

# SurfSentinel

## Content Filtering

## Feature Guide



a *GNAT Box*  
System Software Option



## Copyright

© 1996-2003, Global Technology Associates, Incorporated (GTA). All rights reserved.

Except as permitted under copyright law, no part of this manual may be reproduced or distributed in any form or by any means without the prior permission of Global Technology Associates, Incorporated.

### **Surf Sentinel Feature Guide**

*a GNAT Box System Software Option*

**June 2003**

## Technical Support

GTA's direct customers in the USA should call or email GTA using the telephone and email address below. International customers should contact a local GTA authorized reseller.

**Tel: +1.407.482.6925**

**Email: [support@gta.com](mailto:support@gta.com)**

## Disclaimer

Neither GTA, nor its distributors and dealers, make any warranties or representations, either expressed or implied, as to the software and documentation, including without limitation, the condition of software and implied warranties of its merchantability or fitness for a particular purpose. GTA shall not be liable for any lost profits or for any direct, indirect, incidental, consequential or other damages suffered by licensee or others resulting from the use of the program or arising out of any breach of warranty. GTA further reserves the right to make changes to the specifications of the program and contents of the manual without obligation to notify any person or organization of such changes.

Mention of third-party products is for informational purposes only and constitutes neither an endorsement nor a recommendation for their use. GTA assumes no responsibility with regard to the performance or use of these products.

Every effort has been made to ensure that the information in this manual is accurate. GTA is not responsible for printing or clerical errors.

## Trademarks

GNAT Box is a registered trademark of Global Technology Associates, Incorporated. RoBoX and Surf Sentinel are trademarks of Global Technology Associates, Incorporated.

GTA acknowledges all trademarks appearing in this document. Windows is a trademark of Microsoft Corporation. Cerberian is a trademark of Cerberian, Inc. WELF and WebTrends are trademarks of NetIQ. All other products are trademarks of their respective companies.

### **Global Technology Associates, Inc.**

3505 Lake Lynda Drive, Suite 109 • Orlando, FL 32817 USA

Tel: +1.407.380.0220 • Fax: +1.407.380.6080 • Web: <http://www.gta.com> • Email: [info@gta.com](mailto:info@gta.com)

**Lead Development Team:** Larry Baird, Richard Briley, Brad Plank, Jim Silas.

**Technical Consulting:** David Brooks. **Documentation:** Mary Swanson.

# Contents

<b>1 INTRODUCTION</b>	<b>1</b>
<b>About Surf Sentinel Subscriptions</b>	<b>1</b>
Features	1
Requirements	2
Registration & Activation	2
Support	3
<b>Documentation</b>	<b>3</b>
<b>2 MANAGING INTERNET ACCESS</b>	<b>5</b>
<b>Content Filtering</b>	<b>5</b>
Access Control Lists	5
Local Content Lists	5
HTTP Proxy	6
Remote Logging	6
<b>Internet Access Policy</b>	<b>7</b>
Steps to Implementation	8
<b>3 USING SURF SENTINEL</b>	<b>9</b>
<b>Activation</b>	<b>9</b>
<b>Configuration</b>	<b>10</b>
Access Control Lists	10
Local Content Lists	12
Content Filtering Preferences	13
Internet Access Policy	16
<b>4 SURF SENTINEL PLUS</b>	<b>17</b>
<b>Using Surf Sentinel Plus</b>	<b>17</b>
Login	17
Navigation	18
<b>Web Filter Home</b>	<b>19</b>
Site Submissions	20
Preferences	20
<b>Global Report</b>	<b>20</b>
Category URLs	21
User Requests	22
<b>Single User Report</b>	<b>22</b>
Hits by Category	22
User Requests	23
<b>APPENDIX</b>	<b>25</b>
<b>Categories</b>	<b>25</b>
Denied by Default	25
Allowed by Default	27
<b>INDEX</b>	<b>31</b>



# 1 Introduction

---

## About Surf Sentinel Subscriptions

Surf Sentinel is GTA's Internet access management and content filtering subscription service for GTA Firewalls using 53 content categories and Dynamic Real-Time Rating (DRTR).

Powered by Cerberian Web Filter technology, Surf Sentinel allows organizations to increase productivity and reduce potential legal liability by limiting access to unproductive or inappropriate web sites. This out-sourced model stores the software and categorized lists on off-site servers, so no additional hardware is needed. Multiple server locations provide redundancy, effectively eliminating downtime due to system failures or heavy data traffic.

Surf Sentinel is superior to using Local Content Lists alone. Driven by the Cerberian Web Filter, Surf Sentinel has categorized over 2.5 million sites, with thousands more added every day using Cerberian's exclusive DRTR system. DRTR reads and rates new site URLs as they are requested; Surf Sentinel blocks suspect sites *before* they are downloaded.

The Cerberian Web Filter is a product of Cerberian, Inc., a software applications development company. Information about the company and its product can be found at [www.cerberian.com](http://www.cerberian.com).

## Features

- 53 content categories for access control.
- Dynamic Real-Time Rating (DRTR).
- Easy administration and enforcement of acceptable use policies.
- Economical deployment.
- No additional hardware required.

## Requirements

- GNAT Box System Software version 3.3.3 and above operating on a GTA Firewall (not available on GB-Pro and GB-100).
- Web browser and Internet connection.
- GTA Firewall product registration.
- Surf Sentinel subscription and feature activation code.

## Registration & Activation

Your GTA Firewall must be registered to get the Surf Sentinel feature activation code; retrieve your new code by logging on to your account on the **GTA Support Center**. From your **Account Home** page, select **View Registered Products** and click on the serial number of your GTA Firewall. Copy the Surf Sentinel feature code from the list, and paste it into the first available field in the GNAT Box System Software **Basic Configuration > Features** section. If you have not previously registered, use the instructions below.

### How to Register

---

1. Go to the GTA Support Center (<http://www.gta.com/support/>) and click on the Support Center link. The login screen will appear.
2. Click the New Account button, enter your profile information and choose a user ID and password. Once you have completed the form, click Add to save your account information.
3. Return to the login screen and enter the user ID and password you created. Click Continue. The selection screen will appear.
4. Click Support Center, then click on Product Registration, the Account Home screen for your support information.
5. In the form that appears, enter the serial number and activation code of your GTA Firewall, then click Submit.

Your new product will now appear in the View Registered Products screen, accessible from the Account Home page.

