SonicWALL Content Filter List

Administrator's Guide

Table of Contents

Copyright Notice

Limited Warranty

SonicWALL, Inc. warrants that SonicWALL Network Anti-Virus will perform in accordance to the accompanying written materials for a period of ninety (90) days from the date of receipt.

SonicWALL Inc.'s and its suppliers' entire liability and your exclusive remedy shall be, at SonicWALL's option, either a) return of the price paid, or b) repair or replacement of the PRODUCT that does not meet SonicWALL's Limited Warranty and which is returned to SonicWALL with a copy of your receipt. This Limited Warranty is void if failure of the PRODUCT has resulted from accident, abuse, or misapplication. Any replacement PRODUCT shall be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer.

In no event shall SonicWALL or its suppliers be liable for any damages whatsoever (including, without limitation, special, incidental, indirect, or consequential damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use the PRODUCT.

Some states do not allow the exclusion or limitation of implied warranties or liability for incidental or consequential damages, so the above limitation or exclusion may not apply to you. Where liability may not be limited under applicable law, SonicWALL's liability shall be limited to the amount you paid for the Product. This warranty gives you specific legal rights, and you may have other rights which vary from state to state.

By using this Product, you agree to these limitations of liability.

THIS WARRANTY AND THE REMEDIES SET FORTH ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, ORAL OR WRITTEN, EXPRESS OR IMPLIED.

No dealer, agent, or employee of SonicWALL is authorized to make any extension or addition to this warranty..

Phone:	1-408-752-7819
Fax:	1-408-745-9300
Support:	http://www.sonicwall.com/support/

This warranty does not apply if the SonicWALL is damaged by accident, abuse, misuse, misapplication, or is modified without the written permission of SonicWALL, Inc.

In no event shall SonicWALL, Inc. or its suppliers be liable for any damages, whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or other pecuniary loss) arising out of the use of the SonicWALL, or the inability to use the SonicWALL.

Some states do not allow the exclusion or limitation of implied warranties or liability for incidental or consequential damages, so the above limitation or exclusion may not apply to you. Where liability may not be limited under applicable law, SonicWALL liability is limited to the amount paid for the product. This warranty gives you specific legal rights, and you may have other rights which vary from state to state.

By using the SonicWALL Internet Security Appliance, you agree to the limitations of liability.

THIS WARRANTY AND THE REMEDIES SET FORTH ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, ORAL OR WRITTEN, EXPRESSED OR IMPLIED.

No dealer, agent, or employee of SonicWALL, Inc. is authorized to make any extension or addition to this warranty.

Introduction

The SonicWALL Internet Security Appliance supports Internet Content Filtering via an optional Content Filter List subscription.

Internet content filtering allows schools and business to create and enforce Internet access policies tailored to the needs of the organization. The SonicWALL administrator selects categories to block or monitor, such as pornography or racial intolerance, from a pre-defined list.

Content filtering can improve employee productivity, and help keep children from accessing inappropriate sites. It can help companies avoid litigation from employees whose co-workers are downloading objectional content in the workplace. While blocking objectional sites is important, activities such as chat, auction bidding, and personal finance can also be filtered.

Due to the constantly changing Internet and websites, the optional Content Filter List subscription automatically updates the SonicWALL CyberNOT Filter List on a weekly basis to ensure that access restrictions are up to date and properly enforced.

The Content Filter Administrator Guide covers the activation, installation, and configuration of the SonicWALL Content Filtering feature, including the optional Content Filter List subscription.

Phone:	(408) 745-9600
Fax:	(408) 745-9300
Web:	http://www.sonicwall.com
E-mail:	sales@sonicwall.com

SonicWALL Technical Support

For timely resolution of technical support questions, visit SonicWALL on the Internet at <http://www.sonicwall.com/support>. Resources are available to help you resolve most technical issues, as well as a way to contact one of the SonicWALL Technical Support engineers.

