



# ComSifter

*protect web users now!*



## **Installation Guide**

### **Model CS-8 Pro**

**Version 9.1 January 23, 2006**

The products described in this User's Guide are licensed products of Comsift, Inc. This User's Guide contains proprietary information protected by copyright, and this User's Guide is copyrighted.

Comsift, Inc., hereafter referred to as Comsift, does not warrant that the product will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose.

Comsift has made every effort to ensure that this manual is accurate. However, information in this User's Guide is subject to change without notice and does not represent a commitment on the part of Comsift. Comsift makes no commitment to update or keep current the information in this User's Guide, and reserves the right to make changes to this User's Guide and/or product without notice. Comsift assumes no responsibility for any inaccuracies and omissions that may be contained in this User's Guide. If you find information in this User's Guide that is incorrect, misleading, or incomplete, we would appreciate your comments.

No part of this User's Guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, without the express written permission of Comsift.

Comsift, ComSifter, CSphrase and the Comsift logo are trademarks of Comsift, Inc.

All other trademarks or registered trademarks listed belong to their respective owners.

Copyright 2003-2006 Comsift, Inc.

All rights reserved.

## 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

<b>Table of Contents</b> .....	<b>i</b>
<b>Introduction and Getting Started</b> .....	<b>1-1</b>
<b>Features</b> .....	<b>1-1</b>
<b>How ComSifter Works</b> .....	<b>1-3</b>
Overview .....	1-4
Internet Gateway .....	1-4
Firewall .....	1-4
Filtering System .....	1-4
Navigating Through This Installation Guide .....	1-6
Conventions in This User's Guide .....	1-7
<b>Getting Started</b> .....	<b>1-8</b>
<b>Installing ComSifter</b> .....	<b>2-1</b>
<b>Installation</b> .....	<b>2-2</b>
Security Considerations .....	2-2
Location .....	2-2
AC Power .....	2-2
Network Connections .....	2-2
Power On and Indicator Lights .....	2-2
<b>Connecting a browser to ComSifter</b> .....	<b>2-4</b>
Windows 2000/XP .....	2-5
<b>Making a secure connection</b> .....	<b>2-6</b>
<b>Configuring ComSifter</b> .....	<b>3-1</b>

**Configuration Overview.....3-1**

**Admin .....3-2**

    Understanding Modules and Categories.....3-2

    Security Configuration .....3-3

        Login.....3-3

    ComSifter Admins .....3-5

        Overview .....3-5

        Setting the Username and Password .....3-6

        Assigning Module Rights.....3-7

    Remote Administration..... 3-10

        IP Access Control..... 3-10

        Deny from all IP's ..... 3-11

        Allow from all IP's ..... 3-11

        Allow from only listed IP's ..... 3-11

    System Logs..... 3-12

        Access Log..... 3-13

            Result Messages ..... 3-13

        Firewall ..... 3-15

        Security Log ..... 3-17

        Top Sites Log ..... 3-18

**Network ..... 3-19**

    ADSL Client..... 3-20

    DHCP Configuration..... 3-21

        Using an existing DHCP Server ..... 3-21

        Using the ComSifter DHCP Server ..... 3-21

        Factory Configuration ..... 3-21

        Edit Client Options ..... 3-24

        Add a New Host ..... 3-25

---

Starting and Stopping the DHCP Server .....	3-26
Firewall Advanced .....	3-27
Overview .....	3-27
Masquerading (SNAT) .....	3-29
Firewall Rules .....	3-30
Create Firewall Rules .....	3-32
Action .....	3-32
Logging .....	3-33
Source Zone .....	3-34
Destination Zone .....	3-34
Protocol .....	3-34
Source Ports .....	3-35
Destination Ports .....	3-35
Common Rules .....	3-36
DNS .....	3-36
Client Email (POP3, IMAP, SMTP) .....	3-37
FTP .....	3-38
ICQ/IM .....	3-39
Laplink™ .....	3-40
MSN™ Messenger .....	3-41
NTP (Network Time Protocol) .....	3-42
PCAnywhere™ .....	3-43
Ping & Traceroute .....	3-44
PPTP .....	3-46
Telnet .....	3-48
Vonage™ .....	3-49
VNC .....	3-50
Yahoo™ Chat .....	3-51

---

- Web Access (browsing) ..... 3-52
- Apply Configuration ..... 3-54
- Stop Firewall..... 3-54
- Check Firewall..... 3-55
- Backup ..... 3-55
- Restore..... 3-55
- Firewall Basic (Templates)..... 3-56
  - Template 1, High Security ..... 3-57
  - Template 2, High – Medium Security ..... 3-57
  - Template 3, Medium Security ..... 3-57
  - Template 4, Medium – Low Security..... 3-57
  - Template 5, Low Security..... 3-57
- Network Configuration..... 3-58
  - Network Interfaces (IP Address Configuration)..... 3-58
    - Interfaces Active Now ..... 3-59
    - Interfaces Active at Boot Time..... 3-59
    - WAN Interface Settings (eth0)..... 3-60
    - LAN Interface Settings (eth1) ..... 3-61
  - Virtual Interfaces ..... 3-61
  - Routing and Gateways..... 3-63
  - DNS..... 3-64
  - Completing the DNS/Gateway Configuration..... 3-65
  - Recovering a lost IP address ..... 3-65
- Network Wizards ..... 3-66
  - Static IP ..... 3-67
    - External IP ..... 3-67
    - External Subnet Mask..... 3-67
    - External Gateway ..... 3-67

---

Internal IP.....	3-68
Internal Subnet Mask.....	3-68
Primary DNS.....	3-68
Secondary DNS.....	3-69
DHCP Server for Local LAN.....	3-70
Firewall Template.....	3-70
Dynamic IP.....	3-71
PPPOE.....	3-72
User Name.....	3-72
Password.....	3-72
Current Network Settings.....	3-73
Quality of Service (QOS).....	3-74
Overview.....	3-74
Determining the true Connection Speed.....	3-75
Configure QOS.....	3-77
Connection Speed.....	3-77
Queue Rate and Ceiling.....	3-77
Destination Ports.....	3-78
Destination IP's.....	3-78
Viewing Queue Status.....	3-79
<b>Maintenance.....</b>	<b>3-80</b>
Backup/Restore.....	3-81
Creating a Backup.....	3-81
Restoring the Backup.....	3-82
Denied Access Page.....	3-84
Overview.....	3-84
Local Message.....	3-85
Download/Install IDENTD.....	3-86

---

Downloading the file ..... 3-88

Microsoft Windows Standalone Workstations ..... 3-88

Microsoft Windows 2000/2003 Domain Controller ..... 3-89

Apple Macintosh Standalone Workstation ..... 3-91

Novell Client on Windows Standalone Workstation ..... 3-91

Novell Server -> Novell Client on Windows Standalone  
Workstation ..... 3-91

File Manager ..... 3-92

Information ..... 3-93

    ComSifter Information ..... 3-93

    ComSifter Release Notes ..... 3-95

Internet Connection Test ..... 3-96

Reset Defaults ..... 3-97

System Name ..... 3-98

System Time ..... 3-99

ComSifter Status ..... 3-100

    Active Directory last resync ..... 3-100

    CPU Load Average ..... 3-100

    Content Filter Service ..... 3-100

    DHCP Server ..... 3-101

    DNS Resolving ..... 3-101

    Hardware Health ..... 3-101

    Internet Connected ..... 3-102

    Proxy Server Service ..... 3-102

    Hours of Operation ..... 3-102

Utilities ..... 3-102

    Restart Services ..... 3-103

    Rebuild ComSifter Proxy Cache ..... 3-103



Restart ComSifter .....	3-103
<b>ComSifter Operation.....</b>	<b>4-1</b>
<b>Network Flow .....</b>	<b>4-2</b>
<b>How ComSifter filters.....</b>	<b>4-2</b>
Order of Precedence .....	4-3
Blacklist .....	4-4
Categories .....	4-4
Blacklist Update.....	4-4
CSphrase Filter Technology.....	4-5
<b>Contact Information.....</b>	<b>A-1</b>
<b>Location .....</b>	<b>A-1</b>
<b>Website.....</b>	<b>A-1</b>
<b>Sales .....</b>	<b>A-2</b>
<b>Technical Support.....</b>	<b>A-2</b>
<b>Specifications .....</b>	<b>B-1</b>
Configuration .....	B-1
Network .....	B-1
Number of Computers .....	B-1
Throughput .....	B-2
Typical Access Time .....	B-2
Caching Proxy .....	B-2
Blacklist Update.....	B-2
Mechanical & Environmental.....	B-2
<b>License &amp; Warranty .....</b>	<b>C-1</b>



## 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 firewall 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.
- Eight individually configurable filters. Users may be set to the filter that best fits their filtering needs.
- Active Directory integration.

- 500,000+ site Blacklist updated daily or weekly.
- Built in DHCP server and Caching Proxy.
- Easy to install, no required maintenance.
- Unlimited licensing is standard.

## How ComSifter Works

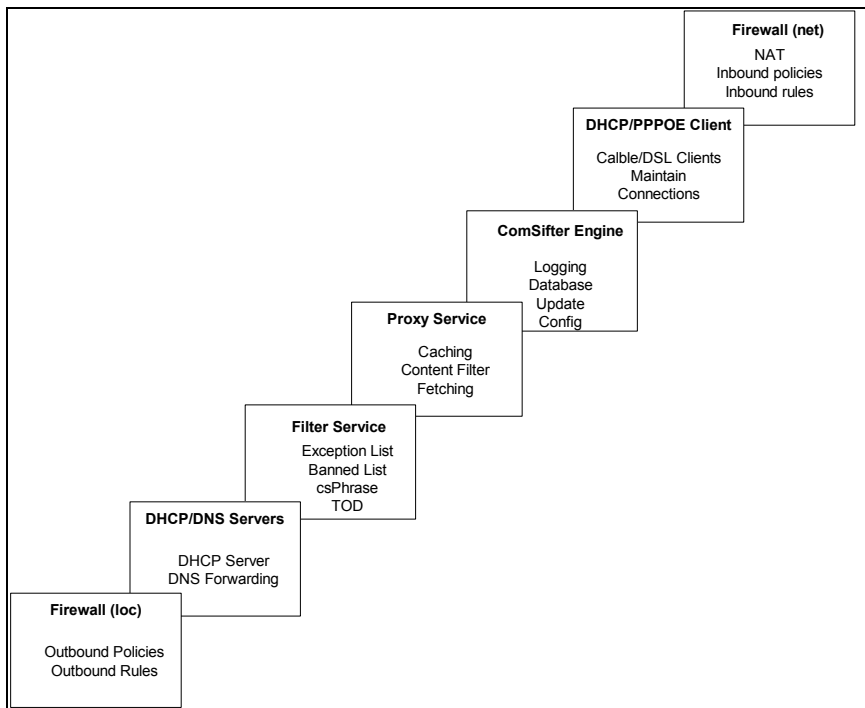


Figure 1-1: ComSifter Architecture

## Overview

ComSifter is a Standalone appliance that connects your internal LAN to the Internet while seamlessly offering firewall and content filtering.

## Internet Gateway

ComSifter may be used as the gateway device from a private LAN to the public Internet. It is able to operate as a standard router or in a Network Address Translation (NAT) mode. In the NAT mode ComSifter converts internal IPs to a public IP, effectively isolating your private network from the Internet.

## Firewall

An industrial strength stealth firewall is included in ComSifter. The Firewall allows complete control of all ports from the Internet to the LAN and from the LAN to the Internet. A high degree of security is available with the Firewall including the ability to stop internal port hopping programs.

## Filtering System

ComSifter CS-8 incorporates eight individual filters. Each filter may be individually configured for the user computers that access the filter. Additionally a global filter allows configuration system wide.

When the user computer accesses a filter, 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 "Denied 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 Installation Guide

This Installation Guide is designed for the technical person that will be installing and configuring the ComSifter network content filtering device. A companion guide, the Operators Guide, describes how to use the ComSifter in day-to-day operation.

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 firewall settings and describing maintenance items.
- Chapter 4, “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, “License and Warranty” — provides information about ComSifter’s Licensing and Warranty.

## Navigating Through This Installation 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.

## Getting Started

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

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

External IP \_\_\_\_\_

(i.e. 63.195.80.100)

External subnet mask \_\_\_\_\_

(i.e. 255.255.255.0)

External Gateway \_\_\_\_\_

(i.e. 63.195.80.1)

Primary DNS \_\_\_\_\_

Secondary DNS \_\_\_\_\_

Internal IP \_\_\_\_\_

(i.e. 192.168.0.1)

External subnet mask \_\_\_\_\_

(i.e. 255.255.255.0)

If you will be using ComSifter's built-in DHCP server the following additional information may be needed.

Static IP device 1 \_\_\_\_\_

Static IP device 2 \_\_\_\_\_

Static IP device 3 \_\_\_\_\_

2. Install ComSifter as described in Chapter 2, Installing ComSifter.
3. Configure ComSifter as described in Chapter 3, Configuring ComSifter.

**Note:** ComSifter includes Network Wizards. The wizards are designed to allow you to bring up your ComSifter by filling in the information on one screen. After installing ComSifter please review [Network Wizards](#) to initially configure your ComSifter.



## 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 between your connection to the Internet and Internal LAN as shown in the diagram below.

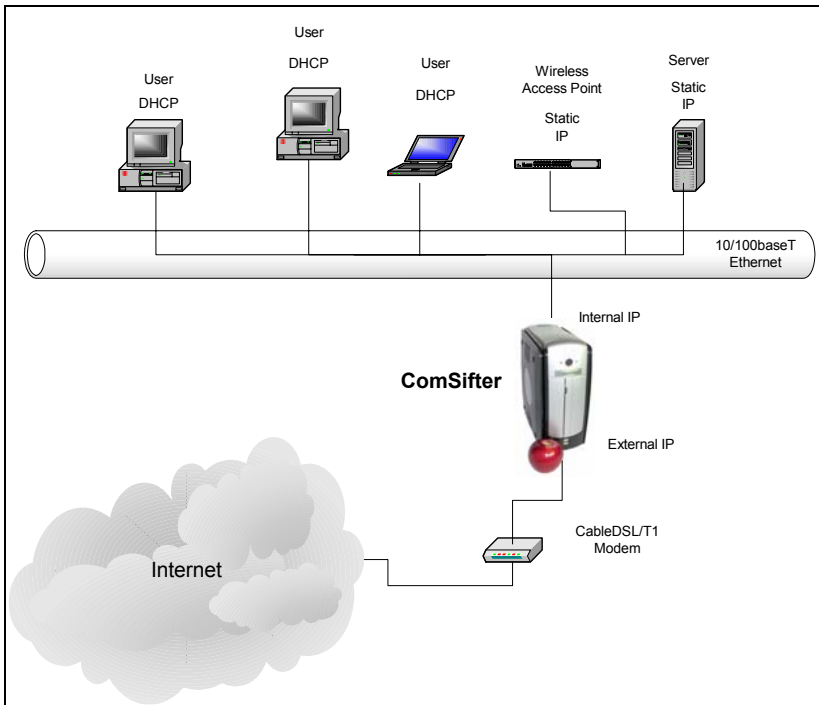


Figure 2-1: ComSifter in the Network

## 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 DSL, Cable or T1 modem connection. The location must be within the operating temperature range of ComSifter (10-35° C). 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 non-stop operation in the event of a momentary power outage.