---

### Note

---

If you cannot retrieve your registration code, or a feature code does not appear under Registered Products, please email support at [support@gta.com](mailto:support@gta.com) with the product serial number and your Support Center user ID in the message subject.

## Support

Support contracts range from support by the incident to full coverage for a year. Contact GTA or an authorized GTA Channel Partner to find out more.

To learn more about GNAT Box System Software, join the GNAT Box Mailing List, monitored by GTA staff. For more information, visit the GTA website at [www.gta.com](http://www.gta.com).

---

## Documentation

The **SURF SENTINEL FEATURE GUIDE** illustrates the activation and use of the Surf Sentinel subscription service for GNAT Box System Software.

### Note

Content Filtering cannot be configured using the Console.

A few conventions are used in this guide to help you recognize specific elements of the text. If you are viewing this in a PDF, color variations are also used to emphasize notes, warnings and new sections.

---

### Documentation Conventions

---

SMALL CAPS	FIELD NAMES IN BODY TEXT.
BOLD SMALL CAPS	NAMES OF PUBLICATIONS.
<b><i>Bold Italics</i></b>	<b><i>Emphasis.</i></b>
Courier	Screen text.
Condensed Bold	Menus, menu items, buttons.

---

For instructions on installation, registration and setup of a GTA Firewall in default configuration, see your Product Guide; for optional features, see the appropriate Feature Guide. User's Guides, Product Guides and Feature Guides are delivered with new GTA products; these manuals and other documentation for registered products can also be found on the GTA website, [www.gta.com](http://www.gta.com).

Documents on the website are either in plain text (\*.txt) or Portable Document Format (PDF; \*.pdf) which requires Adobe Acrobat Reader version 5.0. A free copy of the reader can be obtained at [www.adobe.com](http://www.adobe.com). Documents received from GTA Support may also be in email or Microsoft Word format (\*.doc).

---

## Documentation Map

---

### Products and Options

GTA Firewall Installation .....	Product Guides
GTA Firewall Global Management System .....	GMS User's Guide
Reporting .....	GTA Reporting Suite User's Guide
Content Filtering .....	Surf Sentinel Content Filtering Feature Guide
High Availability .....	H <sub>2</sub> A High Availability Feature Guide
Virtual Private Networking .....	GNAT Box VPN Feature Guide
VPN Examples .....	GNAT Box VPN to VPN Tech Docs

### Utilities & Information

Logging Utilities .....	GNAT Box System Software User's Guide & Addendum
Database Maintenance .....	GMS & GTA Reporting Suite User's Guides
Troubleshooting .....	Product and Feature Guides
Ports & Services .....	Product CDs
Drivers & NICs (GNAT Box Pro, Flash) .....	www.gta.com
Frequently Asked Questions .....	FAQs on www.gta.com
Web Interface, GBAdmin .....	GNAT Box System Software User's Guide
Console interface .....	Console Interface User's Guide

---



## 2 Managing Internet Access

---

### Content Filtering

GTA's Internet access management solutions provide the ability to control web access based on site content. GTA Firewalls have three primary functions for access control: Access Control Lists (ACLs), Local Content Lists (LCLs) and proxy settings. In addition, records of blocked sites can be created and sent to GTA Firewall logs.

#### **Note**

---

See the **GNAT BOX SYSTEM SOFTWARE USER'S GUIDE** for instructions on how to use other content filtering options.

### Access Control Lists

Access Control Lists (ACLs) provide a means to select web access control facilities and specify how they will be applied to web requests. Select Surf Sentinel here to use the service after entering a feature activation code. Local Allow and Deny features, configured under Local Content Lists, are also selected in the Access Control Lists section.

#### **Note**

---

ACLs must be created before enabling the proxy. The proxy is the "on switch" for content filtering; without ACLs, users will be blocked from using TCP port 80 to access the Web.

### Local Content Lists

Local Content Lists (LCLs) allow the administrator to customize content filtering using local allow and deny lists. LCLs take precedence over Surf Sentinel category listings, so you can allow access to specific sites in categories that have been blocked or deny access to sites in categories that are otherwise allowed. This is particularly useful for companies whose policies allow access only to a few specific sites, or for those with policies which allow web requests for a category, but deny specific sites within that category.

## HTTP Proxy

Content filtering requires the use of an HTTP proxy. The Preferences section for content filtering lets the administrator specify whether to use the Traditional or Transparent Proxy for HTTP (Web) requests.

Transparent Proxy is the newer and more common method of implementing an HTTP proxy. It is easy to implement, especially with a large network.

Traditional Proxy is used primarily for systems which were put in place prior to the introduction of transparent proxy methods, and for systems that require more control by directing web requests through a specific port.

## Remote Logging

Both Local Content Lists and Surf Sentinel entries are logged to the GTA Firewall. Two examples, one of an accept (pass) log message and one of a deny (block) message, are illustrated below. Fields relevant to content filtering are defined after the examples.

To learn more about log messages, see the **GNAT BOX SYSTEM SOFTWARE USER'S GUIDE** Remote Logging in the Services section and the Default Log Messages section in the Appendix. To view a PDF of the current user's guide, visit support at [www.gta.com](http://www.gta.com), or locate the PDF on your most recent software installation CD.

```
Oct 29 14:24:18 acmefirewall id=firewall time="2002-10-29 14:24:18"
fw="acmefirewall-ha-1" pri=5 msg="Accept outbound NAT"
cat_action=pass cat_site="Web Communications"
dstname=www.leadcart.com proto=http src=192.168.71.97 srcport=2661
nat=199.120.225.3 natport=2661 dst=205.138.3.133 dstport=80 rule=2
duration=23 sent=536 rcvd=537 pkts_sent=6 pkts_rcvd=5
op=GET arg=/ads1/images/digits/n7.gif
```

### *Logging, Surf Sentinel*

```
Oct 29 14:24:26 acmefirewall id=firewall time="2002-10-29 14:24:26"
fw="acmefirewall-ha-1" pri=4 msg="Block outbound NAT"
cat_action=block cat_site="Local Deny" dstname=ad.doubleclk.net
proto=http src=src=192.168.71.33 srcport=4991
nat=199.20.136.33 natport=4991 dst=205.138.3.82 dstport=80 rule=2
duration=22 sent=861 rcvd=60 pkts_sent=3 pkts_rcvd=1
op=GET arg=/adi/caranddriver.lana.com/kw;;ord=180587622710292244
```

### *Logging, Local Content List*

---

## Content Logging Fields

---

pri	Priority of this message, set in Remote Logging.
msg	Message indicating Accept/Block.
cat_action	Action taken.
cat_site	Surf Sentinel category, Local Accept or Deny.
dstname	Website blocked or accepted by this action.
proto	Protocol (http).
src	Source IP address of web request.
srcport	Port through which web request was made.
op	Operation requested.

