination address for DNAT or REDIRECT ● None ○

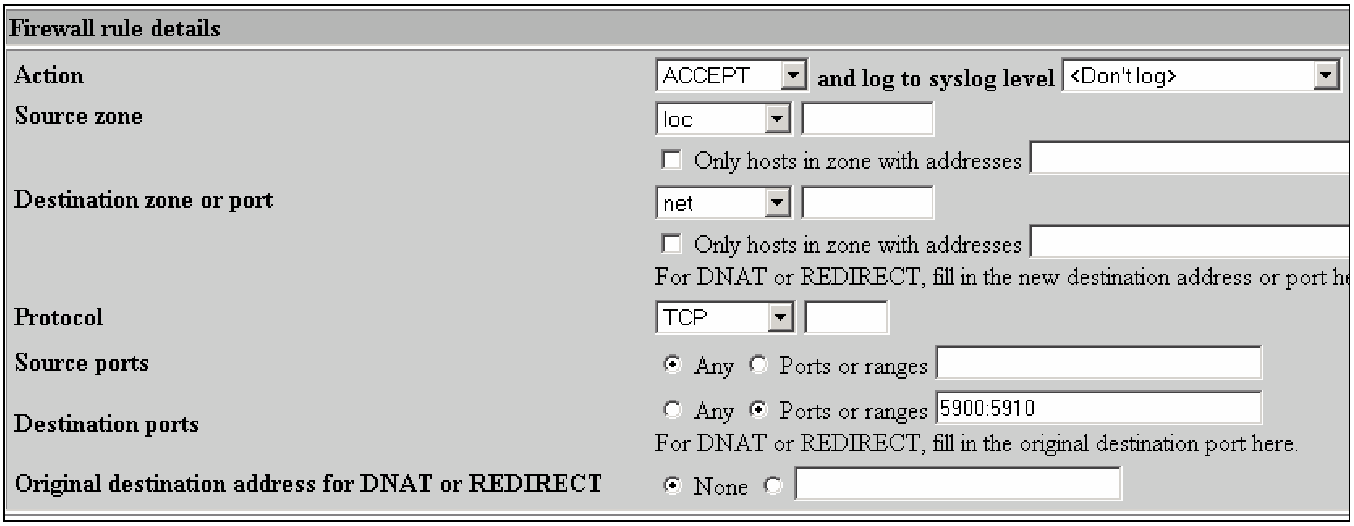
Figure 3-36: Access to Telnet Server

In this rule packets from the Internet destined for port 23 are forwarded to 192.168.1.8 port 23.

VNC

Ports 5500 (TCP), 5900+ (TCP)

To allow client access from the LAN to the Internet use the following rule:



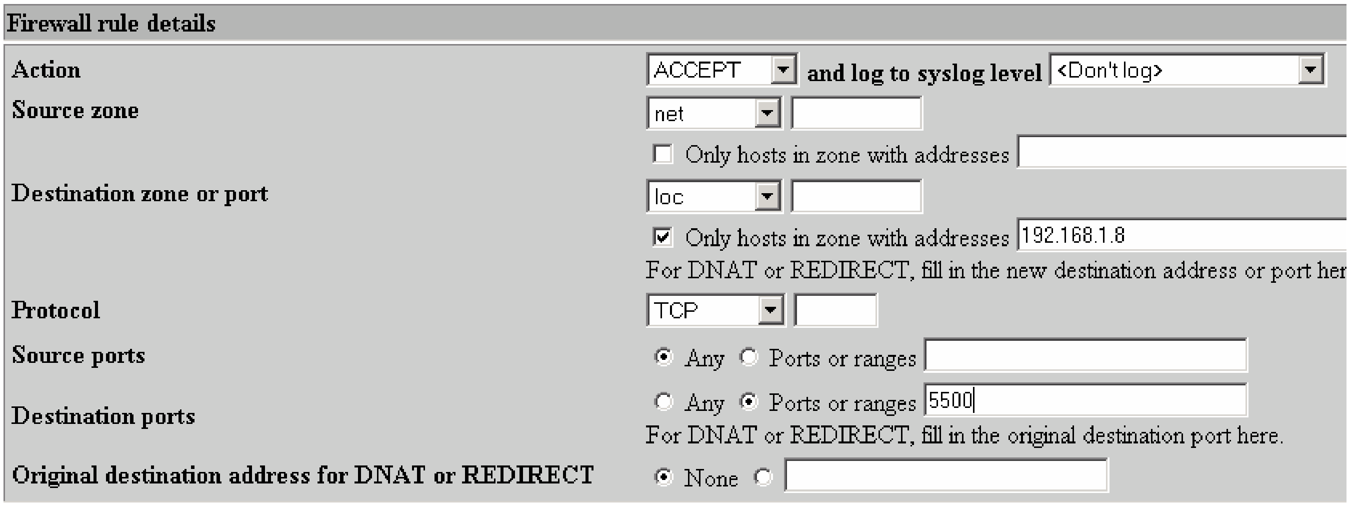
Firewall rule details

Action	ACCEPT **and log to syslog level** <Don't log>
Source zone	loc
	☐ Only hosts in zone with addresses
Destination zone or port	net
	☐ Only hosts in zone with addresses
	For DNAT or REDIRECT, fill in the new destination address or port h
Protocol	TCP
Source ports	● Any ○ Ports or ranges
Destination ports	○ Any ● Ports or ranges 5900:5910
	For DNAT or REDIRECT, fill in the original destination port here.
Original destination address for DNAT or REDIRECT	● None ○

Figure 3-37: Client Access to VNC

Each client accessing VNC outbound will need a separate port. If you expect only one client at a time then only open one port. The above example allows for up to 10 simultaneous clients.

If you have an internal VNC server and you wish to allow access from the Internet to the server add the following rule:



Firewall rule details

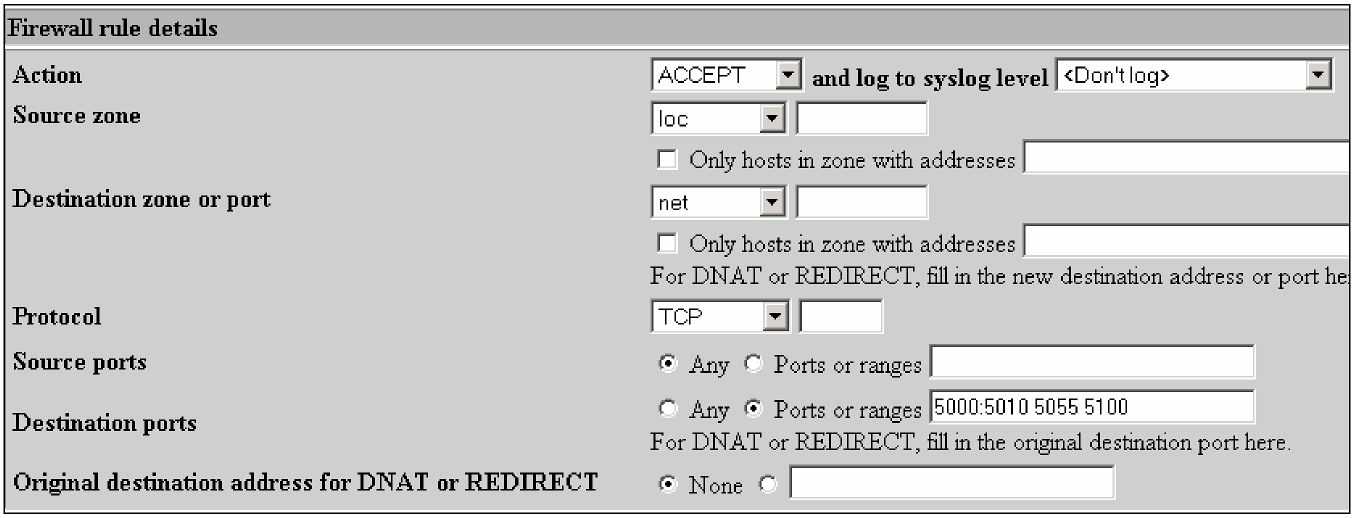
Action	ACCEPT **and log to syslog level** <Don't log>
Source zone	net
	☐ Only hosts in zone with addresses
Destination zone or port	loc
	☑ Only hosts in zone with addresses 192.168.1.8
	For DNAT or REDIRECT, fill in the new destination address or port her
Protocol	TCP
Source ports	● Any ○ Ports or ranges
Destination ports	○ Any ● Ports or ranges 5500
	For DNAT or REDIRECT, fill in the original destination port here.
Original destination address for DNAT or REDIRECT	● None ○

Figure 3-38: Accessing VNC Server

Yahoo™ Chat

Ports 5000-5010 (TCP), 5055 (TCP), 5100 (TCP)

To allow client access from the LAN to the Internet use the following rule:



Firewall rule details

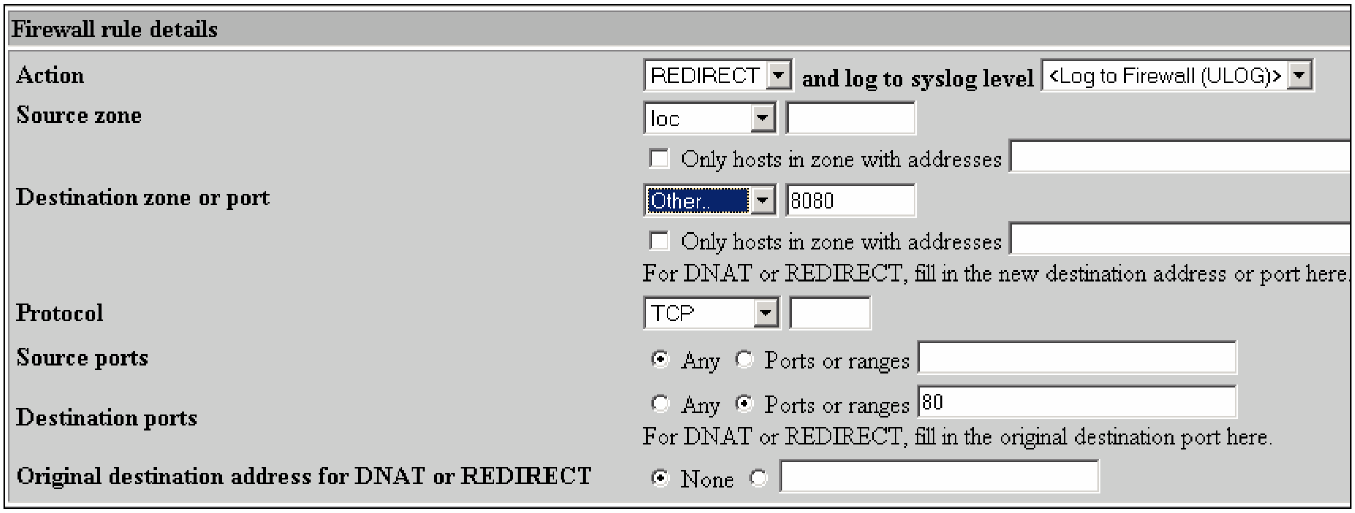
Action	ACCEPT **and log to syslog level** <Don't log>
Source zone	loc
	☐ Only hosts in zone with addresses
Destination zone or port	net
	☐ Only hosts in zone with addresses
	For DNAT or REDIRECT, fill in the new destination address or port he
Protocol	TCP
Source ports	● Any ○ Ports or ranges
Destination ports	○ Any ● Ports or ranges 5000:5010 5055 5100
	For DNAT or REDIRECT, fill in the original destination port here.
Original destination address for DNAT or REDIRECT	● None ○

Figure 3-39: Client Access to Yahoo Chat

Web Access (browsing)

Ports 80 (TCP), 443 (TCP), 8080 (TCP)

To allow client access from the LAN to the Internet use the following rule:



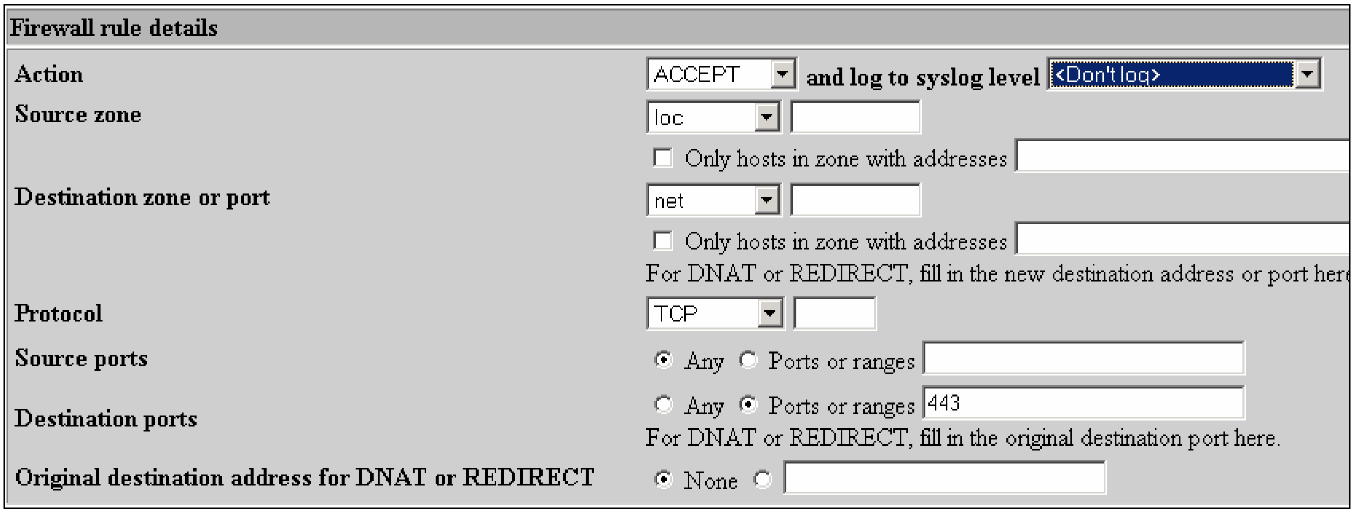
Firewall rule details

Action	REDIRECT and log to syslog level <Log to Firewall (ULOG)>
Source zone	loc
	☐ Only hosts in zone with addresses
Destination zone or port	Other.. 8080
	☐ Only hosts in zone with addresses
	For DNAT or REDIRECT, fill in the new destination address or port here.
Protocol	TCP
Source ports	● Any ○ Ports or ranges
Destination ports	○ Any ● Ports or ranges 80
	For DNAT or REDIRECT, fill in the original destination port here.
Original destination address for DNAT or REDIRECT	● None ○

Figure 3-40: Client Access to the WEB

The above rule will redirect all requests for access to the Internet (http) to port 8080. ComSifter Filter Service is listening on this port. It will intercept the request, retrieve and filter the response and either send the response or a Denied page to the requesting computer.

In addition to allowing normal web browsing you may allow secure authentication (https) by allowing port 443 outbound as shown below

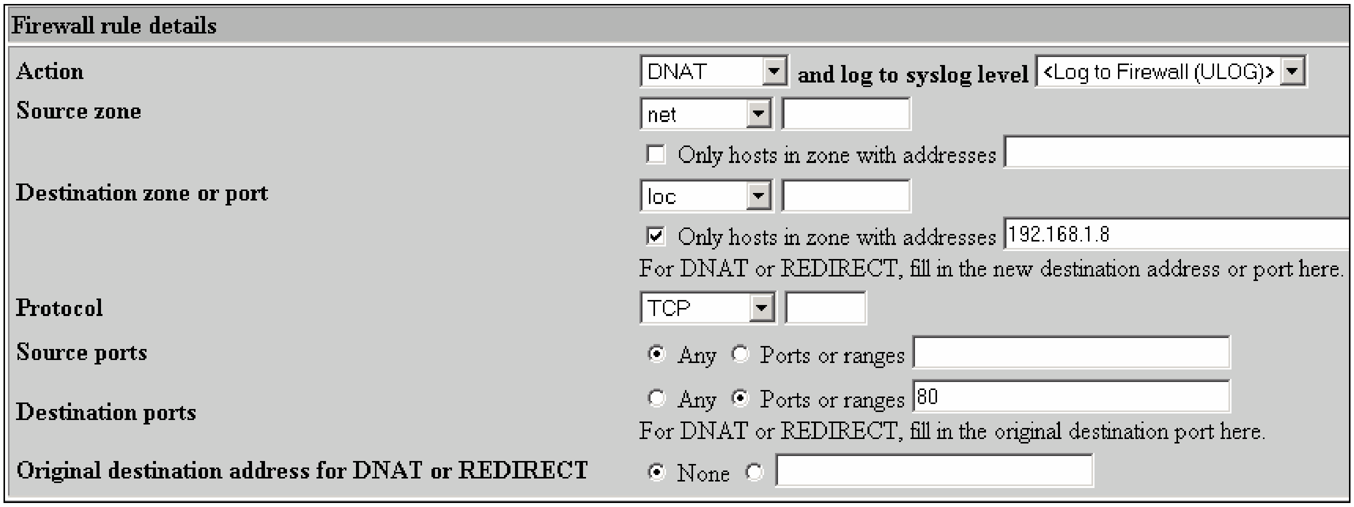


Firewall rule details

Action	ACCEPT and log to syslog level <Don't log>
Source zone	loc
	☐ Only hosts in zone with addresses
Destination zone or port	net
	☐ Only hosts in zone with addresses
	For DNAT or REDIRECT, fill in the new destination address or port her
Protocol	TCP
Source ports	● Any ○ Ports or ranges
Destination ports	○ Any ● Ports or ranges 443
	For DNAT or REDIRECT, fill in the original destination port here.
Original destination address for DNAT or REDIRECT	● None ○

Figure 3-41: Allowing Secure Access to the Internet

To allow access from the Internet to a Web Server located on the LAN use the following rule:



Firewall rule details

Action	DNAT **and log to syslog level** <Log to Firewall (ULOG)>
Source zone	net
	☐ Only hosts in zone with addresses
Destination zone or port	loc
	☑ Only hosts in zone with addresses 192.168.1.8
	For DNAT or REDIRECT, fill in the new destination address or port here.
Protocol	TCP
Source ports	● Any ○ Ports or ranges
Destination ports	○ Any ● Ports or ranges 80 For DNAT or REDIRECT, fill in the original destination port here.
Original destination address for DNAT or REDIRECT	● None ○

Figure 3-42: Web Server Access

This rules routes any incoming port 80 request from the Internet to the Host defined in the Destination Zone.

Apply Configuration

Upon clicking **Apply Configuration** ComSifter will:

1. Run a Check Port Blocker to validate the new Port Blocker rules.
2. If Check Port Blocker is successful the command will continue. If the Check Port Blocker fails you will be notified that the command failed, the new rules will not be installed and the Port Blocker will continue operating with its current rules.
3. Stop all Filtering and Proxy Services.
4. Stop Network Services.
5. Stop the Port Blocker.
6. Restart the Port Blocker with the new rules.
7. Network, Proxy and Filtering Services will restart.

Note: If the Check Port Blocker fails you should manually run the **Check Port Blocker** Command for information why the command failed.

Warning: During an Apply Configuration all Internet traffic is stopped. The Apply Configuration may take up to a minute to complete.

Stop Port Blocker

The **Stop Port Blocker** command will immediately shutdown the Port Blocker and block all ports from incoming or outgoing traffic with the exception of port 10000, which is the port used by ComSifter for configuration.

Check Port Blocker

The Check Port Blocker command is used to verify that the new Port Blocker Rules are valid and that the Port Blocker will start. Check Port Blocker does not validate that the created rule will operate as you think it will, only that the Port Blocker will start. If you receive a failure notice you will have to view the Check Port Blocker output and find the rule that caused the failure.

Backup

Upon clicking the **Backup** button ComSifter will create an internal backup of the existing Port Blocker Rules. A backup should be created any time you are preparing to make changes to the Port Blocker Rules. In the rare event that Check Port Blocker validates a new rule set but the Port Blocker is unable to start; you will be able to return the Port Blocker to its previous state using the Restore feature.

Restore

The Restore button will restore the Port Blocker Rules captured in Backup described above. Upon clicking **Restore** the ComSifter will:

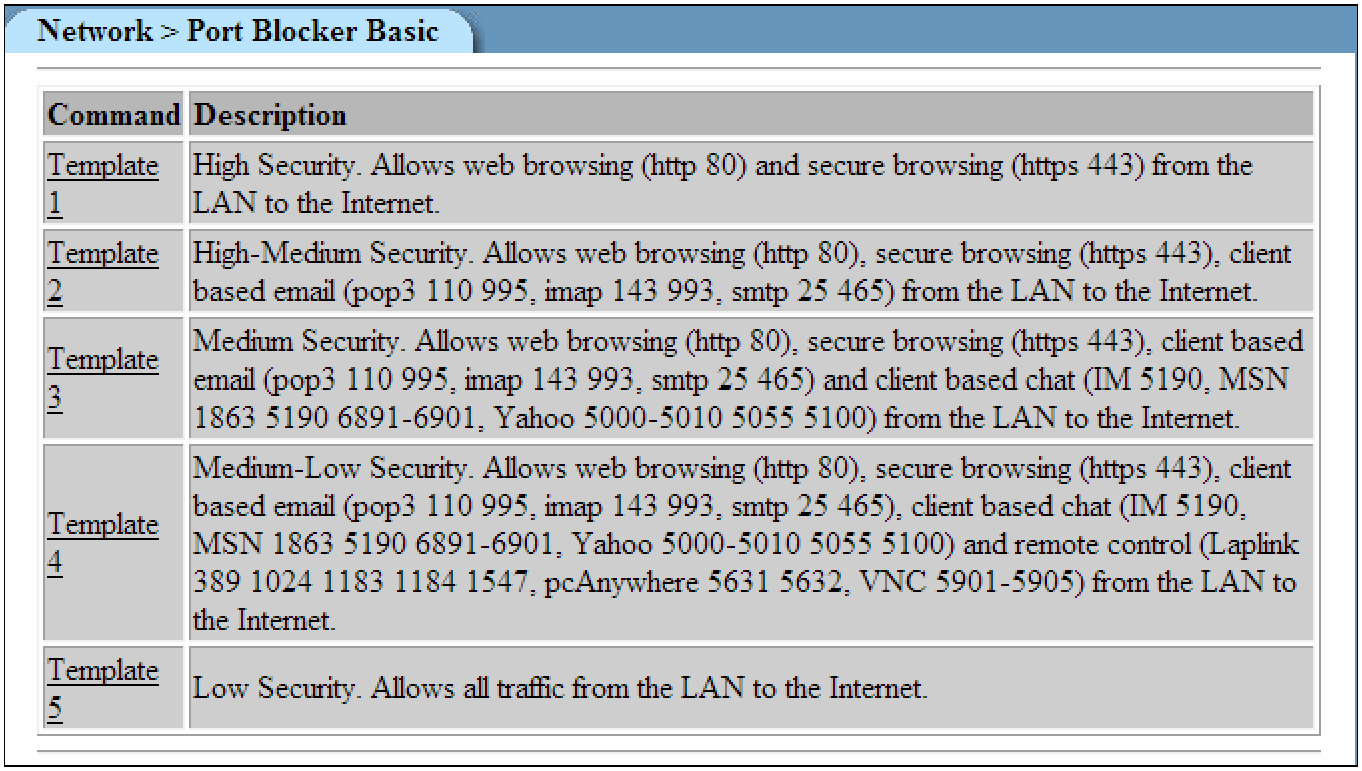
1. Stop Network, Filtering and Proxy Services
2. Load the Port Blocker Rules saved internally by the Backup command
3. Restart the Port Blocker with the backed up rules set.
4. Start Network, Filtering and Proxy Services.

Warning: During Restore all Internet traffic is stopped. The Restore may take up to one minute to complete.

Port Blocker Basic (Templates)

To streamline installation of ComSifter five Port Blocker templates are included. These templates may be used as a starting point for further modification by Port Blocker Advanced.

The Templates are arranged in order from highest security (all outgoing ports except 80 and 443 blocked) to lowest security (all outgoing ports are open).



Network > Port Blocker Basic

Command	Description
Template 1	High Security. Allows web browsing (http 80) and secure browsing (https 443) from the LAN to the Internet.
Template 2	High-Medium Security. Allows web browsing (http 80), secure browsing (https 443), client based email (pop3 110 995, imap 143 993, smtp 25 465) from the LAN to the Internet.
Template 3	Medium Security. Allows web browsing (http 80), secure browsing (https 443), client based email (pop3 110 995, imap 143 993, smtp 25 465) and client based chat (IM 5190, MSN 1863 5190 6891-6901, Yahoo 5000-5010 5055 5100) from the LAN to the Internet.
Template 4	Medium-Low Security. Allows web browsing (http 80), secure browsing (https 443), client based email (pop3 110 995, imap 143 993, smtp 25 465), client based chat (IM 5190, MSN 1863 5190 6891-6901, Yahoo 5000-5010 5055 5100) and remote control (Laplink 389 1024 1183 1184 1547, pcAnywhere 5631 5632, VNC 5901-5905) from the LAN to the Internet.
Template 5	Low Security. Allows all traffic from the LAN to the Internet.

Figure 3-43: Port Blocker Basic

Note:	Templates modify only the ports that are opened to outgoing traffic (from the LAN to the Internet). In all Templates all incoming ports (Internet to the LAN) are blocked. To allow ports from the outside the appropriate rules must be created in Port Blocker Advanced.

Upon selecting a Template ComSifter will:

1. Stop Network, Filtering and Proxy Services
2. Load the Port Blocker Rules from the selected Template
3. Restart the Port Blocker with the Template rules set.
4. Start Network, Filtering and Proxy Services

Template 1, High Security

Template 1 allows no connection from the Internet to the LAN and only allows web browsing (80) and secure web browsing (443). All other ports are blocked.

Template 2, High – Medium Security

Template 2 builds on Template 1 and adds support for email clients such as Outlook, Outlook Express and Eudora. POP3 (110, 995), IMAP (143, 993) and SMTP (25, 465) are opened from the LAN to the Internet.

Template 3, Medium Security

Template 3 builds on Template 2 and adds support for the popular chat programs from Instant Messenger, Yahoo Chat and MSN Messenger. IM (5190), MSN (1863 5190 6891-6901) and Yahoo (5000-5010 5055 5100) are opened from the LAN to the Internet.

Template 4, Medium – Low Security

Template 4 builds on Template 3 and adds support for the popular remote control programs Laplink, pcAnywhere and VNC. Laplink (389 1024 1183 1184 1547), pcAnywhere (5631 5632), VNC (5901-5905) are opened from the LAN to the Internet.

Template 5, Low Security

Template 5 allows opens all ports from the LAN to the Internet. This setting is equivalent to the capabilities of the Port Blocker found in home and small business routers from companies such as Linksys, Netgear and SMC.

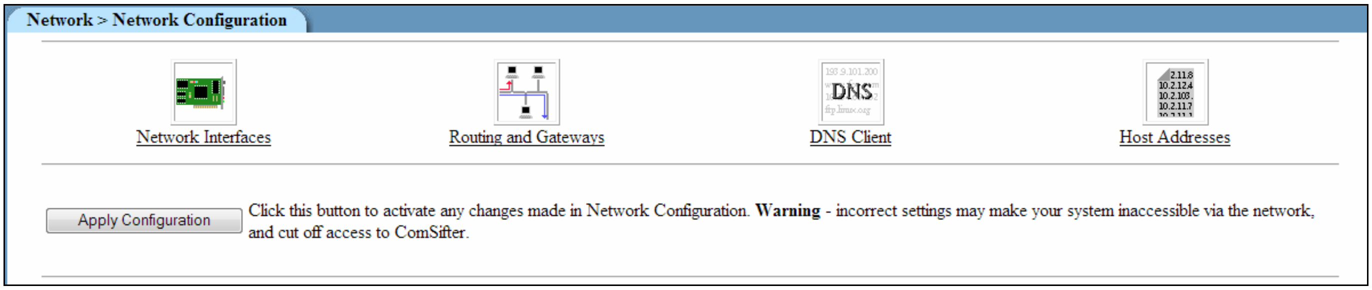
Warning: Although this setting may be the easiest to configure and maintain, it is the least secure. Any program originating on a LAN computer will be able to access the Internet without restriction.

Network Configuration

In this section the Network, DNS, and Gateway settings of your network will be configured.

Note: ComSifter includes Network Wizards. The wizards are designed to automatically configure most network settings defined in this chapter.

To access these settings click on **Network Configuration**. You will be presented with the following choices:



Click this button to activate any changes made in Network Configuration. **Warning** - incorrect settings may make your system inaccessible via the network, and cut off access to ComSifter.

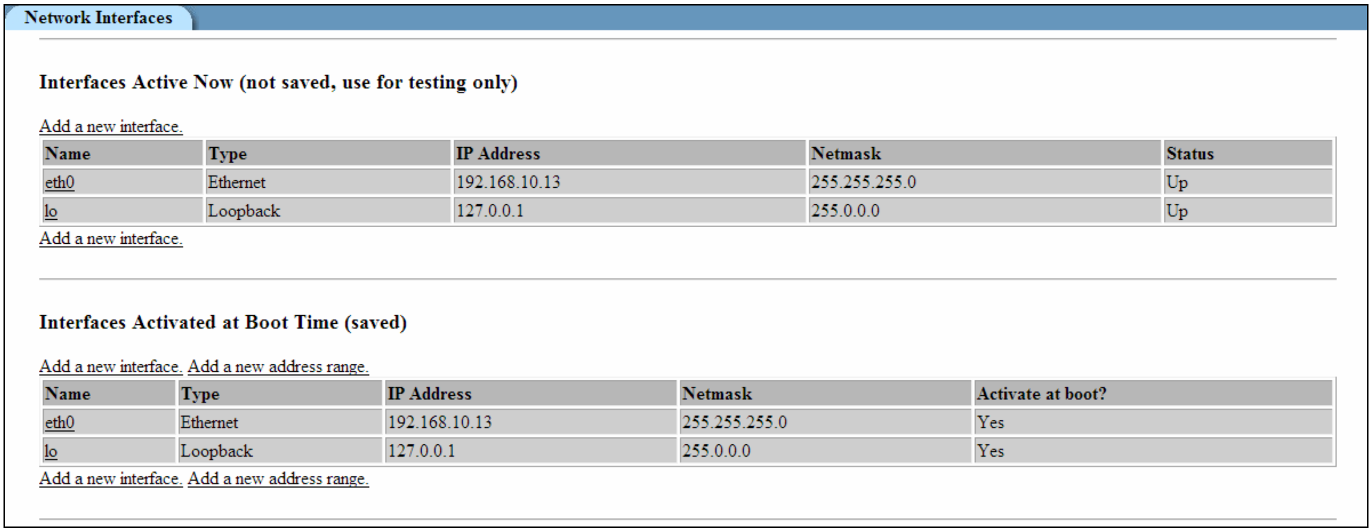
Figure 3-44: Network Configuration Choices

Network Interfaces (IP Address Configuration)

ComSifter is configured with two Ethernet interfaces. Eth0 is connected to the WAN (cable, DSL, TI or upstream device) while eth1 is connected to the internal LAN.