### Network Connections

ComSifter requires two network connections. Connect the top Ethernet connector marked, “WAN”, to your DSL, Cable or T1 modem. Connect the bottom Ethernet connector, marked “LAN”, to your internal LAN switch or hub. Either Ethernet connector may use 10baseT or 100baseT.

### 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, 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](http://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.

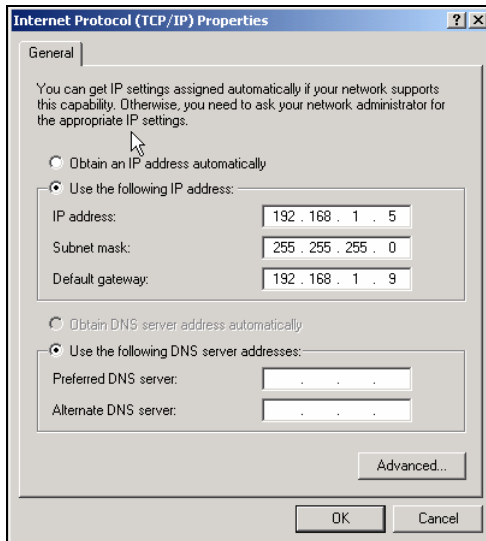
ComSifter is configured from the factory for the 192.168.1.1/255.255.255.0 subnet. If your network is already using this subnet then you are ready to configure ComSifter.

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

1. Right click My Network Places
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.

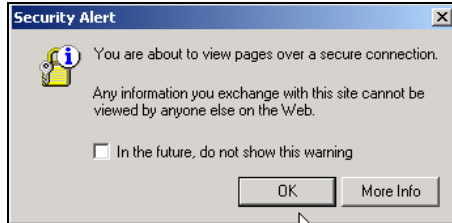


**Figure 2-2: Setting Windows2000/XP IP Address**

**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://192.168.1.1:10000> or the IP you have assigned to ComSifter. Upon a successful connection you will see:



**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.



**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.



**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 three modules and is covered in this Installation Guide.
- 
 Network – this category includes six modules and is covered in this Installation Guide.
- 
 Maintenance – this category includes eleven modules and is covered in this Installation Guide.
- 
 Filter Setup – this category includes ten modules and is covered in the Operators Guide.
- 
 Words/Phrases - this category includes fourteen modules and is covered in the Operators Guide.
- 
 Users - this category includes four modules and is covered in the Operators Guide.

## Security Configuration

### Login

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



**Figure 3-1: ComSifter Login**

The default Username is: admin

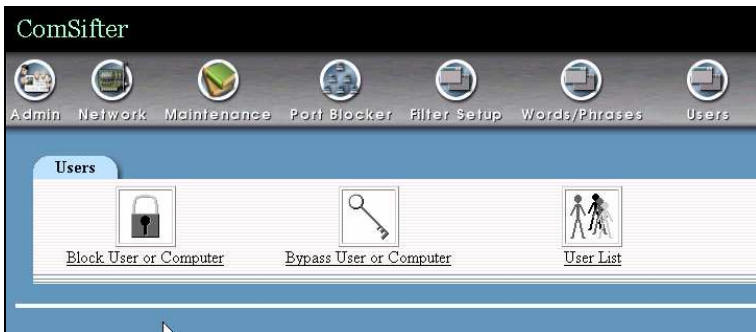
The default Password is: admin

**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.



**Figure 3-2: Select Admin**

After 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

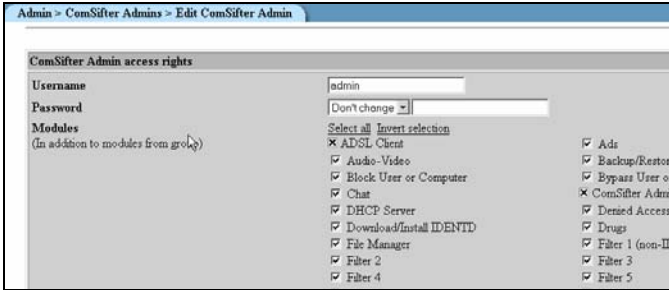
ComSifter Admins are personal that will be configuring ComSifter. Ten ComSifter Admins have been pre-defined. A special ComSifter Admin, “Admin”, is designated as the System Administrator. Admin may edit the username and password of other ComSifter Admins and assign responsibilities to them by assigning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



Figure 3-4: ComSifter Admin Screen

## Setting the Username and Password

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



**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.

## Assigning Module Rights

As Admin you may define new ComSifter Admins and grant them access to all or selected modules. In the following example username Admin1 was changed to “operator”. “operator” is given rights to access modules that allow computers to be blocked or bypassed and to administer the User List.

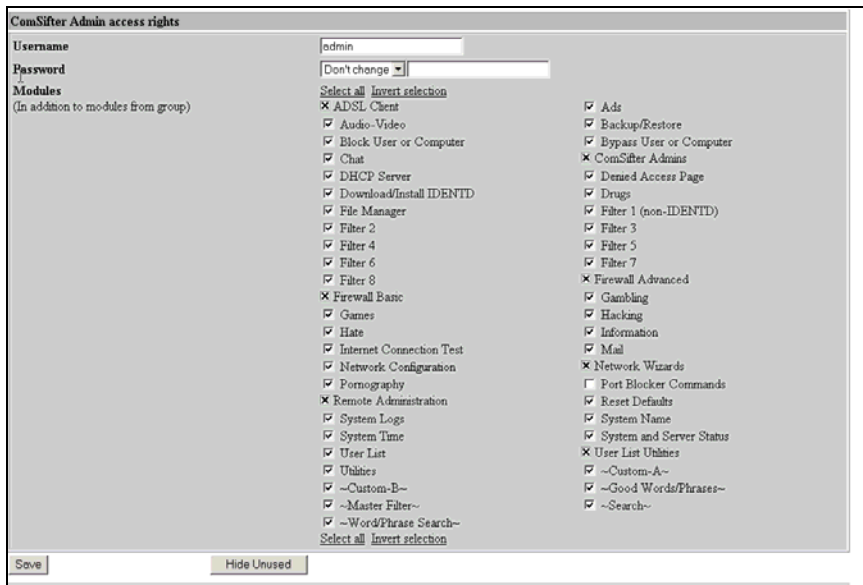


Figure 3-6: Assigning Module Rights

When “operator” logs into ComSifter they will only see the Modules and Categories that they have been granted rights to as shown in the example below.

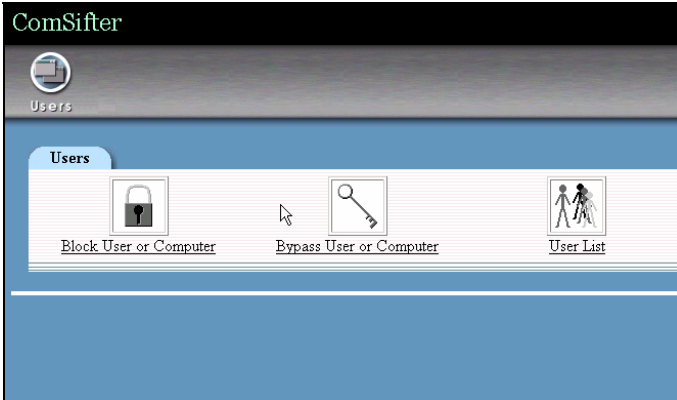


Figure 3-7: Operator Screen

In the next example username Admin2 was changed to “network\_technician”. “network\_technician” is allowed access to the DHCP and Network Configuration Modules.

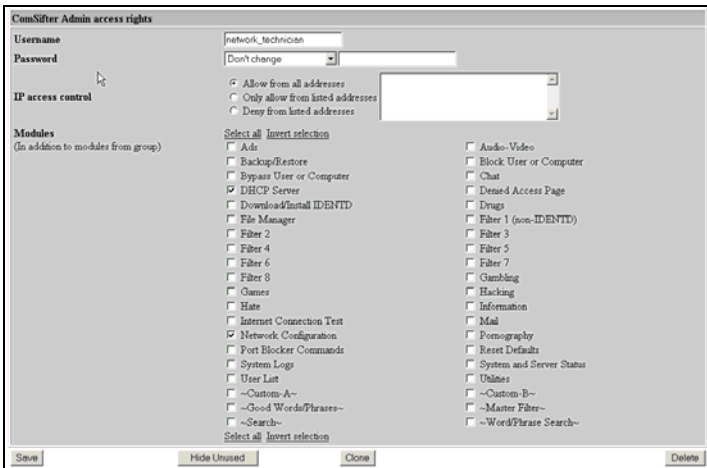


Figure 3-8: Assign Module Rights

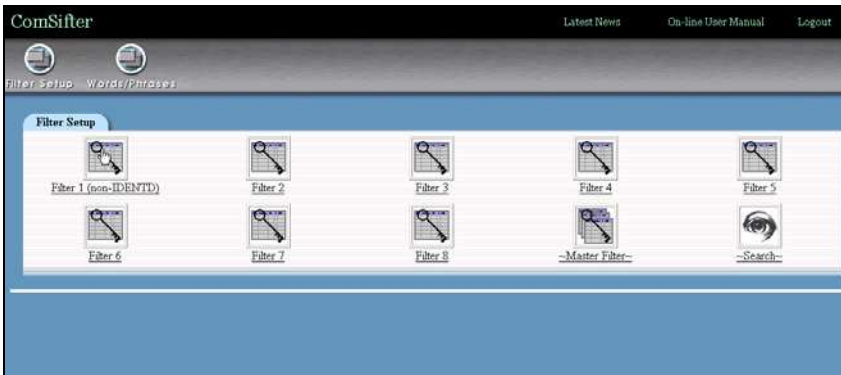
When network\_technician logs into ComSifter they will only see the Modules and Categories that they have been granted rights to as shown in the example below.



**Figure 3-9: Network Technician Screen**

In the final example a ComSifter Admin with the username `filter_specialist` is defined. This admin is allowed only in to the Filter Setup and Words/Phrases Modules.

When `filter_specialist` logs into ComSifter they will only see the Modules and Categories that they have been granted rights to as shown in the example below.



**Figure 3-10: Filter Specialist Screen**

## Remote Administration

ComSifter supports remote administration over the Internet using an encrypted SSL link to port 10000. Additional security is attained by limiting Remote Administration by IP.

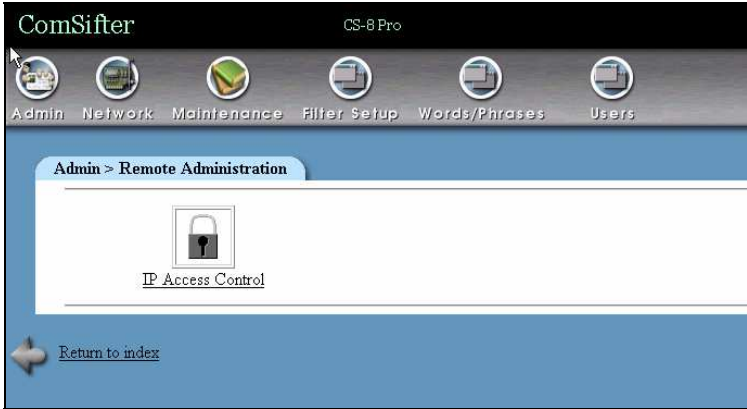


Figure 3-11: Remote Administration

## IP Access Control

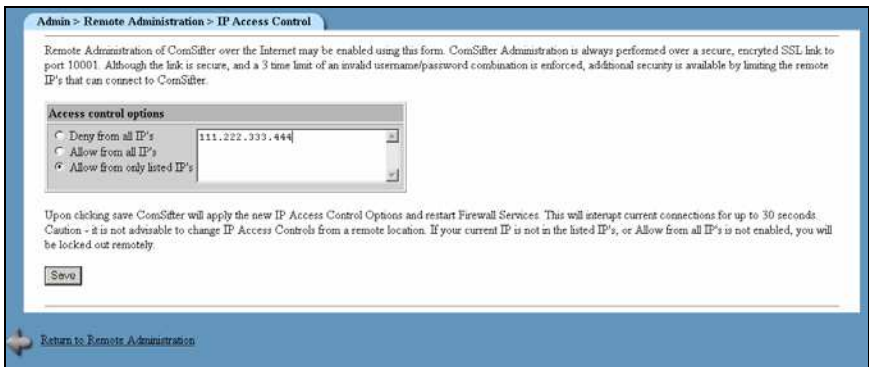


Figure 3-12: IP Access Control

### **Deny from all IP's**

Enabling **Deny all IP's** will disable the Remote Administration function. This is the default setting.

### **Allow from all IP's**

Enabling **Allow from all IP's** will allow any IP from the Internet to connect to Port 10000.

<p><b>Warning:</b> Although further authentication is required before access to the ComSifter is granted, this setting is not advisable due to potential security risks. In the event of a username/password breach the ComSifter would be accessible. Use this setting only if the ComSifter is inside of a trusted LAN or for testing purposes.</p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### **Allow from only listed IP's**

Enable this setting to limit Remote Administration to the listed IP's. This is the preferred setting for Remote Administration and offers excellent security. To gain access remotely the following conditions must be met.

1. The access must be from the listed IP.
2. The access must be to port 10000.
3. SSL must be supported.
4. The security certificate must be accepted.
5. A proper username/password must be entered.

## System Logs

ComSifter records four types of events in its log files. These are:

- Access Log, records all accesses to the Internet that have been processed by the Content Filter.
- Firewall Log, records any access through the firewall.
- Top Sites Visited.
- Security Log, records any login, or attempted login, into ComSifter.



Figure 3-13: System Logs

**Note:** ComSifter keeps the last seven days of data in its logs.



## Access Log

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

- Date and time the event happened.
- Username of the user making the request.
- IP of the computer making the request.
- The result of the request
- The Domain/URL address requested.

## Result Messages

Possible Result 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 192.168.1.35;

- 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 768.