---

Fields and descriptions are in WELF, the default log format.

---

## Internet Access Policy

Surf Sentinel is a dynamic solution to a dynamic problem. Because the Internet changes constantly, Surf Sentinel's DRTR helps you respond to new and changing sites quickly, restricting user access only to material that is consistent with your access policy.

Web filtering can protect a company from drains on bandwidth, potential legal liability and lost productivity. For schools and libraries, policies can be set preventing access to material inappropriate to the age of the workstation user.

When content filtering has been configured and Surf Sentinel is enabled, the Cerberian Web Filter intercepts a request for web pages, compares the requested page and site to its database, then allows or denies the request based on the Access Control Lists created in accordance with your company Internet access policy.

This rating and review process includes not only the sites that a user explicitly requests by clicking on a link or typing a URL, but also protects users from inappropriate material on pages called up inadvertently (i.e., pop-up windows) when accessing sites.

---

## Steps to Implementation

Content Filtering can be implemented as part of a complete Internet Access/Acceptable Use Policy. Prior to implementing Surf Sentinel, GTA suggests completing the following steps:

1. Develop an Internet Access Policy and create acceptable use guidelines. Guidelines and policy examples are available on the Internet.
2. Create address objects on your GTA Firewall to define the various groups whose access you will be controlling with content filtering.
3. Create access control lists (ACLs) on your GTA Firewall for groups defined in the last step, and choose which categories will be accepted and which will be denied.
4. Customize your content filtering further, if desired, by adding any specific pages or sites you wish to allow or deny to the local content lists (LCLs).
5. Turn on content filtering by selecting a proxy method.

## 3 Using Surf Sentinel

This chapter will describe how to activate and configure Surf Sentinel using either the Web interface or GBAdmin. On the Console interface, access to configuration is limited to entering the subscription's feature activation code.

Content filtering on the GTA Firewall requires an efficient DNS server, Access Content Lists and a proxy method.

### Activation

Surf Sentinel is activated by entering your feature activation code, available on the GTA Support site after your GTA Firewall has been registered. (You must register your product and log in with your user name and password.)

To activate Surf Sentinel, log on to your GTA Firewall and go to **Basic Configuration > Features**.

Enter the feature activation code in the next available line. Save the section. If the DESCRIPTION field fills automatically, the code is activated correctly and the service can be enabled.

GNAT-Box Features		
Index	Activation code	Description
1	AAAA.BBBB.CCCC.DDDD	GB-1200 3.4 - Registered
2	AAAA.BBBB.CCCC.DDDD	GB-1200 3.4 - High availability
3	AAAA.BBBB.CCCC.DDDD	GB-1200 3.4 - VPN (5 clients)
4	ENTER SURF SENTINEL ACTIVATION CODE	GB-1200 3.4 - Surf Sentinel
5		
6		
7		

*Feature activation code*

---

# Configuration

The steps for configuring Surf Sentinel must be done in order to ensure continuous Internet access for users. If content filtering is already in use, some of these steps will have already been completed.

## How to Configure Content Filtering

---

1. Define a DNS server (under Basic Configuration) to access your selected list server. (See **GNAT BOX SYSTEM SOFTWARE USER'S GUIDE**, Chapter 5 – Services, for more about defining a DNS server.)
2. Create and enable Access Control Lists (ACLs).
3. Add Allow and Deny Local Content Lists (if desired).
4. Enable Transparent Proxy.

-AND/OR-

4. Create and enable an appropriate Remote Access Filter and then enable Traditional Proxy.

## Access Control Lists

Access Control Lists (ACLs) provide a means to select web access control facilities and specify how they will be applied to web requests. The ACL screen includes settings for Mobile Code Blocking.

Each ACL consists of a description, an Address Object representing a group of IP addresses to be filtered, the ability to specify Mobile Code Blocking preferences for the individual ACL, and, with a Surf Sentinel subscription, content filtering category lists.

### Caution

---

Access Control List order is important. A site higher on the list that denies access will be blocked even if a later item allows access.

## Enable Surf Sentinel

Enable Surf Sentinel in the current ACL by selecting the checkbox.

## Define a Controlled Group

Select a group to be governed by this ACL by choosing an address object from the **SOURCE ADDRESS** field dropdown box. Enter a description for the ACL in the **DESCRIPTION** field. See the **GNAT BOX SYSTEM SOFTWARE USER'S GUIDE** for more about address objects.

To implement multiple policies, you will need to create multiple, separate ACLs. See your product guide for the number of ACLs your GTA Firewall supports.

GNAT-Box Edit Content Access Control List

Disable:

☐

Description:

Summer Interns

Source Address:

ANY\_IP

Content Filtering Facilities

Local allow list:

☐

Local deny list:

☒

Surf Sentinel:

☒

Mobile Code Blocking

JAVA:

☐

JAVA Script:

☐

ActiveX Objects:

☐

Surf Sentinel Categories

Allowed

Abortion

Advertisement

Arts/Entertainment

Business and Economy

Chat/Instant Messaging

Computing and Internet

Cult/Occult

Cultural Institutions

Education

-->

<--

Denied

Adult/Mature Content

Alcohol/Tobacco

Gambling

Hacking/Proxy Avoidance Systems

Illegal Drugs

Illegal/Questionable

Intimate Apparel/Swimsuit

Nudity

Pornography

Back

Copy

Default

Ok

Access Control List

### Choose Categories

Surf Sentinel has default Allowed and Denied categories. Move these categories from one list to another to reflect the Internet access policy. Select the category in one list and then click the appropriate arrow button (-->, <--) to move it to the other list.

#### Note

If LCLs are enabled in this screen, the LCL allow and deny lists will override the Surf Sentinel allowed and denied categories.

Surf Sentinel Categories

Allowed

Abortion

Advertisement

Arts/Entertainment

Business and Economy

Chat/Instant Messaging

Computing and Internet

Cult/Occult

Cultural Institutions

Education

-->

<--

Denied

Adult/Mature Content

Alcohol/Tobacco

Gambling

Hacking/Proxy Avoidance Systems

Illegal Drugs

Illegal/Questionable

Intimate Apparel/Swimsuit

Nudity

Pornography

Move Category from Denied to Allowed

### Default Categories

Categories can be reset to installation defaults by selecting the Default button. See the Appendix of this guide for Surf Sentinel factory defaults settings. The Surf Sentinel list can be defaulted independently of other services.