Additionally a PPP interface is defined that will automatically become active through eth0 when PPPOE is used.

There are two sections to Network Interfaces configuration.



Interfaces Active Now (not saved, use for testing only)

Add a new interface.

Name	Type	IP Address	Netmask	Status
eth0	Ethernet	192.168.10.13	255.255.255.0	Up
lo	Loopback	127.0.0.1	255.0.0.0	Up

Add a new interface.

Interfaces Activated at Boot Time (saved)

Add a new interface. Add a new address range.

Name	Type	IP Address	Netmask	Activate at boot?
eth0	Ethernet	192.168.10.13	255.255.255.0	Yes
lo	Loopback	127.0.0.1	255.0.0.0	Yes

Add a new interface. Add a new address range.

Figure 3-45: Selecting Network Interface

Interfaces Active Now

The first of these is Interfaces Active Now. Interfaces Active Now reflects the current configuration. Any changes made will only last until the next time the ComSifter is restarted. Then the setting in Interfaces Active at Boot Time will become Interfaces Active Now. Interfaces Active Now is only used for temporarily trying out a new setting and is not used in the normal configuration of ComSifter.

Interfaces Active at Boot Time

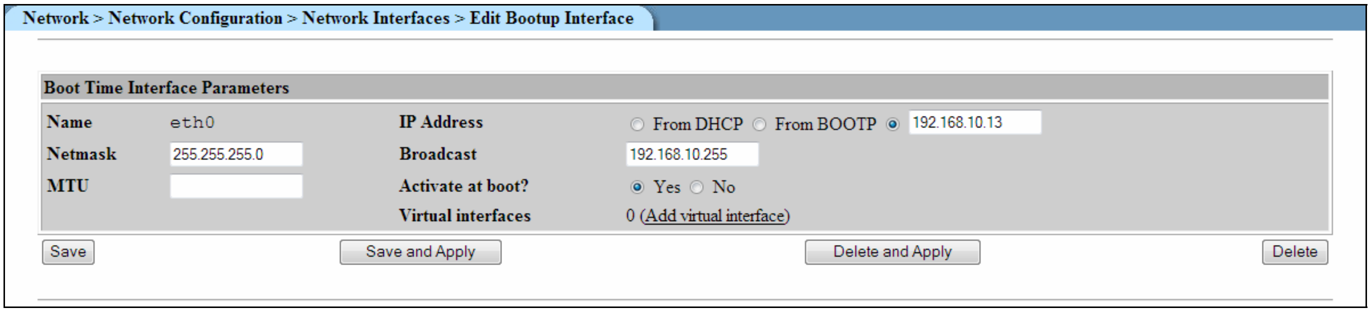
Normal configuration of ComSifter networking is done in this area. Any changes made here will be permanent.

ComSifter is factory configured to an IP of 192.168.1.1 with a subnet mask of 255.255.255.0. If your network does not use these settings then change the IP and netmask of ComSifter as described in this section.

Warning:	Entering the wrong IP address and subnet mask will cause you to lose communication with ComSifter. If you do not remember the information entered you will not be able to reconnect with ComSifter. Also insure that IP Access Control (see Security Configuration) is not configured to an address that will prevent re-logging into ComSifter. If you forget or miss-configure the IP address refer to the section Recovering a lost IP address.

Interface Settings (eth0)

Under Interfaces activated at Boot Time click on **eth0**.



Network > Network Configuration > Network Interfaces > Edit Bootup Interface

Boot Time Interface Parameters

Name	eth0	**IP Address**	○ From DHCP ○ From BOOTP ● 192.168.10.13
Netmask	255.255.255.0	**Broadcast**	192.168.10.255
MTU		**Activate at boot?**	● Yes ○ No
		Virtual interfaces	0 (Add virtual interface)

Figure 3-46: Entering IP and Subnet Mask

1. Netmask - Change the Netmask to reflect your network requirements.
2. MTU - Leave the MTU blank (default) unless your network has special requirements.
3. IP Address - If you obtain the external IP from the attached cable, DSL, T1 modem or upstream device from DHCP then click on **DHCP**. If you have been assigned a static IP then click the button next to then blank field then enter the IP in the blank field.
4. Broadcast - Enter the broadcast address for ComSifter, if different from default. Normally the broadcast address ends in 255.
5. Activate on Boot - Insure that **Yes** is selected.

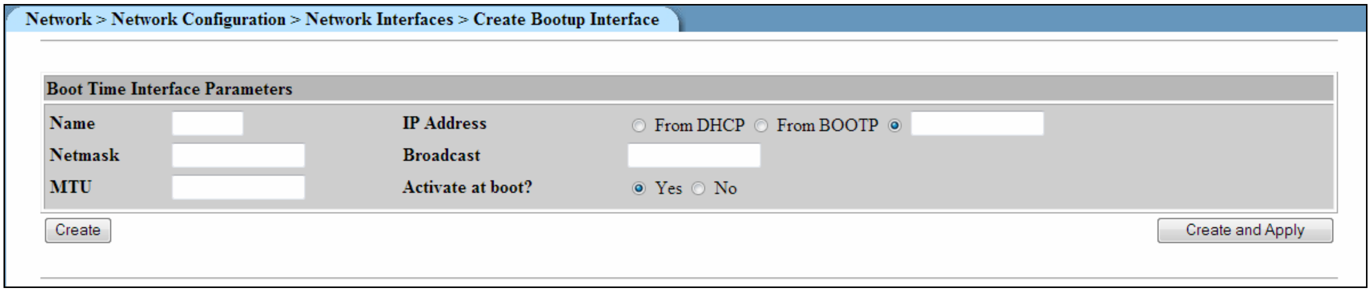
If your network is using only one network range (Class C) i.e. 192.168.1.xxx then click on **Save** and continue to **Routing and Gateways**.

Virtual Interfaces

Note:	The Virtual Interfaces section is for advanced technicians only. The majority of networks will not need Virtual Interfaces. If you have any questions please contact Comsift Technical Support.

ComSifter has the ability to route multiple Networks to one Internet Gateway. For instance it is possible for two Class A networks, a 10.xxx.xxx.xxx network and a 192.xxx.xxx.xxx network to both use a 192.xxx.xxx.xxx gateway. This is accomplished by clicking on **Add Virtual Interface** as shown in Figure

3-7. When a virtual interface is added, ComSifter will need an IP on the new network. Enter the information for the virtual interface and click on **Create**.


Network > Network Configuration > Network Interfaces > Create Bootup Interface
Boot Time Interface Parameters
Name
Netmask
MTU
Create
Create and Apply

IP Address ○ From DHCP ○ From BOOTP ●

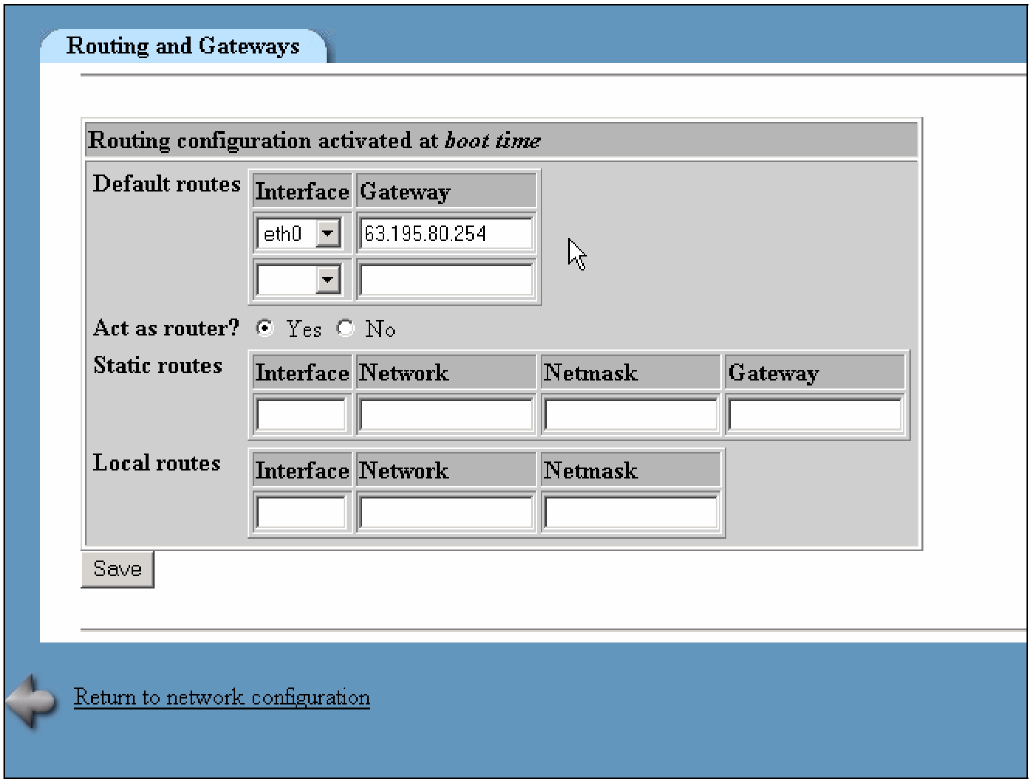
Broadcast

Activate at boot? ● Yes ○ No

Figure 3-47: Adding a Virtual Interface

Note:	If your network consists of two or more Class B networks i.e. 192.168.xxx.xxx it is more straightforward to open the Netmask on the main Interface to 255.255.0.0 than to add virtual interfaces.

Routing and Gateways



Routing and Gateways
Routing configuration activated at *boot time*
Interface
Gateway
Network
Netmask
Save
Return to network configuration

Default routes: Interface eth0, Gateway 63.195.80.254

Act as router? ● Yes ○ No

Static routes

Local routes

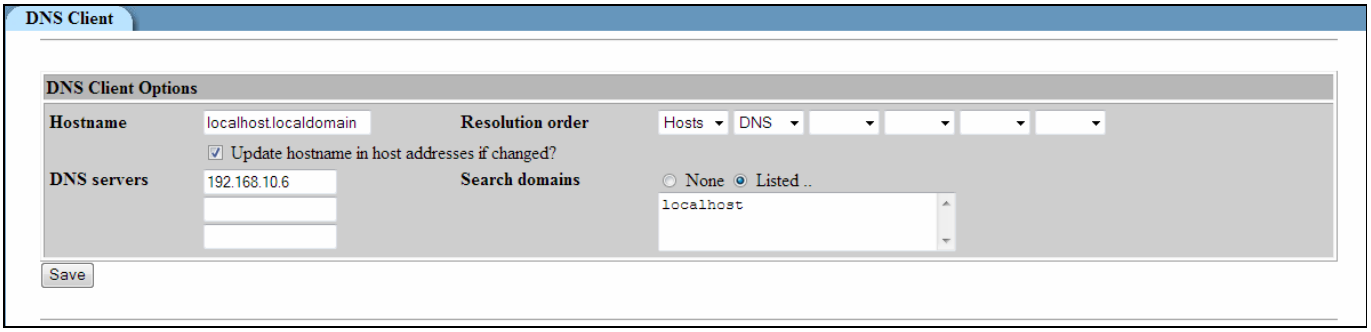
Figure 3-48: Entering Gateway IP

Enter the IP address of the External Gateway that ComSifter will use to access the Internet.

Note: The remaining options are not used in normal operation and may be left blank (default).

When completed click on **Save.**

DNS



Hostname: localhost.localdomain

☑ Update hostname in host addresses if changed?

Resolution order: Hosts, DNS

DNS servers: 192.168.10.6

Search domains: ○ None ● Listed ..

localhost

Figure 3-49: Entering DNS Settings

Enter the DNS server settings that ComSifter will use to resolve Domain Names.

Required Settings are:

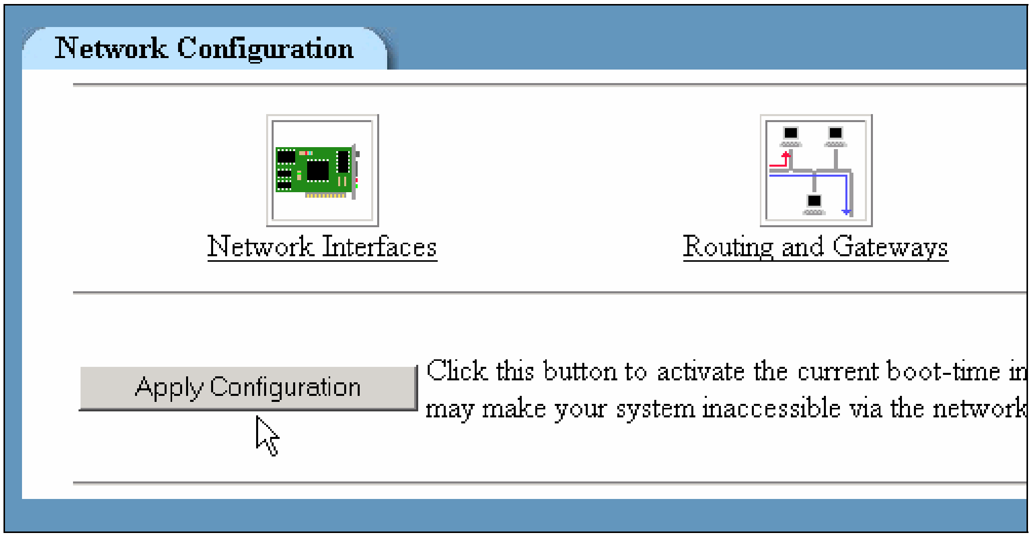
1. Hostname – must be localhost.
2. DNS servers - Enter the DNS server names that ComSifter will use to resolve Domain Names.
3. Resolution order – must be Hosts, DNS.
4. Search domains – must be Listed, localhost.

Warning: Do not change the Hostname, Resolution order or Search domains unless instructed to do so by Comsift Technical Support.

Note: ComSifter includes a Smart DNS feature. Every 15 minutes ComSifter queries the defined DNS servers and calculates their lookup times. If the Secondary DNS server is faster than the Primary DNS server by more than 200ms over 3 queries in a 45 minute period, ComSifter will make the faster Secondary DNS server the Primary DNS server.

When completed click on **Save**.

Completing the DNS/Gateway Configuration



Click this button to activate the current boot-time in
may make your system inaccessible via the network

Figure 3-50: Apply Configuration

The final step in completing the DNS/Gateway configuration is to click the **Apply Configuration** button.

Warning: This step will change the IP of ComSifter. If you have changed the IP of ComSifter, you must reconfigure the computer you are using to configure ComSifter, to reflect the new IP and netmask.

Recovering a lost IP address

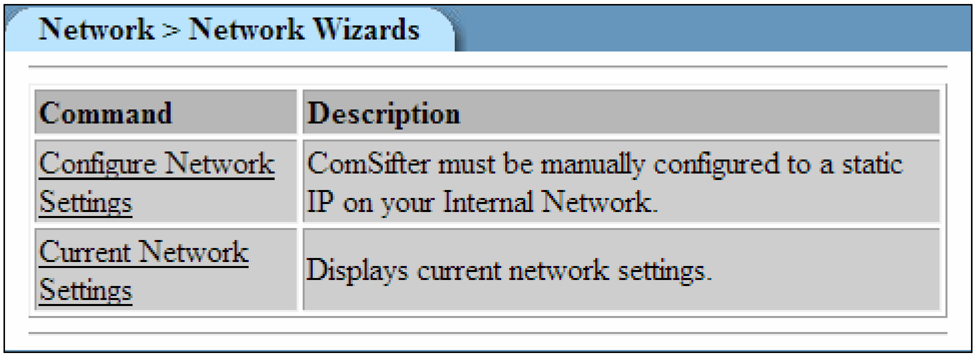
ComSifter includes a failsafe method to determine network settings in the event that the settings are forgotten or miss-configured.

Attach a standard VGA compatible monitor and keyboard to the ComSifter. Restart the ComSifter. At the end of the start up process you will see a screen that says type YES to enter the Emergency Console. You have 30 seconds to enter YES. Upon accessing the Emergency Console you will be prompted to enter a number to View Network Settings. The Network Settings will include the Internal IP of the ComSifter.

Network Wizard

The Network Wizard may be used to quickly configure your ComSifter. The following parameters will be set:

- IP, Netmask and Gateway settings.
- A Port Blocker Basic Template.
- DNS Settings.
- DHCP Server settings (optional).

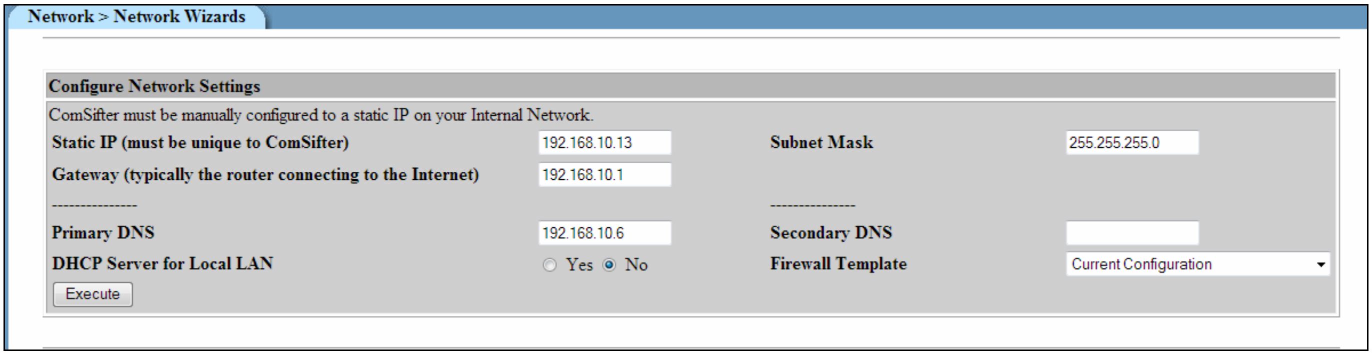


Network > Network Wizards

Command	Description
Configure Network Settings	ComSifter must be manually configured to a static IP on your Internal Network.
Current Network Settings	Displays current network settings.

Figure 3-51: Network Wizards

Configure Network Settings



Network > Network Wizards

Configure Network Settings

ComSifter must be manually configured to a static IP on your Internal Network.

Static IP (must be unique to ComSifter)	192.168.10.13	Subnet Mask	255.255.255.0
Gateway (typically the router connecting to the Internet)	192.168.10.1		
---------------		---------------	
Primary DNS	192.168.10.6	Secondary DNS	
DHCP Server for Local LAN	○ Yes ● No	Firewall Template	Current Configuration

Figure 3-52: Network Wizard - Static IP

IP

Enter the IP for your installation. The IP must be static, not used by any other device and on the same network as your client computers.

Subnet Mask

Enter the Subnet Mask for your installation. The format for this entry is xxx.xxx.xxx.xxx such as 255.255.255.0.

Gateway

Enter the External Gateway for your installation. Typically this will be your router.

DNS

Enter the DNS settings for your network. This setting determines where ComSifter will go to resolve domain names to IP numbers.

Note: If ComSifter is installed in a network that uses a Domain Controller (Windows 2000/2003 Server) then ComSifter may use the same Domain Controller for DNS. Enter the IP address of the Domain Controller.

Note: ComSifter includes DNS forwarding. ComSifter will listen to the LAN network for DNS requests. If a request is received, ComSifter will forward the request to the defined DNS server.

DHCP Server for Local LAN

If enabled, ComSifter will provide DHCP Server services for the network. Default settings for DHCP Server are:

- Scope – xxx.xxx.xxx.30 – xxx.xxx.xxx.230.
- Client Lease time – Eight (8) Days.
- Client DNS Settings – Settings described in Primary and Secondary DNS.
- Client Gateway – ComSifters Internal IP.

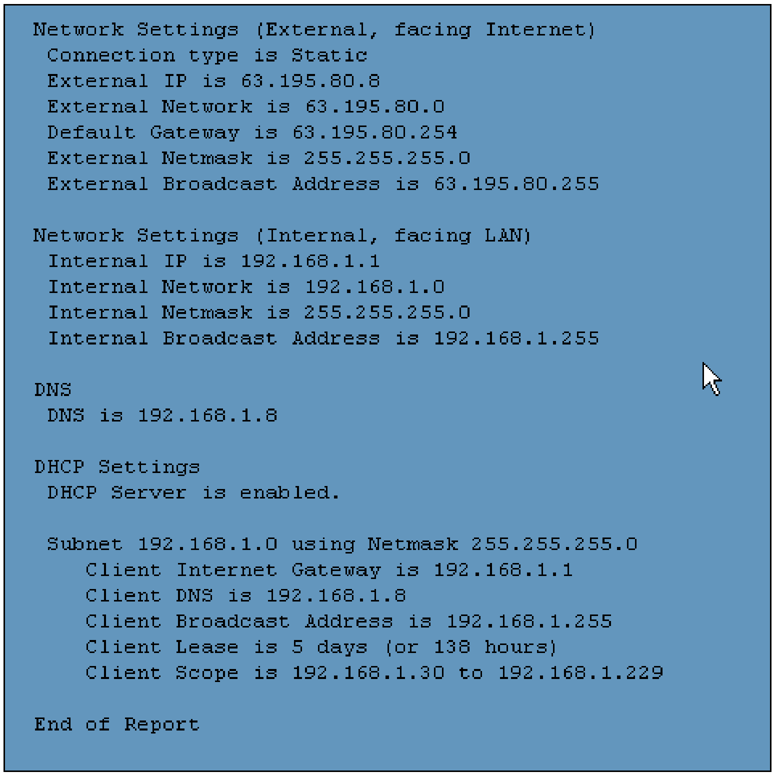
Note: If the network that ComSifter is installed into uses a Domain Controller (Windows 2000/2003 Server) then the Domain Controller may be providing DHCP Services. If so do not enable ComSifters DHCP Server.

Port Blocker Template

Select a **Port Blocker Template** from the drop down box. Port Blocker Templates are described in this manual under Port Blocker Basic (Templates).

Current Network Settings

Current Network Settings will list all current settings.



```
Network Settings (External, facing Internet)
 Connection type is Static
 External IP is 63.195.80.8
 External Network is 63.195.80.0
 Default Gateway is 63.195.80.254
 External Netmask is 255.255.255.0
 External Broadcast Address is 63.195.80.255

Network Settings (Internal, facing LAN)
 Internal IP is 192.168.1.1
 Internal Network is 192.168.1.0
 Internal Netmask is 255.255.255.0
 Internal Broadcast Address is 192.168.1.255

DNS
 DNS is 192.168.1.8

DHCP Settings
 DHCP Server is enabled.

 Subnet 192.168.1.0 using Netmask 255.255.255.0
    Client Internet Gateway is 192.168.1.1
    Client DNS is 192.168.1.8
    Client Broadcast Address is 192.168.1.255
    Client Lease is 5 days (or 138 hours)
    Client Scope is 192.168.1.30 to 192.168.1.229

End of Report
```

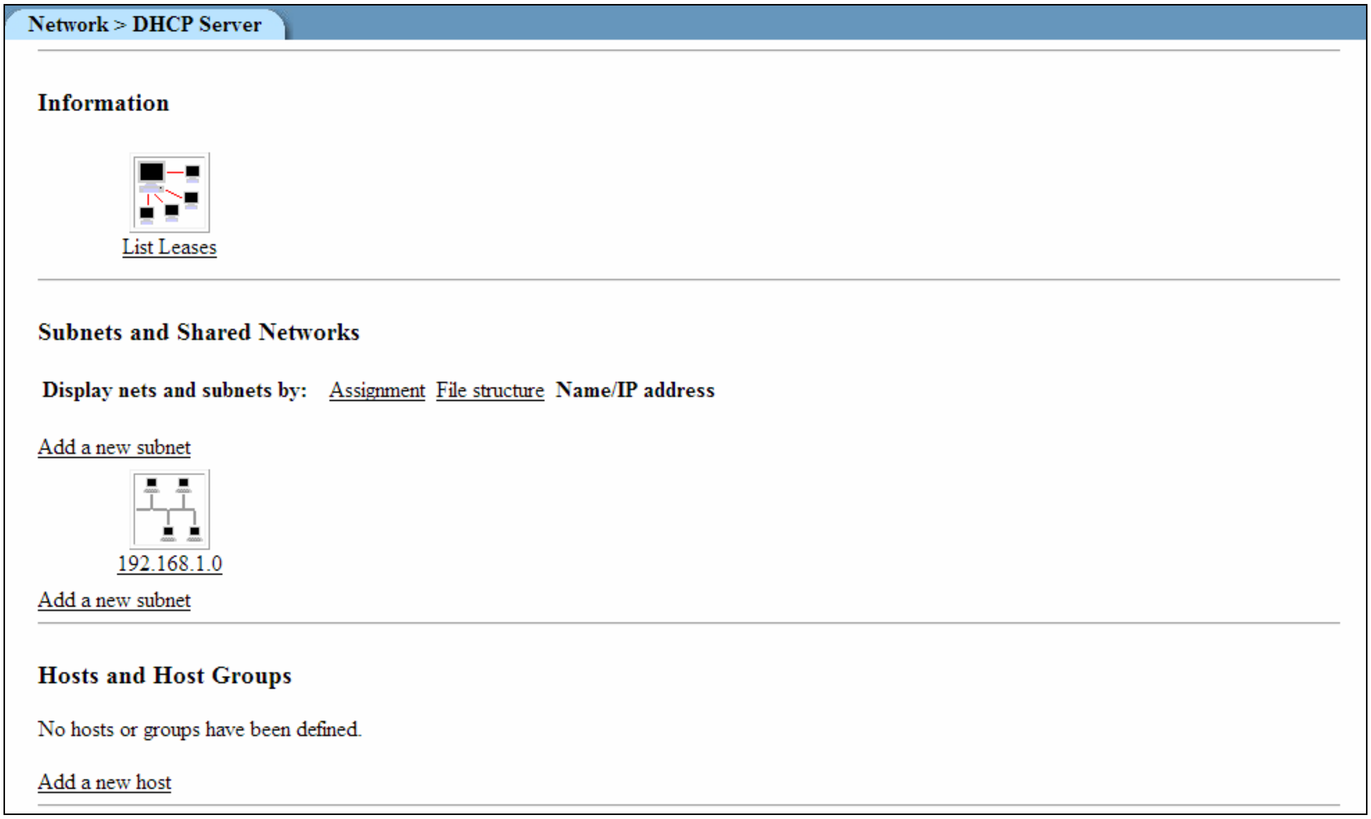
Figure 3-53: Current Network Settings

Using the ComSifter DHCP Server

ComSifters DHCP server is factory configured but not activated when shipped. Following are the factory settings for the DHCP server:

- Scope 192.168.1.10 – 192.168.1.240
- Subnet Mask 255.255.255.0
- Default Router 192.168.1.1
- Default Gateway 192.168.1.1
- Broadcast Address 192.168.1.255
- Lease Time 7 days

It is suggested that Network Wizards be used to initially set up the ComSifter. You may then modify the DHCP files to meet your network needs.



No hosts or groups have been defined.

Figure 3-54: DHCP Server

In the initial DCHP server screen the following options are available.

- Information – Allows you to list leases.
- Subnets and shared networks - This allows the setting of the subnet common address pool options and options that will be given to client work stations.
- Hosts and Host Groups - Allows definition of host(s) that will be excluded from the IP scope.

Information

Allows you to list leases.

List leases

List leases allows you to see the lease database as defined below.