Date	User	User IP	Status	Domain/URL
2005.7.19 10:16:24	charlie	192.168.1.35	*DENIED* Weighted phrase limit of 150 768 (amateur, pom)+(amateur, tits)+(amateur, xxx)+(blonde, pom)+(blonde, xxx)*(naked, xxx)*(pom, xxx)*(teen, pom)*(tinal membership, pom)+(xxx, pom)+(xxx, sex)+naked+breast+boob+boobs+hard core+ pom+busty+amateur+oral sex+ sex+online dating+dating site+membership+xxx +xxx movie+ nude +sexy)	http://www.google.com/search?hl=en&q=naked+breasts
2005.7.19 10:16:16	charlie	192.168.1.35	*OK*	http://www.google.com/intl/en/images/logo.gif
2005.7.19 10:16:15	charlie	192.168.1.35	*OK*	http://www.google.com/
2005.7.19 10:16:02	charlie	192.168.1.35	*DENIED* Banned Domain: casino.com	http://casino.com/
2005.7.19 10:15:53	charlie	192.168.1.35	*EXCEPTION* Exception domain match.	http://download.windowsupdate.com/msdownload/update/c3-19990512/cabpool/E6.0sp1-KB883932-Windows-2000-XP-x86-ENU_00202544ccca5197642f7cab0053ad.ezx
2005.7.19 10:15:48	charlie	192.168.1.35	*EXCEPTION* Exception domain match.	http://comsift.com/images/bg_link.gif
2005.7.19 10:15:47	charlie	192.168.1.35	*EXCEPTION* Exception domain match.	http://comsift.com/derived/productintro.htm_cmp_globalcom_flash010_vbtn.gif

Figure 3-14: Access Log

## Firewall

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

Admin > System Logs > Firewall Log

Last  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=39382	DPT=1027
Jul 19 10:24:39	net2fw-DROP	SRC=70.85.177.66	DST=63.195.80.8	PROTO=UDP	SPT=39382	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=3351
Jul 19 10:23:23	net2fw-DROP	SRC=24.50.61.69	DST=63.195.80.8	PROTO=TCP	SPT=4261	DPT=3351
Jul 19 10:23:17	net2fw-DROP	SRC=24.50.61.69	DST=63.195.80.8	PROTO=TCP	SPT=4262	DPT=3351
Jul 19 10:23:17	net2fw-DROP	SRC=24.50.61.69	DST=63.195.80.8	PROTO=TCP	SPT=4261	DPT=3351
Jul 19 10:23:14	net2fw-DROP	SRC=24.50.61.69	DST=63.195.80.8	PROTO=TCP	SPT=4262	DPT=3351
Jul 19 10:23:14	net2fw-DROP	SRC=24.50.61.69	DST=63.195.80.8	PROTO=TCP	SPT=4261	DPT=3351
Jul 19 10:23:02	net2fw-DROP	SRC=24.50.61.69	DST=63.195.80.8	PROTO=TCP	SPT=4254	DPT=3351
Jul 19 10:23:02	net2fw-DROP	SRC=24.50.61.69	DST=63.195.80.8	PROTO=TCP	SPT=4253	DPT=3351
Jul 19 10:22:56	net2fw-DROP	SRC=24.50.61.69	DST=63.195.80.8	PROTO=TCP	SPT=4254	DPT=3351
Jul 19 10:22:56	net2fw-DROP	SRC=24.50.61.69	DST=63.195.80.8	PROTO=TCP	SPT=4253	DPT=3351
Jul 19 10:22:53	net2fw-DROP	SRC=24.50.61.69	DST=63.195.80.8	PROTO=TCP	SPT=4254	DPT=3351
Jul 19 10:22:53	net2fw-DROP	SRC=24.50.61.69	DST=63.195.80.8	PROTO=TCP	SPT=4253	DPT=3351
Jul 19 10:22:41	net2fw-DROP	SRC=24.50.61.69	DST=63.195.80.8	PROTO=UDP	SPT=3351	DPT=3351
Jul 19 10:22:41	net2fw-DROP	SRC=24.50.61.69	DST=63.195.80.8	PROTO=UDP	SPT=3351	DPT=3351
Jul 19 10:22:41	net2fw-DROP	SRC=24.50.61.69	DST=63.195.80.8	PROTO=TCP	SPT=4245	DPT=3351
Jul 19 10:22:41	net2fw-DROP	SRC=24.50.61.69	DST=63.195.80.8	PROTO=TCP	SPT=4244	DPT=3351
Jul 19 10:22:35	net2fw-DROP	SRC=24.50.61.69	DST=63.195.80.8	PROTO=TCP	SPT=4245	DPT=3351

Figure 3-15: Firewall Log

The Firewall Log shows the following:

1. Date/Time - the Date/Time the event happened.
2. Chain:Action – shows the Chain (direction) of the event and what action was taken.

Possible chains are;

- a. 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
- b. loc2net – the packet was traversing from the internal LAN to the Internet.

- c. fw2lan – the packet was traversing from the ComSifter to the LAN
- d. fw2net – the packet was traversing from the ComSifter to the Internet
- e. net2fw – the packet was traversing from the Internet to the ComSifter.
- f. net2lan – the packet was traversing from the Internet to the LAN.

Possible Actions are;

- a. Accept – a firewall rule was matched and the packet was accepted.
  - b. Drop – a firewall rule was not found or an explicit rule to drop the packet was found. The packet is silently dropped.
  - c. `_redirect` and `_dnat` – a matching rule was found to DNAT or Redirect the packet.
- 3. Source IP – The IP the packet originated from.
  - 4. Destination IP – The IP the packet is destined for.
  - 5. Protocol – The protocol the packet is using.
  - 6. Sport – the port the packet originated from.
  - 7. DPort – the port the packet is destined for.

## 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 in successfully at 7:48.
- Non-existent ComSifter Admin “filter\_specialist” tried to login 5 times and was locked out on the fifth try.
- At 14:13 ComSifter Admin “admin” tried to log in but forgot their password.

The screenshot shows a web interface for viewing security logs. At the top, there is a breadcrumb trail: "Admin > System Logs > Security Log". Below this, there is a search and display control area: "Last 20 lines (10,000 max) of Security Log with text" followed by an input field and a "Refresh" button. The main content is a table with two columns: "Date/Time" and "Action".

Date/Time	Action
Nov 12 07:48:59	Successful login as admin from 192.168.1.230
Nov 12 07:28:30	Non-existent login as filter_specialist from 192.168.1.230
Nov 12 07:28:26	Security alert: Host 192.168.1.230 blocked after 5 failed logins for
Nov 12 07:28:21	Non-existent login as filter_specialist from 192.168.1.230
Nov 12 07:28:14	Non-existent login as filter_specialist from 192.168.1.230
Nov 12 07:28:07	Non-existent login as filter_specialist from 192.168.1.230
Nov 12 07:28:01	Non-existent login as filter_specialist from 192.168.1.230
Nov 12 07:27:46	Logout by admin from 192.168.1.230
Nov 12 07:27:04	Successful login as admin from 192.168.1.230
Nov 12 07:26:56	Non-existent login as bill from 192.168.1.230
Nov 12 07:26:40	Logout by admin from 192.168.1.230
Nov 12 07:25:15	Successful login as admin from 192.168.1.230
Nov 12 07:10:57	Timeout of admin
Nov 12 07:00:21	Successful login as admin from 192.168.1.230
Nov 11 14:32:04	Logout by admin from 192.168.1.230
Nov 11 14:30:06	Successful login as admin from 192.168.1.230
Nov 11 14:24:38	Timeout of admin
Nov 11 14:13:12	Successful login as admin from 192.168.1.230
Nov 11 14:13:06	Invalid login as admin from 192.168.1.230
Nov 11 11:35:06	Timeout of admin

Figure 3-16: Security Log

## Top Sites Log

The screenshot shows a web interface with a blue header bar containing the breadcrumb "Admin > System Logs > Top Sites Log". Below the header, a text line reads "Top Sites from 09-28-2005 until 10-04-2005 based on 31074 connects." Below this is a table with three columns: Rank, Connects, and Domain. The table lists 11 domains, with the first being comsift.com and the last being yahoo.com.

Rank	Connects	Domain
1	3998	<a href="http://comsift.com">comsift.com</a>
2	2266	<a href="http://msn.com">msn.com</a>
3	1587	<a href="http://amazon.com">amazon.com</a>
4	1459	<a href="http://walmart.com">walmart.com</a>
5	1387	<a href="http://rick.com">rick.com</a>
6	1171	<a href="http://neopets.com">neopets.com</a>
7	1125	<a href="http://cartoonnetwork.com">cartoonnetwork.com</a>
8	1088	<a href="http://cnn.net">cnn.net</a>
9	766	<a href="http://foothilladventistschool.com">foothilladventistschool.com</a>
10	733	<a href="http://yimg.com">yimg.com</a>
11	608	<a href="http://yahoo.com">yahoo.com</a>

Figure 3-17: Top Sites Log

Top Sites shows the most frequently visited domains. When this log is accessed ComSifter converts every entry in its Access Log 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.

**Warning:** Top Sites Log is created dynamically every time it is accessed. Depending on the number of log entries this report may take up to one minute to create.

## Network



**Figure 3-18: 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 login names and password for the account.

**DHCP Server** - allows configuration of ComSifters DHCP Server. This includes starting/stopping the server, DHCP scopes, Client DNS and Gateway settings.

**Firewall Advanced** – Configures, Checks, Starts/Stops, Backup, Restores the Firewall.

**Firewall Basic** – includes easy to use Templates to configure the Firewall.

**Network Configuration** – allows setting the ComSifters IP, Gateway and DNS settings.

**Network Wizards** – Include easy to use wizards that allow you to easily set up a Static, DHCP or PPPOE Internet connection.

**Note:** It is suggested that you start with the Network Wizards. The Wizard can configure your ComSifter to your Internet Connection type, set a basic Firewall configuration, set up your internal LAN and optionally enable the DHCP Server.

## ADSL Client

**Network > ADSL Client**

The settings below apply to any new ADSL connection started by your system. If you change them, the connection must be shut down and re-started for the new settings to take effect.

**ADSL client configuration options**

<b>Ethernet interface</b>	eth0 <input type="text"/>	<b>Connect on demand?</b>	<input type="radio"/> Yes, seconds before timeout: <input type="text"/> <input checked="" type="radio"/> No
<b>Login as user</b>	comsif1213@sbcglobe	<b>Login with password</b>	<input type="password"/>
<b>Get DNS from ISP?</b>	<input type="radio"/> Yes <input checked="" type="radio"/> No	<b>Attempt connection for</b>	<input type="radio"/> Forever <input checked="" type="radio"/> 90 seconds
<b>Limit packet size?</b>	<input checked="" type="radio"/> Yes, to 1412 bytes <input type="radio"/> No		

Your ADSL connection is currently inactive. Click this button to start it up with the command `ads1-start`.

Yes  No Change this option to control whether your ADSL connection is brought up at boot time or not.

[Return to index](#)

**Figure 3-19: ADSL Client**



## DHCP Configuration

ComSifter can operate with an existing DHCP server or with its own built-in DHCP server.

### Using an existing DHCP Server

If using an existing DHCP Server the following items must be configured:

1. Ensure that the ComSifter DHCP Server is not started.
2. Ensure that your existing DHCP server points client computers to the ComSifter IP (Internet Gateway)

### Using the ComSifter DHCP Server

ComSifter has a built in DHCP server. It is factory configured but not activated when shipped. If you use the ComSifter DHCP server you will need to modify the existing factory configuration to meet your network parameters, save the configuration and Start the DHCP server

### Factory Configuration

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

## Setting up the Subnet

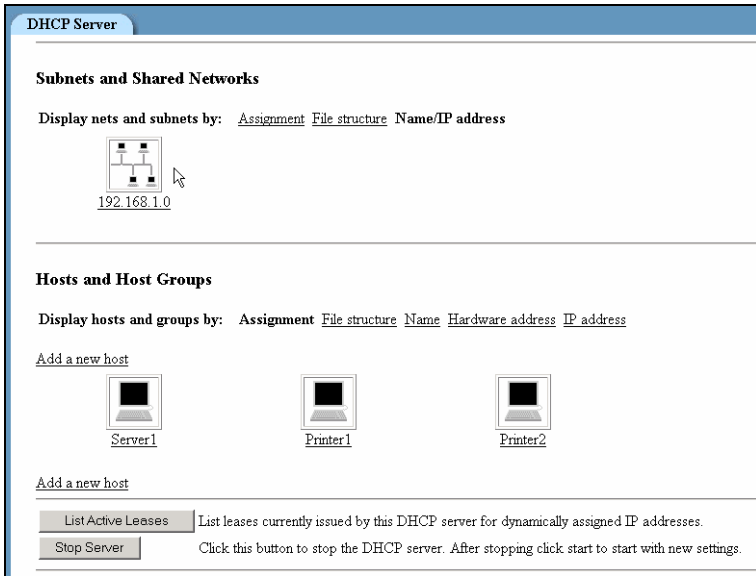


Figure 3-20: Selecting Network

Click on the Subnets IP address as shown above to expose the DHCP subnet settings.

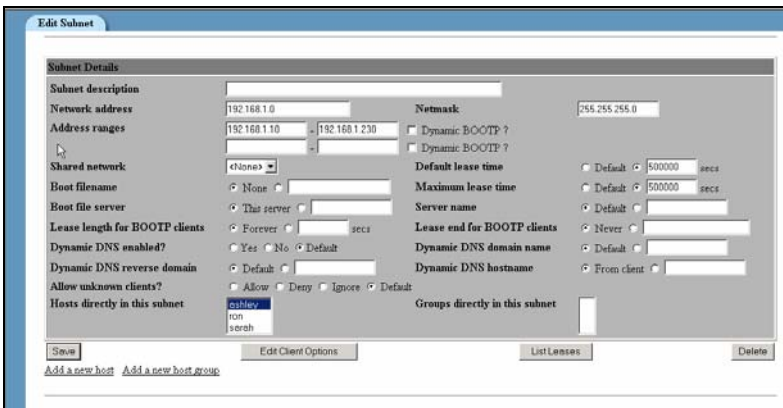


Figure 3-21: Setting the DHCP Subnet

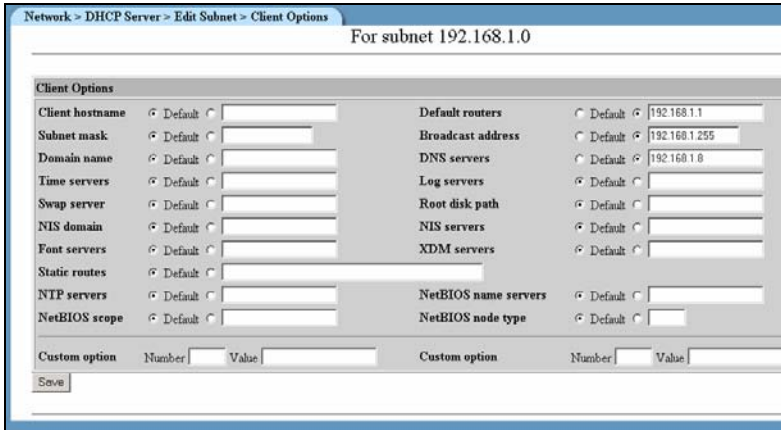
The above example shows the factory defaults for setting the DHCP Subnet. If your network uses a different subnet then replace the values shown with your network's settings.