Getting Started

Before You Start

Before you can configure the SonicWALL **Content Filter List**, the subscription requires you to register your SonicWALL Internet Security Appliance at <http://www.mysonicwall.com.> At this web site, you can create a user account to activate and manage services for all of your SonicWALL Internet Security Appliances.

Note: *For the latest version of this manual and other SonicWALL documentation, go to <http://www.sonicwall.com/products/documentation.html>*

What is mySonicWALL.com?

mySonicWALL.com delivers a convenient, centralized way to register all your SonicWALL Internet Security Appliances and Security Services. It eliminates the hassle of registering individual SonicWALL appliances and upgrades, and streamlines the management of all your SonicWALL security services. Using mySonicWALL.com allows you to have a single user profile where you can manage all your product registrations and security services.

What Can I Do with mySonicWALL.com?

You can use MySonicWALL.com to do the following:

•**Register** all your SonicWALL appliances and services in one place.

•**Access** firmware and security service updates.

•**Get** SonicWALL alerts on services, firmware, and products.

•**Check** status of your SonicWALL services and upgrades linked to each registered SonicWALL Internet security appliance.

•**Manage** (activate, change or delete) your SonicWALL security services online.

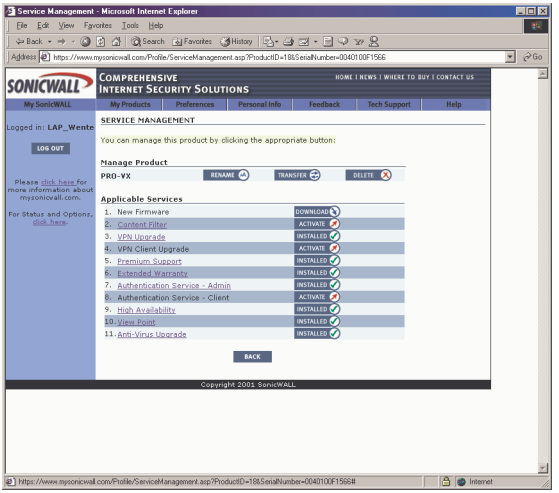
How do I Get Started with mySonicWALL.com?

The first step to using mySonicWALL.com is creating a user account. Go to <http://www.mysonicwall.com> and follow the instructions for setting up a new user account.

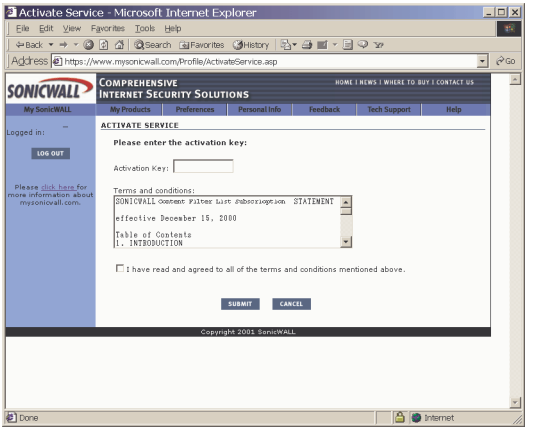
Activating the Content Filter List Subscription

To activate the **Content Filter List** subscription, you must first register your activation key on the SonicWALL website at the SonicWALL registration site <http://www.mysonicwall.com.> Follow the instructions below to activate the Content Filter subscription.

1. Log into your user account, and select the SonicWALL appliance to activate the Content Filter subscription. Click **Activate** next to **Content Filter** in the list of **Applicable Services**.



2. Type the **Activation Key** in the **Activation Key** field, and click **Submit**.



3. Your Content Filter List subscription is activated. You can now download the Filter List through the SonicWALL Management Station.

Managing Content Filtering

This section contains detailed information on the configuration of the SonicWALL **Content Filtering** feature. A Web browser is used to access the SonicWALL Management interface, and the commands and functions of Content Filtering.