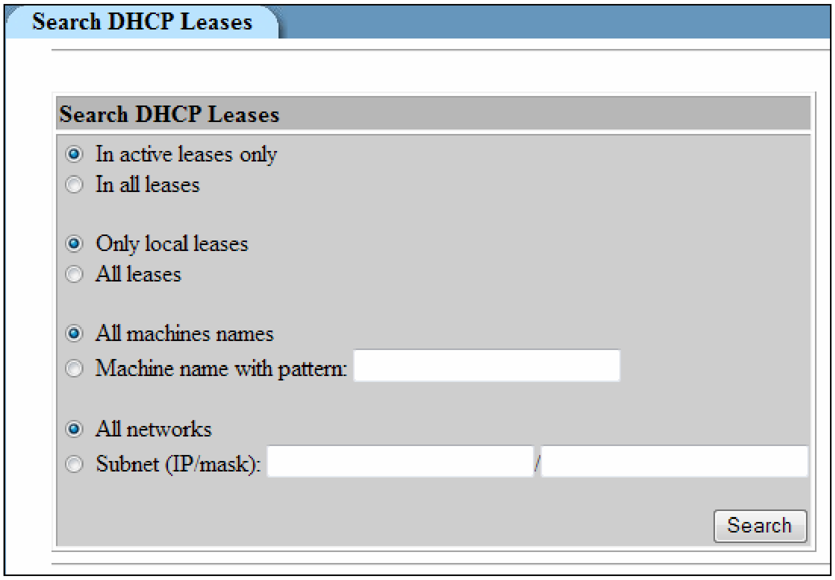


Figure 3-55: DHCP Leases

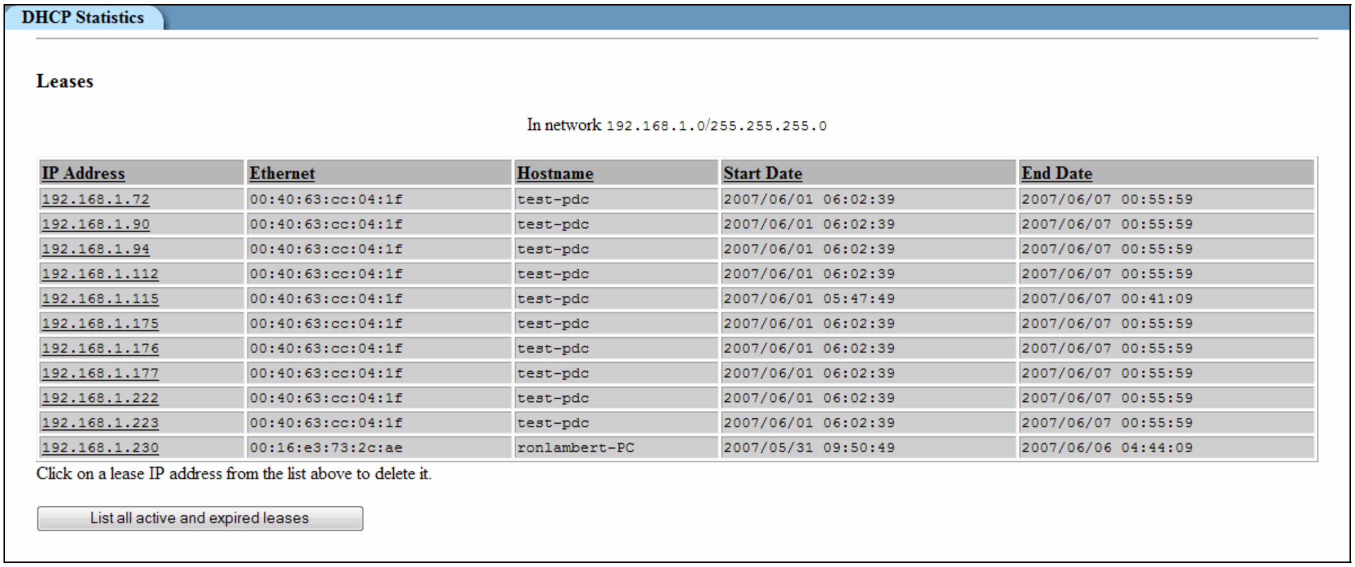
- In active leases only/in all leases - Displays leases that are currently active (within lease period) or displays all leases including leases that have expired.
- Only local leases/all leases – Displays local leases only or displays local leases and remote leases.
- All machines names/Machine name with pattern – All machine names will display all computers with leases. Machine name with pattern may be used to find only one computer using its machine name (netbios).
- All networks/Subnet (IP/mask) – If you have more then one network this field may be used to display anyone’s network using the IP/mask.

Results of List Leases

After a query of Search DHCP Leases a DHCP statistics display will be returned. The following information is displayed:

Leases

- IP Address - The IP Address of the work station with the lease.
- Ethernet - The MAC address of the work station with the lease.
- Hostname - The netbios name of the work station with the lease.
- Start Date - The time and date the lease was issued.
- End Date - The time and date the lease will expire.



Leases

In network 192.168.1.0/255.255.255.0

IP Address	Ethernet	Hostname	Start Date	End Date
192.168.1.72	00:40:63:cc:04:1f	test-pdc	2007/06/01 06:02:39	2007/06/07 00:55:59
192.168.1.90	00:40:63:cc:04:1f	test-pdc	2007/06/01 06:02:39	2007/06/07 00:55:59
192.168.1.94	00:40:63:cc:04:1f	test-pdc	2007/06/01 06:02:39	2007/06/07 00:55:59
192.168.1.112	00:40:63:cc:04:1f	test-pdc	2007/06/01 06:02:39	2007/06/07 00:55:59
192.168.1.115	00:40:63:cc:04:1f	test-pdc	2007/06/01 05:47:49	2007/06/07 00:41:09
192.168.1.175	00:40:63:cc:04:1f	test-pdc	2007/06/01 06:02:39	2007/06/07 00:55:59
192.168.1.176	00:40:63:cc:04:1f	test-pdc	2007/06/01 06:02:39	2007/06/07 00:55:59
192.168.1.177	00:40:63:cc:04:1f	test-pdc	2007/06/01 06:02:39	2007/06/07 00:55:59
192.168.1.222	00:40:63:cc:04:1f	test-pdc	2007/06/01 06:02:39	2007/06/07 00:55:59
192.168.1.223	00:40:63:cc:04:1f	test-pdc	2007/06/01 06:02:39	2007/06/07 00:55:59
192.168.1.230	00:16:e3:73:2c:ae	ronlambert-PC	2007/05/31 09:50:49	2007/06/06 04:44:09

Click on a lease IP address from the list above to delete it.

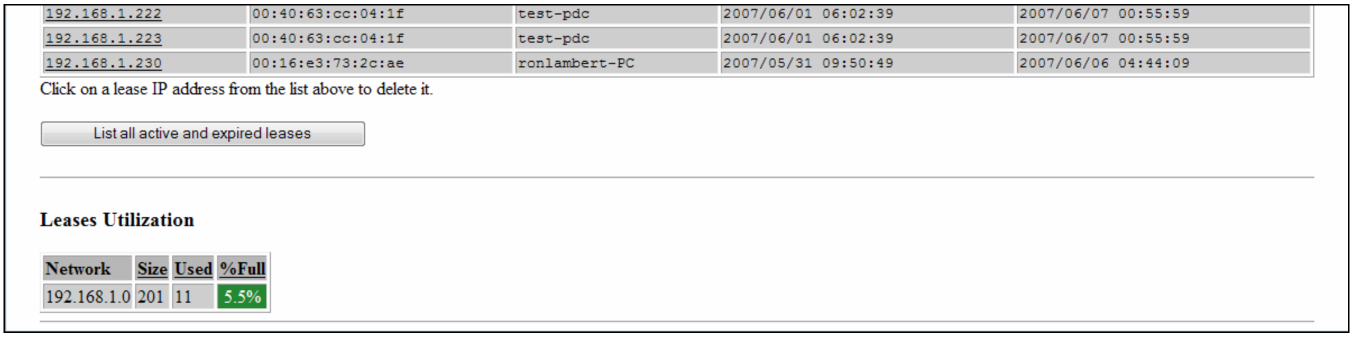
Figure 3-56: DHCP Statistics

Note:	You may sort each column by clicking the column heading.

Leases Utilization

At the bottom of the DHCP Statistics page, Lease Utilization is shown.

- Network - The network being utilized.
- Size - The number of leases defined.
- Used - The number of leases that have been used.
- %Full - The number of leases used as a percentage.



192.168.1.222	00:40:63:cc:04:1f	test-pdc	2007/06/01 06:02:39	2007/06/07 00:55:59
192.168.1.223	00:40:63:cc:04:1f	test-pdc	2007/06/01 06:02:39	2007/06/07 00:55:59
192.168.1.230	00:16:e3:73:2c:ae	ronlambert-PC	2007/05/31 09:50:49	2007/06/06 04:44:09

Click on a lease IP address from the list above to delete it.

Leases Utilization

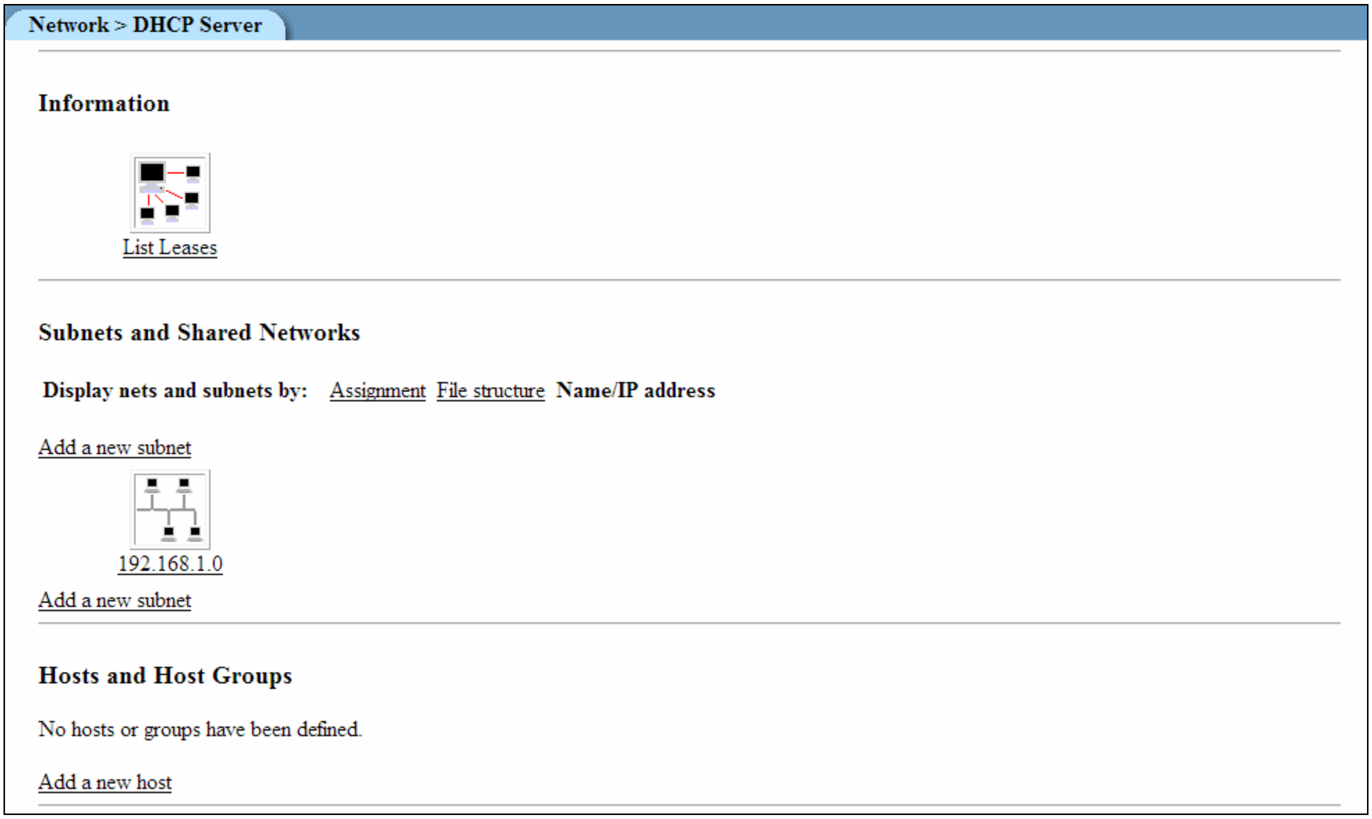
Network	Size	Used	%Full
192.168.1.0	201	11	5.5%

Figure 3-57: Lease Utilization

Note:	If utilization exceeds 90% a warning email message will sent to the DHCP log and any email recipients defined in Maintenance > Utilities > Email Notification Parameters.

Subnets and Shared Networks

Subnets and Shared Networks allows you to define a network over which ComSifter will control DHCP.



Network > DHCP Server

Information

List Leases

Subnets and Shared Networks

Display nets and subnets by: Assignment File structure Name/IP address

Add a new subnet

192.168.1.0

Add a new subnet

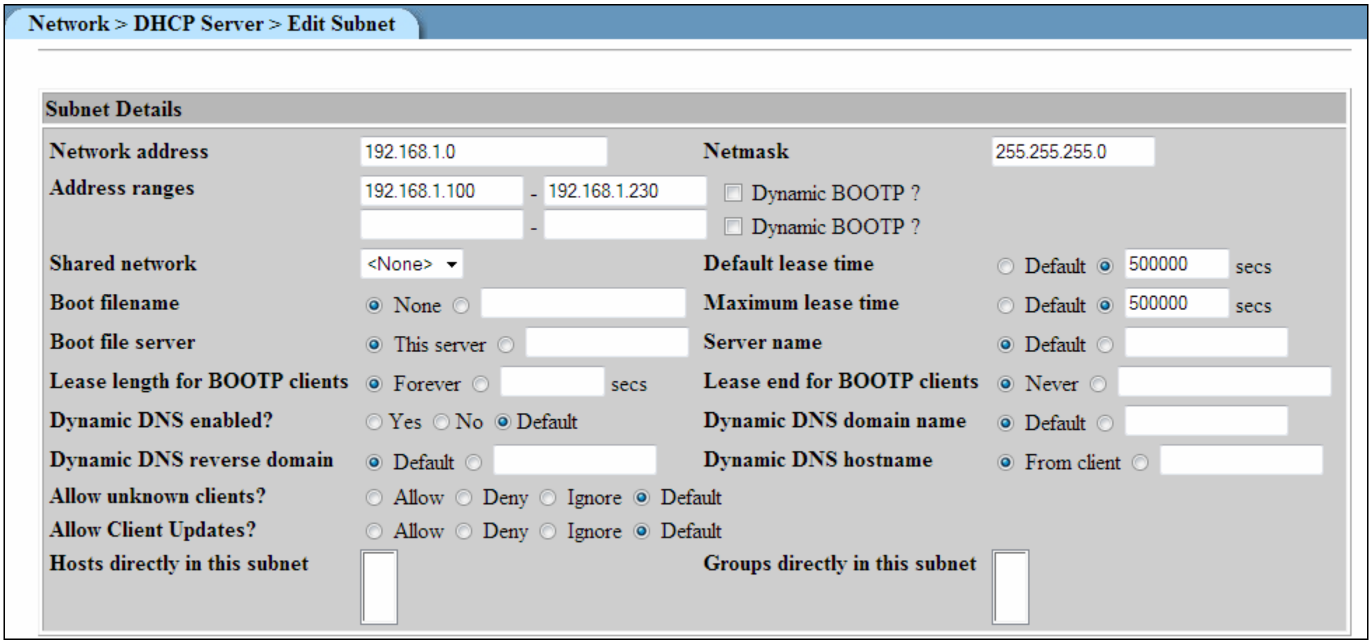
Hosts and Host Groups

No hosts or groups have been defined.

Add a new host

Figure 3-58: Selecting Network

Click on **Add a New Subnet** or click on an existing defined network (as displayed by a small network picture with an appropriate subnet label). The example below is the result of selecting the 192.168.1.0 network.



Network > DHCP Server > Edit Subnet

Subnet Details

Network address	192.168.1.0	**Netmask**	255.255.255.0
Address ranges	192.168.1.100 - 192.168.1.230 ☐ Dynamic BOOTP ? - ☐ Dynamic BOOTP ?		
Shared network	<None>	**Default lease time**	○ Default ● 500000 secs
Boot filename	● None ○	**Maximum lease time**	○ Default ● 500000 secs
Boot file server	● This server ○	**Server name**	● Default ○
Lease length for BOOTP clients	● Forever ○ secs	**Lease end for BOOTP clients**	● Never ○
Dynamic DNS enabled?	○ Yes ○ No ● Default	**Dynamic DNS domain name**	● Default ○
Dynamic DNS reverse domain	● Default ○	**Dynamic DNS hostname**	● From client ○
Allow unknown clients?	○ Allow ○ Deny ○ Ignore ● Default		
Allow Client Updates?	○ Allow ○ Deny ○ Ignore ● Default		
Hosts directly in this subnet		**Groups directly in this subnet**	

Figure 3-59: Setting the DHCP Subnet

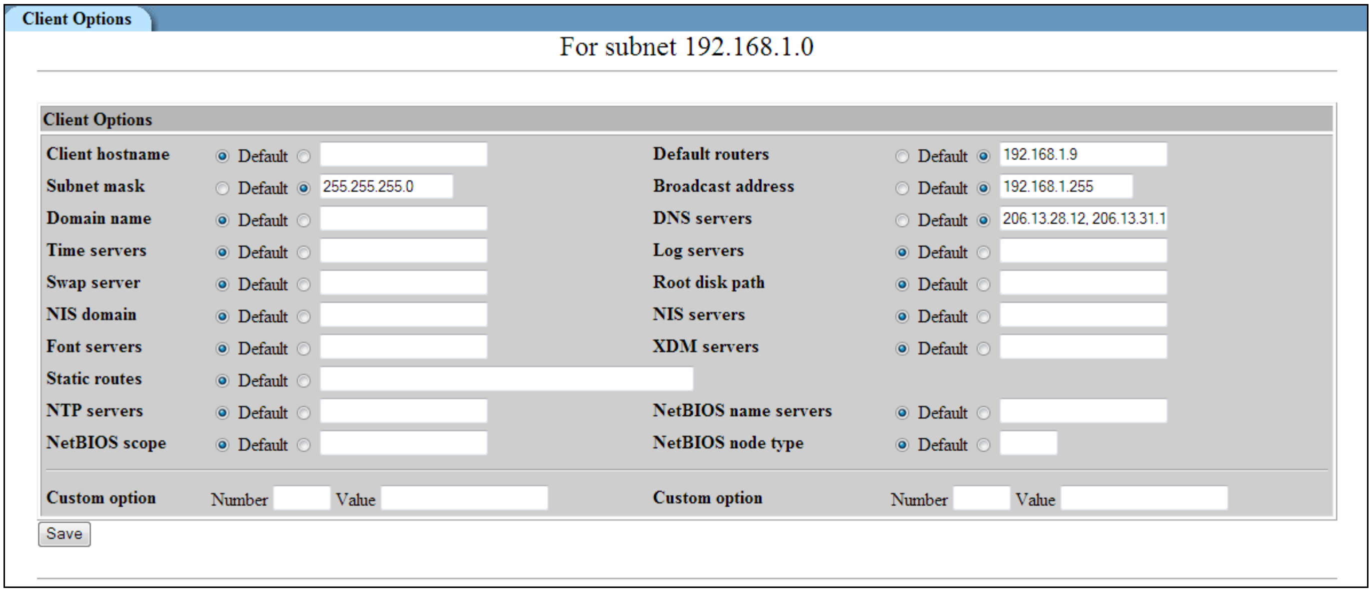
The above example shows the factory defaults for setting the DHCP Subnet. If your network uses a different subnet then replace the values shown with your network's settings.

1. Network Address - Enter the network address. This should end in a 0, i.e. xxx.xxx.xxx.0.
2. Netmask - The netmask of the Network Address defined in step.
3. Edit Client Options - See next section, Edit Client Options.
4. List Leases - List current and expired leases.
5. Address Pools for Subnet – See section Address Pools for Subnet.
6. Add A New Host - See section Add a New Host.

Note: The remaining options are not used in ComSifter and may be left blank (default).

Edit Client Options

The example below shows the factory defaults for setting the DHCP Client options. These options will be delivered to a client requesting a lease. If your network uses different settings, then replace the values shown with your network's settings.



For subnet 192.168.1.0

Client Options

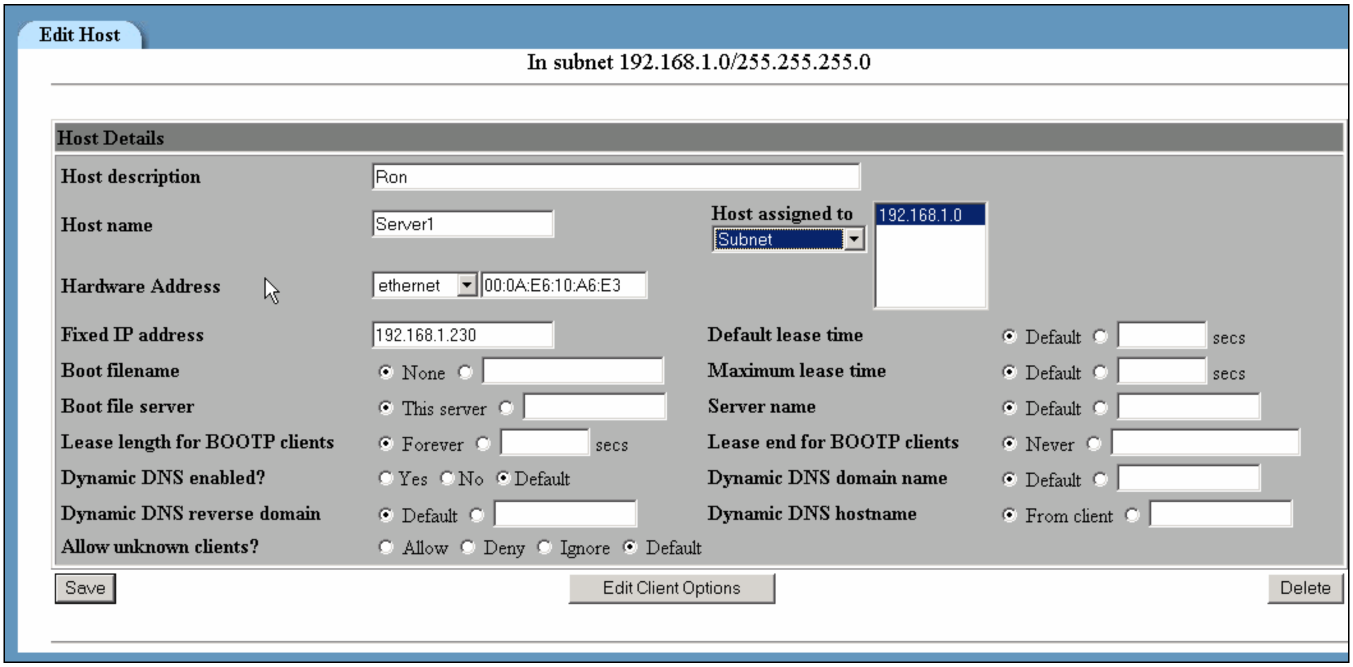
Client hostname	● Default	○	**Default routers**	○ Default	● 192.168.1.9
Subnet mask	○ Default	● 255.255.255.0	**Broadcast address**	○ Default	● 192.168.1.255
Domain name	● Default	○	**DNS servers**	○ Default	● 206.13.28.12, 206.13.31.1
Time servers	● Default	○	**Log servers**	● Default	○
Swap server	● Default	○	**Root disk path**	● Default	○
NIS domain	● Default	○	**NIS servers**	● Default	○
Font servers	● Default	○	**XDM servers**	● Default	○
Static routes	● Default	○			
NTP servers	● Default	○	**NetBIOS name servers**	● Default	○
NetBIOS scope	● Default	○	**NetBIOS node type**	● Default	○
Custom option	Number	Value	**Custom option**	Number	Value

Figure 3-60: Entering Client DHCP Option

1. Subnet mask – enter the subnet mask that client computers should use
2. Default Routers – enter the IP address of ComSifter. This will become the Default Gateway for client computers.
3. Broadcast Address – in the format xxx.xxx.xxx.255.
4. DNS Servers – enter the DNS server(s) that client computers should use. Multiple servers may be entered by placing a space between server entries.

Note:	The remaining options are not used in normal operation and may be left blank (default).

Host and Host Groups



In subnet 192.168.1.0/255.255.255.0

Host Details

Host description	Ron		
Host name	Server1	Host assigned to	Subnet 192.168.1.0
Hardware Address	ethernet 00:0A:E6:10:A6:E3		
Fixed IP address	192.168.1.230	Default lease time	● Default ○ secs
Boot filename	● None ○	Maximum lease time	● Default ○ secs
Boot file server	● This server ○	Server name	● Default ○
Lease length for BOOTP clients	● Forever ○ secs	Lease end for BOOTP clients	● Never ○
Dynamic DNS enabled?	○ Yes ○ No ● Default	Dynamic DNS domain name	● Default ○
Dynamic DNS reverse domain	● Default ○	Dynamic DNS hostname	● From client ○
Allow unknown clients?	○ Allow ○ Deny ○ Ignore ● Default		

Figure 3-61: Add a New Host

The Add Host feature is used to assign a specific IP within the DHCP scope to a specific client on the network based on the clients MAC address. This is useful when the network has clients such as servers and printers that other clients on the network connect to based on IP address. The DHCP server will reserve the IP and only issue it to the device with the specified MAC address.

The following fields are required.

1. Host Description – This may be a friendly name to help describe the Host.
2. Host Name – client computer name.
3. Hardware Address – Type must be Ethernet. Enter the MAC address of the client computer. It must be entered in the format xx:xx:xx:xx:xx:xx.
4. Fixed IP Address – the IP address to be assigned to ComSifter.
5. Host Assigned to – subnet.

Note: The remaining options are not used in ComSifter and may be left blank (default).

The ADD Host feature may appear to be the proper solution for defining fixed IP devices on a network but best practices would suggest otherwise. Since the IP is based on the client device MAC address, if the client computer is changed, thus changing the MAC address, then the settings above would have to be changed. A better solution would be to define the DHCP range to exclude an area reserved for fixed IP devices. ComSifters default settings offer such an excluded range as follows:

- 192.168.1.1 – 192.168.1.9 Not included in DHCP scope. Use for fixed IP devices.
- 192.168.1.10 – 192.168.1.240 Included in DHCP scope. Will be assigned to clients requesting lease.
- 192.168.1.241 – 192.168.1.254 Not included in DHCP scope. Use for fixed IP devices.

Starting and Stopping the DHCP Server

Upon completion of configuring the DHCP server changes must be applied and the server restarted. The server must be started.

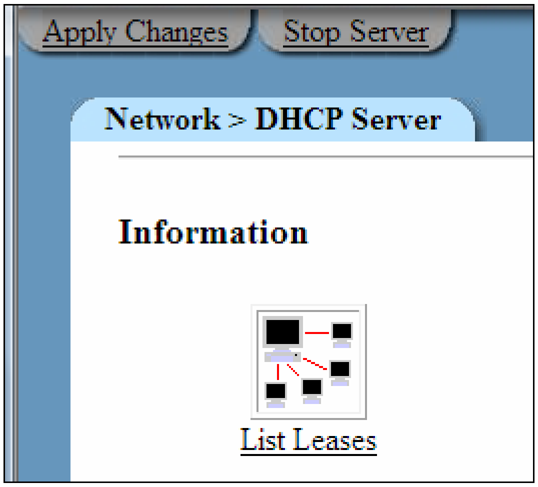


Figure 3-62: Starting/Stopping the DHCP Server

- Apply Changes -This will stop the DCHP server and apply all current changes. You must then start the DHCP server.
- Stop/Start Server – Pressing this link will either stop or start the DHCP service.

Maintenance

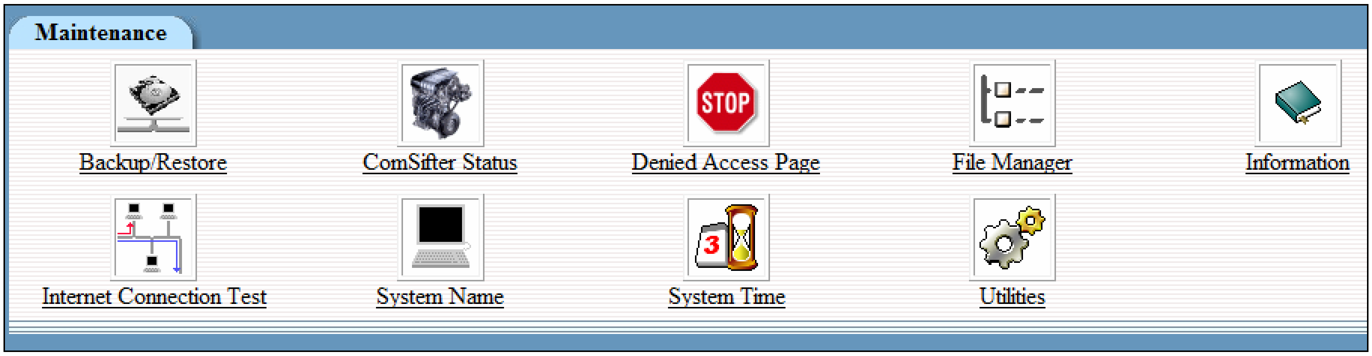


Figure 3-63: Maintenance

This section describes the functions of Maintenance. Maintenance is used to:

- Backup/restore all user-defined settings in ComSifter.
- View the status of all critical services running in ComSifter.
- Change the Denied Access Page.
- Move files into and out of ComSifter using File Manager.
- View Information about ComSifter
- Run an Internet Connection Test.
- Change the ComSifter System Name.
- Set/Change the System Time and Time Zone
- Stop and Start critical services located in Utilities.

Backup/Restore

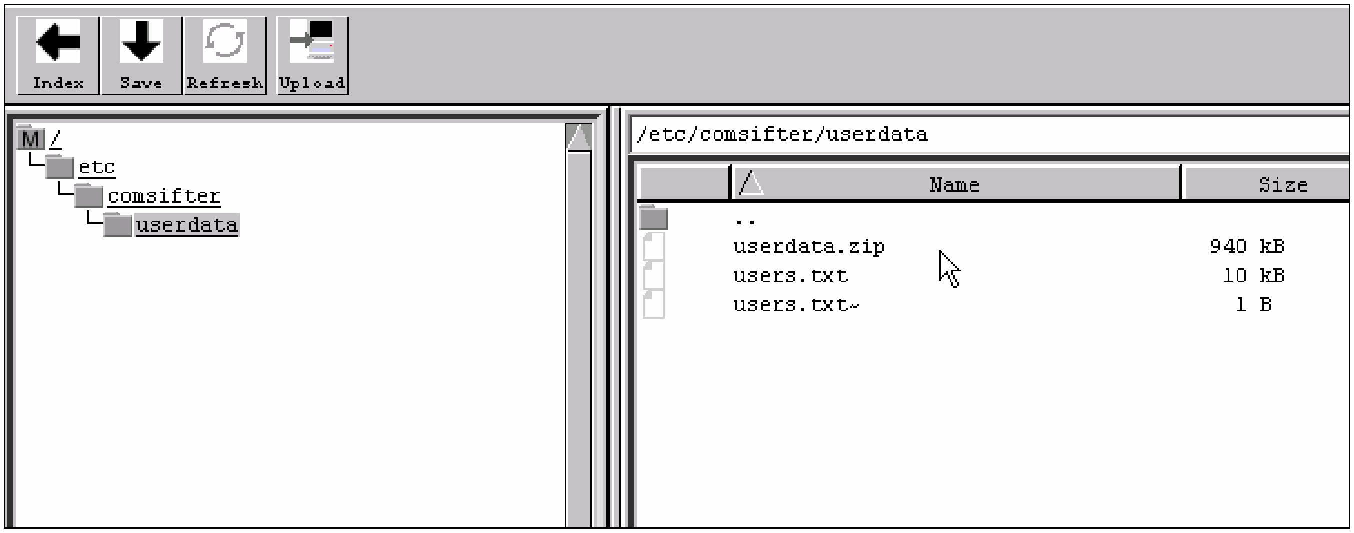
The following user settings are saved during a backup and may be restored during a Restore:

- Server settings
- Network settings
- Port Blocker settings
- Filter and Word/Phrases settings
- User Lists and settings

Creating a Backup

Creating a backup file is accomplished as follows:

1. Click on **Maintenance**, then **Backup/Restore**, then **Save Configuration Data**. Upon clicking backup a file is created containing the user-defined parameters described above.
    5. The file then needs to be moved to a location of your choice. This is done by clicking on **Maintenance**, then **File Manager**. File Manager will open and display the screen shown below.



```
/etc/comsifter/userdata
..
userdata.zip      940 kB
users.txt          10 kB
users.txt~          1 B
```

Figure 3-64: File Manager

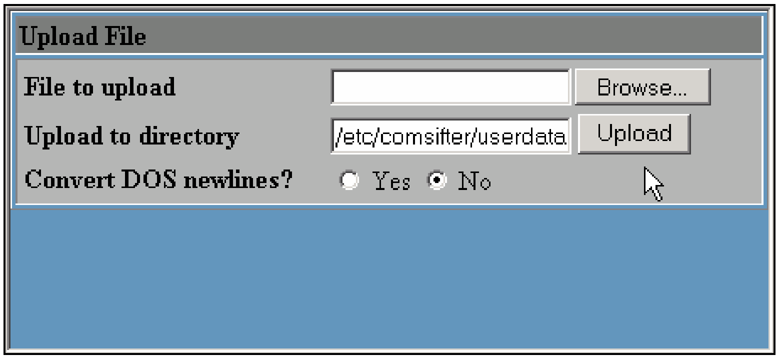
6. Select **userdata.zip** and click on the Save icon.
7. A standard save dialog box for your operating system will open allowing you to save the file to the location of your choice.