1. Network Address – enter the network address. This should end in a 0, i.e. xxx.xxx.xxx.0.
2. Address Range – this is the range of IPs that will be available for lease to client computers.
3. Netmask – the netmask of the Network Address defined in step 1.
4. Default Lease Time – the default amount of time the lease will be active, in seconds.
5. Maximum Lease Time - the maximum amount of time the lease will be active, in seconds.
6. Edit Client Options – see next section, **Edit Client Options**.
7. List Leases – list current and expired leases.
8. Add A New Host – see section **Add a New Host**.

<b>Note:</b> 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.

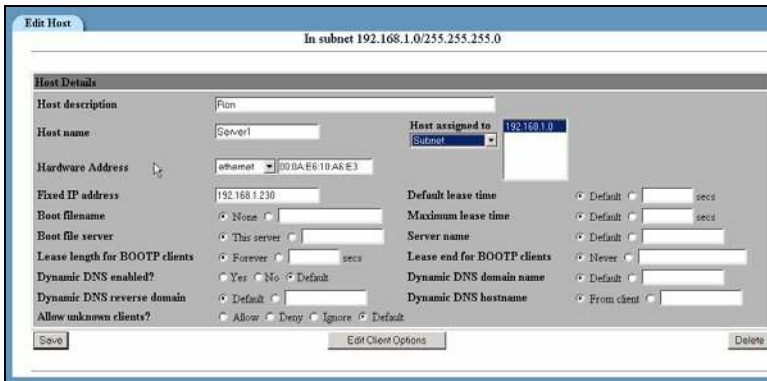


**Figure 3-22: Entering Client DHCP Option**

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 ComSifter and may be left blank (default).

## Add a New Host



**Figure 3-23: 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).

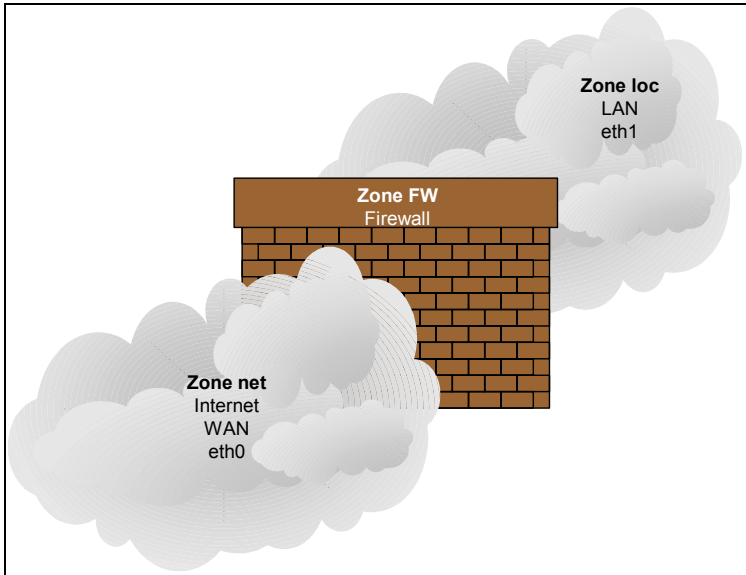
The ADD Host feature may appear to be the proper solution for defining fixed IP devices on a network but best practices would suggest otherwise. Since the IP is based on the client device MAC address, if the client computer is changed, thus changing the MAC address, then the settings above would have 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 the server must be started. Click on **Start Server**, as shown in Fig. 3-12, to accomplish this task.

## Firewall Advanced



**Figure 3-24: Firewall Zones**

### Overview

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

Loc - is connected to the Ethernet interface eth1 and connects to your internal LAN (Local Area Network).

Net - is connected to Ethernet interface eth0, and connects to your external WAN (Wide Area Network).

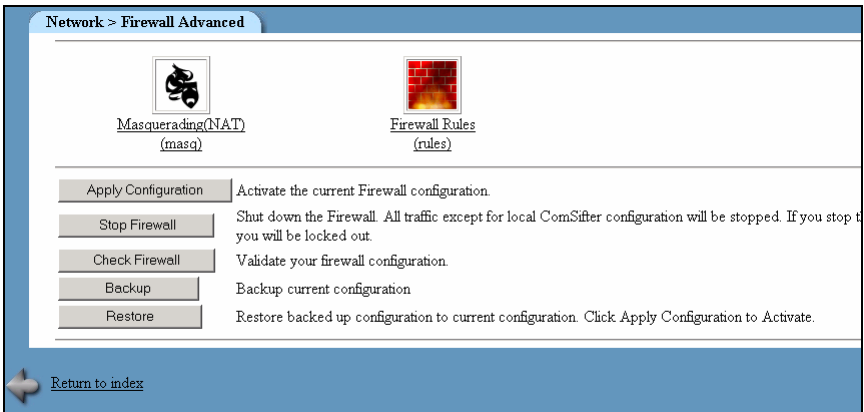
FW - is the firewall itself.

The firewall's 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 Firewall Advanced screen. From this menu you will be able to:

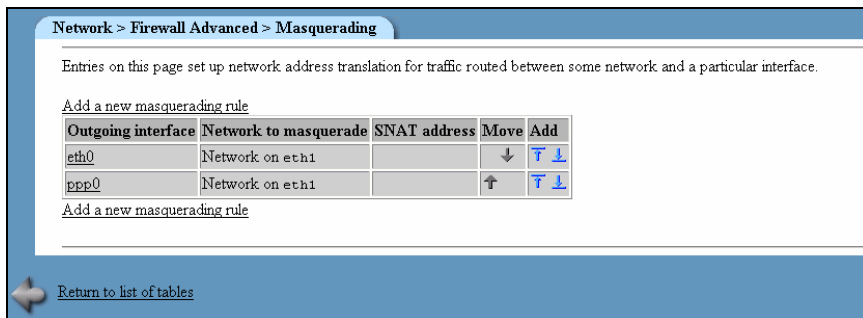
- Enable/disable Masquerading (NAT).
- Create Firewall rules.
- Apply the Firewall Configuration.
- Stop the Firewall.
- Check a new Firewall configuration.
- Backup the existing Firewall.
- Restore a previously backed up configuration.



**Figure 3-25: Firewall Advanced**



## Masquerading (SNAT)



**Figure 3-26: 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.

## Firewall Rules

Firewall 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 Firewall will be examined in order by the Firewall 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 > Firewall Advanced > Firewall Rules

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

[Add a new firewall rule](#)

Action	Source	Destination	Protocol	Source ports	Destination ports	Move	Add
<a href="#">REDIRECT</a>	Zone 10c	Port 8080	TCP	Any	80	↓	<a href="#">T</a> <a href="#">↓</a>
<a href="#">DNAT</a>	Zone net	Host 192.168.1.8 in zone 10c	TCP	Any	80	↑ ↓	<a href="#">T</a> <a href="#">↓</a>
<a href="#">ACCEPT</a>	Zone 10c	Zone net	Any			↑ ↓	<a href="#">T</a> <a href="#">↓</a>
<a href="#">DNAT</a>	Zone net	Host 192.168.1.8:1723 in zone 10c	TCP	Any	1723	↑ ↓	<a href="#">T</a> <a href="#">↓</a>
<a href="#">DNAT</a>	Zone net	Host 192.168.1.8 in zone 10c	47	Any		↑ ↓	<a href="#">T</a> <a href="#">↓</a>
<a href="#">ACCEPT</a>	Zone net	Firewall	ICMP	Any		↑	<a href="#">T</a> <a href="#">↓</a>

[Add a new firewall rule](#)

[Return to list of tables](#)

Figure 3-27: Firewall Rules

ComSifter includes templates located in Basic Firewall 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 firewall to be answered.

## Create Firewall Rules

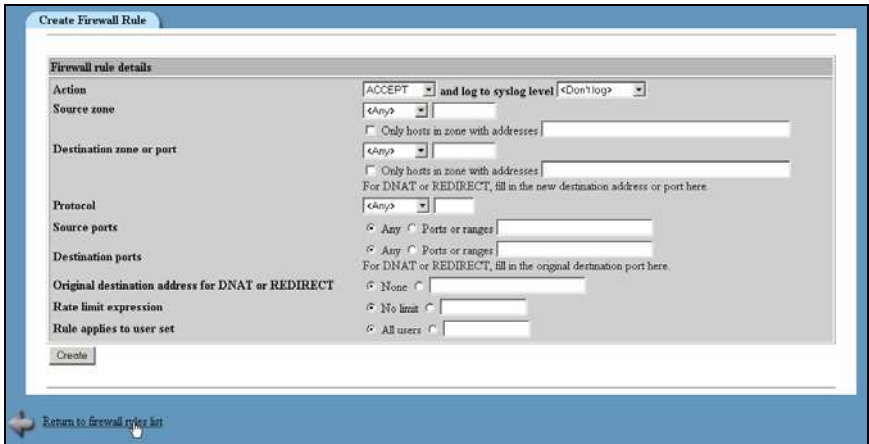


Figure 3-28: Create Firewall Rule

### 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 Firewall 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 firewall 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.

<p><b>Note:</b> 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 firewall will overload the ComSifter, thus denying legitimate traffic.</p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### 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 1<sup>st</sup> 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 1<sup>st</sup> 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 firewall 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
	<input type="checkbox"/> Only hosts in zone with addresses
Destination zone or port	net
	<input type="checkbox"/> Only hosts in zone with addresses
	For DNAT or REDIRECT, fill in the new destination address or port here
Protocol	TCP
Source ports	<input checked="" type="radio"/> Any <input type="radio"/> Ports or ranges
Destination ports	<input type="radio"/> Any <input checked="" type="radio"/> Ports or ranges 53
	For DNAT or REDIRECT, fill in the original destination port here.
Original destination address for DNAT or REDIRECT	<input checked="" type="radio"/> None <input type="radio"/>

Figure 3-29: Client Access to DNS (TCP)

Firewall rule details	
Action	ACCEPT and log to syslog level <Don't log>
Source zone	loc
	<input type="checkbox"/> Only hosts in zone with addresses
Destination zone or port	net
	<input type="checkbox"/> Only hosts in zone with addresses
	For DNAT or REDIRECT, fill in the new destination address or port here
Protocol	UDP
Source ports	<input checked="" type="radio"/> Any <input type="radio"/> Ports or ranges
Destination ports	<input type="radio"/> Any <input checked="" type="radio"/> Ports or ranges 53
	For DNAT or REDIRECT, fill in the original destination port here.
Original destination address for DNAT or REDIRECT	<input checked="" type="radio"/> None <input type="radio"/>

Figure 3-30: 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
Destination zone or port	net
Protocol	TCP
Source ports	Any Ports or ranges
Destination ports	Any Ports or ranges 25 465 110 995 143 993
Original destination address for DNAT or REDIRECT	None

Figure 3-31: 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
Destination zone or port	loc
Protocol	TCP
Source ports	Any Ports or ranges
Destination ports	Any Ports or ranges 110
Original destination address for DNAT or REDIRECT	None

Figure 3-32: 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
Destination zone or port	net
Protocol	TCP
Source ports	Any
Destination ports	Ports or ranges 21
Original destination address for DNAT or REDIRECT	None

**Figure 3-33: 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
Destination zone or port	loc
Protocol	TCP
Source ports	Any
Destination ports	Ports or ranges 21
Original destination address for DNAT or REDIRECT	None

**Figure 3-34: 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
	<input type="checkbox"/> Only hosts in zone with addresses
Destination zone or port	net
	<input type="checkbox"/> Only hosts in zone with addresses
	For DNAT or REDIRECT, fill in the new destination address or port
Protocol	TCP
Source ports	<input checked="" type="radio"/> Any <input type="radio"/> Ports or ranges
Destination ports	<input type="radio"/> Any <input checked="" type="radio"/> Ports or ranges 5190
	For DNAT or REDIRECT, fill in the original destination port here.
Original destination address for DNAT or REDIRECT	<input checked="" type="radio"/> None <input type="radio"/>

**Figure 3-35: 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
Destination zone or port	net
Protocol	TCP
Source ports	Any
Destination ports	Ports or ranges 1547 389 1024 1183:1184
Original destination address for DNAT or REDIRECT	None

**Figure 3-36: 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
Destination zone or port	loc
Protocol	TCP
Source ports	Any
Destination ports	Ports or ranges 1547
Original destination address for DNAT or REDIRECT	None
Rate limit expression	No limit
Rule applies to user set	All users

**Figure 3-37: 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
Destination zone or port	net
Protocol	TCP
Source ports	Any Ports or ranges
Destination ports	Any Ports or ranges 1863 5190 6891:6901
Original destination address for DNAT or REDIRECT	None

Figure 3-38: 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 <input type="checkbox"/> Only hosts in zone with addresses
Destination zone or port	net <input type="checkbox"/> Only hosts in zone with addresses
Protocol	UDP
Source ports	<input checked="" type="radio"/> Any <input type="radio"/> Ports or ranges
Destination ports	<input type="radio"/> Any <input checked="" type="radio"/> Ports or ranges 123 For DNAT or REDIRECT, fill in the original destination port here.
Original destination address for DNAT or REDIRECT	<input checked="" type="radio"/> None <input type="radio"/>

**Figure 3-39: 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
Destination zone or port	net
Protocol	TCP
Source ports	Any
Destination ports	Ports or ranges 5631 5632
Original destination address for DNAT or REDIRECT	None

Figure 3-40: 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
Destination zone or port	loc
Protocol	TCP
Source ports	Any
Destination ports	Ports or ranges 5631 5632
Original destination address for DNAT or REDIRECT	None

Figure 3-41: 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 firewall. 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 Firewall 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
	<input type="checkbox"/> Only hosts in zone with addresses
Destination zone or port	<Firewall>
	<input type="checkbox"/> Only hosts in zone with addresses
	For DNAT or REDIRECT, fill in the new destination address or port
Protocol	ICMP
Source ports	<input checked="" type="radio"/> Any <input type="radio"/> Ports or ranges
Destination ports	<input type="radio"/> Any <input checked="" type="radio"/> Ports or ranges 8
	For DNAT or REDIRECT, fill in the original destination port here
Original destination address for DNAT or REDIRECT	<input checked="" type="radio"/> None <input type="radio"/>

Figure 3-42: 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
	<input type="checkbox"/> Only hosts in zone with addresses
Destination zone or port	net
	<input type="checkbox"/> Only hosts in zone with addresses
	For DNAT or REDIRECT, fill in the new destination address or port
Protocol	ICMP
Source ports	<input checked="" type="radio"/> Any <input type="radio"/> Ports or ranges
Destination ports	<input type="radio"/> Any <input checked="" type="radio"/> Ports or ranges 8
	For DNAT or REDIRECT, fill in the original destination port here
Original destination address for DNAT or REDIRECT	<input checked="" type="radio"/> None <input type="radio"/>