## Access Control Lists (ACL) Fields

Disable	Select this checkbox to disable the designated ACL.
Description	Enter a description for the ACL.
Source Address	If a request matches an element of the specified address object, the packet will be compared to the ACL.

### Content Filtering Facilities

Local Allow List	Select to process against local firewall Allow list.
Local Deny List	Select to process against local firewall Deny list.
Surf Sentinel	Select to process against the Surf Sentinel list.

### Mobile Code Blocking

Built-in mobile code blocking facility for JAVA, JAVA Script and ActiveX objects. These objects appear in inbound HTML on TCP port 443, 80, 8000 and 8080.

### Surf Sentinel Categories

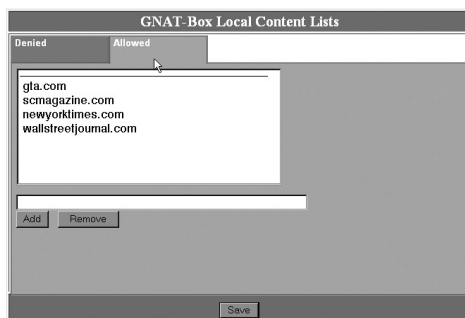
Allow or block URLs in Surf Sentinel categories. Switch a category from one list to the other by selecting the item and clicking the left or right arrow button.

## Local Content Lists

Allowed and Denied lists in the Local Content Lists (LCLs) section can be used in conjunction with Surf Sentinel to customize content filtering choices.

Using LCLs, the administrator can allow or deny either a single domain by entering the entire base URL (e.g., `www.gta.com`), or all domains in the site by leaving out the prefix characters (e.g., `gta.com`). When a specific URL is entered, (e.g., `www.gta.com/index.html`), the entire domain or domains will be filtered.

See your product guide for the number of LCLs in your product. See the **GNAT BOX SYSTEM SOFTWARE USER'S GUIDE** for more information about Local Content Lists.



*Local Content Lists*



### **How to Allow or Deny Specific Sites within a Category**

Local Content List items override Surf Sentinel selections, so you can use LCLs to customize Surf Sentinel.

For example: Your company wishes to block sites in the category “Drugs” for hourly employees, but would like to make a specific health-related drug site available to them as part of employee health benefits.

In the hourly employee ACL, put the category “Drugs” in the Surf Sentinel Denied List. Then, under Local Content Lists, enter the URL of the employee benefit site in the “Allowed” list, and save. This permits a user to request the specified domain or domains, but blocks other sites that provide information about legally obtainable drugs.

## **Content Filtering Preferences**

Content Filtering on a GTA Firewall requires an HTTP proxy. A proxy breaks the connection between sender and receiver. Proxy servers are available for common Internet services; e.g., an HTTP proxy is used for Web access, and an SMTP proxy is used for email. An HTTP proxy allows Web requests to be managed by funneling all user Web requests through the proxy, where content can be filtered.

### **Caution**

ACLs must be created before enabling the proxy. Enabling the proxy before creating ACLs will block HTTP Web access.

With Transparent Proxy, IP addresses that are not explicitly allowed access in the ACLs will not be able to use the Web access port, TCP port 80. If only Traditional Proxy is selected, browsers configured to use Traditional Proxy will be affected; other users will not be prevented from accessing the Web.

The Content Filtering Preferences section allows the administrator to specify the use of the Traditional Proxy and associated port, the Transparent Proxy, or both; in addition, a customized block action (a message or URL) can be set. If an ACL blocks a web address (URL), and a user attempts to load a page from that web address, the user will either see a message or be redirected to a URL, e.g., an internal site defining Internet use policies.

By default, the message, “Local policy denies access to web page,” will appear if a user attempts to reach a web address blocked by an ACL.

### **Caution**

If your site uses SSL encryption, the proxy redirect URL must be formatted for an encrypted page: <https://www.example.com>.

## Traditional Proxy

Traditional Proxy requires users located on Protected Networks to have their browsers configured with the port number and IP address of the proxy. This method allows the most control over web requests by directing all requests through a specific port, allowing the administrator to disallow access through other ports. When a traditional proxy is used for HTTP, it runs on TCP port 2784 by default. To run the proxy on a different port, enter the value in the **PORT** field.

### Remote Access Filter

A Remote Access Filter (RAF) must be in place to use Traditional Proxy. Auto-configure the RAF list to create an appropriate filter, (which is disabled for security); otherwise, enter a filter similar to the default filter example below. Remember that filter order is important.

Description:	Allow all access from the Protected Networks to the Internet
Type:	Accept
Interface:	(Name of selected protected physical interface)
Authentication required:	(Deselect)
Protocol:	TCP
Source Object:	ANY_IP
Destination Object:	ANY_IP
Destination Port:	2784

## Transparent Proxy

Transparent Proxy is the most common method of implementing an HTTP proxy because it is easier to implement than Traditional Proxy, especially when a network is very large or widespread.

Users located on the Protected Network will not have to make any changes or adjustments to use Transparent Proxy; a port is not required, so there is no modification to browsers and no **PORT** field.

However, if the administrator desires very tightly restricted port access, using Transparent Proxy will require filter refinements in order to direct HTTP traffic through selected ports and close other ports to selected protocols. Filters in the default sets for Remote Access and Outbound Filters can be used as examples. (As content filtering is an optional service, filters for use with content filtering proxies are disabled by default.)

## Using Both Types of Proxy

If some browsers are already using the Traditional Proxy and have a proxy port set, or the administrator wants to direct some users' web requests through a specific port in order to increase control, the Transparent and the Traditional Proxy may be enabled simultaneously.

With both types of proxy enabled, users without a proxy port set in their browser will use the Transparent Proxy and users with the proxy port defined must use Traditional Proxy and will be restricted to using the port set in Content Filtering Preferences.

---

### Content Filtering Preferences Fields

---

#### Traditional Proxy

- Enable**      Select to enable the traditional proxy.
- Proxy Port**      Port through which the proxy will run. Default is 2784.

#### Transparent Proxy

- Enable**      Select to enable the transparent proxy.