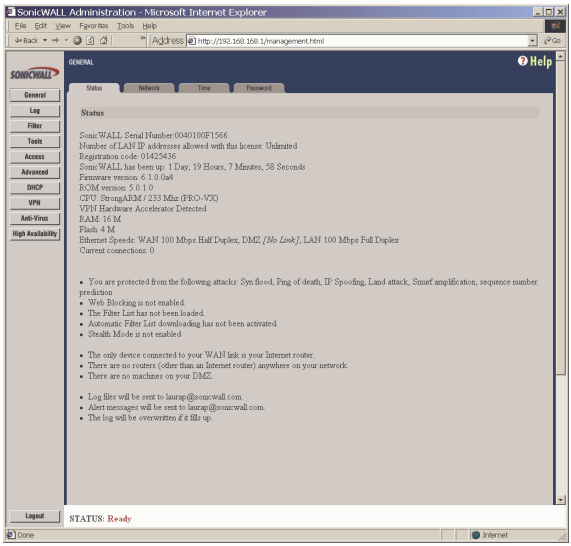
The following sections are in this chapter:

- **Accessing the SonicWALL using a Web browser**
- **Enabling Content Filtering and Blocking**
- **Content Filter List Updates**
- **Customizing the Filter List**
- **Blocking URLs with Keywords**

Accessing the SonicWALL using a Web Browser

Open a Web browser and enter the SonicWALL IP address into the **Address** field, then press **Enter**. When the **Password** dialogue box appears, enter **admin** into the **User Name** field, and enter the administrator password in the **Password** field. Click **Login** to open the Management Station interface.

Click **General** on the left side of the Management interface, and then **Status**.



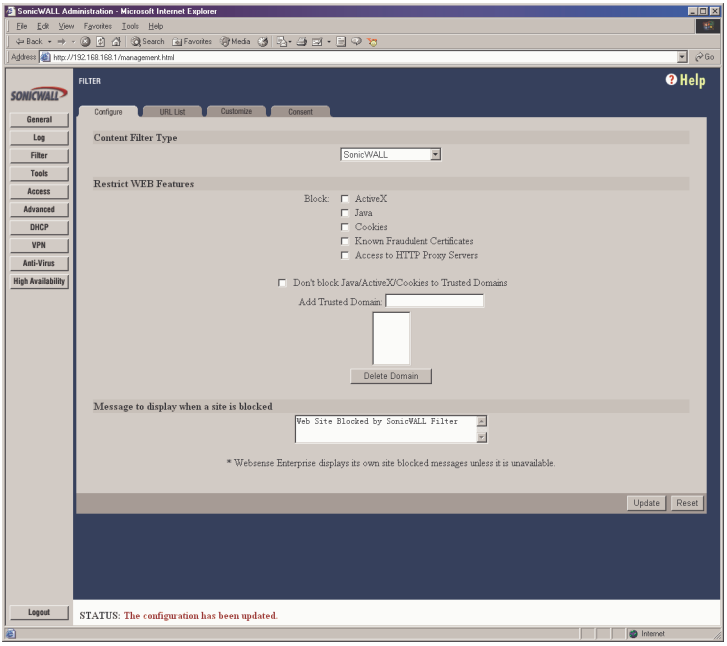
The active tab, **Status**, displays the current status of the SonicWALL. It contains an overview of the SonicWALL settings and configurations as well as any messages generated by the SonicWALL. Be sure to review the **Status** tab after making changes to the SonicWALL to verify that changes are updated by the SonicWALL.

If the message, "This SonicWALL is not yet registered.", is displayed, you must complete the online registration process using the web-based registration form located at <http://www.mysonicwall.com> to register your SonicWALL. After the SonicWALL is registered, you can activate your Content Filter List subscription by clicking **Activate**, and entering your **Activation Key** from the back of this manual. Your SonicWALL can now be managed from the central registration Web site.

Note: *The SonicWALL is not shipped with the Content Filter Subscription activated. Once the subscription is activated on the registration site, an account is created that allows the Content Filter List to be downloaded.*

Configuring SonicWALL Content Filter

Click **Filter** on the left side of the browser window, and then click on the **Configure** tab.