Figure 3-43: 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
Destination zone or port	loc
Protocol	TCP
Source ports	Any
Destination ports	Ports or ranges 1723
Original destination address for DNAT or REDIRECT	None

*Note: In the original image, the 'Destination zone or port' section is expanded to show 'Only hosts in zone with addresses' checked and '192.168.1.8' entered. The 'Destination ports' section also shows 'For DNAT or REDIRECT, fill in the original destination port here.' text.*

Figure 3-44: 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
Destination zone or port	loc
Protocol	Other.. 47
Source ports	Any
Destination ports	Any
Original destination address for DNAT or REDIRECT	None

*Note: In the original image, the 'Destination zone or port' section is expanded to show 'Only hosts in zone with addresses' checked and '192.168.1.8' entered. The 'Destination ports' section also shows 'For DNAT or REDIRECT, fill in the original destination port here.' text.*

Figure 3-45: 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 <input type="checkbox"/> Only hosts in zone with addresses
Destination zone or port	loc <input checked="" type="checkbox"/> Only hosts in zone with addresses 192.168.1.8:1723 For DNAT or REDIRECT, fill in the new destination address or port here.
Protocol	TCP
Source ports	<input checked="" type="radio"/> Any <input type="radio"/> Ports or ranges
Destination ports	<input type="radio"/> Any <input checked="" type="radio"/> Ports or ranges 1723 For DNAT or REDIRECT, fill in the original destination port here.
Original destination address for DNAT or REDIRECT	<input checked="" type="radio"/> None <input type="radio"/>

**Figure 3-46: 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
	<input type="checkbox"/> Only hosts in zone with addresses
Destination zone or port	net
	<input type="checkbox"/> Only hosts in zone with addresses
Protocol	TCP
Source ports	<input checked="" type="radio"/> Any <input type="radio"/> Ports or ranges
Destination ports	<input type="radio"/> Any <input checked="" type="radio"/> Ports or ranges 23
Original destination address for DNAT or REDIRECT	<input checked="" type="radio"/> None <input type="radio"/>

**Figure 3-47: 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
	<input type="checkbox"/> Only hosts in zone with addresses
Destination zone or port	loc
	<input checked="" type="checkbox"/> Only hosts in zone with addresses 192.168.1.8
Protocol	TCP
Source ports	<input checked="" type="radio"/> Any <input type="radio"/> Ports or ranges
Destination ports	<input type="radio"/> Any <input checked="" type="radio"/> Ports or ranges 23
Original destination address for DNAT or REDIRECT	<input checked="" type="radio"/> None <input type="radio"/>

**Figure 3-48: Access to Telnet Server**

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

Vonage™

## 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
Destination zone or port	net
Protocol	TCP
Source ports	Any
Destination ports	5900:5910
Original destination address for DNAT or REDIRECT	None

Figure 3-49: 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
Destination zone or port	loc
Protocol	TCP
Source ports	Any
Destination ports	5500
Original destination address for DNAT or REDIRECT	None

Figure 3-50: 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
Destination zone or port	net
Protocol	TCP
Source ports	Any Ports or ranges
Destination ports	Any Ports or ranges 5000:5010 5055 5100
Original destination address for DNAT or REDIRECT	None

Figure 3-51: 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
Destination zone or port	Other... 8080
Protocol	TCP
Source ports	Any
Destination ports	Any Ports or ranges 80
Original destination address for DNAT or REDIRECT	None

**Figure 3-52: 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
Destination zone or port	net
Protocol	TCP
Source ports	Any
Destination ports	Any Ports or ranges 443
Original destination address for DNAT or REDIRECT	None

**Figure 3-53: 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 <input type="checkbox"/> and log to syslog level <Log to Firewall (ULOG)> <input type="checkbox"/>
Source zone	net <input type="text"/> <input type="text"/>
Destination zone or port	<input type="checkbox"/> Only hosts in zone with addresses <input type="text"/> loc <input type="text"/> <input type="text"/> <input checked="" type="checkbox"/> 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 <input type="text"/> <input type="text"/>
Source ports	<input checked="" type="radio"/> Any <input type="radio"/> Ports or ranges <input type="text"/> <input type="radio"/> Any <input checked="" type="radio"/> Ports or ranges 80 <input type="text"/> For DNAT or REDIRECT, fill in the original destination port here.
Destination ports	
Original destination address for DNAT or REDIRECT	<input checked="" type="radio"/> None <input type="radio"/> <input type="text"/>

**Figure 3-54: Web Server Access**

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

**Note:** If the Check Firewall fails you should manually run the **Check Firewall** 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 Firewall

The **Stop Firewall** command will immediately shutdown the firewall 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 Firewall

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

## Backup

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

## Restore

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

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

<b>Warning:</b> During Restore all Internet traffic is stopped. The Restore may take up to one minute to complete.
--------------------------------------------------------------------------------------------------------------------

## Firewall Basic (Templates)

To streamline installation of ComSifter five firewall templates are included. These templates may be used as they are or may be used as a starting point for further modification by Firewall 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).

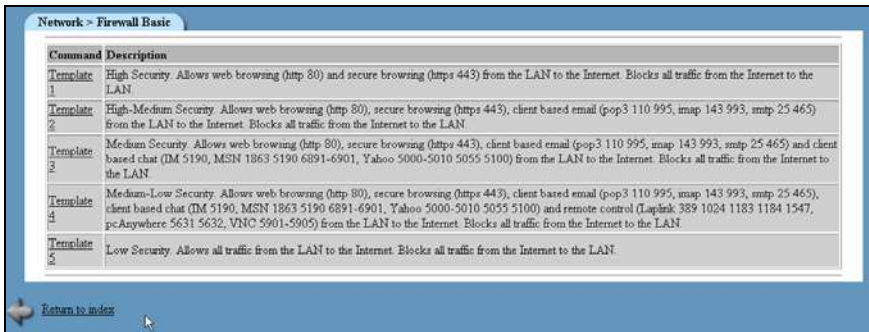


Figure 3-55: Firewall Basic

**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 Firewall Advanced.

Upon selecting a Template ComSifter will:

1. Stop Network, Filtering and Proxy Services
2. Load the Firewall Rules from the selected Template
3. Restart the Firewall 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 firewall found in home and small business routers from companies such Linksys, Netgear and SMC.

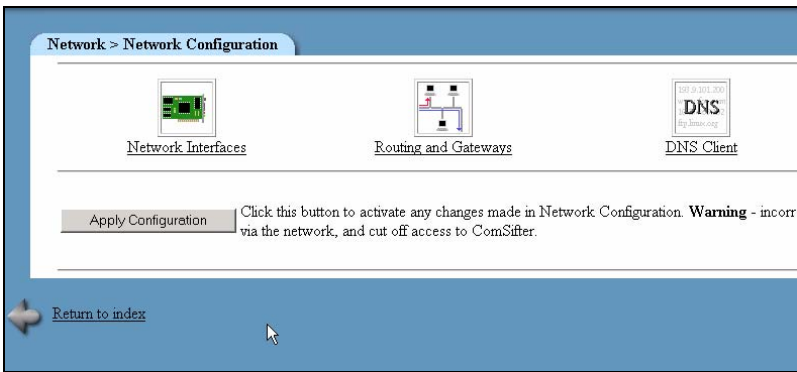
<p><b>Warning:</b> Although this setting may be the easiest to configure and maintain, it is the least secure. Any program originating on a LAN computer will be able to access the Internet without restriction.</p>
------------------------------------------------------------------------------------------------------------------------------------------------------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

## 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:



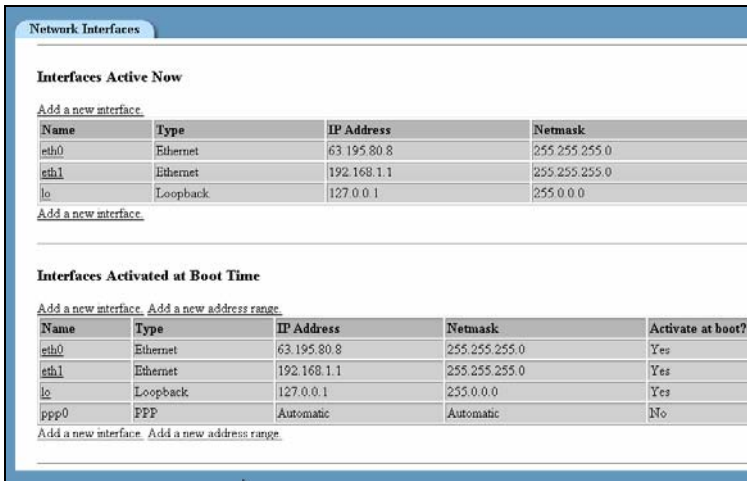
**Figure 3-56: Network Configuration Choices**

### Network Interfaces (IP Address Configuration)

ComSifter is configured with two Ethernet interfaces. Eth0 is connected to the WAN (cable, DSL, T1 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.



**Figure 3-57: 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

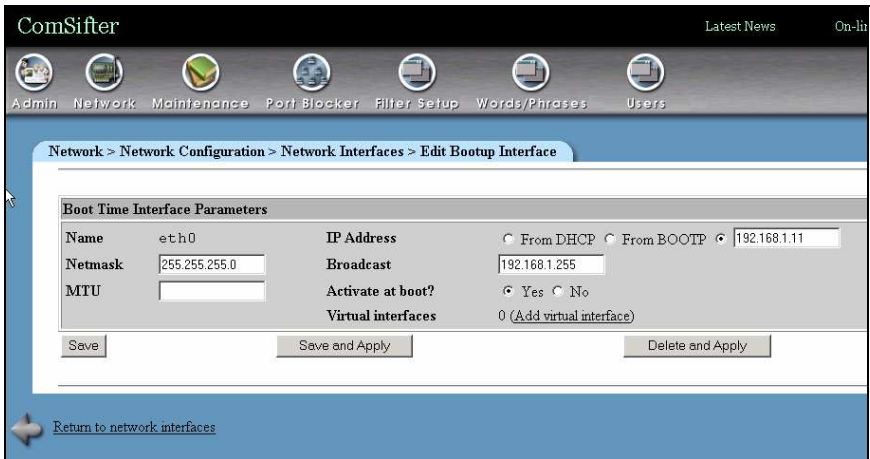
Normal configuration of ComSifter networking is done in this area. Any changes made here will be permanent

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](#).

### WAN Interface Settings (eth0)

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



**Figure 3-58: 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.

### LAN Interface Settings (eth1)

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 – Enter the Internal LAN address for ComSifter. This will also be the gateway for client computers accessing the Internet.
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.

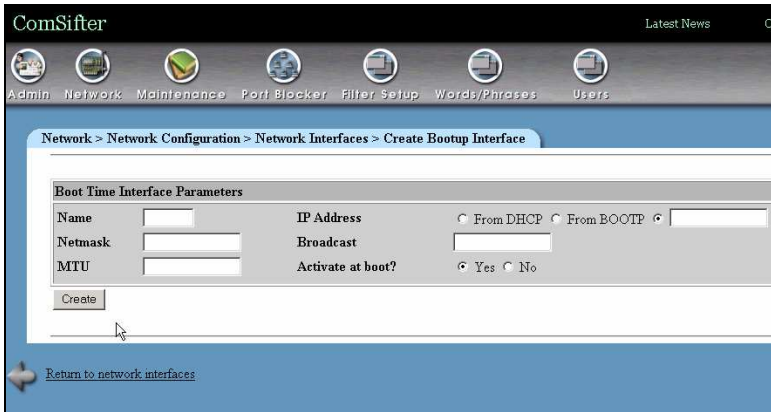
If your network is using only one network range (Class C) i.e. 192.168.1.xxx then click on Save and continue to **Routing and Gateways**.

### Virtual Interfaces

<p><b>Note:</b> 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.</p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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.

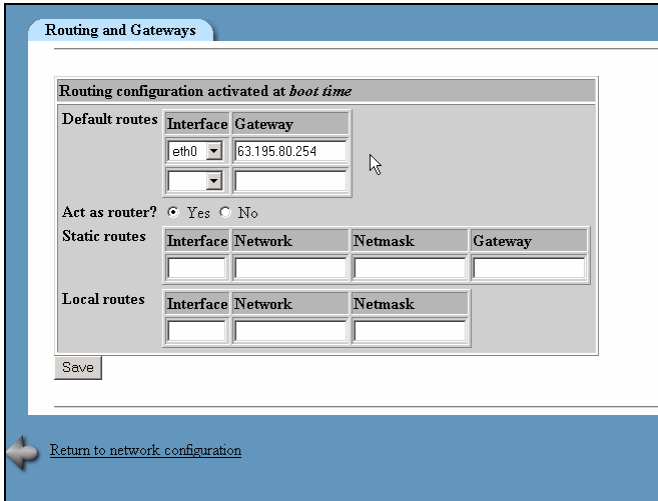


**Figure 3-59: Adding a Virtual Interface**

**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.

Continue to the next section, Routing and Gateways.

## Routing and Gateways



**Figure 3-60: Entering Gateway IP**

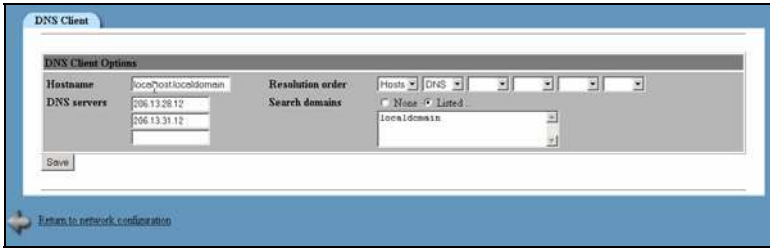
Enter the IP address of the External Gateway that ComSifter will use to access the Internet.

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

When completed click on **Save**.

Continue to the next section, DNS.

## DNS



**Figure 3-61: Entering DNS Settings**

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

Required Settings are:

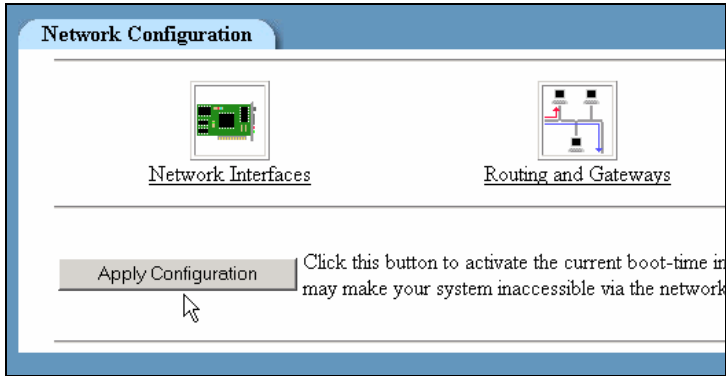
1. Hostname – must be localhost.
2. DNS servers - Enter the DNS server names that ComSifter will use to resolve Domain Names.
3. Resolution order – must be Hosts, DNS.
4. Search domains – must be Listed, localhost.