Restoring the Backup

Restoring a backup file is accomplished as follows:

1. Click on **Maintenance**, then **File Manager**, **File Manger** will open and display as shown in Figure 3-16.

8. Upon clicking Upload Upload the Upload Dialog will be shown.
9. Click the **Browse** button to find the file location of userdata.zip that was saved during Backup.



File to upload

Upload to directory: /etc/comsifter/userdata

Convert DOS newlines? ○ Yes ● No

Figure 3-65: Upload File

10. Click **Upload** to copy the file from the location selected to ComSifter.
11. Click on **Maintenance**, then **Backup/Restore**, then Restore **Configuration Data**. Upon clicking **Restore**, ComSifter will copy the restore file to its working directory and restart.

Warning:	ComSifter will not allow a Restore to be completed if IP Access Control has been enabled in Security Configuration. If allowed, a potential lockout condition could occur if the restored IP is different from that allowed in IP Access Control. To allow the restore to complete you must select **“allow from all addresses”** in IP Access Control. After completion of the restore you may then re-enter the previous settings in IP Access Control.

Warning:	During this restart, ComSifter will power down and restart with the restored settings. This restart may take up to four minutes to complete. During this time user access to the Internet will be denied.

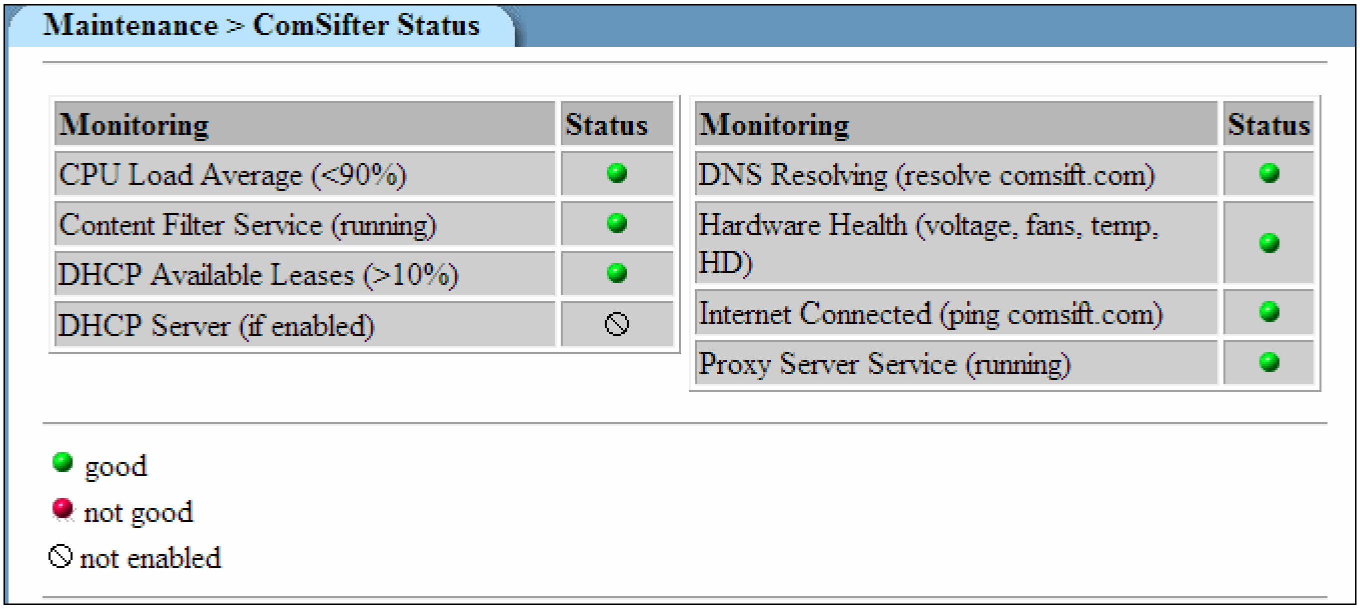
ComSifter Status

ComSifter monitors all of its critical services every five minutes and upon entering this screen. There are three conditions.

⊘ The service or function is not enabled.

🟢 The service or function is on or functioning properly.

🔴 The service or function is off or not functioning properly.



Maintenance > ComSifter Status

Monitoring	Status
CPU Load Average (<90%)	🟢
Content Filter Service (running)	🟢
DHCP Available Leases (>10%)	🟢
DHCP Server (if enabled)	⊘

Monitoring	Status
DNS Resolving (resolve comsift.com)	🟢
Hardware Health (voltage, fans, temp, HD)	🟢
Internet Connected (ping comsift.com)	🟢
Proxy Server Service (running)	🟢

🟢 good

🔴 not good

⊘ not enabled

Figure 3-66: System and Service Status

CPU Load Average

Under normal circumstances ComSifter runs at a 1-5% CPU load with occasional peaks up to 50%. If ComSifter sustains a 50% load for more than one minute this indicator will turn red and a message will be sent to ComSifter Technical Support.

Content Filter Service

Content Filter is the service that is running the filtering process. This indicator should always be green. If the service were to stop the condition would turn red and a message will be sent to ComSifter Technical Support.

DHCP Available Leases

If the percentage of available leases in the lease address pool is greater than 10% the indicator will be green. If the number of available leases is less than 10% the indicator will turn red.

DHCP Server

If ComSifter is not using its built-in DHCP server then an ⊘ indicator is a normal condition. If ComSifter is using its built-in DHCP server then an 🔴 indicator is an abnormal condition and indicates that the DHCP server has stopped. Before contacting Comsift Technical Support try restarting the DHCP server.

DNS Resolving

Upon entering the ComSifter Status screen ComSifter does a quick DNS test. The first DNS server to successfully respond will result in a green condition. If no DNS server responds the condition will turn red. A more comprehensive test is available in Maintenance > Internet Connection Test.

Hardware Health

ComSifter monitors the following critical hardware parameters and if any are out of spec the indicator will turn red. To determine what parameter is out of spec go to Maintenance > Information > ComSifter Information.

- In spec, CPU is operating at full speed
- In spec, System load is 1% over the past 15 minutes (<90% normal)
- In spec, 23713MB of free disk space (>1000MB normal)
- In spec, 225MB of free memory (>50MB normal)
- In spec, VCore voltage is 2.31 volts (2.07min - 2.41max)
- In spec, +5 voltage is 5.14 volts (4.75min - 5.25max)
- In spec, +12 voltage is 12.00 volts (10.8min - 13.2max)
- In spec, +3.3 voltage is 3.38 (3.14min - 3.47max)
- In spec, Hard Drive S.M.A.R.T. health is good

Internet Connected

Upon entering the ComSifter Status screen ComSifter does a ping test to the Comsift web site. A reply will result in a green condition. If a reply is not received the condition will turn red. A more comprehensive test is available in Maintenance > Internet Connection Test.

Proxy Server Service

Proxy Server is the service that is running the proxy process. This indicator should always be green. If the service were to stop the condition would turn red and a message will be sent to ComSifter Technical Support

Hours of Operation

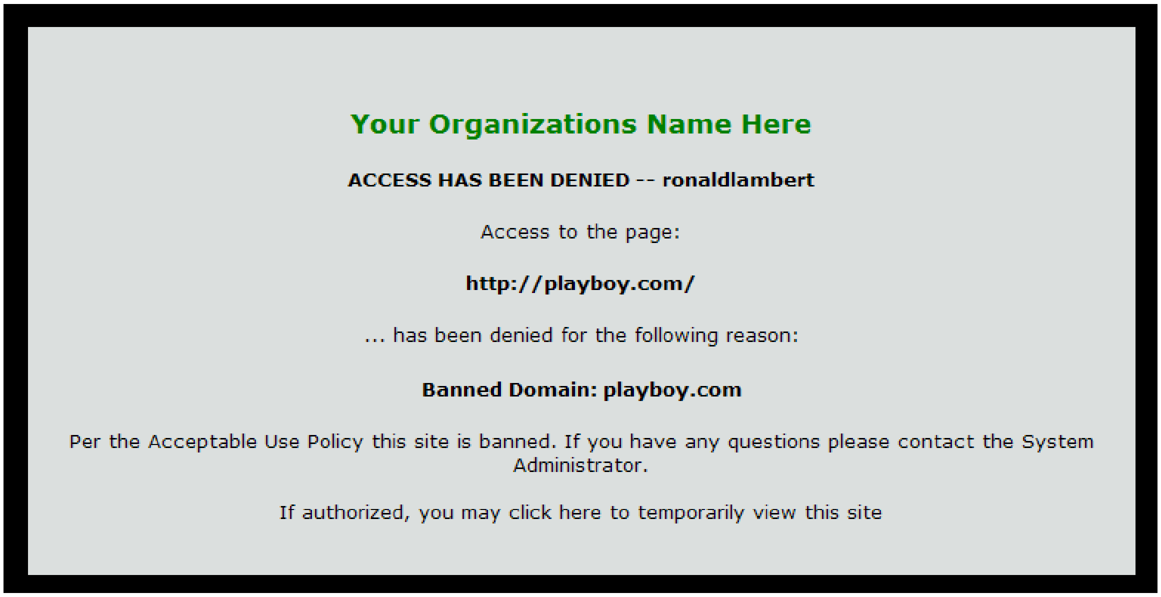
Shows the current Hours of Operation schedule for each Filter and if the schedule is allowing Internet Access (🟢) or is not allowing Internet Access (🔴).

Denied Access Page

Overview

The Denied Access Page is shown in the user computers browser whenever ComSifter blocks a request.

Note:	When viewing the Denied Access Page it may initially appear that the page is blank. Scrolling down the page will reveal the example shown below. The reason for the white space is due to how ad servers display their ads on a page. When a banned ad site tries to put an ad on a page they will receive only white space from ComSifter and will then display that white space instead of the ad.



Your Organizations Name Here

ACCESS HAS BEEN DENIED -- ronaldlambert

Access to the page:

http://playboy.com/

... has been denied for the following reason:

Banned Domain: playboy.com

Per the Acceptable Use Policy this site is banned. If you have any questions please contact the System Administrator.

If authorized, you may click here to temporarily view this site

Figure 3-67: Denied Access Page

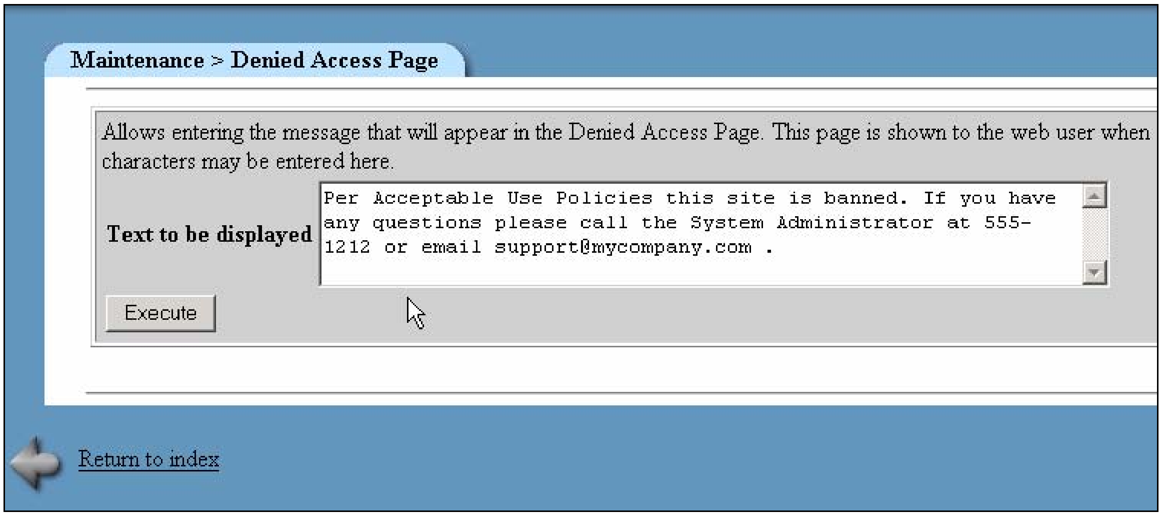
In the example we see that user ronaldlambert tried to access www.playboy.com. He was denied because that domain was a banned site in the Blacklist Domain List.

Next we see the local message (described in Local Message).

Next we see the Warn-and-Go option. If the users filter is configured to allow warn-and-go then clicking on **“If Authorized, you may ……..”** will allow the user to view the page. If the users filter is not configured to allow Warn-and-Go then nothing will happen.

Local Message

A local message may be inserted in the Denied Access Page. This message may be up to 256 alphanumeric characters. It may include spaces, the _ symbol and the @ symbol.

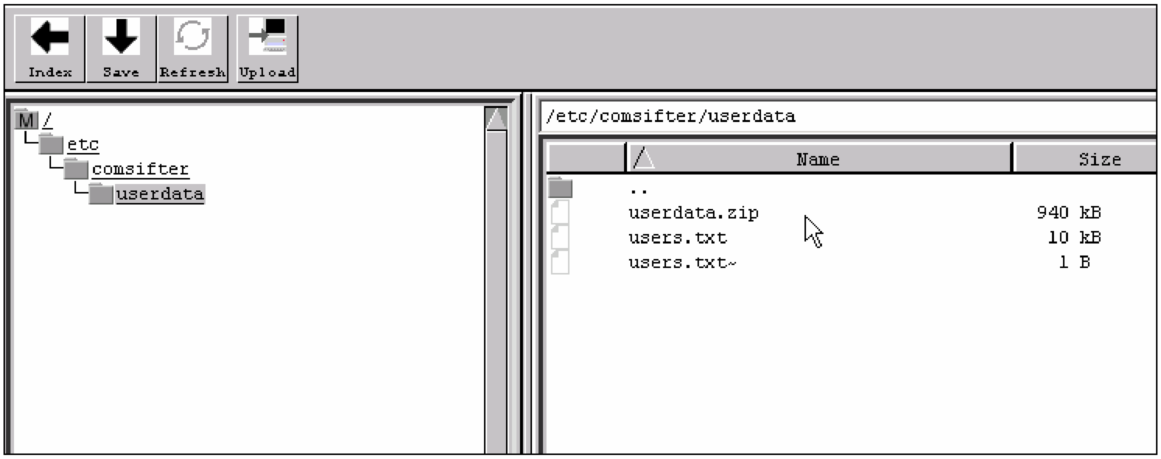


Allows entering the message that will appear in the Denied Access Page. This page is shown to the web user when characters may be entered here.

Text to be displayed: Per Acceptable Use Policies this site is banned. If you have any questions please call the System Administrator at 555-1212 or email support@mycompany.com .

Figure 3-68: Denied Access Page Message

File Manager



/etc/comsifter/userdata

Name	Size
..	
userdata.zip	940 kB
users.txt	10 kB
users.txt~	1 B

Figure 3-69: File Manager

File Manager is used to move files into and out of ComSifter. The following functions use File Manger.

Backup/Restore – this function is defined in Backup/Restore.

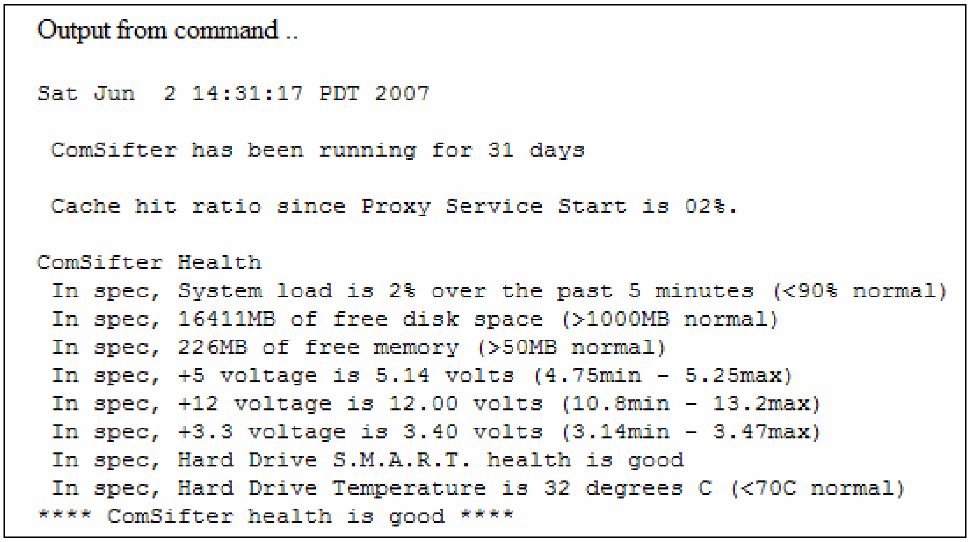
Merge User Names – this function is defined in Chapter 6, Merge User Names from File.

Note:	File Manager requires the use of Java™. If you need to obtain Java it is available for download courtesy of Sun Microsystems™ at www.sun.com .

Information

ComSifter Information

To view information about ComSifter, click on **Maintenance**, then **ComSifter Information**. ComSifter will respond as shown below.

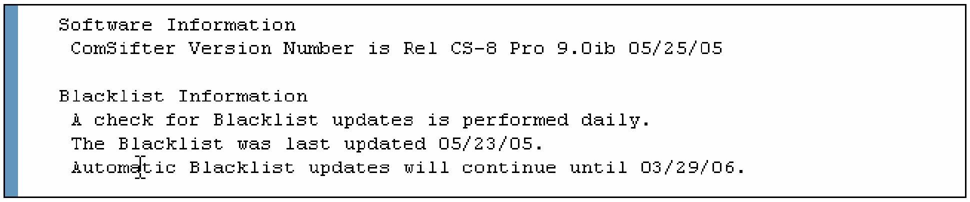


Output from command ..

```
Sat Jun  2 14:31:17 PDT 2007

 ComSifter has been running for 31 days

 Cache hit ratio since Proxy Service Start is 02%.

ComSifter Health
 In spec, System load is 2% over the past 5 minutes (<90% normal)
 In spec, 16411MB of free disk space (>1000MB normal)
 In spec, 226MB of free memory (>50MB normal)
 In spec, +5 voltage is 5.14 volts (4.75min - 5.25max)
 In spec, +12 voltage is 12.00 volts (10.8min - 13.2max)
 In spec, +3.3 voltage is 3.40 volts (3.14min - 3.47max)
 In spec, Hard Drive S.M.A.R.T. health is good
 In spec, Hard Drive Temperature is 32 degrees C (<70C normal)
**** ComSifter health is good ****
```

Figure 3-70: ComSifter Information

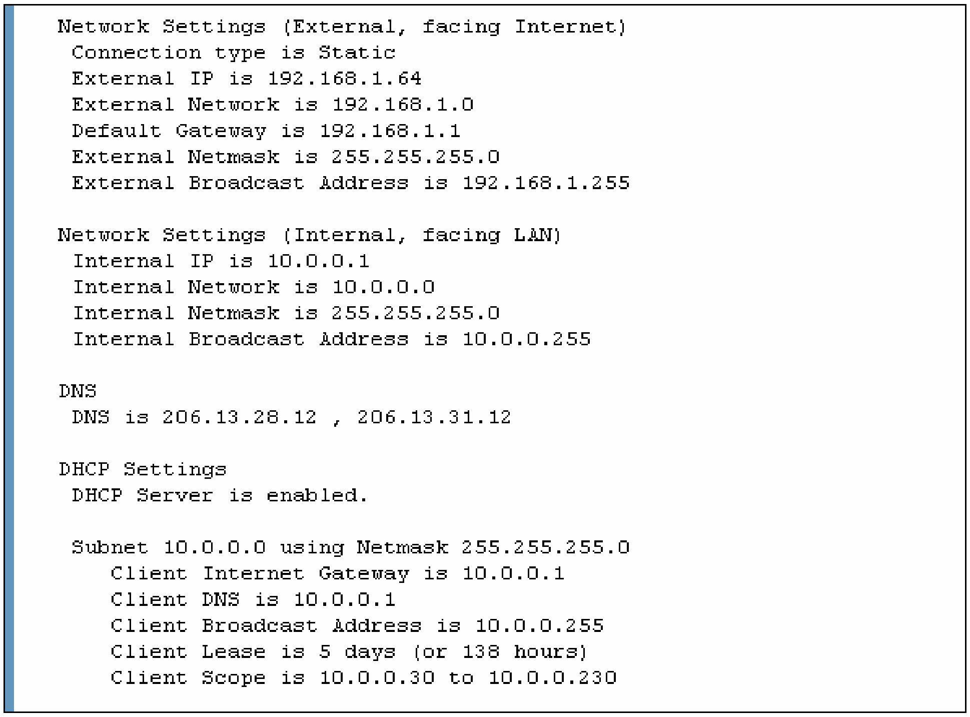
- ComSifter Time - Displays ComSifters internal time.
- Uptime - Shows the amount of time the ComSifter has been running.
- Cache hit ratio - Shows the efficiency of the cache.
- ComSifter Health - Displays the condition of ComSifter hardware.
- Software Information - Shows ComSifter revision number.



```
Software Information
 ComSifter Version Number is Rel CS-8 Pro 9.0ib 05/25/05

Blacklist Information
 A check for Blacklist updates is performed daily.
 The Blacklist was last updated 05/23/05.
 Automatic Blacklist updates will continue until 03/29/06.
```

Figure 3-71: Software and Blacklist info

- Blacklist Information – Displays how often the blacklist will be updated, when the blacklist was last updated, and when blacklist updates will expire, based on your service contract.
- Network Settings – displays ComSifter network configuration settings.



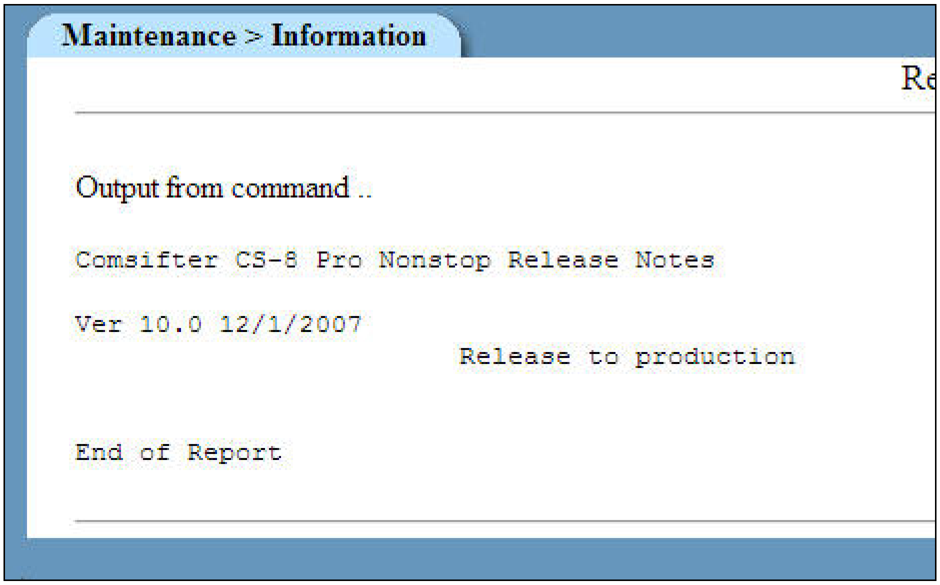
```
Network Settings (External, facing Internet)
 Connection type is Static
 External IP is 192.168.1.64
 External Network is 192.168.1.0
 Default Gateway is 192.168.1.1
 External Netmask is 255.255.255.0
 External Broadcast Address is 192.168.1.255

Network Settings (Internal, facing LAN)
 Internal IP is 10.0.0.1
 Internal Network is 10.0.0.0
 Internal Netmask is 255.255.255.0
 Internal Broadcast Address is 10.0.0.255

DNS
 DNS is 206.13.28.12 , 206.13.31.12

DHCP Settings
 DHCP Server is enabled.

 Subnet 10.0.0.0 using Netmask 255.255.255.0
    Client Internet Gateway is 10.0.0.1
    Client DNS is 10.0.0.1
    Client Broadcast Address is 10.0.0.255
    Client Lease is 5 days (or 138 hours)
    Client Scope is 10.0.0.30 to 10.0.0.230
```

Figure 3-72: Network Settings

- ComSifter DNS - displays ComSifter DNS configuration settings.
- DHCP Settings - displays ComSifter DHCP configuration settings.

ComSifter Release Notes

To view information about Release Notes click on **Maintenance** >**Information** >**Release Notes > Execute**. ComSifter will respond as shown below.



Output from command ..

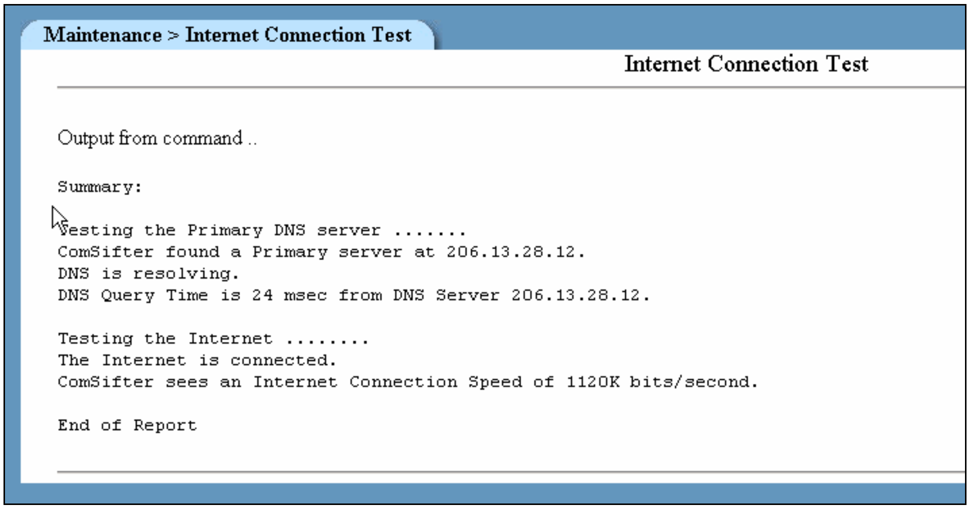
```
Comsifter CS-8 Pro Nonstop Release Notes

Ver 10.0 12/1/2007
                              Release to production


End of Report
```

Figure 3-73: Release Notes

Internet Connection Test

The Internet Connection test is useful for determining if DNS is working properly and ComSifters actual communication speed.

This test will download a compressed graphics file from the Comsift website. If ComSifter is properly connected to the Internet the following screen will display.



Output from command ..

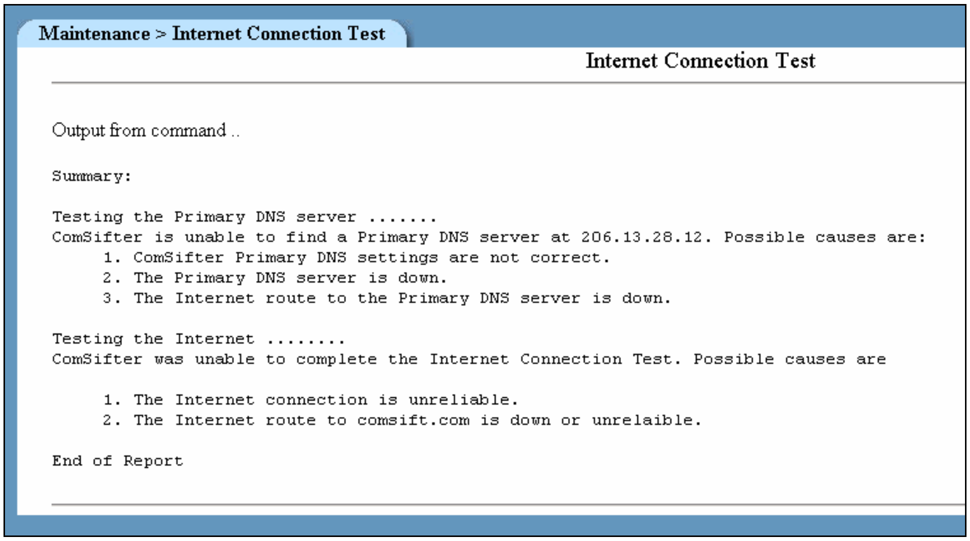
```
Summary:

Testing the Primary DNS server .......
ComSifter found a Primary server at 206.13.28.12.
DNS is resolving.
DNS Query Time is 24 msec from DNS Server 206.13.28.12.

Testing the Internet ........
The Internet is connected.
ComSifter sees an Internet Connection Speed of 1120K bits/second.

End of Report
```

Figure 3-74: Internet Connection Test

Each DNS Server, as defined in Network > Network Configuration > DNS will be tested. If DNS passes then an Internet Connection Speed will be performed. Upon completion an average speed will be displayed.