Note: *Content Filtering applies only to URL requests from devices behind the SonicWALL LAN.*

Configure the following settings on the **Configure** pane:

Content Filter Type

There are now three Content Filter Lists available for selection:

- **SonicWALL** - Selecting **SonicWALL** for the **Content Filter List Type** allows you use the URL list and completely customize your Content Filter feature including allowed and forbidded domains as well as filtering using keywords.
- **N2H2** - **N2H2** is a third party content filter list package supported by SonicWALL. You can obtain more information on N2H2 at <http://www.n2h2.com>. If you select N2H2 from the list, an **N2H2** tab is available to configure the location of the N2H2 server and other settings.

•**Websense Enterprise** - Websense Enterprise is also a third party Internet filtering package supported by SonicWALL. You can obtain more information on Websense Enterprise at <http://www.Websense.com>.

If you select **Websense Enterprise** from the list, a **Websense** tab is available to configure the location of the Websense server and other settings.

Restrict Web Features

Block:

•**ActiveX**

ActiveX is a programming language that embeds scripts in Web pages. Malicious programmers can use ActiveX to delete files or compromise security. Select the **ActiveX** check box to block ActiveX controls.

•**Java**

Java is used to download and run small programs, called applets, on Web sites. It is safer than ActiveX since it has built-in security mechanisms. Select the **Java** check box to block Java applets from the network.

•**Cookies**

Cookies are used by Web servers to track Web usage and remember user identity. Cookies can also compromise users' privacy by tracking Web activities. Select the **Cookies** check box to disable Cookies.

•**Known Fraudulent Certificates**

Digital certificates help verify that Web content and files originated from an authorized party. Enabling this feature protects users on the LAN from downloading malicious programs warranted by these fraudulent certificates. If digital certificates are proven fraudulent, then the SonicWALL blocks the Web content and the files that use these fraudulent certificates.

Known fraudulent certificates blocked by SonicWALL include two certificates issued on January 29 and 30, 2001 by VeriSign to an impostor masquerading as a Microsoft employee.

•**Access to HTTP Proxy Servers**

When a proxy server is located on the WAN, LAN users can circumvent content filtering by pointing their computer to the

proxy server. Check this box to prevent LAN users from accessing proxy servers on the WAN.

- **Don't Block Java / ActiveX / Cookies to Trusted Domains**

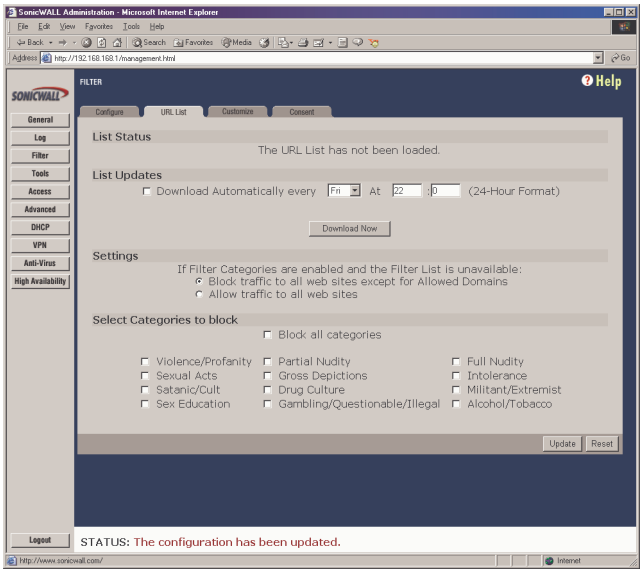
  Select this option if you have trusted domains using Java, ActiveX, and Cookies. To add a trusted domain, enter the domain name into the **Add Trusted Domain** field. Click **Update** to add the domain to the list of trusted domains. To delete a domain, select it from the list, and then click **Delete**.