**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



**Figure 3-62: 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

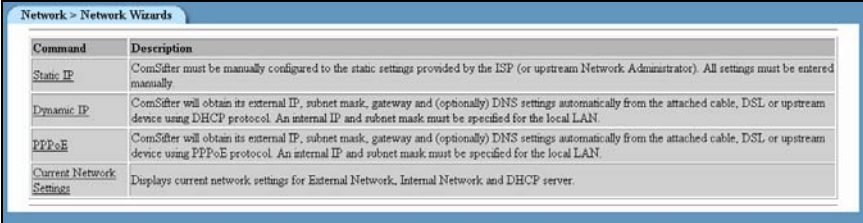
ComSifter includes a failsafe method to determine network settings in the event that the settings are forgotten or miss-configured.

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 Wizards

Network Wizards may be used to quickly configure your ComSifter. Depending on the Wizard selected the following parameters will be set:

- A Static, DHCP or PPPOE connection method.
- External IP, Netmask and Gateway settings.
- A Firewall Basic Template.
- Internal IP and Netmask.
- DNS Settings (optional).
- DHCP Server settings (optional).



Command	Description
Static IP	ComSifter must be manually configured to the static settings provided by the ISP (or upstream Network Administrator). All settings must be entered manually.
Dynamic IP	ComSifter will obtain its external IP, subnet mask, gateway and (optionally) DNS settings automatically from the attached cable, DSL or upstream device using DHCP protocol. An internal IP and subnet mask must be specified for the local LAN.
PPPoE	ComSifter will obtain its external IP, subnet mask, gateway and (optionally) DNS settings automatically from the attached cable, DSL or upstream device using PPPoE protocol. An internal IP and subnet mask must be specified for the local LAN.
Current Network Settings	Displays current network settings for External Network, Internal Network and DHCP server.

**Figure 3-63: Network Wizards**

After selecting a Network Wizard, further refinements to Network and Firewall settings may be performed from ADSL Client, Network Configuration and Firewall Advanced.

## Static IP

Use this wizard if your connection to the Internet uses a static IP that does not change. Typically this IP is assigned by the service provider.

Figure 3-64: Network Wizard - Static IP

## External IP

Enter the external IP for your installation. Typically this will be assigned by your service provider and will be a public IP accessible from the Internet. The format for this entry is xxx.xxx.xxx.xxx such as 63.195.80.100.

## External Subnet Mask

Enter the External Subnet Mask for your installation. Typically this will be assigned by your service provider. The format for this entry is xxx.xxx.xxx.xxx such as 255.255.255.0.

## External Gateway

Enter the External Gateway for your installation. Typically this will be assigned by your service provider. The format for this entry is xxx.xxx.xxx.xxx such as 63.195.80.1

### Internal IP

Enter the Internal IP for your installation. This may be any Class A, B, or C Internet Address but typically will be a non-routable address in the following IP ranges:

- 10.0.0.0
- 90.0.0.0
- 172.0.0.0
- 192.168.0.0

The format for this entry is xxx.xxx.xxx.xxx such as 192.168.0.1

**Note:** Using a non-routable IP address adds an extra layer of security to your installation as these addresses may not be used directly on the Internet. Instead they must be translated to the public IP before going out on the Internet.

### Internal Subnet Mask

Enter the Internal Netmask for your installation. Typically this will be 255.255.255.0. This setting will allow all 254 IP's of the Internal IP defined above.

### Primary DNS

Enter the Primary 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. This feature may simplify LAN installation as ComSifter may be used as the Primary DNS.

### Secondary DNS

Enter the Secondary DNS settings for your network. This field is optional.

**Note:** ComSifter includes a Smart DNS feature. Every 15 minutes ComSifter queries the 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.

## 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.

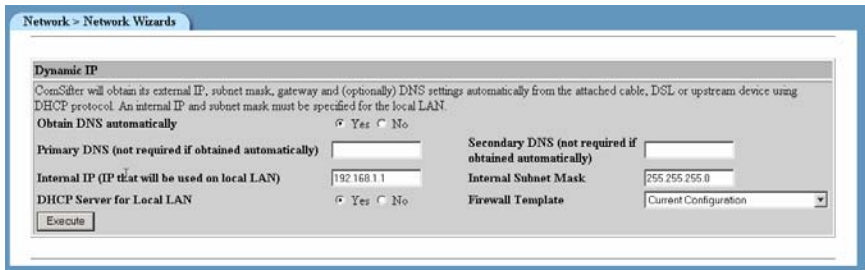
**Note:** If the network that ComSifter is installed into uses a Domain Controller (Windows 2000/2003 Server) then the Domain Controller may be providing DHCP Services. If so do not enable ComSifters DHCP Server.

## Firewall Template

Select a Firewall Template from the drop down box. Firewall Templates are described in this manual under [Firewall Basic \(Templates\)](#).

## Dynamic IP

Use this wizard if your service provider does not supply a permanent or static IP. Dynamic IP uses the DHCP protocol to obtain an External IP, Netmask and Gateway from the attached Cable, DSL, T1 or upstream device. Also included is a lease time, or the amount of time that the information will be valid. The lease time is determined by the provider of the information and may range from hours to days. When the lease expires ComSifter will ask for a new lease. The lease may contain the same information or may contain new information. In this arrangement the external IP cannot be guaranteed as the provider may change it dependent on their network requirements.



The screenshot shows a window titled "Network > Network Wizards" with a sub-tab "Dynamic IP". The main text reads: "ComSifter will obtain its external IP, subnet mask, gateway and (optionally) DNS settings automatically from the attached cable, DSL or upstream device using DHCP protocol. An internal IP and subnet mask must be specified for the local LAN." Below this, there are several configuration options:

Obtain DNS automatically	<input checked="" type="radio"/> Yes <input type="radio"/> No	Secondary DNS (not required if obtained automatically)	<input type="text"/>
Primary DNS (not required if obtained automatically)	<input type="text"/>	Internal Subnet Mask	255.255.255.0
Internal IP (IP that will be used on local LAN)	192.168.1.1	Firewall Template	Current Configuration
DHCP Server for Local LAN	<input checked="" type="radio"/> Yes <input type="radio"/> No		

An "Execute" button is located at the bottom left of the configuration area.

**Figure 3-65: Network Wizard - Dynamic IP**

Configuration of Dynamic IP is the same as described in [Static IP](#).

## PPPOE

PPPOE is connection method very similar to dial up services. When there is a request for Internet Access the ComSifter connects with the service provider and logs on. After a predetermined period of inactivity the ComSifter logs out of the connection. In this arrangement the External IP of the ComSifter may change many times per day.

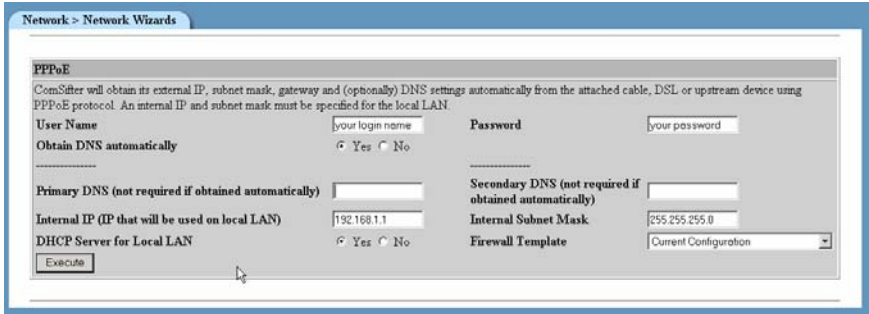


Figure 3-66: Network Wizard - PPPOE

### User Name

Enter the User Name supplied by your provider.

### Password

Enter the password supplied by your provider.

The remainder of the configuration options are the same as those described in [Static IP](#).

## 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 3-67: Current Network Settings**

## Quality of Service (QOS)

### Overview

An Internet connection consists of an upstream and downstream connection. Typically these connection speeds are asymmetrical, a high speed for downloads and a lower speed for uploading. To provide fast uploading and downloading the ISP (Internet Service Provider) will configure large buffers that optimize file transfer performance. These large buffers help file transfer performance but degrade the interactive performance of the network. An example of this is when one user is uploading a large file from the local network to another location on the Internet (this could be a file transfer, large email or even an FTP upload). As this file is being uploaded another user starts downloading a file. One would assume that the downloading would not be affected by the upload but this is not true. As downloaded packets arrive they are acknowledged back to the sender by way of an ACK packet. This packet must traverse the same path as the file being uploaded. And since the uploaded file is filling the buffers at the ISP the ACK packet must wait its turn to be processed at the ISP. This delay causes the downloaded file to begin to slow as the ACK packets have not made their way back to the sender.

To resolve this dilemma ComSifter incorporates a QOS feature that removes the upstream buffer from the ISP and moves it to the ComSifter. Since ComSifter has control over the buffer we can now configure the buffer.

<b>Note:</b>	ComSifter can only control the upstream buffer, i.e. data that has not been sent. ComSifter cannot control the downstream data as this data has already been sent.
--------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------

## Determining the true Connection Speed

For ComSifter to effectively control the upstream buffer it must know the true speed of the upstream connection. Advertised ISP speeds are typically the sync rate of the Cable/DSL modem. These rates do not include the protocol between the Cable/DSL modem and the ISP or the TCP/IP protocol used over the Internet. These protocols may cumulatively add 15-20% overhead. An advertised speed of 128Kbps upstream may only be able to move customer data at 102Kbps. Since ComSifter QOS is buffering customer data it will need to use the 102Kbps, not the advertised 128Kbps.

The best method to determine the upload speed of your network is to use a connection test provided by a third party. The following links will take you to locations on the Internet providing connection tests.

[www.dslreports.com/stest](http://www.dslreports.com/stest)

<http://www.speakeasy.net/speedtest/>

<http://www.dsl-speed.org/test.htm>

**Note:** Speed tests should only be run when your network is not being used such as early in the morning or late at night. It is also suggested that multiple tests be run to insure repeatability.

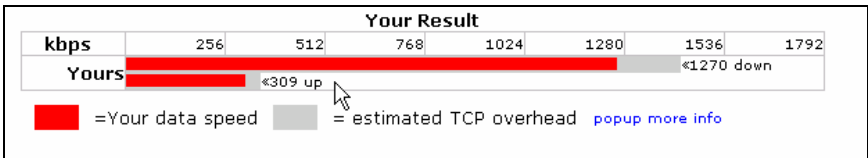


Figure 3-68: Results of Speed Test

In the example above we ran a speed test from [www.dslreports.com/stest](http://www.dslreports.com/stest) . Upstream speed was 309Kbps. We will take 1% off this figure (306) and use it as our Up Speed in ComSifter

QOS incorporates three Queues. These are default (no user control), High Priority and Low priority. A fourth queue, called Special Network, is available in the event that ComSifter is routing into another network that is a part of your LAN. Each of these queues has two parameters, a rate and a ceiling. The rate of a queue is the transmission speed of the queue when there is traffic in a higher priority queue. Ceiling is the maximum transmission speed of the queue when traffic is not present in a higher priority queue.

By default all traffic starts in the Default Queue. The Default Queue is calculated at 1/4 of the Up Speed. If the Low and Highest Queues are not defined then the traffic in the Default Queue will share equally the bandwidth defined in Ceiling. If the Low or High Priority Queues are defined then traffic in those queues will get more bandwidth than the default Queue. In the example shown below ports 25 (SMTP), 465 (secure SMTP) and 80 (web browsing) have been given extra bandwidth by being moved to the Low Priority Queue. Port 53 (DNS) has been moved to the High Priority Queue giving DNS lookups the most bandwidth.

<p><b>Note:</b> ComSifter is configured to automatically move ACK packets and short packets (less than 1000 bytes) into the highest priority queue. This insures that uploads will not adversely affect downloads.</p>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



## Configure QOS

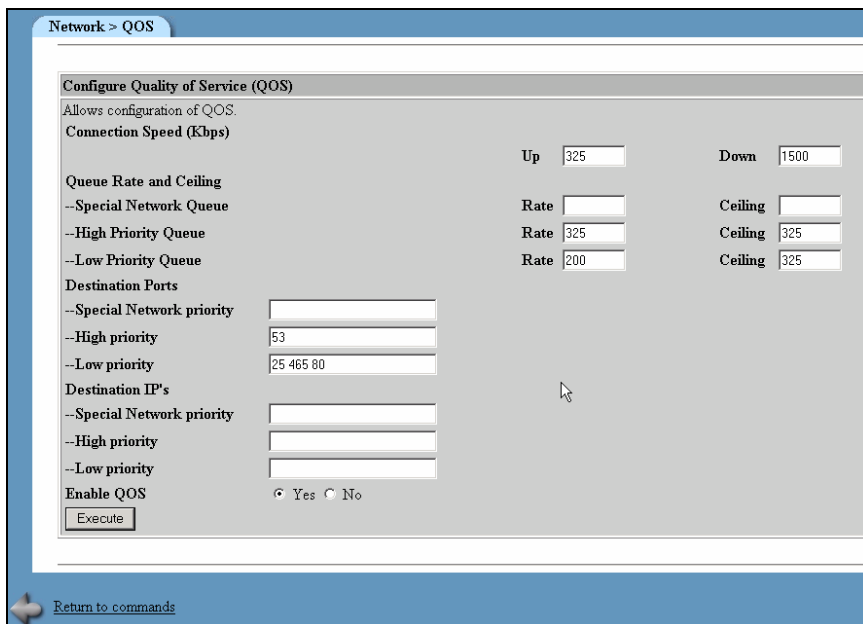


Figure 3-69: Configure QOS

### Connection Speed

Up – enter the upstream speed derived from the tests above.

Down – enter your advertised downstream rate.

### Queue Rate and Ceiling

Entries will determine the bandwidth available to each Queue.

Special Network Queue – This queue is designed for installations where ComSifter is not routing directly to the Internet but is routing upstream into another network that is a part of your LAN. The upstream network may have the gateway to the Internet and may also have resources, such as a Domain Controller, that clients on

ComSifters network need to access. Since these resources may be accessed at LAN speeds (10 or 100mbps) the Special Networks Queue allows these speeds to be realized.

Queue Rate and Ceiling - determine how fast each queue will operate.

Rate – is the speed the queue will operate at when other queues have data.

Ceiling – is the maximum speed the queue will operate at when higher priority queues do not have data.