Note: The above example was the result of a test over a standard 1.5mb DSL connection.

Note: ComSifter will try to resolve DNS once, for 5 seconds, for each DNS server. If unable to reach a DNS server the speed test will not be run and the following screen will appear indicating DNS failure. This may indicate that ComSifter is not properly connected to the Internet, DNS settings are invalid or the Internet connection is down.

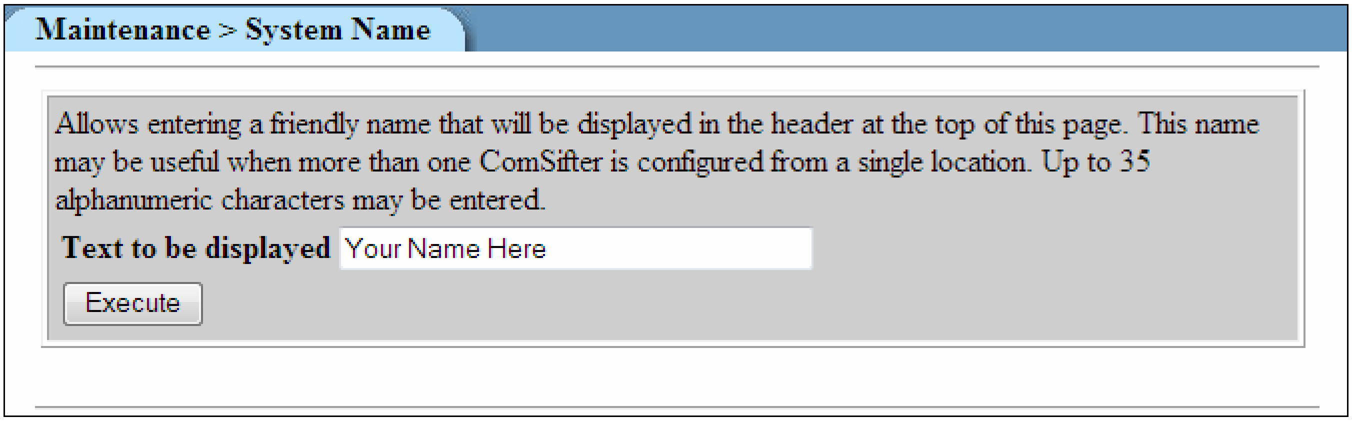


Output from command ..

```
Summary:

Testing the Primary DNS server .......
ComSifter is unable to find a Primary DNS server at 206.13.28.12. Possible causes are:
     1. ComSifter Primary DNS settings are not correct.
     2. The Primary DNS server is down.
     3. The Internet route to the Primary DNS server is down.

Testing the Internet ........
ComSifter was unable to complete the Internet Connection Test. Possible causes are

     1. The Internet connection is unreliable.
     2. The Internet route to comsift.com is down or unrelaible.

End of Report
```

Figure 3-75: Failed Internet Connection Test

System Name



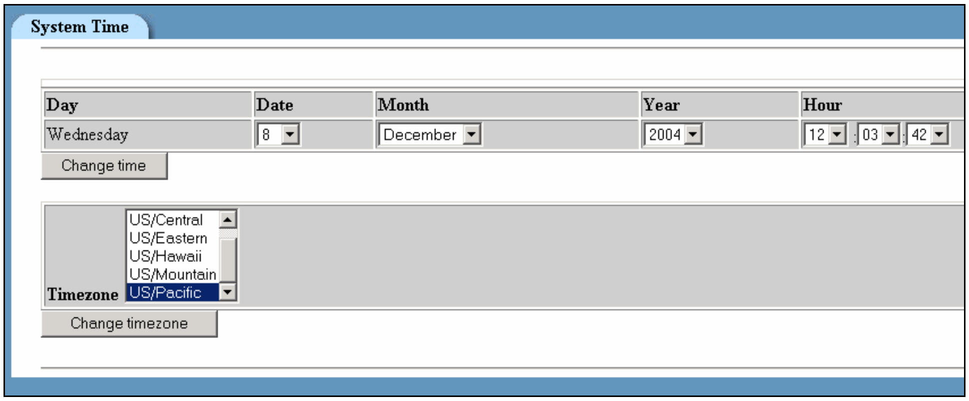
Allows entering a friendly name that will be displayed in the header at the top of this page. This name may be useful when more than one ComSifter is configured from a single location. Up to 35 alphanumeric characters may be entered.

Text to be displayed Your Name Here

Figure 3-76: System Name

System Name is a friendly name that will display in the header bar of ComSifter Configuration. This name may be useful if more than one ComSifter is being accessed by ComSifter Admins. The name may be up to 35 alphanumeric characters and can include spaces, the _ symbol and the @ symbol.

System Time



Day	Date	Month	Year	Hour
Wednesday	8	December	2004	12 : 03 : 42

Timezone US/Pacific

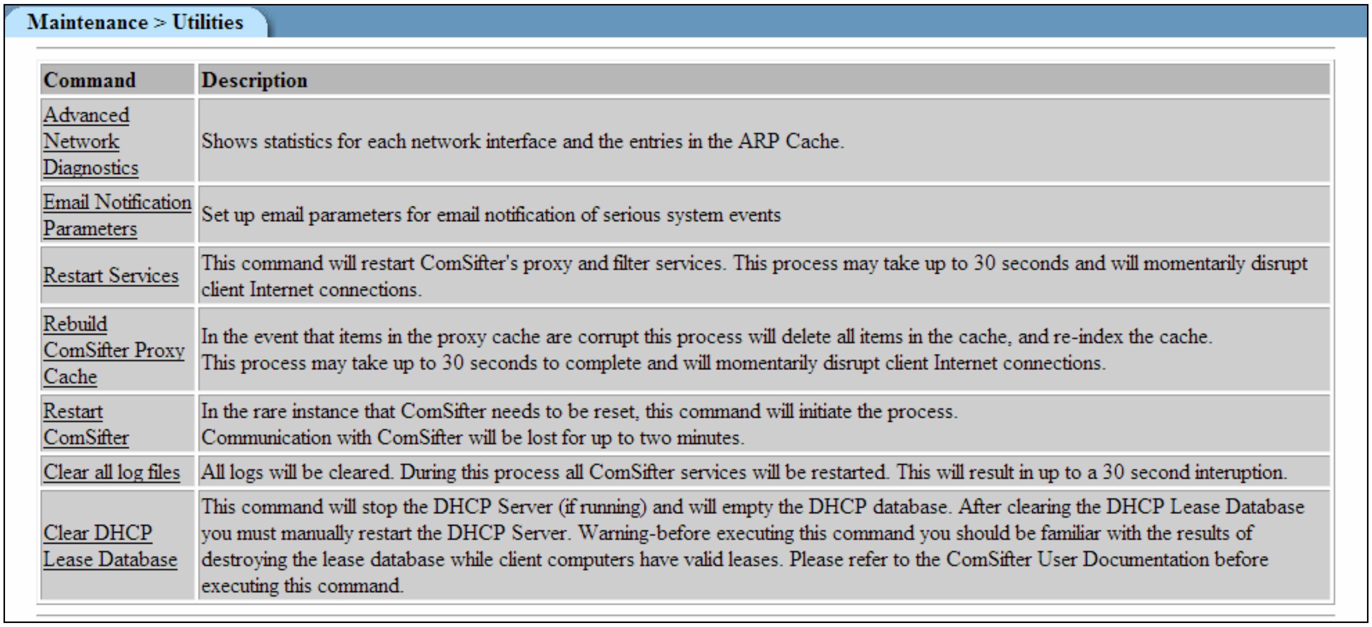
Figure 3-77: System Time

System Time is used to set ComSifter to your local time and Time Zone. Correct time is necessary for Hours of Operation Scheduling and for System Log entries.

Note: ComSifter uses Network Time Protocol (NTP) to keep its clock accurate after the System Time has been set. NTP is checked at least twice during any 24 hour period and during any power up of ComSifter. Any changes to the System Time are logged to the DHCP Log.

Utilities

A set of Utilities are included for use in the rare event that ComSifter Services need to be restarted or ComSifter itself needs to restart.



Command	Description
Advanced Network Diagnostics	Shows statistics for each network interface and the entries in the ARP Cache.
Email Notification Parameters	Set up email parameters for email notification of serious system events
Restart Services	This command will restart ComSifter's proxy and filter services. This process may take up to 30 seconds and will momentarily disrupt client Internet connections.
Rebuild ComSifter Proxy Cache	In the event that items in the proxy cache are corrupt this process will delete all items in the cache, and re-index the cache. This process may take up to 30 seconds to complete and will momentarily disrupt client Internet connections.
Restart ComSifter	In the rare instance that ComSifter needs to be reset, this command will initiate the process. Communication with ComSifter will be lost for up to two minutes.
Clear all log files	All logs will be cleared. During this process all ComSifter services will be restarted. This will result in up to a 30 second interuption.
Clear DHCP Lease Database	This command will stop the DHCP Server (if running) and will empty the DHCP database. After clearing the DHCP Lease Database you must manually restart the DHCP Server. Warning-before executing this command you should be familiar with the results of destroying the lease database while client computers have valid leases. Please refer to the ComSifter User Documentation before executing this command.

Figure 3-78: Utilities

Advanced Network diagnostics

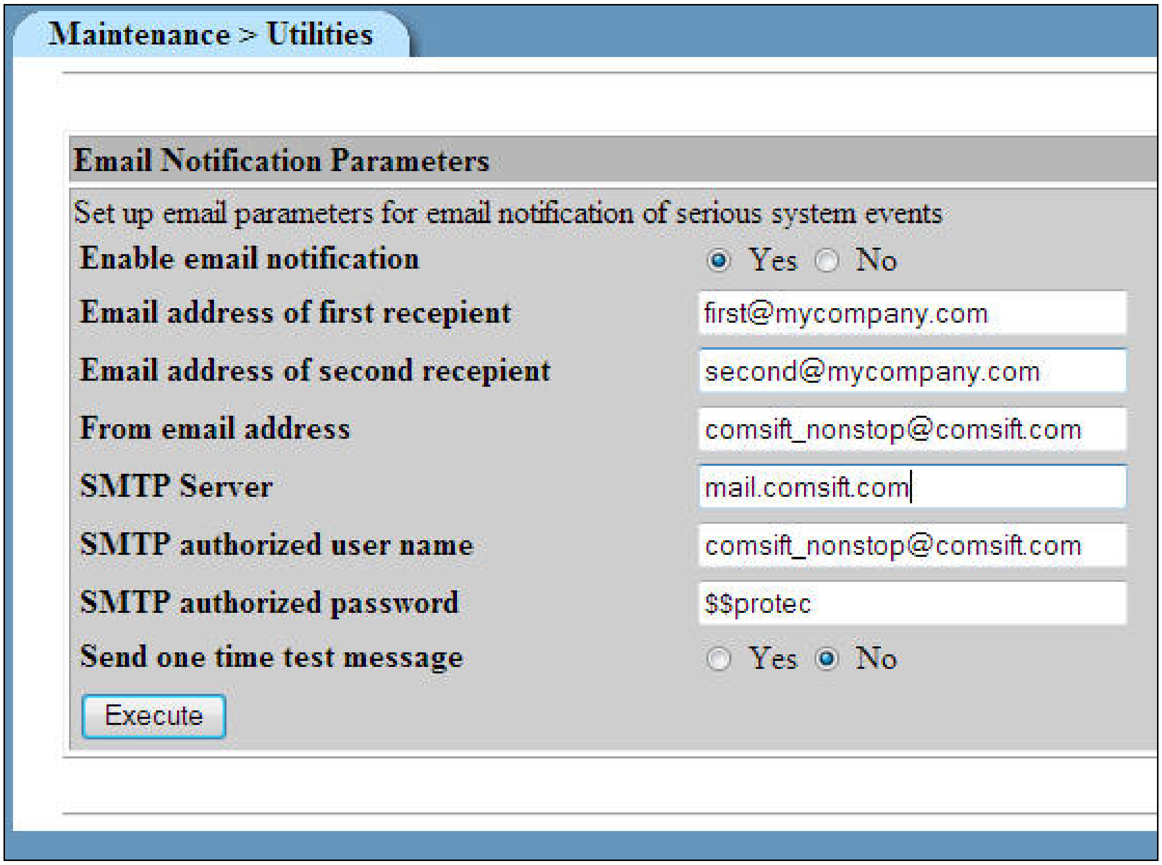
Advanced Network Diagnostics is for use by Comsift Technical Support on an as needed basis.

Email Notification Parameters

Set up parameters for email notification of serious system events. These events include but are not limited to:

- Low lease level in DHCP pool.
- Changing of external IP or DNS.
- Hardware health in or out of specification.
- LAN/WAN Cable connect or disconnect.
- Service Contact Expiration
- IP change from Follow My IP
- IP change from Dynamic DNS

Note: Email messages are queued and delivered every 5 minutes.



Email Notification Parameters

Set up email parameters for email notification of serious system events

Enable email notification	● Yes ○ No
Email address of first recepient	first@mycompany.com
Email address of second recepient	second@mycompany.com
From email address	comsift_nonstop@comsift.com
SMTP Server	mail.comsift.com
SMTP authorized user name	comsift_nonstop@comsift.com
SMTP authorized password	$$protec
Send one time test message	○ Yes ● No

Figure 3-79: Email Notification Parameters

Note: As a courtesy Comsift has a built in SMTP account for the Comsift. The account information is in the Figure shown above. Comsift does not monitor this account other than to check if it is being used for spam.

- Enable email notification - Enables or disables the sending of notifications.
- Email address of first recipient - Email address of the first of two possible recipients.
- Email address of second recipient - Email address of the second of two possible recipients.
- From email address - A valid email address the Comsifter can use to send emails.
- SMTP Server - The Simple Mail Transport Protocol Server that the Comsifter will use to send emails.
- SMTP authorized user name - A user name authorized to use the SMTP server.
- SMTP authorized password - A password for the username authorized to use the SMTP Server.
- Send one time test message – Will send a one time test message to the recipients defined above.

Restart Services

This command will restart ComSifter's proxy and filter services. This process may take up to 30 seconds and will momentarily disrupt client Internet connections.

Rebuild ComSifter Proxy Cache

This command will stop Content Filter Service and Proxy Server Service. The Proxy Server cache will be completely deleted, then rebuilt and re-indexed. The rebuild will take up to 30 seconds to complete and will disrupt client Internet connections. This should only be used if ComSifter Status indicates the service is stopped, suspected corruption has appeared on client web pages or if instructed to do so by Comsift Technical Support.

Restart ComSifter

This command will restart ComSifter as if the power were turned off, then on. The restart will take up to two minutes to complete and will disrupt client Internet connections. This should only be used if instructed to do so by Comsift Technical Support.

Clear all log files

All logs will be cleared. During this process all ComSifter services will be restarted. This will result in up to a 30 second interruption.

Clear DHCP Lease Database

This command will stop the DHCP Server (if running) and will empty the DHCP database. After clearing the ComSifter DHCP Lease Databases you must manually restart the DHCP Server.

Warning: Before executing this command you should be familiar with the results of destroying the lease database while client computers have valid leases.

Chapter 4

Filter Setup

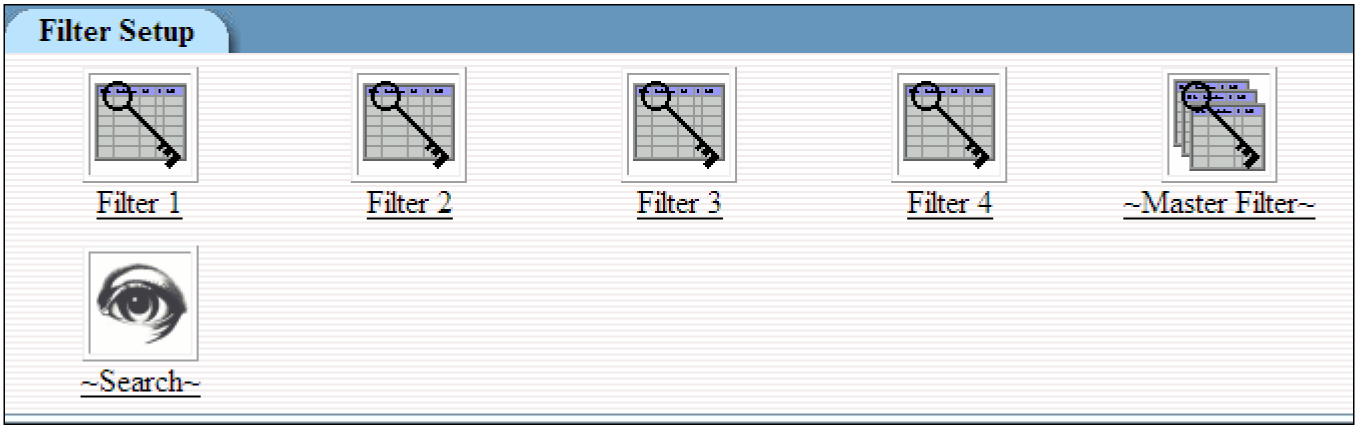
Overview

Before you start

Four Template filters are available. The template filters are pre-configured as shown in Appendix B. You may determine that one of these templates will meet your organizations requirements. If not you may modify them. There is also a master filter which affects all filters.

Each template may be individually configured. Each template allows customization of:

- The good and bad words that will be used in CSphrase Filtering.
- What blacklist categories will be included in the filter?
- What additional domains and URLs are to be fully or partially banned?
- What domains and URLs are to be excepted?
- The CSphrase sensitivity threshold.



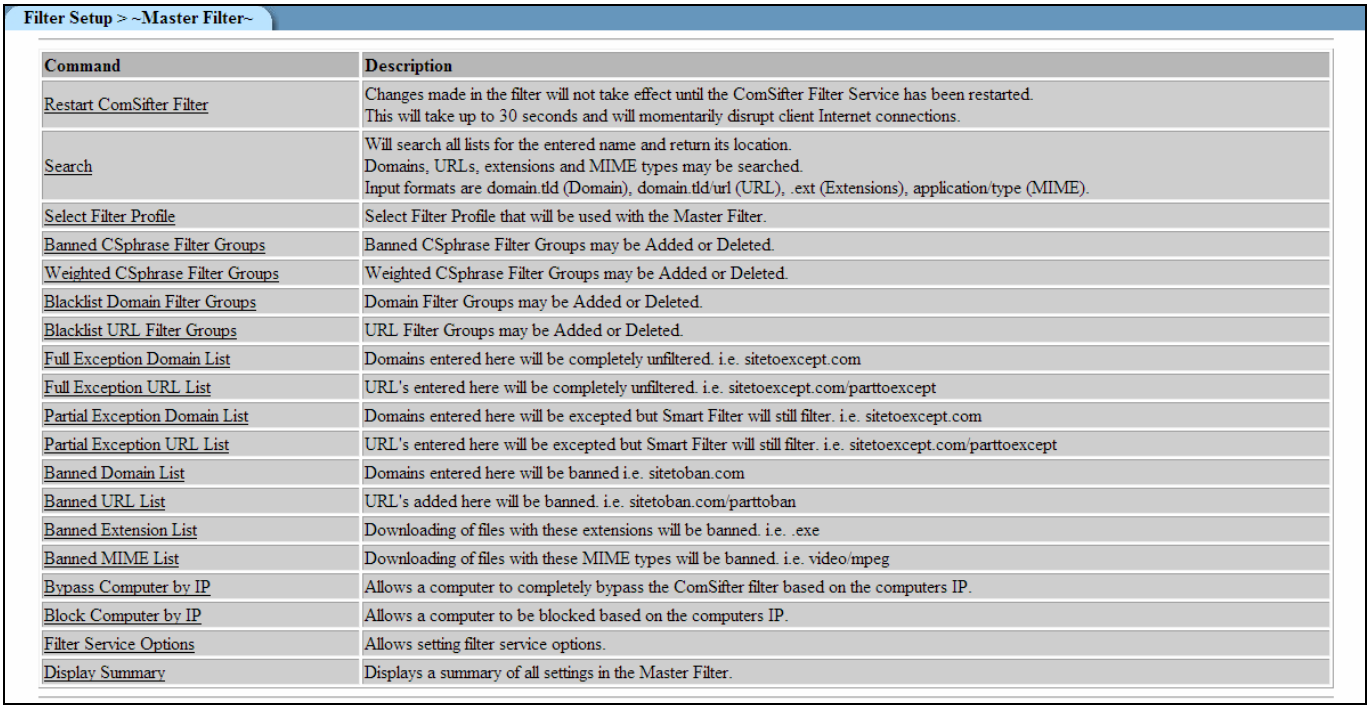
In addition to each template, all of the groups and lists selected in the Master Filter will be applied. The Master Filter settings are used when a setting is required on all filters.

Master Filter

Items entered in the Master List affect all users. If you have a domain, URL, extension or MIME type that you either want to ban or except system wide it should be entered in the Master List.

Additionally the Master List includes:

- A utility to restart the ComSifter Filter service.
- A powerful search facility.
- A command that allows filter templates to be changed.
- A report that lists all settings in the Master List.



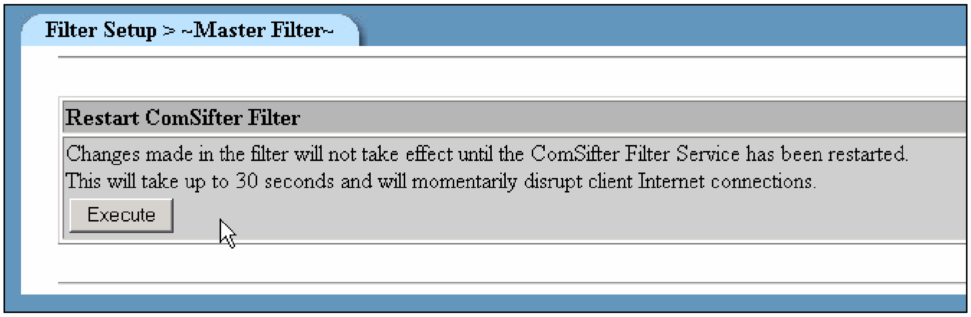
Filter Setup > ~Master Filter~

Command	Description
Restart ComSifter Filter	Changes made in the filter will not take effect until the ComSifter Filter Service has been restarted. This will take up to 30 seconds and will momentarily disrupt client Internet connections.
Search	Will search all lists for the entered name and return its location. Domains, URLs, extensions and MIME types may be searched. Input formats are domain.tld (Domain), domain.tld/url (URL), .ext (Extensions), application/type (MIME).
Select Filter Profile	Select Filter Profile that will be used with the Master Filter.
Banned CSphrase Filter Groups	Banned CSphrase Filter Groups may be Added or Deleted.
Weighted CSphrase Filter Groups	Weighted CSphrase Filter Groups may be Added or Deleted.
Blacklist Domain Filter Groups	Domain Filter Groups may be Added or Deleted.
Blacklist URL Filter Groups	URL Filter Groups may be Added or Deleted.
Full Exception Domain List	Domains entered here will be completely unfiltered. i.e. sitetoexcept.com
Full Exception URL List	URL's entered here will be completely unfiltered. i.e. sitetoexcept.com/parttoexcept
Partial Exception Domain List	Domains entered here will be excepted but Smart Filter will still filter. i.e. sitetoexcept.com
Partial Exception URL List	URL's entered here will be excepted but Smart Filter will still filter. i.e. sitetoexcept.com/parttoexcept
Banned Domain List	Domains entered here will be banned i.e. sitetoban.com
Banned URL List	URL's added here will be banned. i.e. sitetoban.com/parttoban
Banned Extension List	Downloading of files with these extensions will be banned. i.e. .exe
Banned MIME List	Downloading of files with these MIME types will be banned. i.e. video/mpeg
Bypass Computer by IP	Allows a computer to completely bypass the ComSifter filter based on the computers IP.
Block Computer by IP	Allows a computer to be blocked based on the computers IP.
Filter Service Options	Allows setting filter service options.
Display Summary	Displays a summary of all settings in the Master Filter.

Figure 4-1: Master Filter

Restart ComSifter Filter

Any changes made in the Master Filter will not become effective until the ComSifter Filter is restarted. ComSifter is designed to allow you to quickly make multiple changes to filter settings and then apply the changes by restarting the filter.



Restart ComSifter Filter

Changes made in the filter will not take effect until the ComSifter Filter Service has been restarted. This will take up to 30 seconds and will momentarily disrupt client Internet connections.

Note: A restart may take up to 30 seconds to complete. During this time all Internet connections will be disrupted.

Search

ComSifter incorporates a comprehensive search facility that allows you to search for all instances of a domain, URL, extension or MIME type. The search will check all filters and all lists for the search term and return the filter and list in which the search term was found.

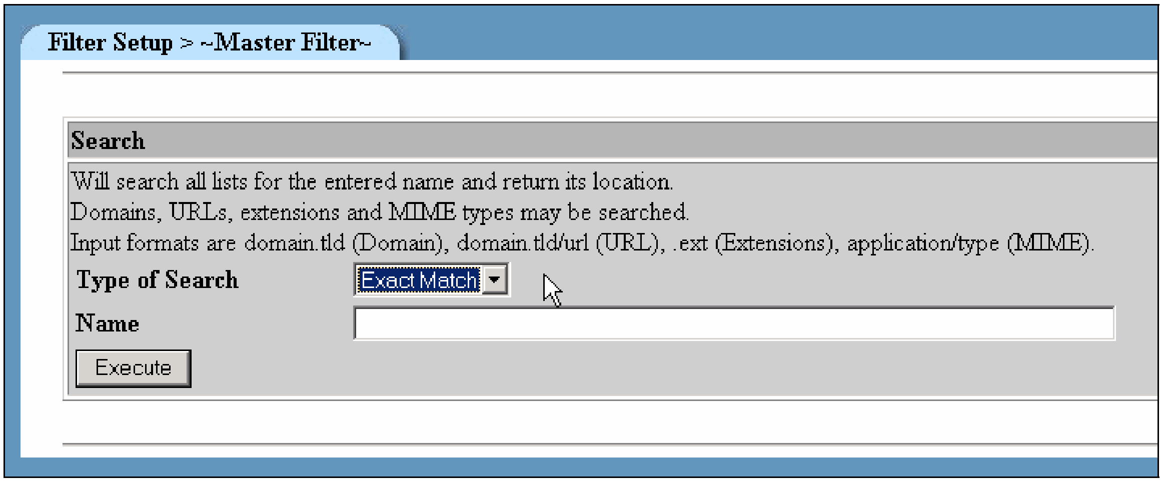
Search is useful when a site, domain, extension or MIME type is banned and you need to know why and where it is banned. Search is also useful if you believe a site, domain, extension or MIME type should be banned and it is not.

Note: Search will search through all filters and lists. This includes the blacklist that Comsift controls. A search report will show if an item was found in the Comsift controlled blacklist or the administrator controlled lists. Items in the Comsift controlled blacklist are not accessible or configurable. If an item is banned and you do not want it banned you must except the item by using the Exception Domain List or the Exception URL List.

There are three types of search. Each is explained in detail in the following paragraphs.

Exact Match

Exact Match will search for an exact match of the search term. In the following example a search for badsite.com is performed.



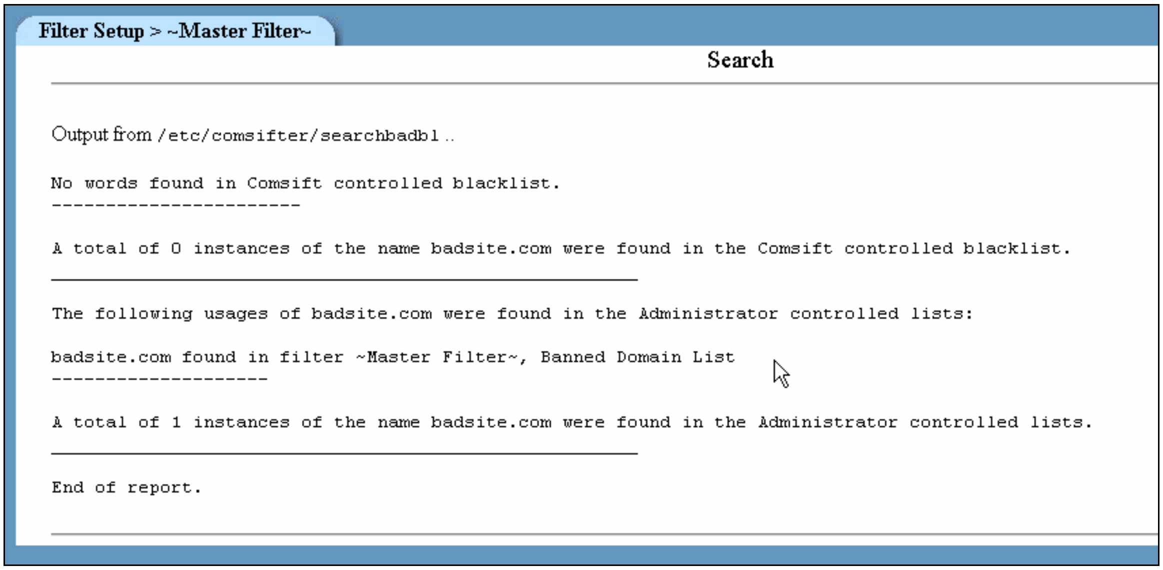
Search

Will search all lists for the entered name and return its location.
Domains, URLs, extensions and MIME types may be searched.
Input formats are domain.tld (Domain), domain.tld/url (URL), .ext (Extensions), application/type (MIME).

