

TechNote

Introduction

The Consent Page is described in the Content Filter Service (CFS) section of the SonicOS Standard or Enhanced Administrator's Guide. This feature can be used to display warnings and terms of use information. This feature does not require the administrator to configure user accounts. It can be easily implemented for Wireless Guest Services, for example in libraries or hotels. It will block access to the Internet until the user acknowledges the notice and provides consent. The administrator can configure several options including bypassing the content filter.

Requirements

- SonicWALL appliance with CFS license
- Web page containing the terms of use and links to the appropriate pages on the SonicWALL for accepting or declining content filtering
- A Web Server (IIS or 3rd party) to publish the above page
- Internet connectivity

This article was tested with the following settings in a Lab environment:

- SonicWALL LAN IP: 192.168.168.168
 - Web Server IP: 192.168.168.101
- Note:** This Web server can be placed on the WAN of the SonicWALL.

Procedure

The SonicWALL security appliance can be configured to optionally enforce content filtering for all computers on the LAN. When a user opens a Web browser on a computer using optional content filtering, a specified Web page is displayed. You must create the Web page that appears when the Web browser is opened. It can contain text from the company's terms of use 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 or WLAN. Placing the Web page on an external Internet server is acceptable. This page must also include a link to a consent page contained in the SonicWALL security appliance that tells the device that the user does or does not agree to have filtering enabled. The link agreeing to filtering must be <192.168.168.168/iAcceptFilter.html> and the link providing unfiltered access must be <192.168.168.168/iAccept.html>, where the SonicWALL LAN IP Address is used instead of 192.168.168.168.

To configure a consent page and content filtering:

1. Create a Web page with the company's terms of use, name it **Opt.html** and publish it on the Web server so that the page is accessible as a URL on the network. Figure 1.1 shows a sample Optional Content Filtering page.

Try accessing the optional filtering page from the network by pointing your browser to:
http://(Web server IP)/Opt.html

The **Click Here** hyperlink signifying agreement to have content filtering applied must be:
http://(SonicWALL LAN IP)/iAcceptFilter.html

The link requesting Internet access without filtering must be:
http://(SonicWALL LAN IP)/iAccept.html

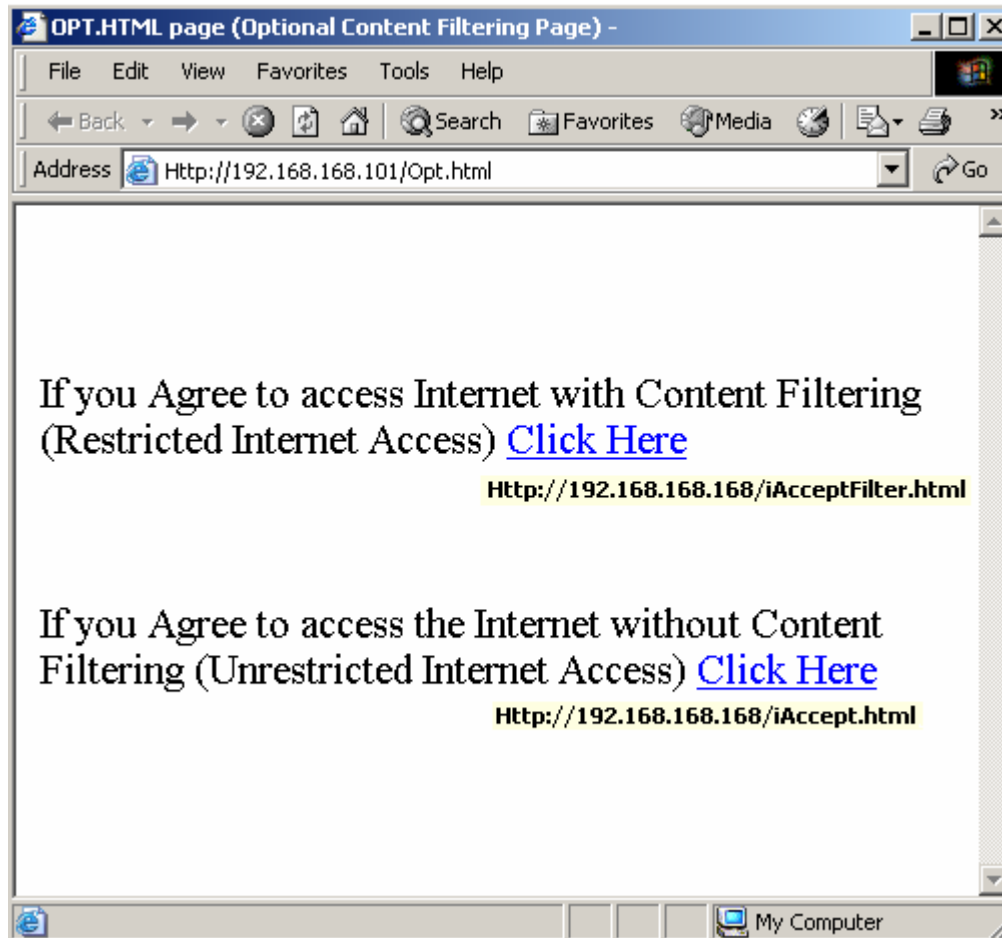
Note: If you are filtering wireless users connected to the WLAN zone with SonicOS Enhanced, you will use the Sonicwall WLAN IP address.