#### Block Action

- Block Action**      Select “Use message” or “Redirect to URL.”
- Message**      Enter a custom message or select the default, “Local Policy denies access to web page.”
- URL**      Enter the address of the web page to which blocked users will be redirected.
- 

GNAT-Box Preferences	
Traditional Proxy	
Enable:	<input type="checkbox"/>
Port:	<input type="text" value="2784"/>
Transparent Proxy	
Enable:	<input type="checkbox"/>
Block action	
Block action:	<input type="text" value="Use message"/>
Message:	<input type="text" value="Local policy denies access to web page."/>
URL:	<input type="text"/>
<input type="button" value="Default"/> <input type="button" value="Save"/> <input type="button" value="Reset"/>	

*Content Filtering Preferences*

---

## Internet Access Policy

Once ACLs have been created, the Proxy has been selected, and Remote Access Filters have been created and enabled (if using Traditional Proxy), content filtering is activated and functional.

Remote Access and Outbound Filter choices may require further adjustment to allow or deny access to groups of users or to sites or categories, according to your company policy. See **GNAT BOX SYSTEM SOFTWARE USER'S GUIDE** and **3.4 ADDENDUM** for more information about filters.

## 4 Surf Sentinel Plus

### Using Surf Sentinel Plus

Surf Sentinel Plus offers all the benefits of Surf Sentinel, plus concise web-based reports on Internet usage. The administrator can see how the company's Internet connection is being used, and what percentage of traffic is in a specific category.

Reports are organized according to allowed/denied sites and individual IP addresses. Drilldowns allow the administrator to use a site URL as a hotlink to the site to verify content. Reports can be generated for the current date or a date range of up to 60 days.

### Login

Log in to your firewall and click Content Filtering under the Links section. Click Surf Sentinel, then the **Access Surf Sentinel Plus** link. The Web Reports system login screen will display. For quick access without logging on to the firewall, bookmark the system login page.

Enter the user name and password provided by GTA; these are case-sensitive and not user-modifiable. (If you have trouble logging in, verify that the user name matches the customer ID in the web address.)



Surf Sentinel

Web Filter Home

Home

System Login

Welcome to your Cerberian Web Filter Administration site. Please login using your Username and Password.

Name

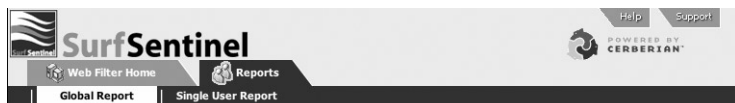
Password  [For help, click here](#)

Submit

*Cerberian Web Filter Login*

## Navigation

The primary navigation for Web Reports are tabs. The two main tabs are Web Filter Home and Reports. Web Filter Home includes the Home and Preferences tabs, while Reports includes the Global Report and Single User Report tabs.



### *Tabs*

Navigation links are provided at the bottom of each site page for **Web Filter Home**, **Reports**, **Help** and **Logout**. Cerberian online help is also accessible from the **Help** link at the top of each page and from the **How do I?** link.

Page specific navigation is also available at the bottom of each report page, and as chart and text links within reports. To maintain report parameters, use page navigation tools in preference to browser back and forward buttons.

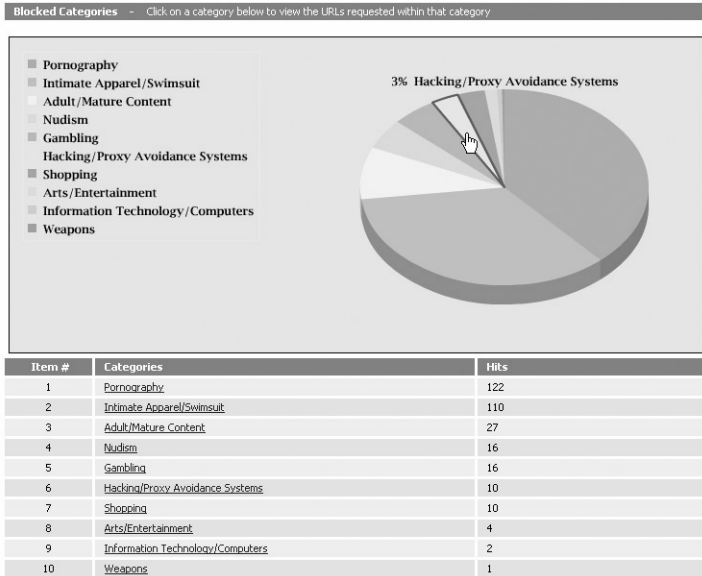
## Percentage Data

When legend items or pie chart sections are highlighted within reports, they provide percentage data on the category selected. To view a percentage in the selected report, hover the mouse pointer over a category in either a pie chart or legend. See illustration on the next page.

## Report Type, Date Range

Reports have selection dropdown lists for date range and/or report type. Click on the dropbox arrow and select from the list displayed: the Report Type selections allow you to generate a report for Blocked or Allowed categories; the Date Range selections allow you to generate a report for the current 24-hour day or a range of 3, 5, 7, 14 or 30 or 60 days.

Click **Run Report** or press <Return> to generate a report. Selected parameters persist through report drilldowns.



*Chart and Text Links*

## Web Filter Home

The opening page displays the Web Filter Home and Reports main tabs; under Web Filter Home, there are two selections: Home (the opening page) and Preferences.



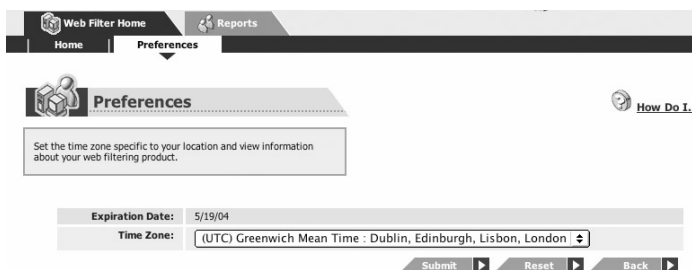
*Web Filter Home*

## Site Submissions

Use the **Site Submissions** link to check on the category of a URL or report a URL that requires categorization. (A link for website review is also available on the initial Surf Sentinel page.)

## Preferences

Preferences includes a time zone selection dropdown box and the date of expiration for the user's Surf Sentinel contract.