Type of Search Exact Match

Name

Figure 4-2: Exact Match Search



```
Output from /etc/comsifter/searchbadbl ..

No words found in Comsift controlled blacklist.
-----------------------

A total of 0 instances of the name badsite.com were found in the Comsift controlled blacklist.

The following usages of badsite.com were found in the Administrator controlled lists:

badsite.com found in filter ~Master Filter~, Banned Domain List
--------------------

A total of 1 instances of the name badsite.com were found in the Administrator controlled lists.

End of report.
```

Figure 4-3: Exact Match Report

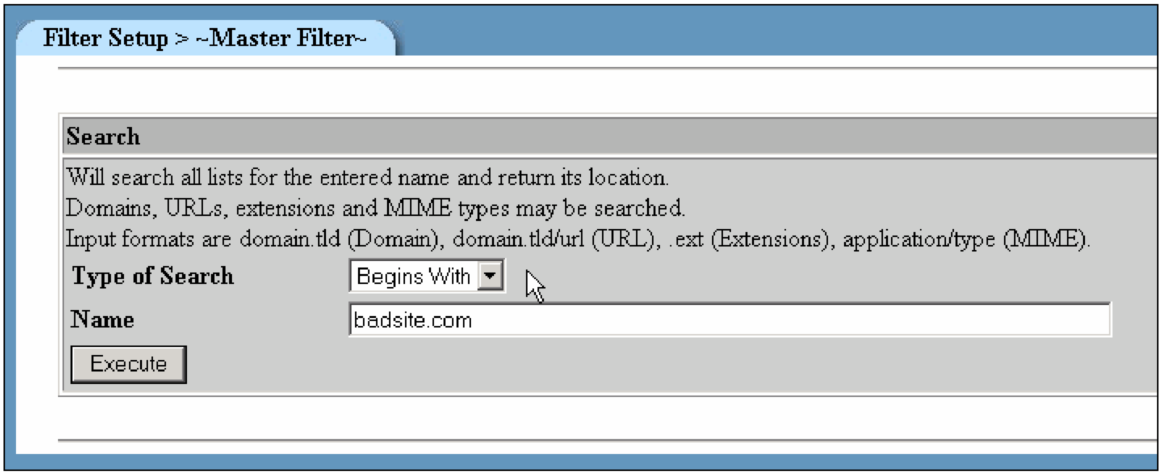
The search report shows us that badsite.com was not found in the ComSifter controlled blacklists but was found in the Master Filter, Banned Domain List.

With this information we can then go to the Master Filter and look in the Banned Domain List for badsite.com

Begins With

Begins With will search all filters and list for instances where the search term is matched at the beginning of a string.

This is useful when looking for domains that have county extensions or when looking for all the URLs that are listed within a domain.



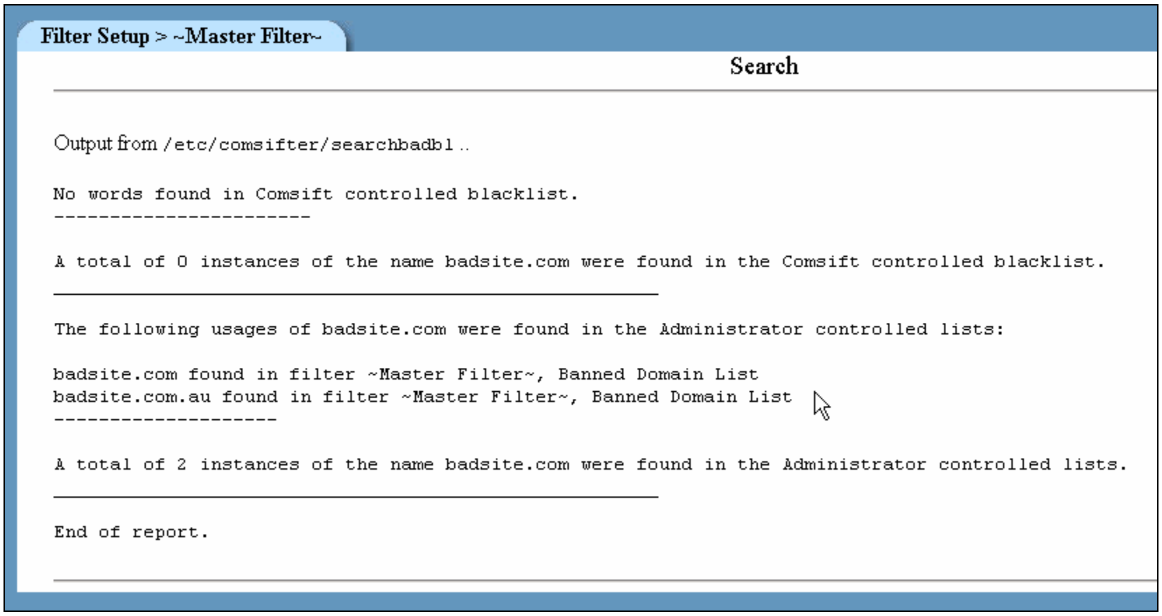
Search

Will search all lists for the entered name and return its location.
Domains, URLs, extensions and MIME types may be searched.
Input formats are domain.tld (Domain), domain.tld/url (URL), .ext (Extensions), application/type (MIME).

Type of Search: Begins With

Name: badsite.com

Figure 4-4: Begins With Search



Search

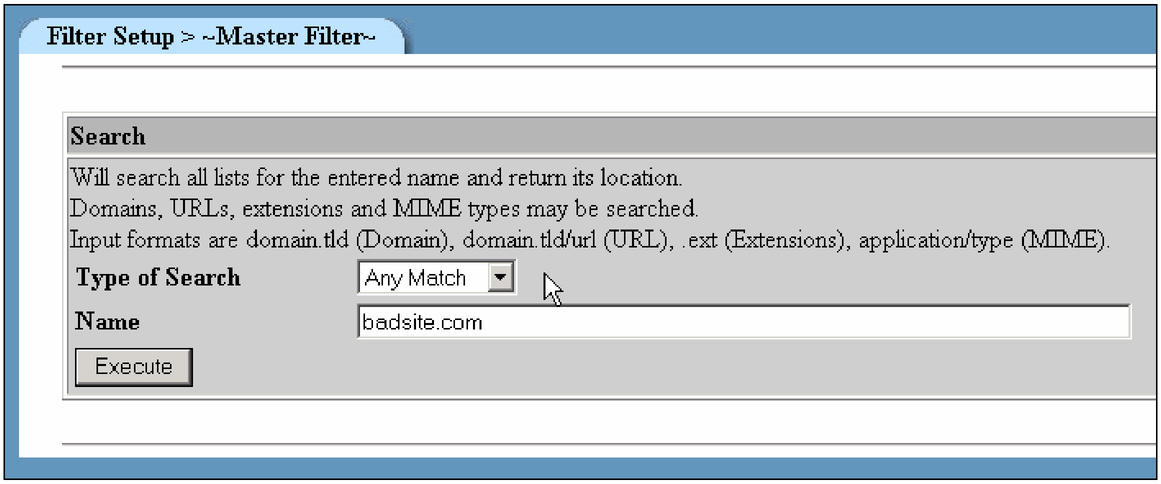
```
Output from /etc/comsifter/searchbadbl ..

No words found in Comsift controlled blacklist.
-----------------------

A total of 0 instances of the name badsite.com were found in the Comsift controlled blacklist.
________________________________________________________

The following usages of badsite.com were found in the Administrator controlled lists:

badsite.com found in filter ~Master Filter~, Banned Domain List
badsite.com.au found in filter ~Master Filter~, Banned Domain List
--------------------

A total of 2 instances of the name badsite.com were found in the Administrator controlled lists.
________________________________________________________

End of report.
```

Figure 4-5: Begins With Report

In the example we see that badsite.com was found in the Master Filter, Banned Domain List. We see that badsite.com.au was also found in the same list.

Any match

Any Match will match the search word if it is found anywhere in the string.



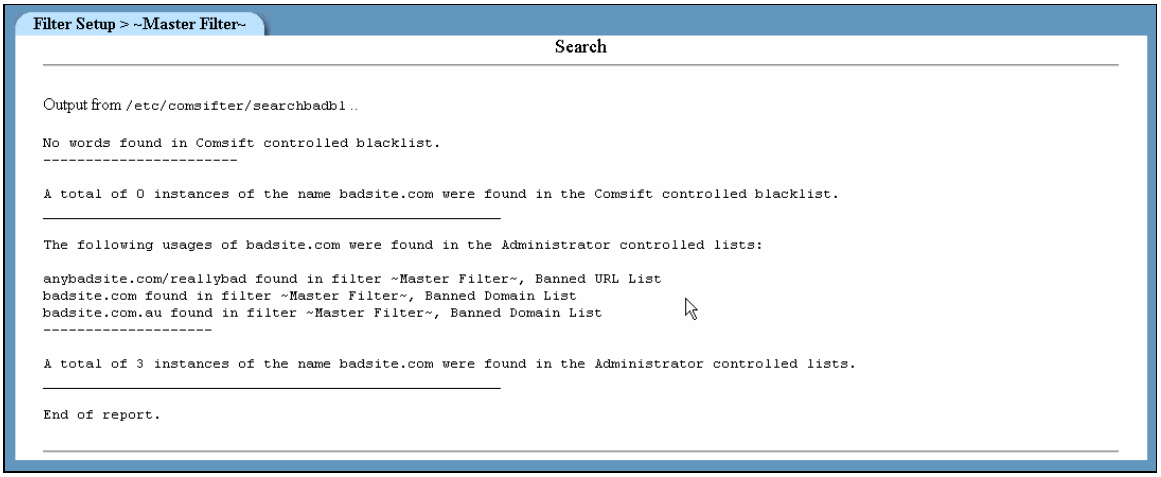
Search

Will search all lists for the entered name and return its location.
Domains, URLs, extensions and MIME types may be searched.
Input formats are domain.tld (Domain), domain.tld/url (URL), .ext (Extensions), application/type (MIME).

Type of Search Any Match

Name badsite.com

Figure 4-6: Any Match Search



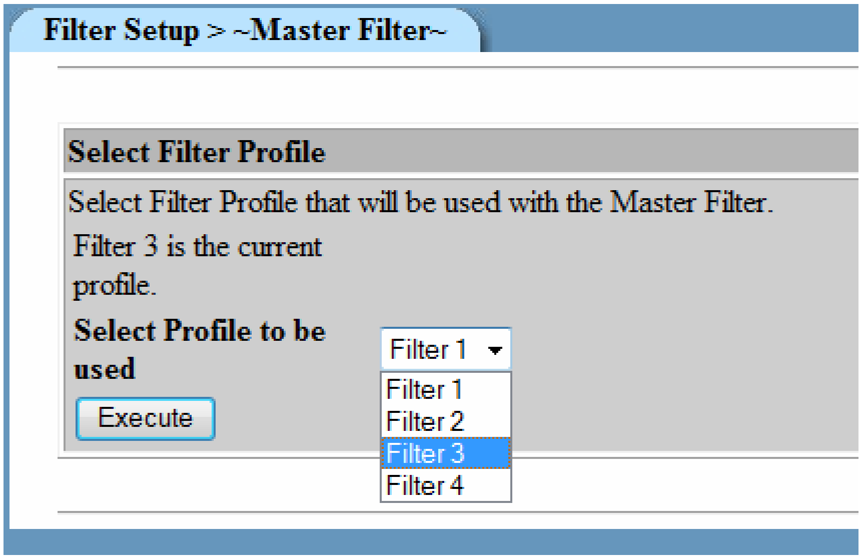
```
Output from /etc/comsifter/searchbadbl ..

No words found in Comsift controlled blacklist.
-----------------------

A total of 0 instances of the name badsite.com were found in the Comsift controlled blacklist.
______________________________________________________

The following usages of badsite.com were found in the Administrator controlled lists:

anybadsite.com/reallybad found in filter ~Master Filter~, Banned URL List
badsite.com found in filter ~Master Filter~, Banned Domain List
badsite.com.au found in filter ~Master Filter~, Banned Domain List
--------------------

A total of 3 instances of the name badsite.com were found in the Administrator controlled lists.
______________________________________________________

End of report.
```

Figure 4-7: Any Match Report

In the example we see that;

- anybadsite.com/reallybad was found in the Master Filter, Banned URL List.
- badsite.com was found in the Master Filter, Banned Domain List
- badsite.com.au was found in the Master Filter, Banned Domain List.

Select Filter Profile



Filter Setup > ~Master Filter~

Select Filter Profile

Select Filter Profile that will be used with the Master Filter.

Filter 3 is the current profile.

Select Profile to be used: Filter 1

Figure 4-8: Select Filter Profile

Select Filter Profile allows the selection of the template that will be used in conjunction with the Master Filter.

Filter Template 3 is selected by default from the factory.

Banned CSphrase Filter Groups

ComSifter has available ten Banned CSphrase filter groups. If a word or phrase is in the filter group, the filter is activated and the word is found on a web page the page will be banned.

> **Note:** The actual words/phrases that are in each of these filter groups are located in the Words/Phrases category.

These groups may be activated or deactivated, depending on the requirements of your installation. The groups are;

- Ads
- Audio-video
- Chat
- Custom – A
- Custom - B
- Drugs
- Gambling
- Hate
- Hacking
- Mail

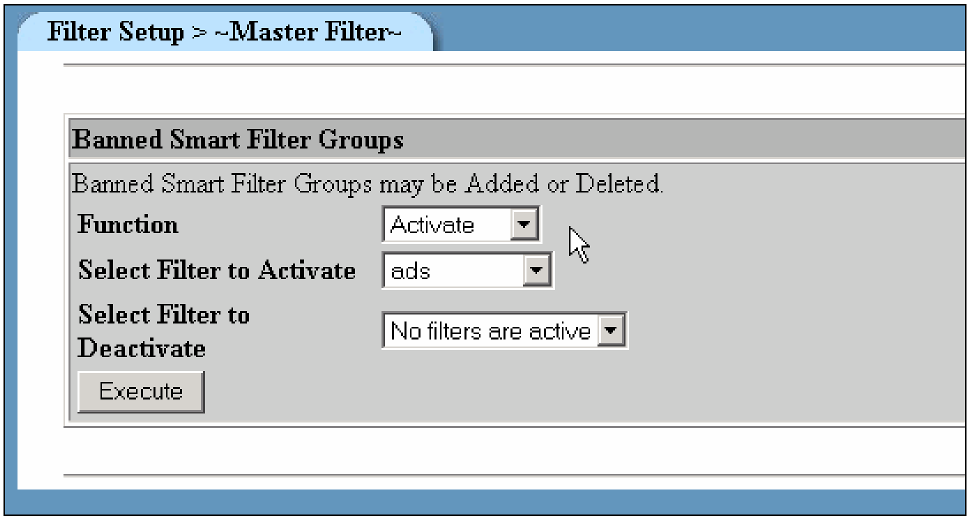
In addition to the above list there are two groups that are permanently engaged. These are;

- Pornography
- Good Words/Phrases

Activating Filters

To activate a filter;

1. Select **Activate** in the Function drop down box.
2. Select the filter to activate in the Select Filter to Activate drop-down box.
3. Click **Execute**.



Filter Setup > ~Master Filter~

Banned Smart Filter Groups

Banned Smart Filter Groups may be Added or Deleted.

Function: Activate

Select Filter to Activate: ads

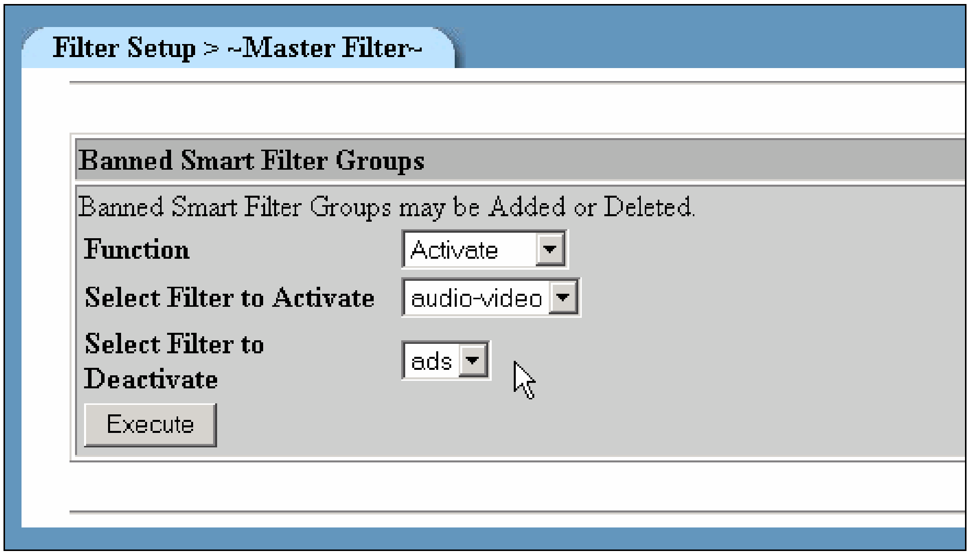
Select Filter to Deactivate: No filters are active

Figure 4-9: Activating a Filter

Deactivating Filters

To deactivate a filter;

1. Select **Deactivate** in the Function drop down box.
2. Select the filter to deactivate in the Select Filter to Deactivate drop-down box.
3. Click **Execute**.



Filter Setup > ~Master Filter~

Banned Smart Filter Groups

Banned Smart Filter Groups may be Added or Deleted.

Function	Activate
Select Filter to Activate	audio-video
Select Filter to Deactivate	ads

Figure 4-10: Deactivating a Filter

Weighted CSphrase Filter Groups

ComSifter has available ten Weighted CSphrase filter groups. If a word or phrase is in the filter group, the filter is activated and the word is found on a web page the CSphrase Sensitivity counter will increment by the weight assigned to the word/phrase. If there are any Good Words/Phrases on the same page the CSphrase Sensitivity counter will decrement by the weight assigned to the word/phrase. After analyzing all the words on a page ComSifter will compare it's Sensitivity Counter with the Sensitivity Threshold set for the individual filter. If the threshold is exceeded the page will be banned.

Note: The actual words/phrases that are in each of these filter groups are located in the Words/Phrases category and are discussed in Chapter 4.

These groups may be activated or deactivated, depending on the requirements of your installation. The groups are;

- Ads
- Audio-video
- Chat
- Custom – A
- Custom - B
- Drugs
- Gambling
- Hate
- Hacking
- Mail

In addition to the above list there are two groups that are permanently engaged. These are;

- Pornography
- Good Words/Phrases

Blacklist Domain Filter Groups

ComSifter has available nine Blacklist Domain filter groups. A domain is a top level Internet address such as comsift.com. If a domain is in the filter group and the filter is activated the site will be banned.

Note: These groups are maintained by Comsift and any changes are made by Comsift by way of the daily or weekly update (dependent on your service contract). If you find a site that you do not believe should be banned, the site may be excepted by placing it in the Exception Domain List.

These groups may be activated or deactivated, depending on the requirements of your installation. The groups are:

- Ads
- Audio-video
- Chat
- Drugs
- Gambling
- Hate
- Hacking
- Mail

In addition to the above list there is a pornography group. This group is permanently enabled.

Blacklist URL Filter Groups

ComSifter has available nine Blacklist URL filter groups. A URL is a subset of a domain and is typically denoted by the “/” symbol. If a URL is in the filter group and the filter is activated the site will be banned.

Note: These groups are maintained by Comsift and any changes are made by Comsift by way of the daily or weekly update (dependent on your service contract). If you find a site that you do not believe should be banned, the site may be excepted by placing it in the Exception Domain List.

These groups may be activated or deactivated, depending on the requirements of your installation. The groups are:

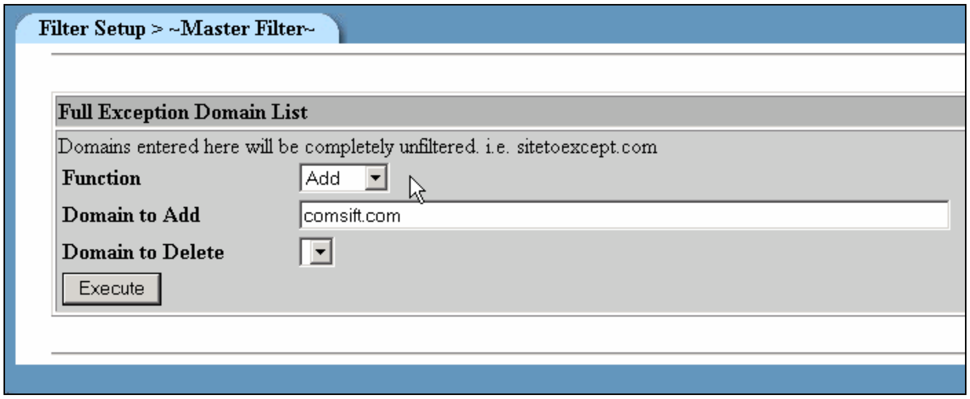
- Ads
- Audio-video
- Chat
- Drugs
- Gambling
- Hate
- Hacking
- Mail

In addition to the above list there is a pornography group. This group is permanently enabled.

Full Exception Domain List

The full Exception Domain List allows you to enter a domain that you do not want to be filtered. This may be in response to a site being banned by the ComSifter or may be proactive, such as a local home page or site that you deem safe. If ComSifter sees this domain it will not filter any portion of it including its URLs, unless the URL is listed in the Banned Domain List.

Add


Filter Setup > ~Master Filter~

Full Exception Domain List

Domains entered here will be completely unfiltered. i.e. sitetoexcept.com

Function: Add

Domain to Add: comsift.com

Domain to Delete:

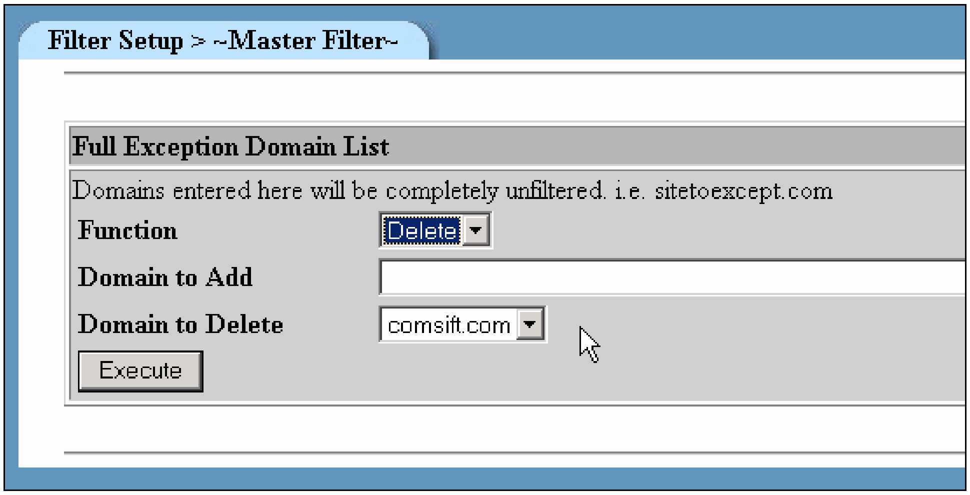
Figure 4-11: Add Domain to Full Exception List

1. To add a Domain to be excepted select **Add** in the Function drop-down box.
2. Enter the domain to be excepted.
3. Click **Execute**

Note: To except all of a domain enter only the domain name without the www. It is possible to except the domain prefix by putting in the appropriate protocol, i.e. www or mail.

Note: ComSifter will allow alphanumeric characters, the “/” symbol and the “.” symbol. Additionally the length of the domain name may not exceed 127 characters.

Delete


Filter Setup > ~Master Filter~

Full Exception Domain List

Domains entered here will be completely unfiltered. i.e. sitetoexcept.com

Function: Delete

Domain to Add:

Domain to Delete: comsift.com

Figure 4-12: Delete Domain from Full Exception List

1. To delete an excepted domain select **Delete** in the Function drop-down box.
2. Select the domain from the Domain to Delete.
3. Click **Execute**

Full Exception URL List

The full Exception URL List allows you to enter a URL that you do not want to be filtered. This may be in response to a site being banned by the ComSifter or may be proactive, such as a local home page or site that you deem safe. If ComSifter sees this URL it will not filter any portion of it including its URLs, unless the URL is listed in the Banned Domain List.

Add

1. To add a URL to be excepted select **Add** in the Function drop-down box.
2. Enter the URL to be excepted.
3. Click **Execute.**

Note: ComSifter will allow alphanumeric characters, the "/" symbol and the "." symbol. Additionally the length of the URL may not exceed 127 characters.

Delete

1. To delete an excepted URL select **Delete** in the Function drop-down box.
2. Select the URL from the URL to Delete.
3. Click **Execute.**

Partial Exception Domain List

The Partial Exception Domain List allows you to enter a domain that you do not want to be completely excepted but instead allow CSphrase Filtering to determine if the site is appropriate based on good words/phrases and bad words/phrases. This feature may be useful in instances where you want a site to be accessed but at times the content may be questionable. When the content is questionable CSphrase filtering will block the page.

Add

1. To add a domain select **Add** in the Function drop-down box.
2. Enter the domain to be partially excepted.
3. Click **Execute.**

Note: ComSifter will allow alphanumeric characters, the "/" symbol and the "." symbol. Additionally the length of the domain name may not exceed 127 characters.

Delete

1. To delete a domain select **Delete** in the Function drop-down box.
2. Select the domain from the Domain to Delete.
3. Click **Execute.**

Partial Exception URL Filter List

The Partial Exception URL List allows you to enter a URL that you do not want to be completely excepted but instead allow CSphrase Filtering to determine if the site is appropriate based on good words/phrases and bad words/phrases. This feature may be useful in instances where you want a URL to be accessible but at times the content may be questionable. When the content is questionable CSphrase filtering will block the page.

Add

1. To add a URL select **Add** in the Function drop-down box.
2. Enter the URL to be partially excepted.
3. Click **Execute**.

> **Note:** ComSifter will allow alphanumeric characters, the "/" symbol and the "." symbol. Additionally the length of the URL may not exceed 127 characters.

Delete

4. To delete a URL select **Delete** in the Function drop-down box.
5. Select the URL from the URL to Delete.
6. Click **Execute**.

Banned Domain List

The Banned Domain List allows you to enter a domain name that you want to be banned. Add

1. To add a domain select **Add** in the Function drop-down box.
2. Enter the domain to be banned.
3. Click **Execute**.

> **Note:** ComSifter will allow alphanumeric characters, the "/" symbol and the "." symbol. Additionally the length of the domain name may not exceed 127 characters.

Delete

1. To delete a domain select **Delete** in the Function drop-down box.
2. Select the Domain from the URL to Delete.
3. Click **Execute**.

Banned URL Filter List

The Banned URL List allows you to enter a URL name that you want to be banned.

Add

1. To add a URL, select **Add** in the Function drop-down box.
2. Enter the URL to be banned.
3. Click **Execute**.

> **Note:** ComSifter will allow alphanumeric characters, the "/" symbol and the "." symbol. Additionally the length of the URL may not exceed 127 characters.

Delete

1. To delete a URL select **Delete** in the Function drop-down box.
2. Select the URL from the URL to Delete.
3. Click **Execute**.

Banned Extension List

The Banned Extension List allows you to enter a file extension that you would like to prevent from being downloaded. If ComSifter sees a user trying to download a file with the extension type the page will be banned.

Add

1. To add an extension select **Add** in the Function drop-down box.
2. Enter the extension to be banned.
3. Click **Execute**.

Note: ComSifter allows extensions of up to 5 characters. This will accommodate MAC, UNIX, Linux and Windows operating systems. It will also accommodate the current Java classes.

Delete

1. To delete an extension select **Delete** in the Function drop-down box.
2. Select the Extension from the Extension to Delete.
3. Click **Execute**.

Banned MIME Type List

ComSifter has the ability to ban MIME Types. MIME Types are used by web browsers to associate files of a certain type with helper applications that display files of that type. A comprehensive listing of MIME Types may be found at the Internet Assigned Numbers Authority web site http://www.iana.org/assignments/media-types .

Add

1. To add a MIME Type select **Add** in the Function drop-down box.
2. Enter the MIME Type to be banned.
3. Click **Execute**.

Note: ComSifter allows MIME Types in the format xxx/yyy.

Delete

1. To delete a MIME Type select **Delete** in the Function drop-down box.
2. Select the MIME Type from the MIME Type to Delete.
3. Click **Execute**.

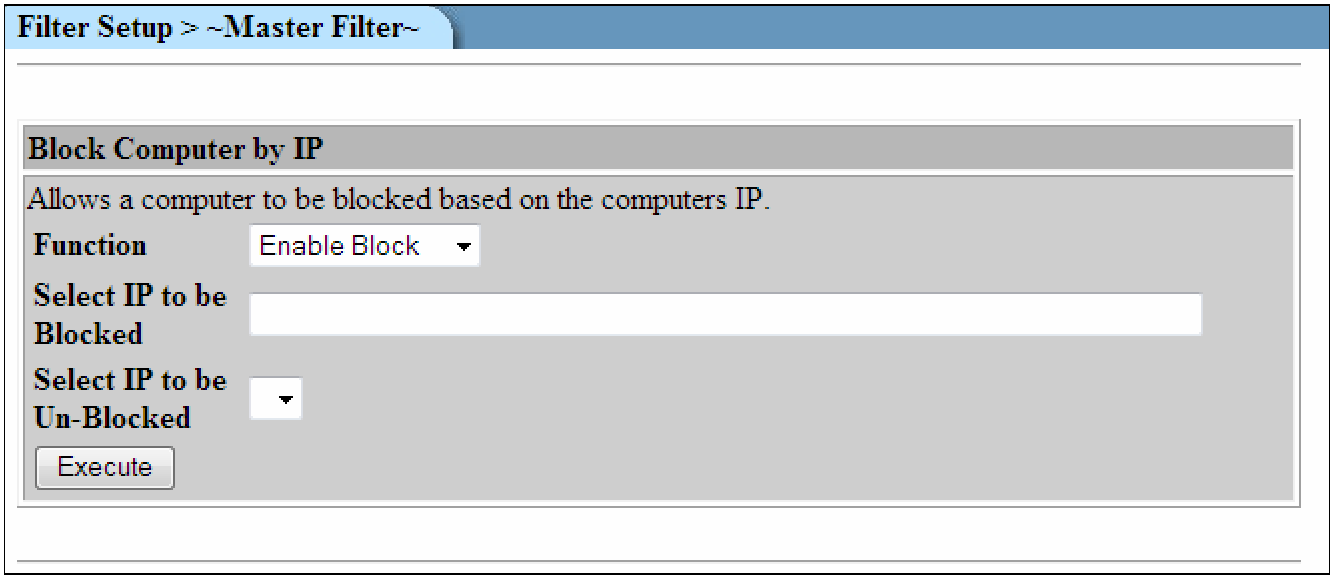
Bypass Computer by IP

The Block Computer command allows you to block a computer by the computers IP address.

Enable Block

To Block a computer:

- Set Function to Enable Block.
- Enter the IP address of the computer to be blocked in Select **IP to be Blocked.**
- Click on **Execute**.