Message to display when a site is blocked

Enter your customized text to display to the user when access to a blocked site is attempted. The default message is **Web Site blocked by SonicWALL Filter**. Any message, including embedded HTML, up to 255 characters long, can be entered in this field.

URL List

The **URL List** page allows you to see the status of the Content Filter List as well as configure a specific time to download the list. You can also determine how the SonicWALL responds when a Content Filter List is unavailable. Selecting categories to block is also configured on this page.



List Status

This section of the **URL List** tab indicates the status of the URL list. If the Content Filter List is loaded, a status message is displayed in this section.

List Updates

Download Automatically every

Selecting **Download Automatically every** allows you to configure a specific time to download your Content Filter List. Select a day of the week and a time (24-hour format), for example, Sun. at 22:00 hours.

Or, you can click Download Now to immediately download your Content Filter List.

Note: *It is recommended to download the URL List at a time when access to the Internet is at a minimum as downloading the URL List disrupts connectivity to the Internet.*

Settings

If you have enabled blocking by Filter Categories and the URL List becomes unavailable, there are two options available:

- **Block traffic to all web sites except for Allowed Domains**

  Selecting this option blocks traffic to all web sites until the URL List is available.

- **Allow traffic to all web sites**

  Selecting this option allows traffic to all web sites without the URL List. However, **Forbidden Domains** and **Keywords**, if enabled, are still blocked.

Select Categories to block

- **Block all categories**

  The SonicWALL uses a **URL List** generated by CyberPatrol to block access to objectional Web sites. CyberPatrol classifies objectional Web sites based upon input from a wide range of social, political, and civic organizations. Select the **Block all categories** check box to block all of these categories. Alternatively, you can select categories individually by selecting the appropriate check box.

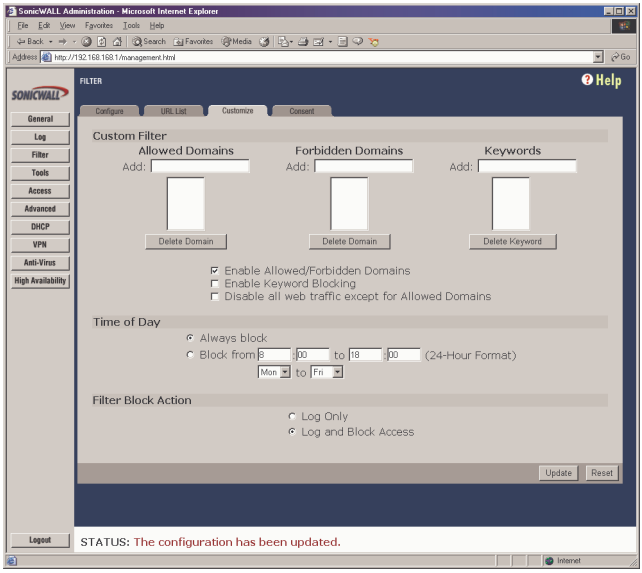
The following is a list of the **Content Filter List** categories:

Violence / Profanity	**Satanic / Cult**
Partial Nudity	**Drugs / Drug Culture**
Full Nudity	**Militant / Extremist**
Sexual Acts	**Sex Education**
Gross Depictions	**Questionable / Illegal Gambling**
Intolerance	**Alcohol & Tobacco**

Visit<http://www.sonicwall.com/Content-Filter/categories.html> for a detailed description of the criteria used to define Content Filter List categories.

Customizing the Content Filtering List

The **Customize** tab allows you to customize your URL List by manually entering domain names or keywords to be blocked or allowed.



Custom Filter

You can customize your URL list to include Allowed Domains, Forbidden Domains, and Keywords. By customizing your URL list, you can include specific domains to be allowed (accessed), forbidden (blocked), and include specific keywords to be used to block sites.

Customize window allows you to customize the Content Filter List by manually blocking or allowing Web site access.

To allow access to a Web site that is blocked by the Content Filter List, enter the host name, such as "www.ok-site.com", into the Allowed Domains fields. 256 entries can be added to the Allowed Domains list.