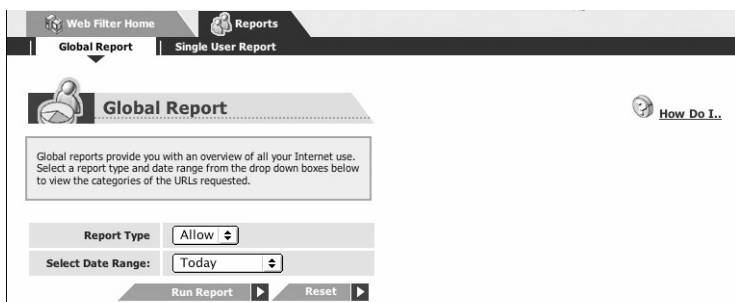
The screenshot shows the 'Preferences' dialog box. At the top, there are tabs for 'Web Filter Home' and 'Reports'. Below the tabs, the 'Preferences' tab is selected. The dialog box contains a text area with the instruction: 'Set the time zone specific to your location and view information about your web filtering product.' Below this, there are two dropdown menus: 'Expiration Date' set to '5/19/04' and 'Time Zone' set to '(UTC) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London'. At the bottom, there are three buttons: 'Submit', 'Reset', and 'Back'.

*Preferences*

## Global Report

Reports contains two selections: Global Report and Single User Report. The Global Report tab appears automatically.

A Global Report provides an overview of Internet use by user IP address. A Global Report can be run for either the Allowed or Blocked categories. The Date Range dropdown list allows you to generate a report for the current 24-hour day, or a range of 3, 5, 7, 14, 30 or 60 days. To create a Global Report, select a report type and date range, then click **Run Report**.



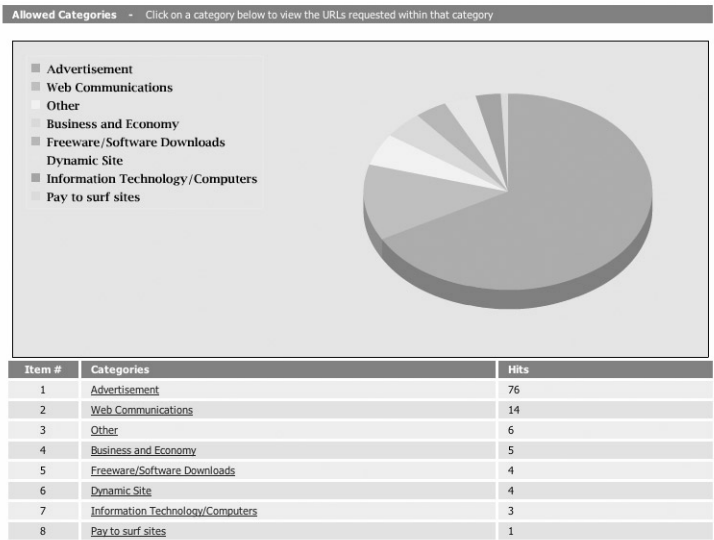
The screenshot shows the 'Global Report' dialog box. At the top, there are tabs for 'Web Filter Home' and 'Reports'. Below the tabs, the 'Global Report' tab is selected. The dialog box contains a text area with the instruction: 'Global reports provide you with an overview of all your Internet use. Select a report type and date range from the drop down boxes below to view the categories of the URLs requested.' Below this, there are two dropdown menus: 'Report Type' set to 'Allow' and 'Select Date Range' set to 'Today'. At the bottom, there are two buttons: 'Run Report' and 'Reset'.

*Global Report dialog*



When activated, the pie chart and legend at the top of the report display percentage of Internet use by category. The list below the chart displays categories (allowed or blocked) by number of hits.

To view a percentage in the selected report, hover the mouse pointer over a category in either a pie chart or legend.



*Global Report*

## Category URLs

Click a category in the list or in the pie chart above for a drilldown by URL of the sites requested and the number of hits. Each URL links to a report of users who accessed or attempted to access the selected site by workstation IP address. Each IP address is a link to a Single User Report for that category.



*IP Addresses*

## User Requests

Click an IP address link to display a **Single User Report** for that address. See the Single User Report illustration on the next page.

## Single User Report

A Single User Report provides details of the total Internet use for an individual IP address. The All Users list, all IP addresses by number of hits, displays by default. By default, the Single User Report is run for 60 days.

Global Report | Single User Report

**Single User Report** [How Do I...](#)

Single user reports provide details of a single user's Internet usage.

To find a user, enter the username in the search field below. You may also display all users by clicking on 'All'.

Search to find a specific User by Username. Or you may select All to display all users.

Search by Username:

All Users All

Submit Reset Back

Search Results » User Name

### *Single User Report dialog*

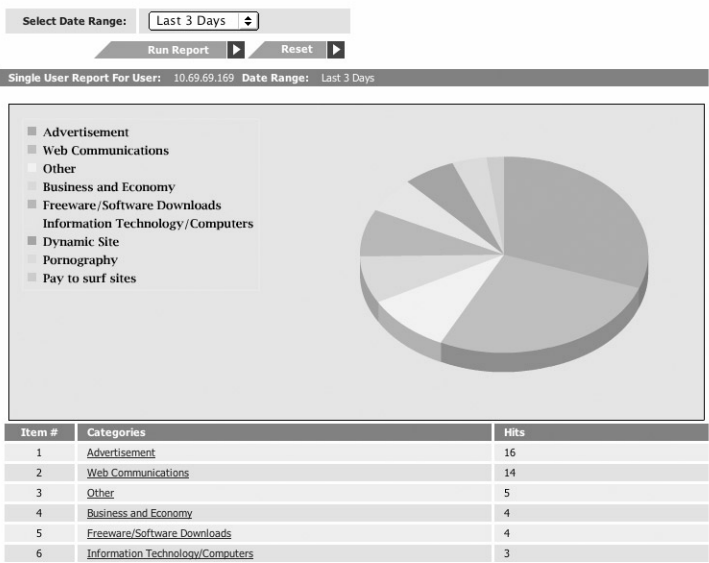
To run a Single User Report, select an IP address from the All Users list, or enter an IP address in the SEARCH BY USERNAME field and click **Submit**. The user IP address will display; click on it to display the report results.

In the report screen, use the Date Range dropdown list to generate a report for the current 24-hour day, or a range of 3, 5, 7, 14 or 30 days.

## Hits by Category

When activated, the pie chart and legend at the top of the report display percentage of Internet use by category. The list below the chart displays categories (allowed **and** blocked) by number of hits.