Note: On SonicOS Standard there must also be a firewall access rule allowing *HTTP Management* from the WLAN.



Tech Note

Figure 1.1 – CFS Optional Content Filtering page (Opt.html):



2. Login to the SonicWALL Management Interface and navigate to **Security Services > Content Filter**.

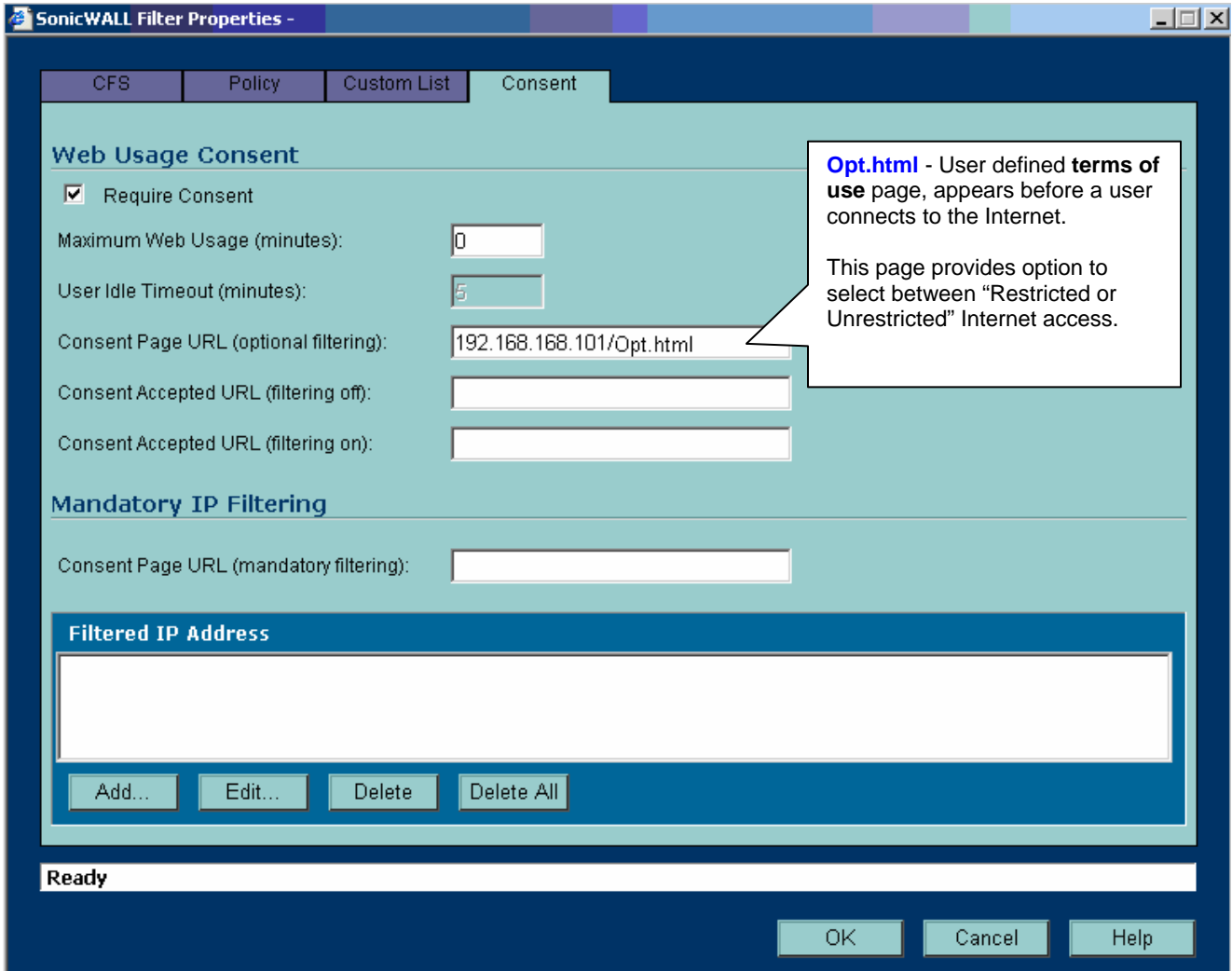
Note: Enforce the Content Filtering Service per zone from the **Network > Zones** page on SonicOS Enhanced, or per interface from the **Network > Settings** page on SonicOS Standard.

3. Select SonicWALL CFS as the Content Filtering Type and then click **Configure**. The **SonicWALL Filter Properties** window is displayed (Figure 1.2).
4. On the **Consent** tab, select **Require Consent** to enable the **Consent** properties.
5. In the **Consent Page URL (optional filtering)** field, enter **192.168.168.101/Opt.html**

SonicWALL will redirect to the above URL when the users on the network try to access the Internet.

Tech Note

Figure 1.2 – SonicWALL Filter Properties window:



6. Click **OK**.

Test the settings by accessing the Internet from any workstation on your network. The SonicWALL appliance should redirect the user to the optional page to review the terms of use and decide whether or not to have content filtering applied before accessing the Internet.

Note: The following fields should be left blank:

- **Consent Accepted URL (filtering off):**
- **Consent Accepted URL (filtering on):**

Document created: 7/26/07
Last updated: 2/4/08