Note: *An Allowed Domain is not the same as a Trusted Domain. You may allow access to a domain (Allowed Domain), but block ActiveX, Java, cookies, etc.*

To block a Web site that is not blocked by the **Content Filter List**, enter the host name, such as "www.bad-site.com" into the **Forbidden Domains** field. 256 entries can be added to the **Forbidden Domains** list.

Note: *Do not include the prefix "http://" in either the Allowed Domains or Forbidden Domains the fields. All subdomains are affected. For example, entering "yahoo.com" applies to "mail.yahoo.com" and "my.yahoo.com".*

To remove a trusted or forbidden domain, select it from the appropriate list, and click **Delete Domain**. Once the domain has been deleted, a message is displayed at the bottom of the Web browser window.

To enable blocking using **Keywords**, select the **Enable Keyword Blocking** check box.

Enter the keyword to block in the **Add Keyword** field, and click **Update**. Once the keyword has been added, a message confirming the update is displayed at the bottom of the browser window.

To remove a keyword, select it from the list and click **Delete Keyword**. Once the keyword has been removed, a message confirming the update is displayed at the bottom of the browser window.

Click **Update**. Once the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the browser window.

Note: *Customized domains do not have to be re-entered when the Content Filter List is updated each week and do not require a URL list subscription.*

- **Enable Allowed/Forbidden Domains**

To deactivate **Custom Filter** customization, clear the **Enable Allowed/Forbidden Domains**, and click **Update**. This option allows you to enable and disable customization without removing and re-entering custom domains.

- **Enable Keyword Blocking**

  Select the **Enable Keyword Blocking** if you want to block Web traffic based on your list of customized keywords.

- **Disable all web traffic except for Allowed Domains**

  When the **Disable Web traffic except for Allowed Domains** check box is selected, the SonicWALL only allows Web access to sites on the **Allowed Domains** list. With careful screening, this can be nearly 100% effective at blocking pornography and other objectional material.

Time of Day

The Time of Day feature allows you to define specific times when Content Filtering is enforced. For example, you could configure the SonicWALL to filter employee Internet access during normal business hours, but allow unrestricted access at night and on weekends.

Note: *Time of Day restrictions only apply to the Content Filter List, Customized blocking and Keyword blocking. Consent and Restrict Web Features are not affected.*

- **Always Block**

  When selected, **Content Filtering** is enforced at all times.

- **Block Between**

  When selected, **Content Filtering** is enforced during the time and days specified. Enter the time period, in 24-hour format, and select the starting and ending day of the week that Content Filtering is enforced.

Filter Block Action

- **Log Only**

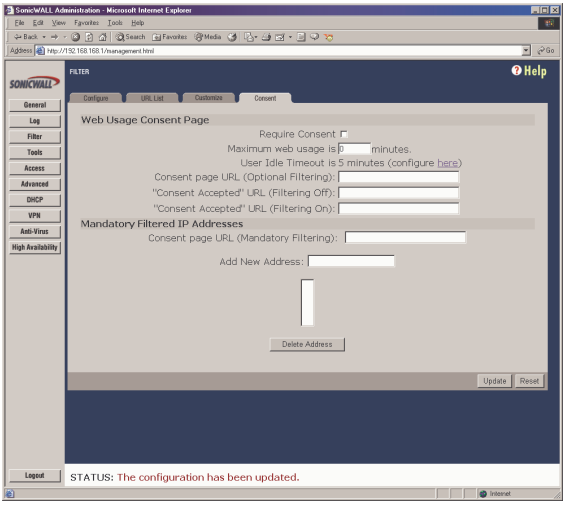
  If this check box is selected, the SonicWALL logs and then allows access to all sites on the Content Filter, custom, and keyword lists. The **Log Only** check box allows you to monitor inappropriate usage without restricting access.