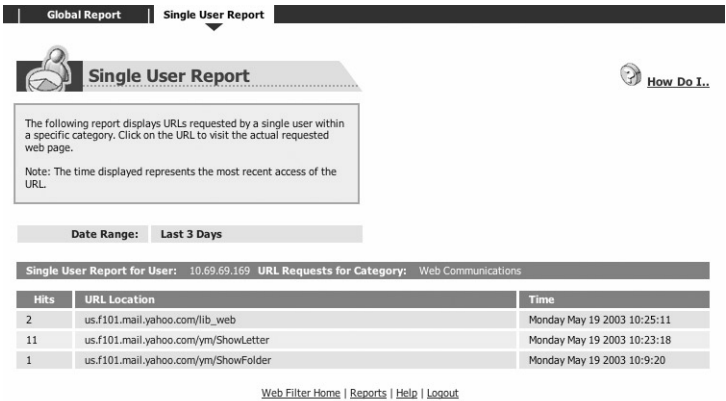
Identical times listed indicate that more than one page of a site loaded or attempted to load almost simultaneously. This can happen when one site loads several windows (pop-ups) or page elements, such as stock tickers, graphics, frames and dynamic content.



Single User Report

# User Requests

Click a category in the list or in the pie chart above to display each site or page in this category that the user visited or attempted to visit, by time and date. The site URL links on this page will open in a new browser window. The administrator can use URLs to learn more about the site, if necessary. To see more URLs (if any), click the **Next** button.



Single User Report



# Appendix

## Categories

Surf Sentinel contains 53 categories for the administrator to use when customizing access control lists. A special category for pages that do not fit neatly into a category and for requests that do not return a rating is “Rating Unavailable.” Category descriptions are up-to-date as of June 2003.

When Surf Sentinel is first activated, each category is placed by default into either the “allowed” or the “denied” list in the ACL. Default settings are based on Cerberian classifications. Categories classified as “Potential Liability or Objectionable Content” are denied by default. Categories classified as “Potentially Non-productive” are allowed by default.

### **Caution**

GTA strongly recommends reviewing default category settings and modifying them to match your company's Internet Access Policy.

## Denied by Default

The default blocked list contains the following categories:

	Category	Description of Sites
	Adult/Mature Content	Contain sexually explicit information that is not of a medical or scientific nature.
	Alcohol/Tobacco	Promote or offer for sale alcohol/tobacco products or the means to create them; supply recipes or paraphernalia; glorify, tout, or encourage consumption or intoxication.
	Gambling	Allow user to place a bet or participate in a betting pool (including lotteries) online; provide information, assistance or recommendations on placing a bet; instruct, assist or train to participate in games of chance. Does not include gambling products or machines sales.*

Hacking/Proxy Avoidance Systems	Provide information on illegal or questionable access to, or use of, communications equipment/software; how to bypass proxy server features; or how to gain access to URLs in any way that bypasses the proxy server.
Illegal Drugs	Promote, offer, sell, supply, encourage or otherwise advocate the recreational or illegal use, cultivation, manufacture or distribution of drugs, pharmaceuticals, intoxicating plants, chemicals or related paraphernalia.
Illegal/Questionable	Advocate or advise on performing illegal acts such as service theft, evading law enforcement, fraud, burglary techniques and plagiarism and cheating. Provide instructions about or promote crime, unethical/dishonest behavior or evasion of prosecution thereof.
Intimate Apparel/Swimsuit	Offer pictures of models in lingerie, swimwear or other types of suggestive clothing. Category does not include sites selling undergarments as a sub-section of other products offered.*
Nudity	Contain nude or semi-nude depictions of the human body which are not necessarily sexual in intent or effect. Category includes nudist or naturist sites that contain revealing pictures and may also include sites containing nude paintings or photos of an artistic nature.
Pornography	Contain sexually explicit material for the purpose of arousing a sexual or prurient interest.
Sex Education	Provide information on reproduction, sexual development, sexually transmitted disease, contraception, safe sex practices, sexuality and sexual orientation. Category does not include sites offering tips on having better sex.*
Violence/Hate/Racism	Advocate or instruct on physical harm to people or property through use of weapons, explosives, pranks or other types of violence.
Weapons	Sell, review or describe weapons such as guns, knives or martial arts devices, or provide information on the use or modification of these weapons.

\* Excluded subgroups are covered in another category.

## Allowed by Default

The default allowed list contains the following categories:

	Category	Description of Sites
	Abortion	Provide information or arguments in favor of, or against, abortion; describe abortion procedures; offer help in obtaining or avoiding abortion; provide testimonials on the physical, social, mental, moral, or emotional effects, or the lack thereof, of abortion.
	Advertisement	Specifically designed as ads, such as pop-up advertisements or banners.
	Arts & Entertainment	Promote and provide information about motion pictures, television, music and programming guides, non-news radio, books, magazines, circuses, theatre, broadcasting firms, online museums, galleries, artist sites, and reviews on entertainment.
	Business & Economy	Devoted to individual business firms excluding e-commerce sites and those involved in the sale of tobacco or alcohol, travel services, weaponry or vehicles.*
	Chat/Instant Messaging	Provide chat and Instant Messaging capability.
	Computing & Internet	Sponsor or provide information on computers, technology, the Internet and technology-related organizations.
	Cult/Occult	Promote or offer methods, means of instruction, or resources to affect or influence real events through the use of spells, curses, magic powers or supernatural beings.
	Cultural Institutions	Promote or provide information about museums, galleries, theatres (not movie theatres*) and other cultural institutions or groups.
	Education	Provide distance education and trade school information or programs. Sponsored by schools, educational facilities, faculty or alumni groups.
	Email	Offer Web-based email services.
	Financial Data & Services	Provide information on financial data and services (banking, mortgages, loans, etc.). Allow users to perform banking-related functions online.

	Freeware/ Software Downloads	Offer or promote free software or products for general download or trial purposes.
	Gay & Lesbian Issues	Provide information on or cater to gay and lesbian lifestyles. Does not include sexually-oriented sites.*
	Government/Legal	Sponsored by or providing information on government, governmental agencies, political parties, interest groups focused on elections or legislation, local, national and international political sites, as well as government services such as taxation and emergency services.
	Health	Provide advice and information on fitness, personal health, medical services, alternative and complementary therapies, medical insurance, dentistry, optometry and medical information about ailments, conditions and legal non-prescription and prescription drugs, as well as general psychiatry, mental well-being, psychology, self-help books and self-help organizations.
	Humor/Jokes	Focus primarily on comedy, jokes, fun, etc. Does not include sites with jokes of a mature or adult nature.*
	Internet Auctions	Support the offering and exchange of goods between individuals.
	Job Search/ Careers	Provide assistance in finding employment and tools for locating prospective employers through the use of employment search engines and boards.
	Kid Friendly	Designed specifically for children.
	MP3/Streaming	Support or allow users to download music and media files such as MP3, MPG, MOV, etc. Also sites that provide streaming media (radio, movie, TV).
	Military	Promote or provide information about military branches or the armed services.
	News & Media	Reports, information or commentary on current events or contemporary issues. Items like sports, weather, editorials and human interest, within the context of major news sites, are assigned to this category.
	News Groups	Offer access to Usenet News Groups or similar sites.