Filter Setup > ~Master Filter~

Block Computer by IP

Allows a computer to be blocked based on the computers IP.

Function: Enable Block

Select IP to be Blocked:

Select IP to be Un-Blocked:

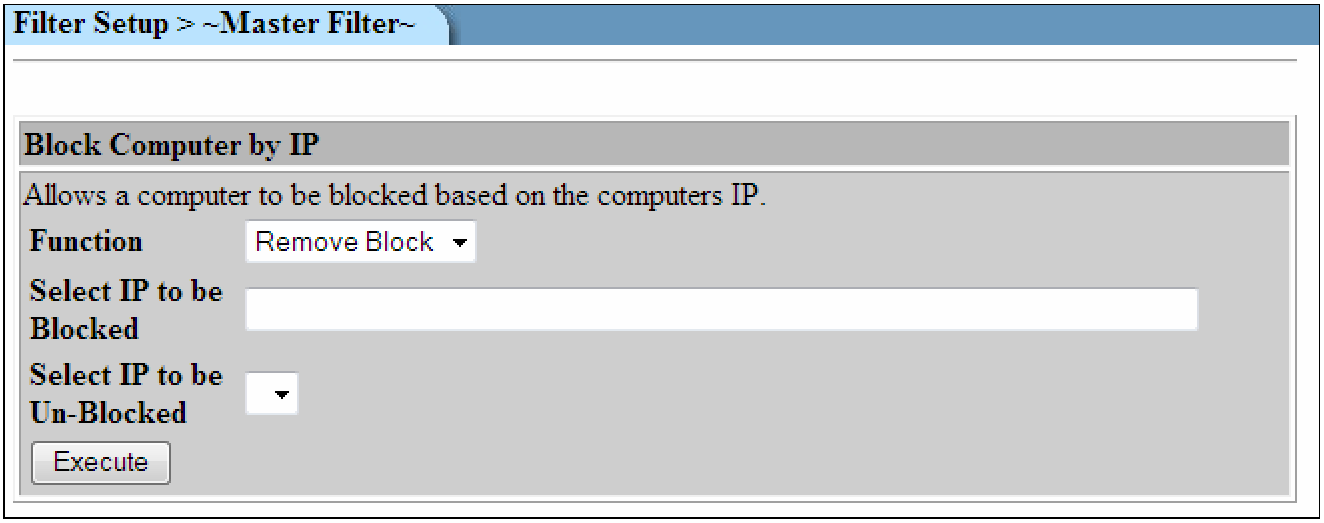
Figure 4-13: Block Computer by IP

Note:	Upon clicking **Execute**, ComSifter Filter Service will restart automatically. This may take up to 30 seconds and will disrupt other Internet users during the restart.

Disable Block

To remove a block:

- Set Function to Remove Block.
- Select IP to be Un-Blocked.
- Click on **Execute**.



Filter Setup > ~Master Filter~

Block Computer by IP

Allows a computer to be blocked based on the computers IP.

Function: Remove Block

Select IP to be Blocked:

Select IP to be Un-Blocked:

Figure 4-14: Removing Blocked Computer by IP

Note:	Upon clicking **Execute**, ComSifter Filter Service will restart automatically. This may take up to 30 seconds and will disrupt other Internet users during the restart.

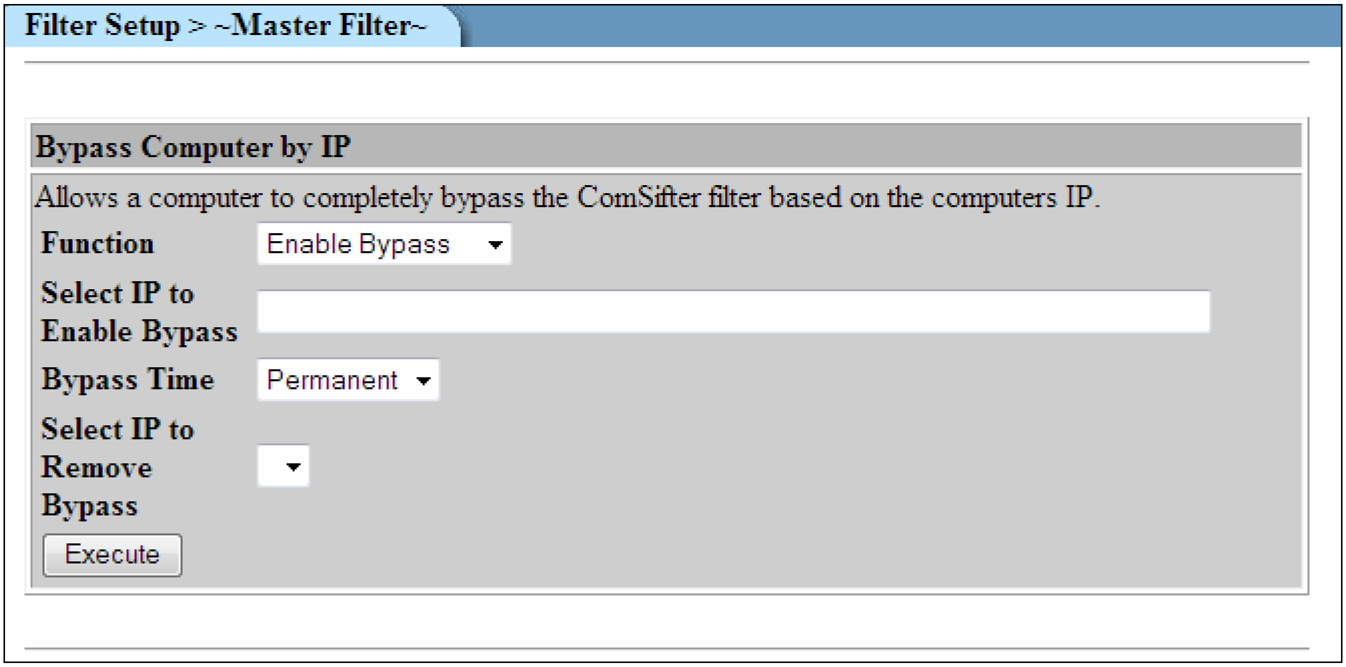
Bypass Computer by IP

The Bypass Computer command allows you to bypass a computer based on the computers IP address.

Enable Bypass

To bypass a computer:

- Set Function to Enable Bypass.
- Enter the IP address of the computer to be bypassed in Select **IP to Enable Bypass.**
- Click on **Execute**.



Filter Setup > ~Master Filter~

Bypass Computer by IP

Allows a computer to completely bypass the ComSifter filter based on the computers IP.

Function: Enable Bypass

Select IP to Enable Bypass:

Bypass Time: Permanent

Select IP to Remove Bypass:

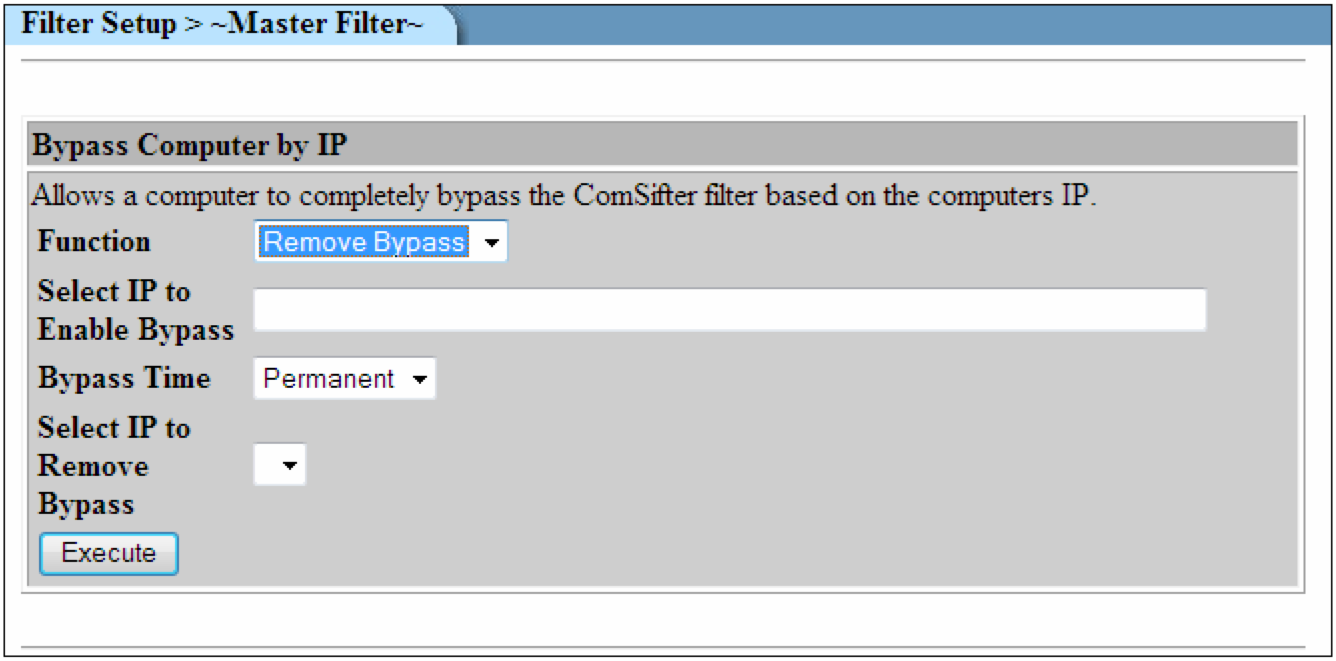
Figure 4-15: Enable Computer Bypass

Note: Upon clicking **Execute**, ComSifter Filter Service will restart automatically. This may take up to 30 seconds and will disrupt other Internet users.

Remove Bypass

To remove a bypass:

- Set Function to Remove Bypass.
- Select IP to Remove Bypass.
- Click on **Execute**.



Bypass Computer by IP

Allows a computer to completely bypass the ComSifter filter based on the computers IP.

Function: Remove Bypass

Select IP to Enable Bypass:

Bypass Time: Permanent

Select IP to Remove Bypass:

Figure 4-16: Remove Computer Bypass

Note:	Upon clicking **Execute**, ComSifter Filter Service will restart automatically. This may take up to 30 seconds and will disrupt other Internet users.

Enable Transparent Proxy Operation

Transparent operation does not require proxy settings in the browser thus reducing the amount of time to set up the filter. It does pose a security risk as ComSifter can only see and filter port 8080, and in transparent mode all ports can be used.

Not enabling transparent mode will enable Proxy mode. In this mode ComSifter will only accept connections on Port 8080 using the proxy protocol of the browser. Client browsers must be set to proxy protocol and pointed at the ComSifters IP port 8080. This mode is more difficult to set up but results in a very secure environment.

Enable Full Logging

When enabled ComSifter will log every request. A typical web site may have 10 – 40 requests per page. In a week this may translate in up to a million log entries. To reduce the size of the logs and increase the speed of log searching Comsift recommends turning this feature off. When not enabled only text files will be logged. This can easily reduce the size of the log files by a factor of 10 to 50 times.

Enable Exception Logging

When enabled Exceptions are logged. Since Exceptions are typically sites or users that you want to have extra access then logging them may just fill up the logs. If that is the case then not enabling this feature will result in Exceptions not being logged.

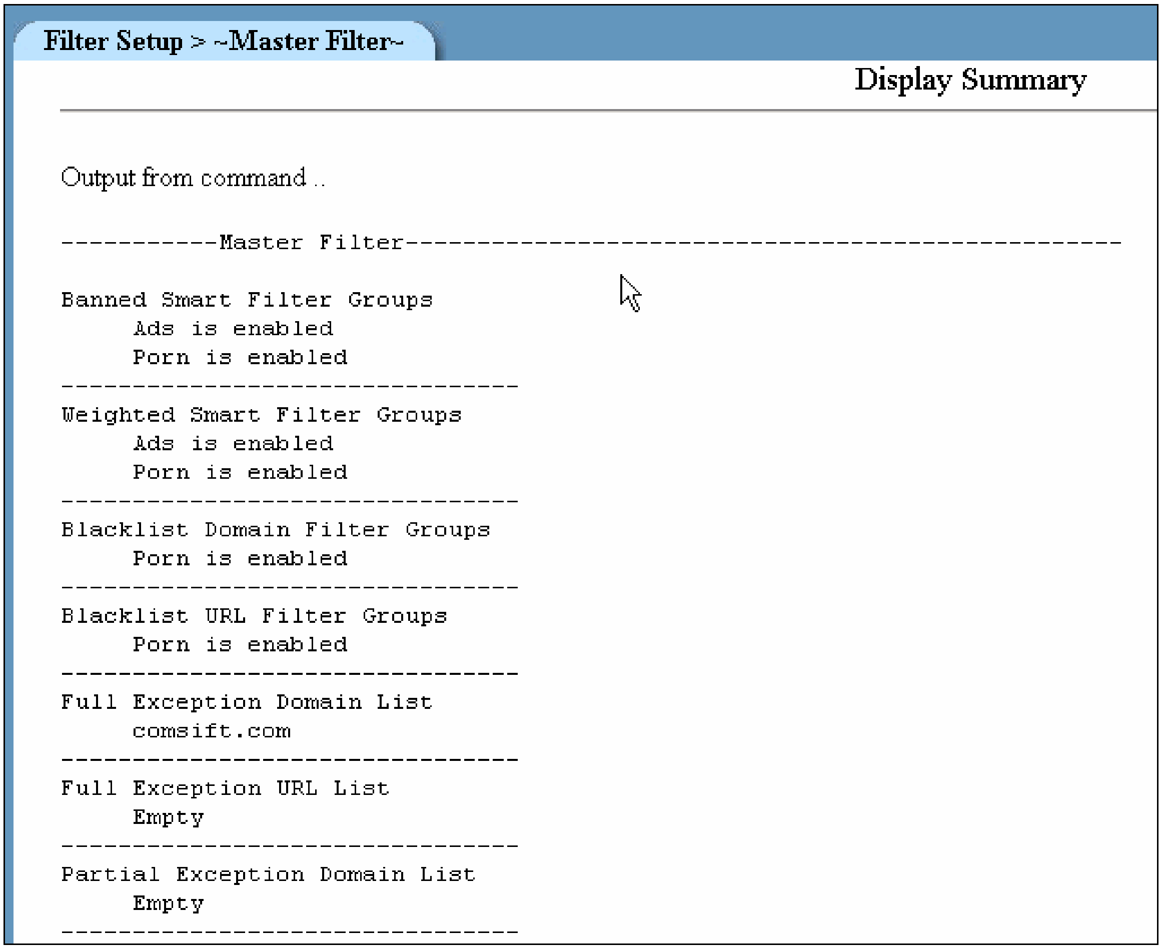
Display Summary

Display Summary displays a report of the configuration of the Master Filter. This report is useful for understanding at a glance how the Master Filter is configured. It includes:

CSphrase Filter Groups that are active.

Blacklist Filter Groups that are active.

All domains, URLs, extensions and MIME Types that are in there respective lists.



Output from command ..

```
-----------Master Filter--------------------------------------------------

Banned Smart Filter Groups
     Ads is enabled
     Porn is enabled
--------------------------------
Weighted Smart Filter Groups
     Ads is enabled
     Porn is enabled
--------------------------------
Blacklist Domain Filter Groups
     Porn is enabled
--------------------------------
Blacklist URL Filter Groups
     Porn is enabled
--------------------------------
Full Exception Domain List
     comsift.com
--------------------------------
Full Exception URL List
     Empty
--------------------------------
Partial Exception Domain List
     Empty
--------------------------------
```

Figure 4-17: Display Summary Report

Individual Filters

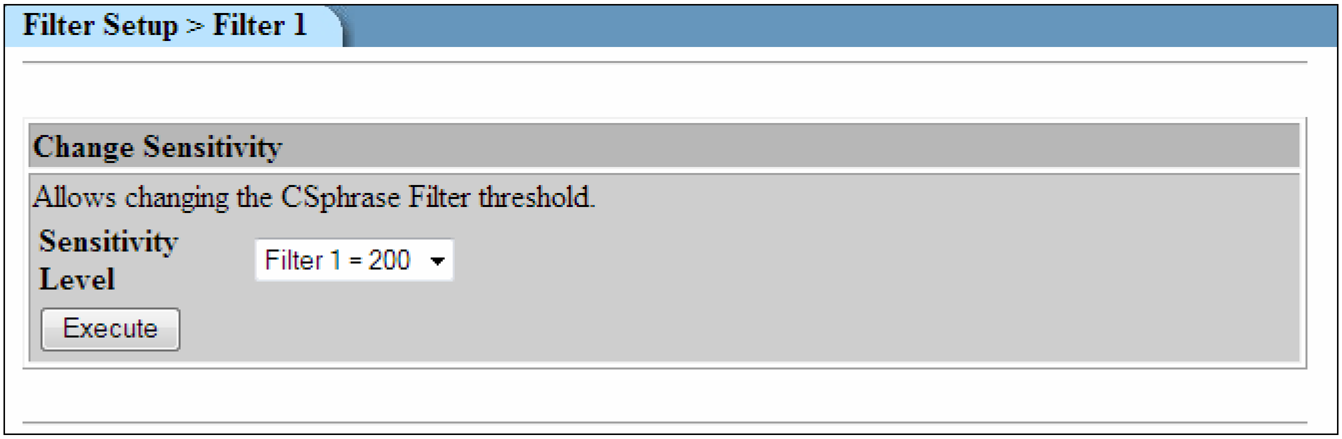
Individual filters are configured in the same manner as the Master Filter. Please refer to the previous section for configuration details with the following exceptions:

Individual filters do not have a Change Filter Name Command.

Individual Filters have one additional command; Sensitivity Level.

Change Sensitivity

This command will set the CSphrase Sensitivity Level for the filter. If a word or phrase is in the filter group, the filter is activated and the word is found on a web page the CSphrase Sensitivity counter will increment by the weight assigned to the word/phrase. If there are any Good Words/Phrases on the same page the CSphrase Sensitivity counter will decrement by the weight assigned to the word/phrase. After analyzing all the words on a page ComSifter will compare it's Sensitivity Counter with the Sensitivity Threshold set for the individual filter. If the threshold is exceeded the page will be banned.



Change Sensitivity

Allows changing the CSphrase Filter threshold.

Sensitivity Level: Filter 1 = 200

Figure 4-18: Sensitivity Threshold

Sensitivity Level Guidelines

Comsift suggests the following guidelines for Sensitivity Levels.

Age Group	Sensitivity Level
Preschool	50
Grade School	100
High School	150
Adult	200

Chapter 5

Words/Phrases

Overview

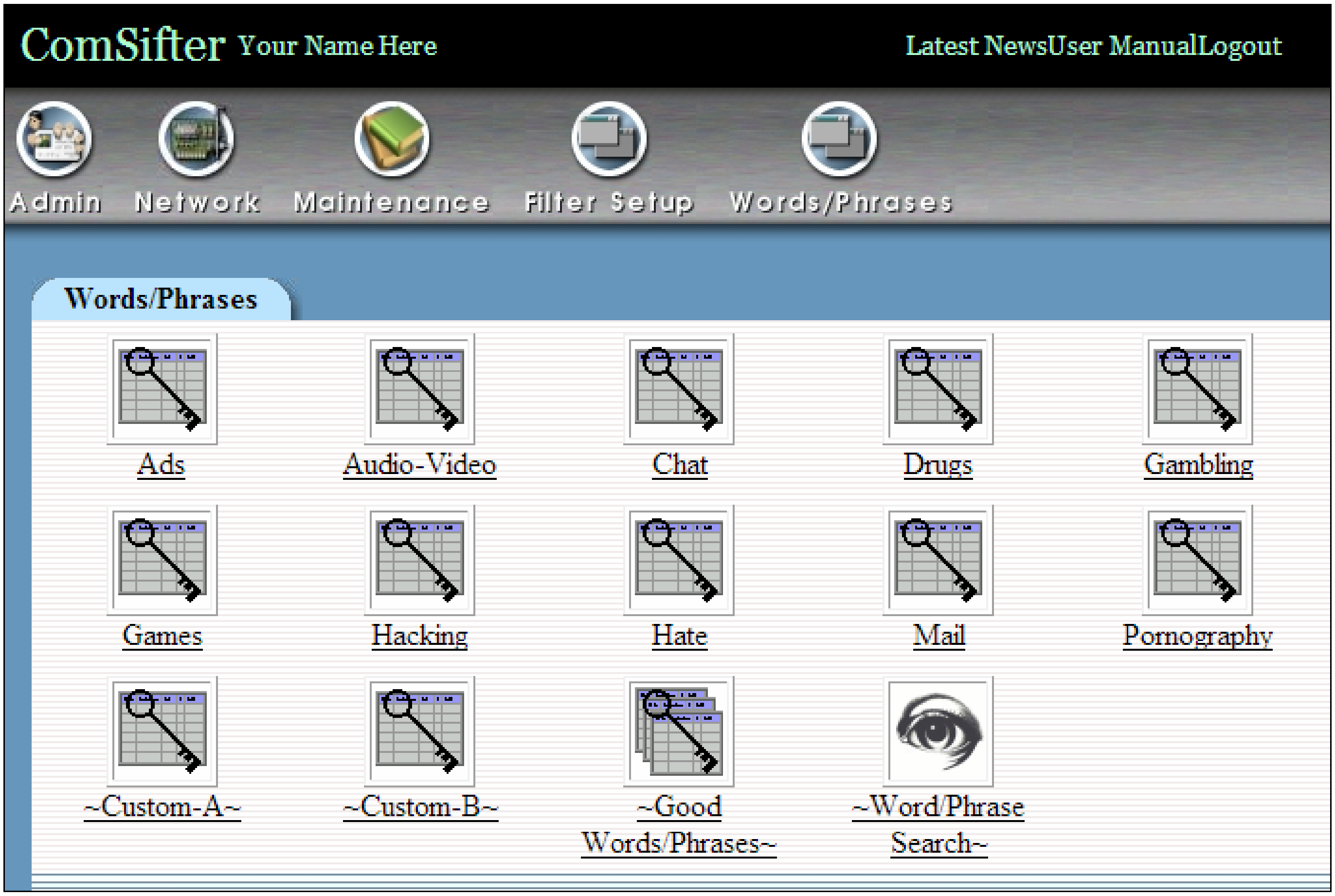


Figure 5-1: Initial Words/Phrases Screen

CSphrase Filtering Technology is used in ComSifter to analyze every word or phrase in a web page. Before passing a web page to a user for viewing, CSphrase technology:

1. Analyzes the source, including Metadata and assigns a numerical value to every word and phrase based on the weighting defined in Words/Phrases.
2. Analyzes what the user will see and assigns a numerical value to every word and phrase based on the weighting defined in Words/Phrases.
3. Good words/phrases have a negative value while bad words/phrases have a positive value. These values are kept internally in a Sensitivity Counter.
4. Upon completing the analysis CSphrase Technology compares the Sensitivity Counter with the Sensitivity Threshold for the users filter. If the threshold is exceeded the Access Denied Page is given to the user and the event is logged in ComSifter Access log, if the threshold is not exceeded, the contents of the web page are shown.

There are twelve groups of bad words/phrases and one group of good words and phrases. The words/phrases found within these groups determine how CSphrase Filter Technology will analyze each web page. The bad words/phrases are found in:

- Ads
- Audio-Video
- Chat
- Drugs
- Gambling
- Games
- Hacking
- Hate
- Mail
- Pornography
- Custom – A
- Custom - B

Within the twelve bad groups there are Banned Words/Phrases and Weighted Words/Phrases.

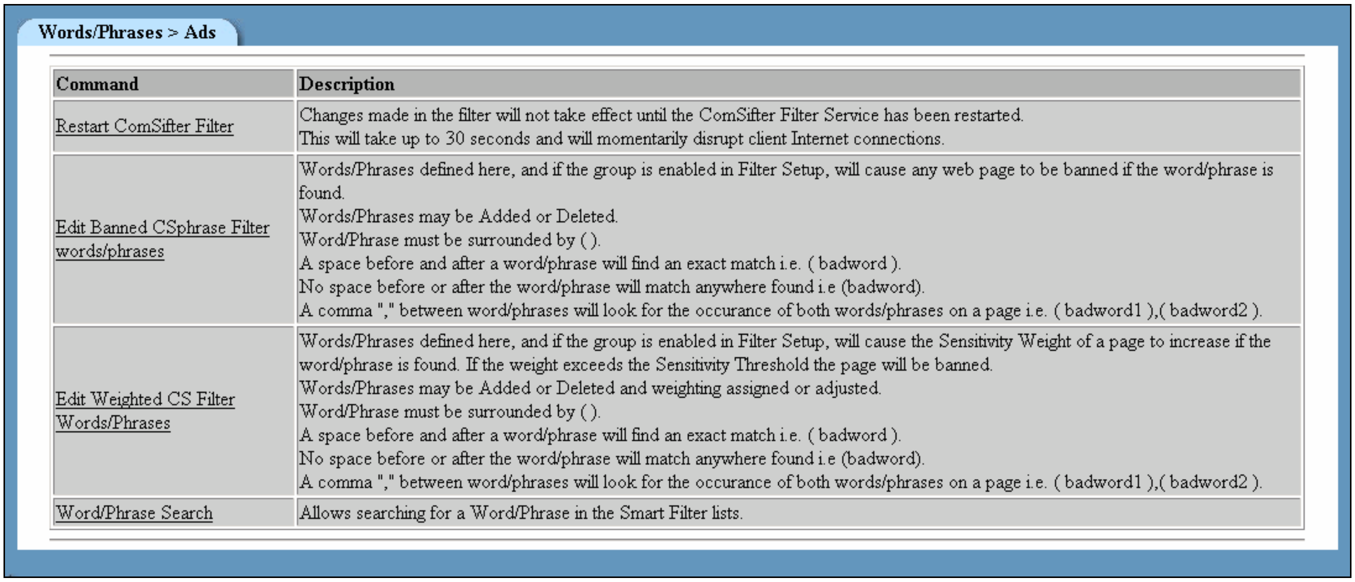
In addition to the twelve bad groups there is a good words/phrase group. This group will modify what is found in the bad groups.

As an example if a web site contains the word “breast”, CSphrase Filter will increment its Sensitivity counter by 5. If on the same page it sees the word “research” it will decrement its Sensitivity counter by 20.

When configuring words/phrases the following conditions apply;

- The word/phrase must be enclosed in parenthesis ( ).
- If an exact match of the word/phrases is required then a space must be placed before and after the word. In the example if we want to only ban gambling then the proper format would be; (gambling). Thus if the web page said “Visit our casino to gamble at your favorite games”, the page would be banned
- If a match of a word beginning with gambling is required then the proper format would be; (gambling). Thus if the web page said “Solve your gamblingfever”, the page would be banned.
- If a match of a word ending in with gambling is required then the proper format would be; (gambling). Thus if the web page said “Casinogambling”, the page would be banned.
- If any match of the word gambling is required the proper format would be; (gambling). Thus if a web page said “Casinogamblingfever”, the page would be banned.
- A further refinement of word/phrases is possible by looking for multiple words/phrases. This is accomplished by separating the words/phrases with a comma. If we wanted to ban any web page that contained the word “casino” and the word “gambling” the proper format would be (casino),(gambling). Thus if the web page said “our casino has gambling for all games” the page would be banned.

Configuring Words/Phrases



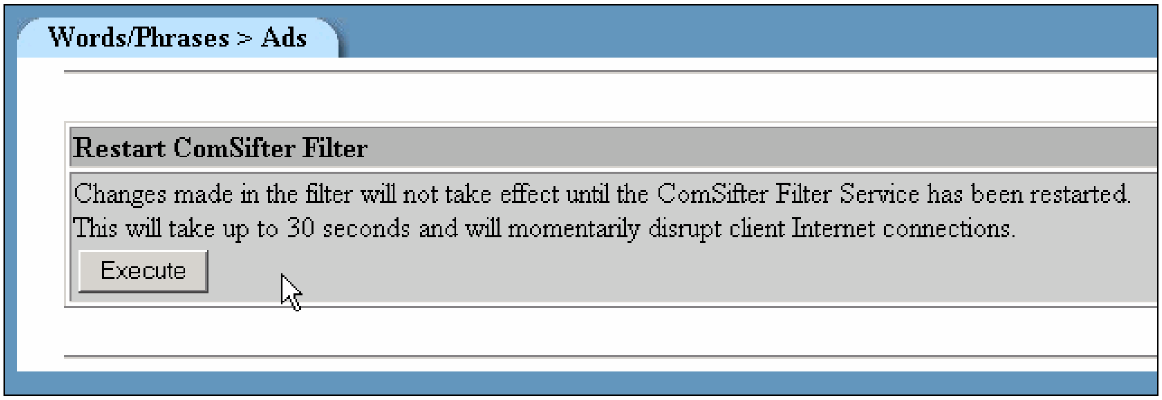
Words/Phrases > Ads

Command	Description
Restart ComSifter Filter	Changes made in the filter will not take effect until the ComSifter Filter Service has been restarted. This will take up to 30 seconds and will momentarily disrupt client Internet connections.
Edit Banned CSphrase Filter words/phrases	Words/Phrases defined here, and if the group is enabled in Filter Setup, will cause any web page to be banned if the word/phrase is found. Words/Phrases may be Added or Deleted. Word/Phrase must be surrounded by ( ). A space before and after a word/phrase will find an exact match i.e. (badword). No space before or after the word/phrase will match anywhere found i.e (badword). A comma "," between word/phrases will look for the occurance of both words/phrases on a page i.e. (badword1),(badword2).
Edit Weighted CS Filter Words/Phrases	Words/Phrases defined here, and if the group is enabled in Filter Setup, will cause the Sensitivity Weight of a page to increase if the word/phrase is found. If the weight exceeds the Sensitivity Threshold the page will be banned. Words/Phrases may be Added or Deleted and weighting assigned or adjusted. Word/Phrase must be surrounded by ( ). A space before and after a word/phrase will find an exact match i.e. (badword). No space before or after the word/phrase will match anywhere found i.e (badword). A comma "," between word/phrases will look for the occurance of both words/phrases on a page i.e. (badword1),(badword2).
Word/Phrase Search	Allows searching for a Word/Phrase in the Smart Filter lists.