### **Destination Ports**

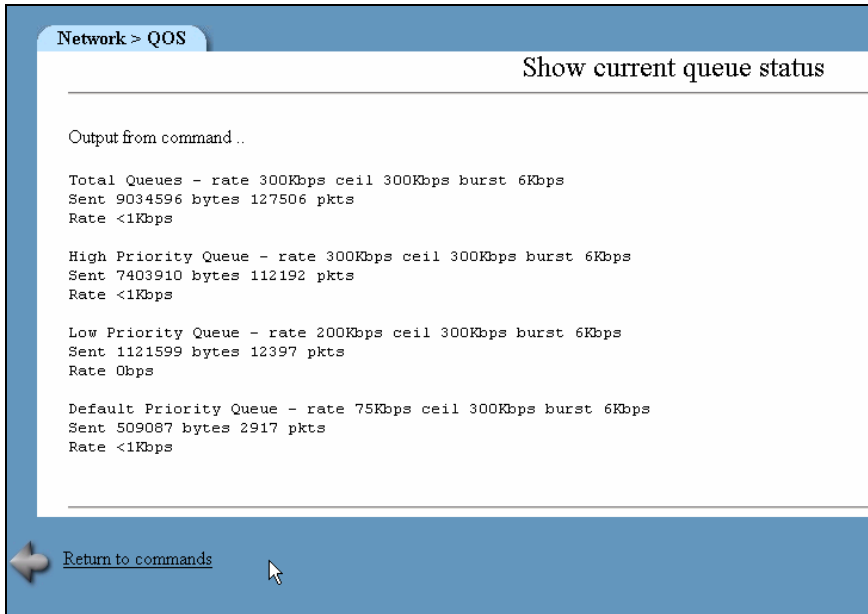
In this field enter the destination port or ports that you want to have higher priority. Multiple ports may be entered by separating the ports by a space.

### **Destination IP's**

In this field enter the destination IP address or addresses of addresses that you want to have a higher priority. Multiple IP's may be entered by placing a space between each IP. Entire networks may be entered using CIDR notation. If the upstream network is 192.168.1.0 and you wish this entire class C network to have priority then enter 192.168.1.0/24. A Class B network would be xxx.xxx.xxx.xxx/16. A Class A network would be xxx.xxx.xxx.xxx/8.

## Viewing Queue Status

Once QOS has been configured and enabled you may review the current queue status with this command.



```
Network > QOS                                     Show current queue status

Output from command ..

Total Queues - rate 300Kbps ceil 300Kbps burst 6Kbps
Sent 9034596 bytes 127506 pkts
Rate <1Kbps

High Priority Queue - rate 300Kbps ceil 300Kbps burst 6Kbps
Sent 7403910 bytes 112192 pkts
Rate <1Kbps

Low Priority Queue - rate 200Kbps ceil 300Kbps burst 6Kbps
Sent 1121599 bytes 12397 pkts
Rate 0bps

Default Priority Queue - rate 75Kbps ceil 300Kbps burst 6Kbps
Sent 509087 bytes 2917 pkts
Rate <1Kbps

Return to commands
```

**Figure 3-70: Queue Status**

Each Queue will display:

- The rate and ceiling it has been configured to.
- The number of bytes/packets that have been sent since QOS was started (ComSifter will accumulate these figures until ComSifter is restarted or QOS has been restarted from Configure Quality of Service).
- The current transmission rate of the queue.

## Maintenance



**Figure 3-71: 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.
- Download/Install IDENTD.
- Move files into and out of ComSifter using File Manager.
- View Information about ComSifter
- Run an Internet Connection Test.
- Reset ComSifter to factory defaults.
- 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:

- DHCP Server setting
- Network settings
- Firewall 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.
2. 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.

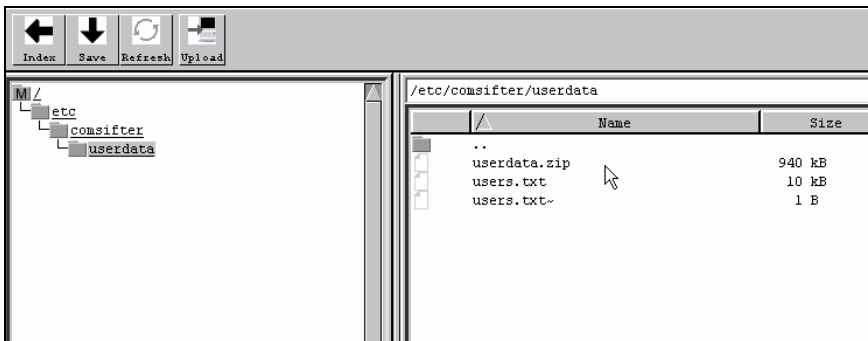


Figure 3-72: File Manager

3. Select `userdata.zip` and click on the  icon.

4. 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.



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

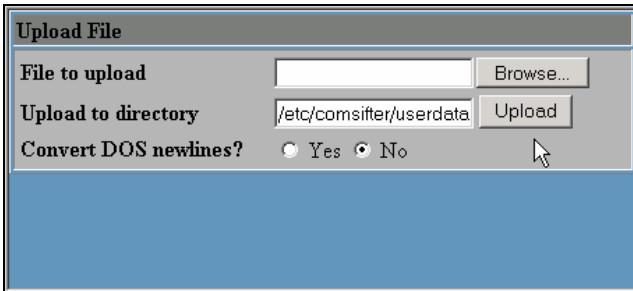


Figure 3-73: Upload File

4. Click Upload to copy the file from the location selected to ComSifter.
5. 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.

## 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.

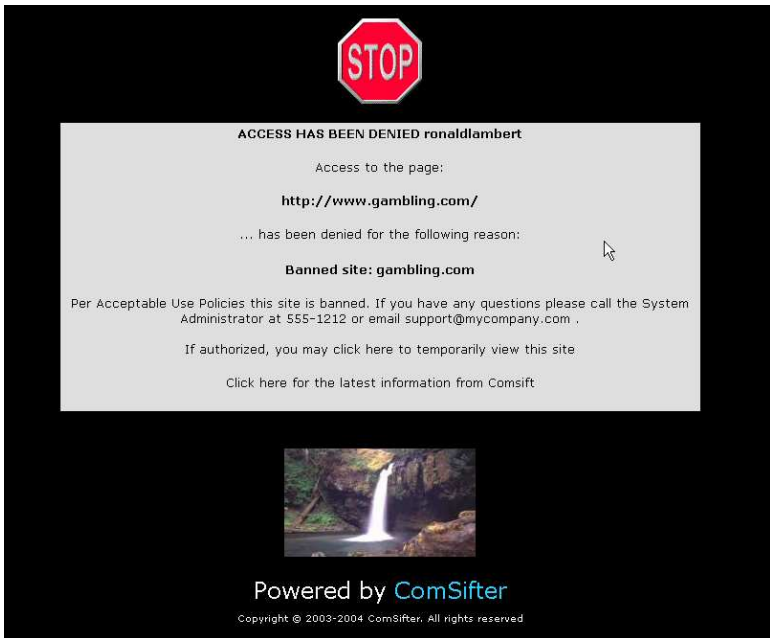


Figure 3-74: Denied Access Page



In the example we see that user ronaldlambert tried to access [www.gambling.com](http://www.gambling.com). He was denied because that domain was a banned site in the Blacklist Domain List.

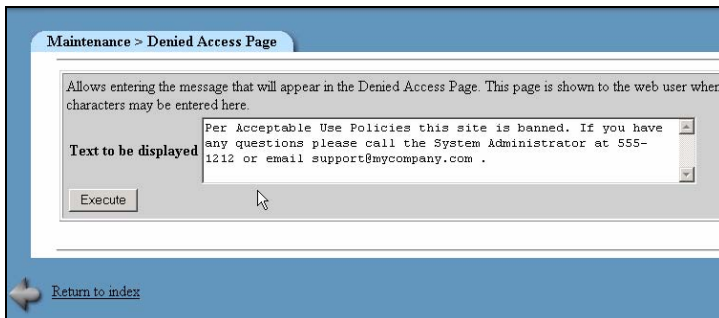
Next we see the local message (described in Local Message).

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.

The last item is “Click here for the latest Information from Comsift”. This link will take the user to a special place on the Comsift website where recent information discovered by Comsift is posted. Web Site operators are constantly changing their sites and many times, especially with Advertising, they will route through ad servers without any information to the user that they are doing this. Visiting this link may be helpful in certain troubleshooting situations such as “why did a site come through last week but this week it is blocked”.

## 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.



The screenshot shows a web-based configuration interface for the Denied Access Page. At the top, there is a breadcrumb trail: "Maintenance > Denied Access Page". Below this, a text box contains the instruction: "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." To the left of the text input area is the label "Text to be displayed". The text input area contains the message: "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 .". Below the text input area is an "Execute" button. At the bottom left of the interface, there is a "Return to index" link with a small icon next to it.

Figure 3-75: Denied Access Page Message

## Download/Install IDENTD

IDENTD is the small software program that must be installed on each user's computer if multiple filters are to be used in ComSifter. The program may be installed and executed locally on each client computer or may be installed on a Domain Controller and pushed to client computers on user login. If a Domain Controller is available this is considered a best practice as the program is installed once and is installed from a secure source.

As part of configuring ComSifter usernames must be entered in the User List and a filter level associated with the username. During normal operation when a user computer requests a web site the ComSifter will query the IP of the requesting computer and ask for its IDENTD. The IDENTD program will respond with the username of the user currently logged into the computer.

ComSifter then matches the username with the filter associated in the User List and applies the filter settings appropriate for that filter. By using IDENTD, multiple users may log into and out of a computer during the day and they will be filtered based on their username, not the computer.

If a user computer that does not have IDENTD installed is queried, and thus does not respond, ComSifter will automatically assign that computer user the username "nousername". By default, "nousername" is automatically routed to the non-IDENTD filter. This default behavior may be changed by adding "nousername" to the ComSifter "user list" and assigning an appropriate filter.

Identd must be executed on the local client computers. This execution may be performed by installing Identd on each client computer or may be installed under the auspices of a Windows 2000/2003 Domain Controller or a Novell Server. Procedures for both installations are described below.

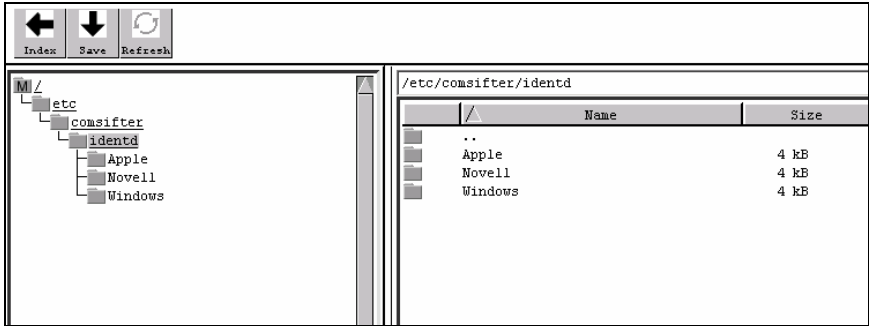
**Warning:** Identd listens on Port 113 of the client computer. If client computers have personal firewalls Port 113 must be opened. If Port 113 is not opened Internet access will fail.

**Warning:** ComSifter CS-8 relies on secure authentication from the client workstation. Windows NT/2000/XP, Apple Mac and Linux are able to provide this secure authentication. Windows 95/98/ME is unable to provide secure authentication. As a result Comsift is unable to officially support Windows 95/98/ME. If you have a mixed environment that includes these unsupported Operating Systems, Comsift suggests the following best practices.

Option 1: The identification program Comsift uses, IDENTD, should be executed from a file server or domain controller, which requires proper authentication. Do not load the IDENTD program from a local hard drive.

Option 2: Do not use the IDENTD program on Windows 95/98/ME workstations. Without IDENTD, client workstations will be routed automatically to the non-IDENTD filter. Configure this filter for your Windows 95/98/ME clients.

**Note:** Administrator privileges are required for all operating systems to properly install Identd.



**Figure 3-76: Download/Install IDENTD**

**Downloading the file**

1. Select Identd.zip from within the directory for the type of installation being performed and click on the **Save** icon.
2. A standard save dialog box for your operating system will open allowing you to save the file to the location of your choice.
3. Unzip the program using any standard zip/unzip program to a location of your choice.

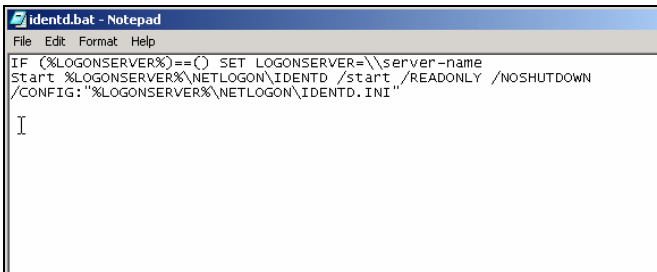
**Microsoft Windows Standalone Workstations**

1. Right click and copy the IDENTD.exe program (from step 3 above).
2. In Windows 98, Windows 2000, and Windows XP operating systems right click the start menu.
3. Select Open All Users.
4. Double click the Programs folder.
5. Double click the Startup folder.
6. Paste IDENTD.exe into the folder.
7. Restart the computer.

The IDENTD program will now start every time the computer is started.

## Microsoft Windows 2000/2003 Domain Controller

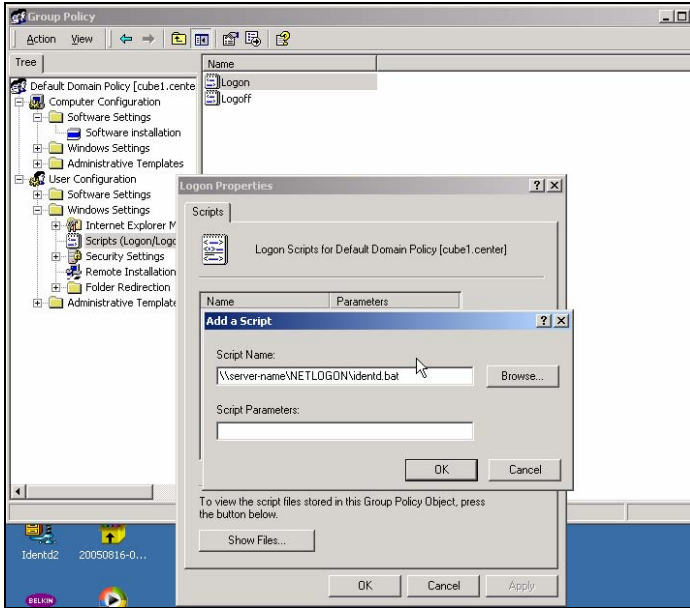
1. Unzip the three files that are in identd.zip. This file is found on the Documentation and Utilities CD or in the ComSifter under Maintenance > Download/Install Identd > Windows.
2. Extract the three files into your domain controller NETLOGON directory which by default is in c:\winnt\sysvol\sysvol\yourdomainname\scripts
3. Edit the first line of identd.bat file by changing server-name to the computer name of your server (not your domain name).



```
identd.bat - Notepad
File Edit Format Help
IF (%LOGONSERVER%)==( ) SET LOGONSERVER=\\server-name
Start %LOGONSERVER%\NETLOGON\IDENTD /start /READONLY /NOSHUTDOWN
/CONFIG: "%LOGONSERVER%\NETLOGON\IDENTD.INI"
I
```

**Figure 3-77: Identd Server Batch File**

4. In Control Panel open Administrative Tools > Active Directory Users and Computers.
5. Right click your domain name and click properties.
6. Click the tab that says Group Policies
7. Open Default Group Policy
8. Open User Configuration -> Windows Settings -> Scripts(logon/logoff) ->Logon -> Add



**Figure 3-78: Server Logon Script**

9. In the Script Name field enter the UNC path to your server (\\your servername\NETLOGON\identd.bat) (netlogon is case sensitive)
10. There are no Script Parameters

The IDENTD program will now be installed and started every time a Domain User logs into a Domain Computer.