- **Log and Block Access**

  Select the check box and the SonicWALL blocks access to sites on the Content Filter, custom, and keyword lists. The SonicWALL then logs attempts to access these sites.

Consent

The **Consent** tab allows you to enforce content filtering on designated computers and provide optional filtering on other computers. Consent can be configured to require the user to agree to the terms outlined in an **Acceptable Use Policy** window before Web browsing is allowed. Click **Filter** on the left side of the browser window, and then click the **Consent** tab.



Web Usage Consent Page

- **Require Consent**

Select the **Require Consent** check box to enable the **Consent** features.

- **Maximum Web usage**

In an environment where there are more users than computers, such as a classroom or library, time limits are often imposed. The SonicWALL can be used to remind users when their time has expired by displaying the page defined in the **Consent** page URL field. Enter the time limit, in minutes, in the **Maximum Web usage** field. When the default value of zero (0) is entered, this feature is disabled.

- **User Idle Timeout is 5 minutes (configure here)**

  After a period of Web browser inactivity, the SonicWALL requires the user to agree to the terms outlined in the **Consent** page before any additional Web browsing is allowed. To configure the value, follow the link to the **Users** window and enter the desired value in the **User Idle Timeout** section.

- **Consent page URL (Optional Filtering)**

  When a user opens a Web browser on a computer requiring consent, they are shown a consent page and given the option to access the Internet with or without content filtering. You must create this Web

(HTML) page. It can contain the text from, or links to an Acceptable Use Policy (AUP).

This page must contain links to two pages contained in the SonicWALL, which, when selected, tell the SonicWALL if the user wishes to have filtered or unfiltered access. The link for unfiltered access must be <192.168.168.168/iAccept.html> and the link for filtered access must be <192.168.168.168/iAcceptFilter.html>, where the SonicWALL LAN IP Address is used instead of "192.168.168.168".

- **"Consent Accepted" URL (Filtering Off)**

  When a user accepts the terms outlined in the **Consent** page and chooses to access the Internet without the protection of **Content Filtering**, they are shown a Web page confirming their selection. Enter the URL of this page in the **"Consent Accepted" (Filtering Off)** field. This page must reside on a Web server and be accessible as a URL by users on the LAN.

- **"Consent Accepted" URL (Filtering On)**

  When a user accepts the terms outlined in the **Consent** page and chooses to access the Internet with the protection of Content Filtering, they are shown a Web page confirming their selection. Enter the URL of this page in the **"Consent Accepted" (Filtering On)** field. This page must reside on a Web server and be accessible as a URL by users on the LAN.

Mandatory Filtered IP Addresses

- **Consent page URL (Mandatory Filtering)**

  When a user opens a Web browser on a computer using mandatory content filtering, a consent page is displayed. You must create the Web page that appears when the web browser is opened. It can contain the

text from an Acceptable Use Policy, and notification that violations are logged or blocked.

This Web page must reside on a Web server and be accessible as a URL by users on the LAN. This page must also contain a link to a page contained in the SonicWALL that tells the SonicWALL that the user agrees to have filtering enabled. The link must be <192.168.168.168/iAcceptFilter.html>, where the SonicWALL LAN IP Address is used instead of "192.168.168.168".

Enter the URL of this page in the **Consent** page URL (Mandatory Filtering) field and click **Update**. Once the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the Web browser window.

- **Add New Address**

  The SonicWALL can be configured to enforce content filtering for certain computers on the LAN. Enter the IP addresses of these computers in the

  Add New Address field and click **Submit** button. Up to 128 IP addresses can be entered.

  To remove a computer from the list of computers to be filtered, highlight the IP address in the **Mandatory Filtered IP Addresses** list and click **Delete Address**.

Content Filter Subscription Activation Key

SonicWALL, Inc.
1160 Bordeaux Drive
Sunnyvale, CA 94089-1209
Phone: 408-745-9600
Fax: 408-745-9300
E-mail: sales@sonicwall.com
Web: http://www.sonicwall.com

Part # 232-000296-00
Rev A. 03/02