	Online Brokerage & Trading	Offer online trading of securities and management of investments. Category includes sites that offer financial investment strategies, quotes and news.
	Online Games	Provide information and support game playing or downloading, video, computer and electronic games, tips and advice on games or how to obtain cheat codes, journals and magazines dedicated to game playing, online games, as well as sites that support or host online games, including sweepstakes and giveaways.
	Pay to surf sites	Pay users for clicking on specific links or locations.
	Personals & Dating	Promote interpersonal relationships. Does not include sites pertaining to gay and lesbian issues.*
	Political/Advocacy Groups	Sponsored by or devoted to organizations that promote change or reform in public policy, public opinion, social practice, economic activities and relationships. Excludes commercially sponsored sites dedicated to electoral politics or legislation.
	Rating Unavailable	Either not yet categorized, or rating is temporarily unavailable.
	Real Estate	Provide information on renting, buying and selling real estate or properties.
	Reference	Contain personal, professional or educational reference, including online dictionaries, maps, language translation, censuses, almanacs, library catalogs and topic-specific search engines.
	Religion	Promote and provide information on religious or quasi-religious subjects; churches, synagogues or other houses of worship; conventional or unconventional religions such as Buddhism, Baha'i, Christianity, Christian Science, Hinduism, Islam, Judaism, Mormonism, Shinto, Sikhism or Atheism; and including "alternative" faiths or religious beliefs such as Wicca and witchcraft.
	Restaurants & Dining	List, review, advertise or promote food, catering or dining services.
	Search Engines & Portals	Support searching the Web or news groups, or indices or directories thereof.

	Shopping	Provide the means to obtain, either by online transaction, fax, phone, email or physical address, products or services that satisfy human wants or needs. This does not include products or services principally marketed to satisfy industrial or commercial needs.*
	Society & Lifestyle	Provide information on matters of daily life. Category does not include sites relating to entertainment, sports, jobs or sex.*
	Sports/Recreation	Promote or provide information about spectator sports.
	Travel	Promote or provide travel planning, particularly finding and making travel reservations.
	Vehicles	Provide information on or promote vehicles, including those sites that support online purchase of vehicles or parts.
	Web Communications	Offer or allow web-based communications.
	Web Hosting	Host personal Web pages or Web communities.

\* Excluded subgroups are covered in another category.

# Index

## A

- acceptable use. *See* access policy
- Access Control Lists 5, 7, 10
- access policy 7
  - multiple policies 11
- ACL. *See* Access Control Lists
  - number 11
- activation code 5, 9
- ActiveX 12
- Allowed categories 18
- armed services (category-related) 28
- autos (category-related) 30

## B

- bandwidth 7
- betting, gambling (category-related) 25
- Blocked categories 18
- Block Action 15

## C

- cars (category-related) 30
- case-sensitive 17
- cat\_action 7
- cat\_site 7
- categories, number of 1, 25
- Cerberian 1, 7
- children (category-related) 28
- code, activation 2
- computer crime (category-related) 26
- computer games (category-related) 29
- Console interface 3, 9
- content categories, number 1
- Content Filtering 4
- contract, Surf Sentinel 20
- controlled group 10
- conventions, documentation 3

## D

- date range 17, 18, 20
- defaults, installation 11
- denied by default 25
- dictionaries (category-related) 29

DNS server 10

- documentation
  - additional 3
  - map 3

Drivers 4

DRTR, Dynamic Real-Time Rating 7

drugs, prescription (category-related) 28

dstname 7

## E

- enable Surf Sentinel 5
- explicit material 25

## F

- factory settings 11
- feature code. *See* activation code
- format, log 7

## G

- GBAdmin 4
- GBAdmin interface 4
- Global Report 18, 20, 21
- guns (category-related) 26

## H

- High Availability 4
- HTTP proxy 6

## I

- IM (category-related) 27
- Internet access policy 7, 25
- Internet (category-related) 27

## J

JAVA 12

## L

- LCL. *See* Local Content Lists
- legend 18, 21, 22
- liability, legal 1, 7
- libraries 7
- libraries (category-related) 29
- list order 10
- Local Content Lists 1, 5, 10, 12
- logging 5, 6
- login 2, 17
- log format, WELF 7

## M

- mailing list 3

message log 6  
Mobile Code Blocking 12  
movies (category-related) 27  
msg 7  
multiple policies 11

## N

notes 2, 3, 5  
number  
    activation 2  
    content categories 1  
    of ACLs 11  
    of content categories 1  
    serial 2

## O

on switch 5  
op 7  
order is important, filters 14  
order to enable service 10  
Outbound Filter 14, 16  
override 11, 13

## P

paraphernalia (category-related) 26  
PDF 3  
percentage data 18  
pie chart 18, 21, 23  
pop-ups (category-related) 27  
pop-up windows 7  
port  
    2784 14  
    443 12  
    80 5, 12, 13  
    8000 12  
    8080 12  
    none for Transparent Proxy 14  
pri 7  
productivity 1  
proto 7  
proxy  
    both types of 15  
    port 14  
    transparent 6, 10, 13

## R

RAF. *See* Remote Access Filter  
    for Traditional Proxy 14  
redirect URL 13  
Registration, Product 2  
Remote Access Filter 10, 14

remote logging 6  
report type 18, 20

## S

schools 7  
schools (category-related) 27  
serial number 2  
server locations 1  
settings, factory default 11  
Single User Report 22  
Site Submissions 20  
Source address 10  
src 7  
srcport 7  
SSL encryption 13  
start Surf Sentinel 5  
subscription 1  
support 2  
Surf Sentinel  
    enable 5  
survey for access policy 8

## T

TCP port 80 5, 13  
Technical support ii  
time zone 20  
Traditional Proxy 6, 15  
Transparent Proxy 6, 10, 13, 15  
turn on Surf Sentinel 5

## U

Usenet (category-related) 28

## V

VPN 4

## W

Web Filter Home 19  
Web interface 4  
Web Reports 18  
WELF ii