### **Apple Macintosh Standalone Workstation**

To be supplied.

### **Novell Client on Windows Standalone Workstation**

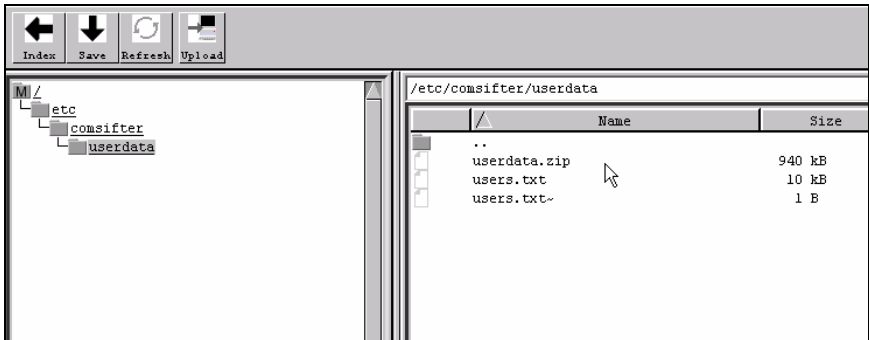
This installation is only for Windows workstations that are using the Novell Client. Instead of returning the currently logged in Windows Username, the currently logged in Novell Username will be returned.

1. Right click and copy the identdnov.exe program (from step 3 above).
2. In Windows 98, Windows 2000, and Windows XP operating systems right click the start menu.
3. Select Open All Users.
4. Double click the Programs folder.
5. Double click the Startup folder.
6. Paste identdnov.exe into the folder.
7. Restart the computer.

### **Novell Server -> Novell Client on Windows Standalone Workstation**

1. Copy identdnov.exe to the sys:public directory of your Novell Server. Add reference to this executable in the users login script.

## File Manager



**Figure 3-79: 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 the Operators Manual.

**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](http://www.sun.com) .



## Information

### ComSifter Information

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

The screenshot shows a web interface with a blue header bar containing 'Maintenance > Information' and 'ComSifter Information'. Below the header, the text reads: 'Output from command ..', 'Wed May 25 14:13:28 PDT 2005', and 'ComSifter Health'. A list of system metrics follows, including CPU speed, system load, disk and memory space, various voltages, fan speed, processor temperature, and hard drive health. The output concludes with '\*\*\*\* ComSifter health is good \*\*\*\*'.

```

Maintenance > Information
ComSifter Information

Output from command ..

Wed May 25 14:13:28 PDT 2005

ComSifter Health
In spec, CPU is operating at full speed
In spec, System load is 1% over the past 15 minutes (<90% normal)
In spec, 11029MB of free disk space (>1000MB normal)
In spec, 316MB 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, System fan speed is 5328 rpm (3000min - 9000max)
In spec, CPU fan speed is 6488 rpm (2000min - 7000max)
In spec, Processor temp is 47 degrees C (10Cmin - 90Cmax)
In spec, Hard Drive S.M.A.R.T. health is good
In spec, Hard Drive Temperature is 49 degrees C (<70C normal)
**** ComSifter health is good ****
  
```

**Figure 3-80: ComSifter Information**

- ComSifter Time – Displays ComSifters internal time.
- ComSifter Health – displays the condition of ComSifter hardware.
- Software Information – shows ComSifter revision number.

The screenshot displays two sections: 'Software Information' and 'Blacklist Information'. The software section shows the version number as 'Rel CS-8 Pro 9.0ib 05/25/05'. The blacklist section states that updates are performed daily, the last update was on 05/23/05, and automatic updates will continue until 03/29/06.

```

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 3-81: 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 3-82: Network Settings**

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

## ComSifter Release Notes

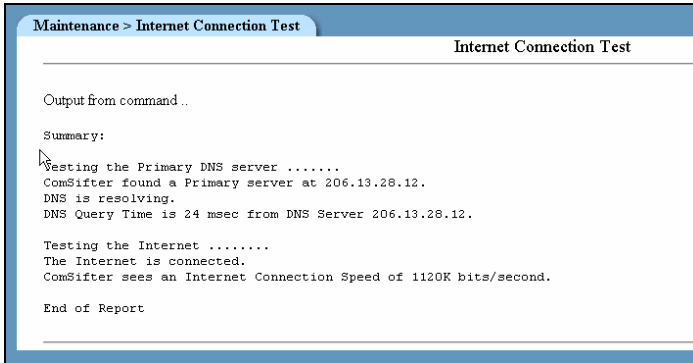
To view information about Release Notes click on **Maintenance**, then **Release Notes**. ComSifter will respond as shown below.

**Figure 3-83: 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.

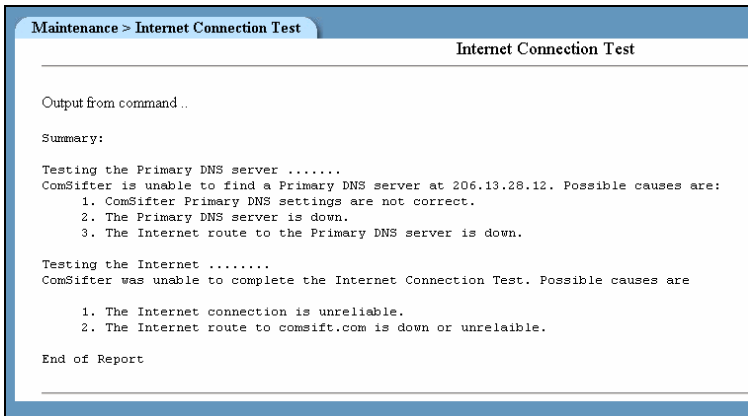


**Figure 3-84: Internet Connection Test**

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.

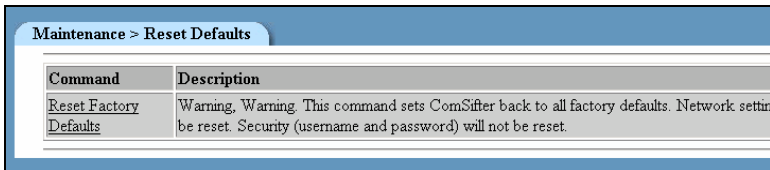


**Figure 3-85: Failed Internet Connection Test**

## Reset Defaults

Upon execution of Reset Factory Defaults the ComSifter will set all of its Network, Port Blocker, Filter Setup, Words/Phrases and Users data back to factory default conditions.

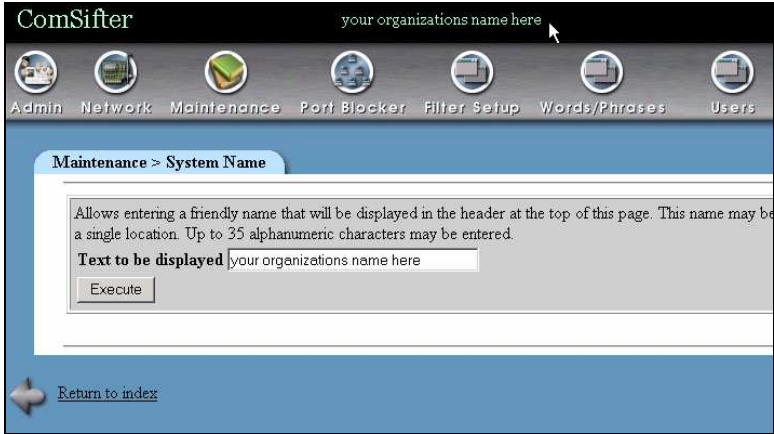
ComSifter will not change any of the ComSifter Admins usernames, passwords, or module rights.



**Figure 3-86: Reset Defaults**

**Warning:** Use this command with caution. Any changes to Network, Filter List, Words/Phrases and the User List will be destroyed and will be unrecoverable. Additionally communication with ComSifter may be lost as network settings will be set to factory default.

## System Name



**Figure 3-87: 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

Change time

Timezone: US/Pacific

Change timezone




**Figure 3-88: System Time**

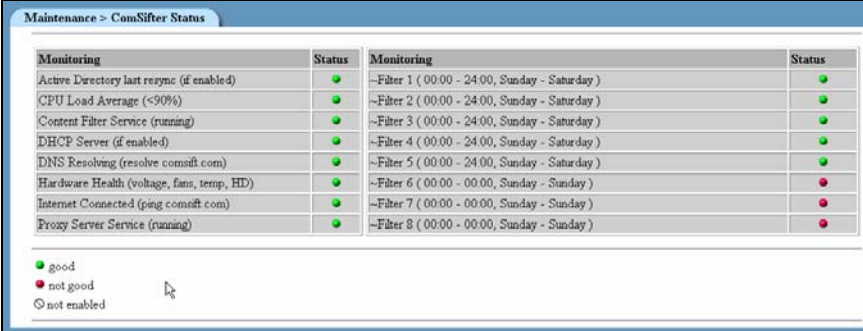
System Time is used to set ComSifter to your local time and Time Zone. Correct time is necessary for Hours of Operation Scheduling and for System Log entries.

















**Note:** ComSifter uses Network Time Protocol (NTP) to keep its clock accurate after the System Time has been set. NTP is checked weekly and during any power up of ComSifter.

## ComSifter Status

ComSifter monitors all of its critical services every five minutes and when 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.



Monitoring	Status	Monitoring	Status
Active Directory last resync (if enabled)		~Filter 1 ( 00:00 - 24:00, Sunday - Saturday )	
CPU Load Average (<90%)		~Filter 2 ( 00:00 - 24:00, Sunday - Saturday )	
Content Filter Service (running)		~Filter 3 ( 00:00 - 24:00, Sunday - Saturday )	
DHCP Server (if enabled)		~Filter 4 ( 00:00 - 24:00, Sunday - Saturday )	
DNS Resolving (resolve comsift.com)		~Filter 5 ( 00:00 - 24:00, Sunday - Saturday )	
Hardware Health (voltage, fans, temp, HD)		~Filter 6 ( 00:00 - 00:00, Sunday - Sunday )	
Internet Connected (ping comsift.com)		~Filter 7 ( 00:00 - 00:00, Sunday - Sunday )	
Proxy Server Service (running)		~Filter 8 ( 00:00 - 00:00, Sunday - Sunday )	




 good  
 not good  
 not enabled

Figure 3-89: System and Service Status

### Active Directory last resync

Displays the status of the last Active Directory Resync. Active Directory resync is performed every hour, 8 minutes after the hour. If the resync was successful this indicator will be green, if not the indicator will be red.

### 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 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, System fan speed is 4551 rpm (3000min - 9000max)

- In spec, CPU fan speed is 5957 rpm (2000min - 7000max)
- In spec, Processor temp is 39 degrees C (10Cmin - 90Cmax)
- 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 (🔴).

### **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.

Maintenance > Utilities	
Command	Description
<a href="#">Restart Services</a>	This command will restart ComSifter's proxy and filter services. This process may take up to 30 seconds to complete and will momentarily disrupt client Internet connections.
<a href="#">Rebuild ComSifter Proxy Cache</a>	In the event that items in the proxy cache are corrupt this process will delete all items in the cache and rebuild it. This process may take up to 30 seconds to complete and will momentarily disrupt client Internet connections.
<a href="#">Restart ComSifter</a>	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.

**Figure 3-90: Utilities**

### Restart Services

This command will stop and then start Content Filter Service and Proxy Server Service. The restart 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 or if instructed to do so by Comsift Technical Support.

### 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.



## Chapter 4

# 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.

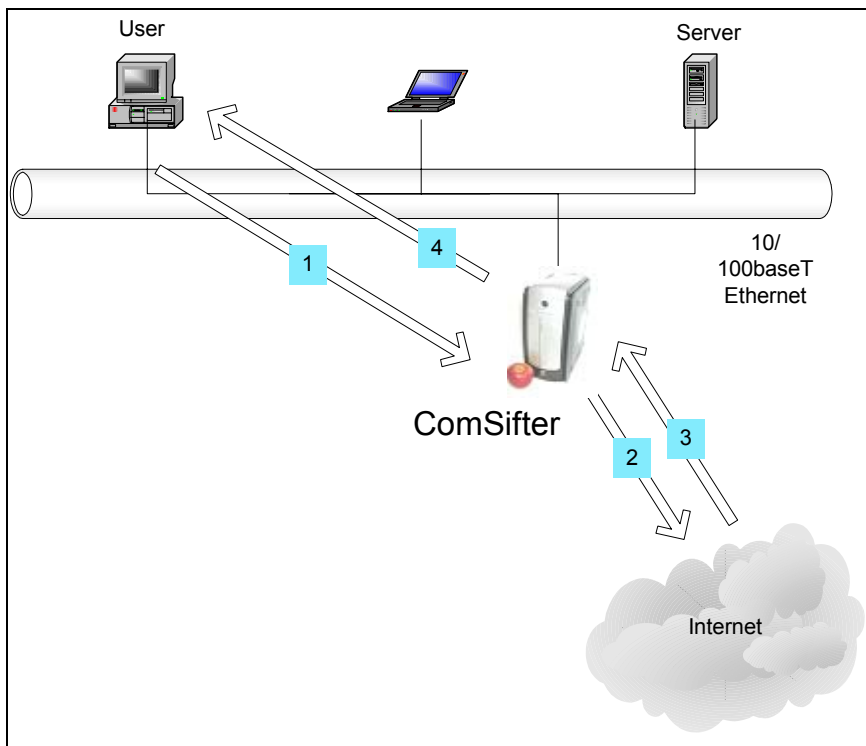


Figure 4-1: ComSifter Operation

## 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.

- 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

<b>Note:</b> Each of the above items is described in detail in the Operators Guide.
-------------------------------------------------------------------------------------

## Blacklist

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

### Categories

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

<p><b>Note:</b> 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.</p>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



## 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.

<p><b>Note:</b> 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".</p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



## 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](http://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](mailto: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](http://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 Firewall 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, 75watts

Temperature - 50 - 95° F (10 -35° C)

## Appendix C

# 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 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-export 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.