Figure 5-2: Banned or Weighted Words/Phrases

Restart ComSifter Filter

Any changes made in Words/Phrases will not become effective until the ComSifter Filter is restarted. ComSifter is designed to allow you to quickly make multiple changes to Words/Phrases and then apply the changes by restarting the filter.



Words/Phrases > Ads

Restart ComSifter Filter

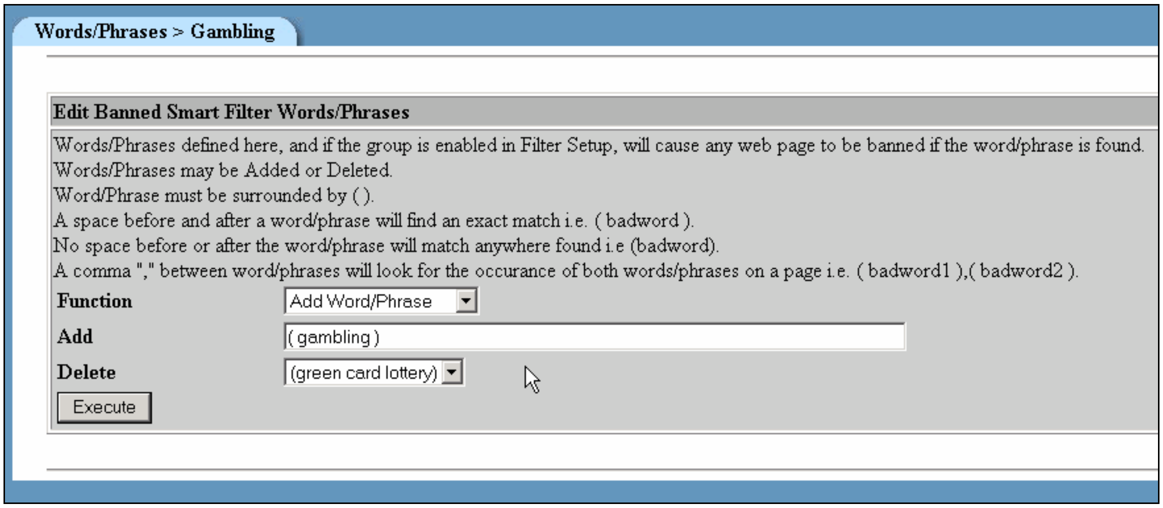
Changes made in the filter will not take effect until the ComSifter Filter Service has been restarted. This will take up to 30 seconds and will momentarily disrupt client Internet connections.

Figure 5-3: Restart ComSifter Filter

Note: A restart may take up to 30 seconds to complete. During this time all Internet connections will be disrupted.

Editing Banned Words/Phrases

A word or phrase placed in the Banned list will result in an Access Denied Page to the user if the Banned word or phrase is found anywhere on the requested web page.



Edit Banned Smart Filter Words/Phrases

Words/Phrases defined here, and if the group is enabled in Filter Setup, will cause any web page to be banned if the word/phrase is found.
Words/Phrases may be Added or Deleted.
Word/Phrase must be surrounded by ( ).
A space before and after a word/phrase will find an exact match i.e. (badword).
No space before or after the word/phrase will match anywhere found i.e (badword).
A comma "," between word/phrases will look for the occurance of both words/phrases on a page i.e. (badword1),(badword2).

Function Add Word/Phrase
Add (gambling)
Delete (green card lottery)

Figure 5-4: Adding or Deleting Words/Phrases

Add

1. To add a word to the Banned CSphrase Word/Phrase list:
2. Select **Add Word/Phrase** in the Function drop down box.
3. Enter the Word/Phrase to be banned following the syntax rules described at the beginning of this chapter.
4. Click **Execute**.

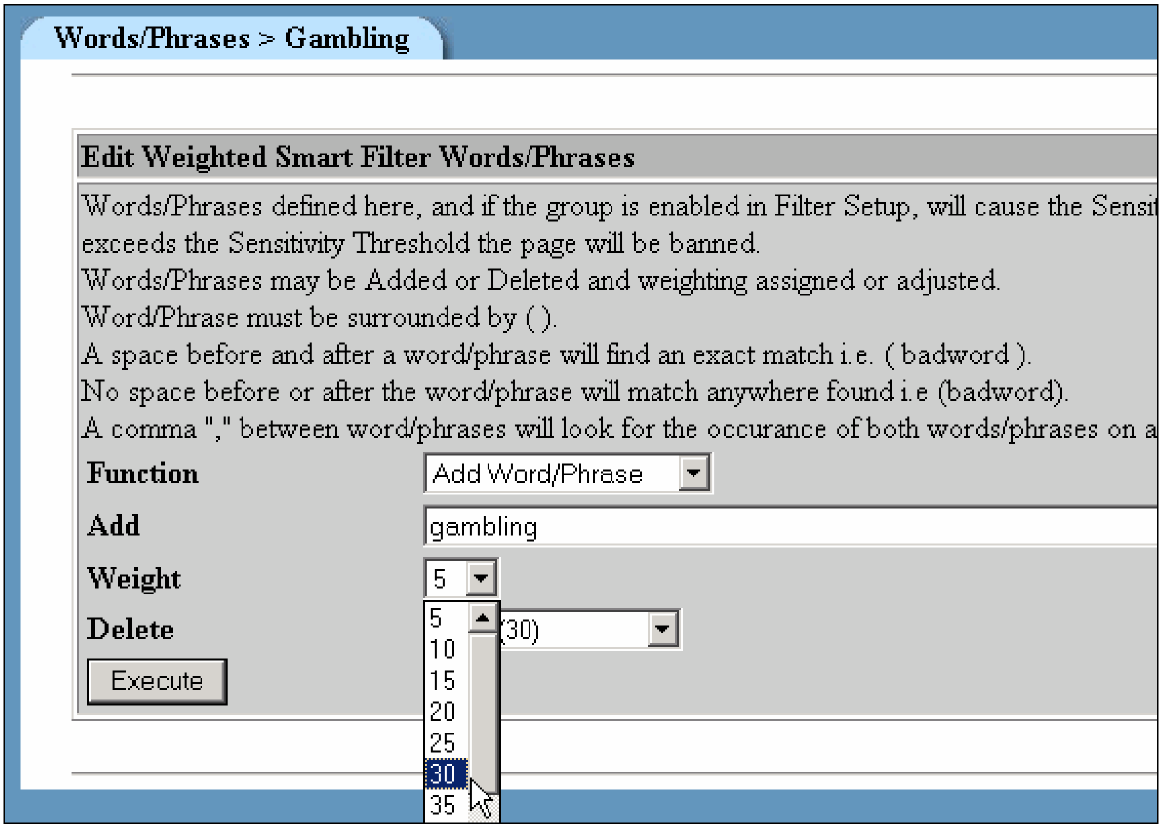
Delete

To remove a word in the Banned CSphrase Word/Phrase list:

1. Select **Delete Word/Phrase** in the Function drop down box.
2. Select the **Word/Phrase** to be removed from the Delete drop down box.
3. Click **Execute**.

Editing Weighted Words/Phrases

A word or phrase placed in the Weighted list will result in CSphrase Filtering Technology applying the weight of the word/phrase to its Sensitivity Counter if the word/phrase is found on the requested web page. After analyzing the complete web page, CSphrase Filter will compare its Sensitivity Counter with the Sensitivity Threshold. If the threshold is exceeded the user will receive an Access Denied Page". If the threshold is not exceeded the user will be allowed to view the web page.



Words/Phrases > Gambling

Edit Weighted Smart Filter Words/Phrases

Words/Phrases defined here, and if the group is enabled in Filter Setup, will cause the Sensit
exceeds the Sensitivity Threshold the page will be banned.
Words/Phrases may be Added or Deleted and weighting assigned or adjusted.
Word/Phrase must be surrounded by ( ).
A space before and after a word/phrase will find an exact match i.e. (badword).
No space before or after the word/phrase will match anywhere found i.e (badword).
A comma "," between word/phrases will look for the occurance of both words/phrases on a

Function Add Word/Phrase

Add gambling

Weight 5

Delete (30)

Figure 5-5: Editing Weighted Words/Phrases

Add

1. To add a word to the Weighted CSphrase Word/Phrase list:
2. Select **Add Word/Phrase** in the Function drop down box.
3. Enter the Word/Phrase to be banned following the syntax rules described at the beginning of this chapter.
4. Assign a weight to the word/phrase
5. Click **Execute**.

Delete

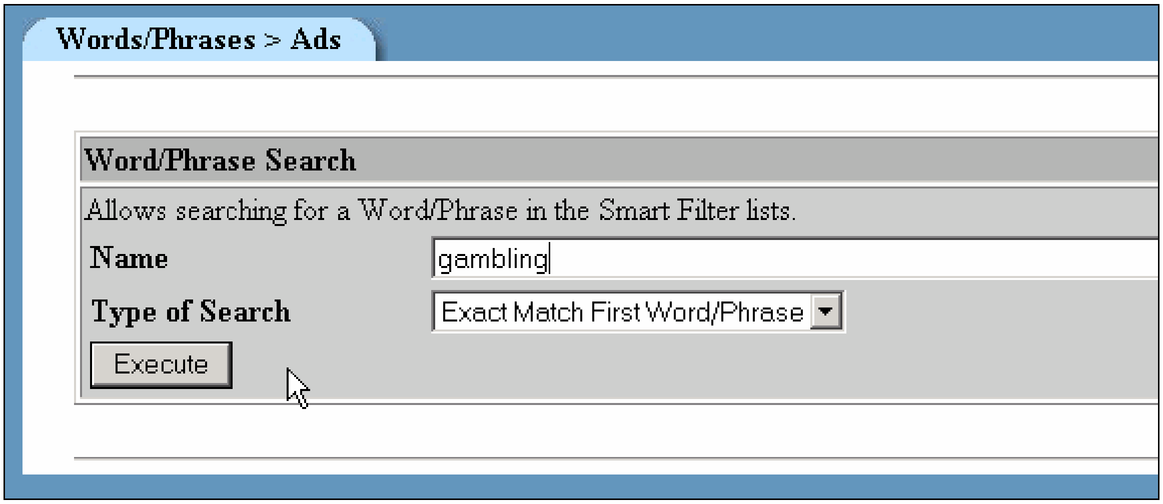
To remove a word in the Weighted CSphrase Word/Phrase list:

1. Select **Delete Word/Phrase** in the Function drop down box.
2. Select the Word/Phrase to be removed from the Delete drop down box.
3. Click **Execute**.

Search

ComSifter incorporates a comprehensive search facility that allows you to search for a Word or Phrase. The search will check all Word/Phrase groups and return where the search term was found.

In the following example we are searching for the word “gambling”.

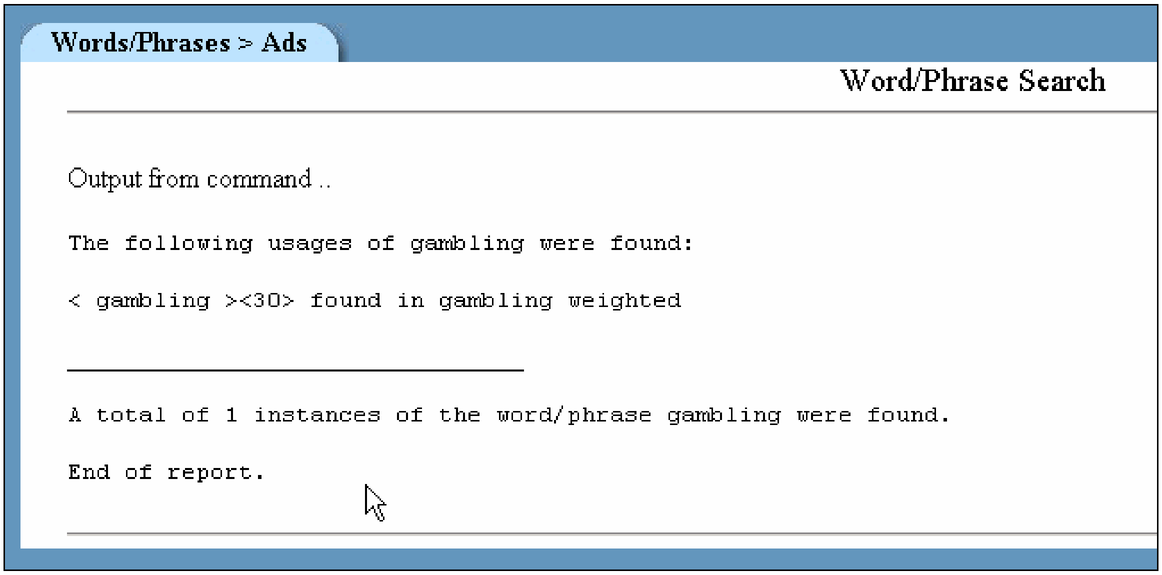


Word/Phrase Search

Allows searching for a Word/Phrase in the Smart Filter lists.

Name	gambling
Type of Search	Exact Match First Word/Phrase

Figure 5-6: Word/Phrase Search



Word/Phrase Search

Output from command ..

```
The following usages of gambling were found:

< gambling ><30> found in gambling weighted

________________________________

A total of 1 instances of the word/phrase gambling were found.

End of report.
```

Figure 5-7: Word/Phrase Search Result

Search returns a report that tells us gambling was found in “gambling weighted” and has a weight of 30.

Chapter 6

ComSifter Operation

ComSifter operates as an in-line filter between the requesting computer and the Internet. The diagram below shows how a request is routed through ComSifter.

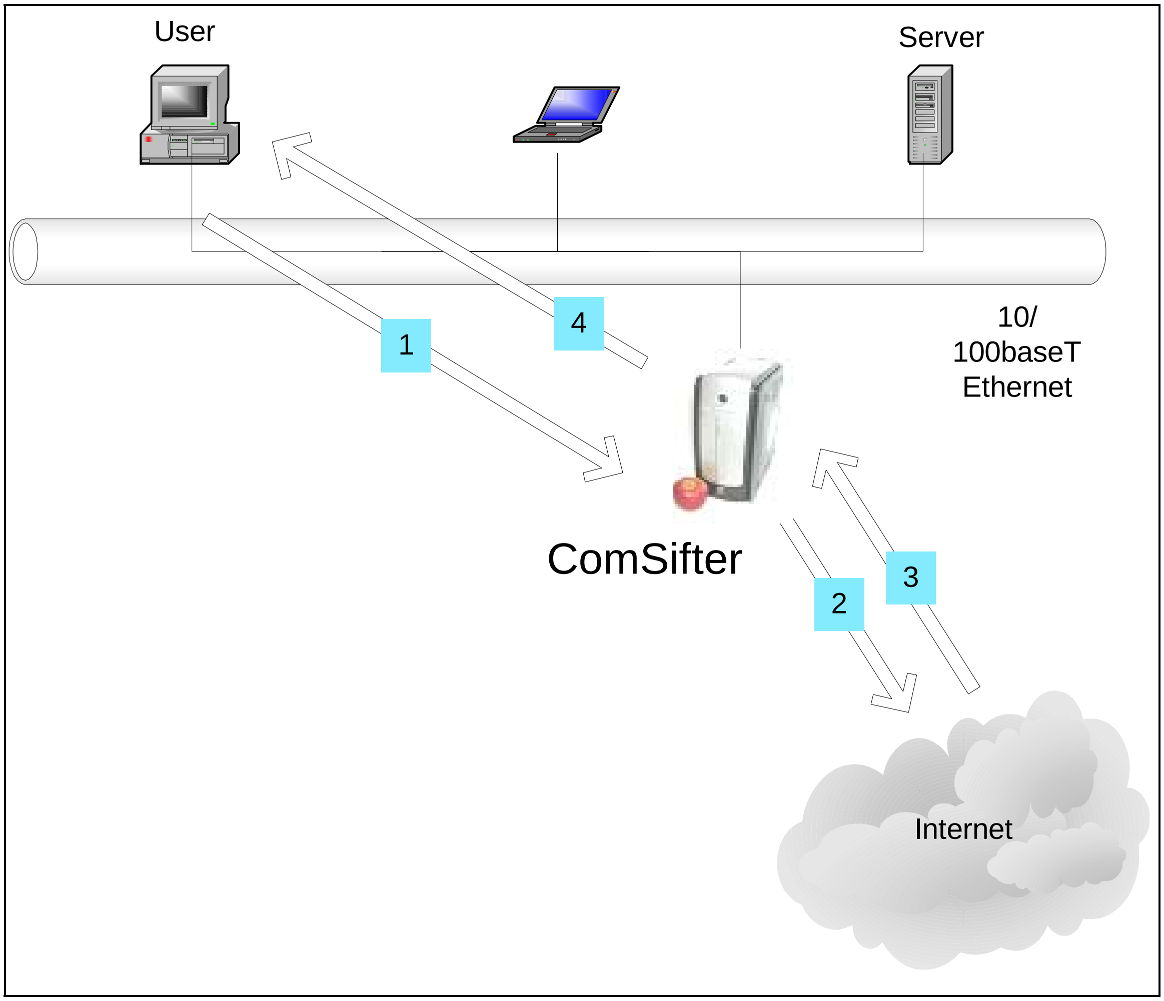


Figure 6-1 ComSifter Operation

Network Flow

1. User requests web page (1).
2. ComSifter queries User Computer for Identification (username) (4).
3. Identd on user computer responds with username (1).
4. ComSifter looks up username in database and determines filter to be applied to page.
5. ComSifter checks internal cache for page. If locally cached, ComSifter goes to step 8.
6. If not locally cached ComSifter requests page from Internet (2).
7. Page is retrieved from Internet (3).

8. If clean ComSifter serves page to end user (4). If not clean ComSifter sends "Access Denied" page (4).

How ComSifter filters

Two levels of filtering insure that ComSifter will stop inappropriate content.

1. ComSifter first checks the requested URL against its Exception IP List to see if the site is excepted.
2. Next ComSifter checks the URL against it Exception Site list to see if it is excepted.
3. Next ComSifter checks the URL against its blacklist. This list has over 500,000 entries and is categorized by content.
4. ComSifter then loads the complete page into memory and scans every word on the page. It then applies its CSphrase Filter Technology to determine if the page is acceptable or not.
5. If acceptable the page is sent to the requesting computer.
6. If the page is deemed unacceptable the “Access Denied” page is sent to the requesting computer.

Order of Precedence

Following is the Order of Precedence ComSifter uses when filtering. ComSifter will process the first rule that matches. Once a rule has matched Comsifter stops rule processing.

An example would be a download ban of all exe files. Exe would be entered in the appropriate Banned Extension List. But you would like to allow users to download from a trusted site. If that site were placed in the Exception Site List then the rule would stop when it matched in the Exception Site List.

- Bypass Computer
- Bypass User
- Hours of Operation
- Full Exception Domain List
- Full Exception URL List
- Blanket Block
- Blocked Computer
- Blocked User
- Banned URL List
- Blanket IP Block
- Banned Domain List
- Banned MIME List
- Banned Extension List
- CSphrase Filter Exception Words/Phrases
- CSphrase Filter Banned Words/Phrases
- CSphrase Filter Weighted Words/Phrases

Blacklist

ComSifter maintains a Blacklist of sites that have been deemed unacceptable. The list is categorized as follows:

Categories

Advertising
Audio-video
Chat
Drugs
Gambling
Games
Hacking
Hate
Mail
Pornography

Blacklist Update

The staff at ComSifter constantly adds and removes sites from its blacklists. ComSifter will update its blacklists either daily or weekly, depending on the service contract you have acquired.

- The daily update is performed at a random time between 11:00 PM and 6:00 AM, local time.
- The weekly update is performed Sunday, at a random time, between 11:00 PM and 6:00 AM, local time.
- The update is automatic and requires no user intervention.

Note: Upon a Blacklist update ComSifter will restart with the new list. A restart may take up to one minute to complete. During this time user access to the Internet will be denied.

CSphrase Filter Technology

Blacklists are very effective if the offending web site is known. 100’s of new sites catering to pornography and other inappropriate content are added to the Internet weekly.

To insure that these sites are blocked, until they can be added to the Blacklist, ComSifter uses CSphrase Filtering Technology. CSphrase Filtering scans and assigns a numeric weight to each word on the requested page. Appropriate words are assigned a negative value while inappropriate words are assigned a positive value. ComSifter then adds these weights together and derives a value for the page. This value is then compared with the Sensitivity threshold described in Filter Setup. If the threshold is exceeded the page is denied. If the threshold is not exceeded the page is displayed.

An example of this in action is a search engine search for “nude breasts”. The page will be denied as it brings up multiple pornographic sites and the threshold is exceeded.

A search on the phrase “breast cancer” is not blocked. The good words found on the page modify the bad words—allowing the page to be displayed.

Note: CSphrase Filtering is biased to “not show the page if in doubt”. This reduces the chance that web users will be exposed to inappropriate content. As a result of this bias there may be cases where a user believes they have entered a very safe query but the page is blocked. If so, a more defined search may bring better results. Using the example above a search on “breast cancer” will yield better results than “breast” Even better would be “breast cancer research”.

Appendix A

Contact Information

For your convenience, Comsift provides a number of ways for you to contact us.

Location

Comsift, Inc. is located at:

1646 Elderberry Way
San Jose, CA 95125

Phone,	Main	866-875-1254 (toll free in U.S.)
	Sales	866-875-1254 x 701 (toll free in U.S.)
	Support	866-875-1254 x 702 (toll free in U.S.)
	Fax	408-265-5249

Website

Our website is at www.comsift.com (If you're reading this document as a PDF file and are currently on-line, please click the URL above and you'll be transported to our website.) On our website, you will find the latest information about our leading-edge solutions, product announcements along with a form you can use for general information requests.

Sales

Our friendly and knowledgeable sales staff is available to answer your sales-related questions. Hours of operation are from Monday through Friday, 8:00am to 5:00pm Pacific Time at 866 875-1254 x 701.

Technical Support

Comsift provides technical phone support at 866 875-1254 x 702. Email support is available at support@comsift.com. You can also fax your questions to us at our 24-hour fax number: 408-265-5249.

Appendix B

Specifications

Configuration

Although ComSifter may be configured from any computer using Windows ME, Windows 2000, Windows XP, MAC OS X or Linux as its operating system, the preferred arrangement is Windows 2000/XP using Internet Explorer 5 or above with a screen resolution of 1024 x 768 or greater. Additionally the File Manager and System Time modules require the use of Java™. If you need to obtain Java it is available for download courtesy of Sun Microsystems™ at www.sun.com .

Network

Network Type - 10/100baseT

Number of Computers

ComSifter is not limited to a certain number of computers but rather will be limited by the load presented by the computers requesting connection to the Internet. ComSifters filtering service is able to filter a page in less than 10ms, resulting in 100 requests per second. Up to 1000 simultaneous HTTP connections are supported. With typical user viewing patterns this can translate to hundreds of computers being connected to ComSifter at once.

Throughput

Raw throughput through ComSifter is 40mbps. This figure may be reduced based on the number of concurrent connections, the size of pages that are being filtered and the number of Port Blocker Rules that have been implemented.

Typical Access Time

Access time per HTTP request is less than 10ms.

Caching Proxy

ComSifter incorporates a caching proxy that caches web pages that have been accessed and filtered. Subsequent accesses to these pages are served from the caching proxy – not from the Internet. Access time from the cache is near instantaneous and depending on network usage patterns may result in a substantial reduction in Internet network traffic.

Blacklist Update

The Blacklist is updated automatically between 11:00 PM and 6:00 AM daily local time or between 11:00 PM and 6:00 AM Sundays, depending on the Service Contract. The update takes a few seconds over a typical 1.5mbps line.

Mechanical & Environmental

Dimensions – HxWxD 11.5” x 5.5” x 10.5”

Weight – 10 lbs

Electrical - 115VAC, 40watts

Temperature - 50 - 95° F (10 -35° C)

Appendix C

Filter Defaults

	Filter 1	**Filter 2**	**Filter 3**	**Filter 4 - 8**
Banned CSphrase Filter Groups	Porn	Porn Ads Audio-video Chat Custom-a Custom-b Drugs Gambling Games Hacking Hate Mail	Porn Ads Audio-video Custom-a Custom-b Drugs Gambling Games Hacking Hate	Porn
Weighted CSphrase Filter Groups	Porn	Porn Ads Audio-video Chat Custom-a Custom-b Drugs Gambling Games Hacking Hate Mail	Porn Ads Audio-video Custom-a Custom-b Drugs Gambling Games Hacking Hate	Porn
Blacklist Domain Filter Groups	Porn	Porn Ads Audio-video Chat Drugs Gambling Games Hacking Hate Mail	Porn Ads Audio-video Drugs Gambling Games Hacking Hate	Porn
Full Exception Domain List	Porn	Porn Ads Audio-video Chat Drugs Gambling Games Hacking Hate Mail	Porn Ads Audio-video Drugs Gambling Games Hacking Hate	Porn

	Filter 1	Filter 2	Filter 3	Filter 4 - 8
Banned Extension List		.asf .avi .bin .bz2 .cdr .cpl .cue .dll .dmg .exe .gz .hlp .hqx .inf .ini .ins .iso .isp .mda .mdb .mde .mdn .mdt .mdw .mdz .mp3 .mpeg .msc .mst .ogg .ops .otf .pcd .pif .prf	.asf .avi .bin .bz2 .cdr .cpl .cue .dll .dmg .exe .gz .hlp .hqx .inf .ini .ins .iso .isp .mda .mdb .mde .mdn .mdt .mdw .mdz .mp3 .mpeg .msc .mst .ogg .ops .otf .pcd .pif .prf	
		.rar .reg .scr .sct .sea .sh .shs .sit .smi .sys .tar .tgz .vxd .wmf .zip	.rar .reg .scr .sct .sea .sh .shs .sit .smi .sys .tar .tgz .vxd .wmf .zip	
Sensitivity	200	100	150	200
Hours of Operation	Always On	Always On	Always On	Always On
Warn-and-Go	Disabled	Disabled	Disabled	Disabled

Appendix D

License & Warranty

COMSIFT, INC. APPLIANCE LICENSE AND WARRANTY AGREEMENT

1. Limited Warranty:
Comsift warrants that the Appliance will operate in substantial compliance with the written documentation accompanying the Appliance for a period of thirty (30) days from the date of purchase of the Appliance. Your sole remedy in the event of a breach of this warranty will be that Comsift will, at its option, repair or replace any defective Appliance returned to Comsift within the warranty period or refund the money you paid for the Appliance.

Comsift warrants that the hardware component of the Appliance (the “Hardware”) shall be free from defects in material and workmanship under normal use and service and substantially conform to the written documentation accompanying the Appliance for a period of three hundred sixty-five (365) days from the date of purchase of the Appliance. Your sole remedy in the event of a breach of this warranty will be that Comsift will, at its option, repair or replace any defective Hardware returned to Comsift within the warranty period.

The warranties contained in this agreement will not apply to Hardware which:

A. has been altered, supplemented, upgraded or modified in any way; or
B. has been repaired except by Comsift or its designee.
Additionally, the warranties contained in this agreement do not apply to repair or replacement caused or necessitated by: (i) events occurring after risk of loss passes to You such as loss or damage during shipment; (ii) acts of God including without limitation natural acts such as fire, flood, wind earthquake, lightning or similar disaster; (iii) improper use, environment, installation or electrical supply, improper maintenance, or any other misuse, abuse or mishandling; (iv) governmental actions or inactions; (v) strikes or work stoppages; (vi) Your failure to follow applicable use or operations instructions or manuals; or (vii) such other events outside Comsift’s reasonable control.

Upon discovery of any failure of the Hardware, or component thereof, to conform to the applicable warranty during the applicable warranty period, You are required to contact us within ten (10) days after such failure and seek a return material authorization (“RMA”) number. Comsift will promptly issue the requested RMA as long as we determine that you meet the conditions for warranty service. The allegedly defective Appliance, or component thereof, shall be returned to Comsift, securely and properly packaged, freight and insurance prepaid, with the RMA number prominently displayed on the exterior of the shipment packaging and with the Appliance. Comsift will have no obligation to accept any Appliance which is returned without an RMA number.

Upon completion of repair or if Comsift decides, in accordance with the warranty, to replace a defective Appliance, Comsift will return such repaired or replacement Appliance to You, freight and insurance prepaid. In the event that Comsift, in its sole discretion, determines that it is unable to replace or repair the Hardware, Comsift will refund to You the F.O.B. price paid by You for the defective Appliance. Defective Appliances returned to Comsift will become the property of Comsift.

Comsift does not warrant that the Appliance will meet your requirements or that operation of the Appliance will be uninterrupted or that the Appliance will be error-free.

THE ABOVE WARRANTIES ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. THIS

WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE.

2. Disclaimer of Damages:
SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL COMSIFT OR ITS LICENSORS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF COMSIFT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL COMSIFT'S OR ITS LICENSORS' LIABILITY EXCEED THE PURCHASE PRICE FOR THE APPLIANCE. The disclaimers and limitations set forth above will apply regardless of whether you accept the Software or the Appliance.

3. Open Source Software:
Open Source Software consists of the open source code software known as Linux, DansGuardian, Webmin, Squid, Shorewall, ISC DHCPD and Ulog included with the Appliance. Open Source Software is licensed under the GNU General Public License, Version 2, June 1991. The license entitles you to receive a copy of the source code for these programs only upon request at a nominal charge. If you are interested in obtaining a copy of such source code, please contact Comsift Customer Service at the above addresses for further information.

4. Export Regulation: You agree to comply strictly with all applicable export control laws, including the US Export Administration Act and its associated regulations and acknowledge Your responsibility to obtain licenses as required to export, re-exp ort or import the Appliance. Export or re-export of the Appliance to Cuba, North Korea, Iran, Iraq, Libya, Syria or Sudan is prohibited.

5. General:
This Agreement will be governed by the laws of the State of California, United States of America. This Agreement is the entire agreement between You and Comsift relating to the Appliance and: (i) supersedes all prior or contemporaneous oral or written communications, proposals and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment or similar communications between the parties. This Agreement may only be modified by a written document which has been signed by both You and Comsift. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and shall return the Appliance to Comsift. The disclaimers of warranties and damages and limitations on liability shall survive termination. Should you have any questions concerning this Agreement, or if you desire to contact Comsift for any reason, please write: Comsift Customer Service, 1646 Elderberry Way, San Jose, CA 95125.