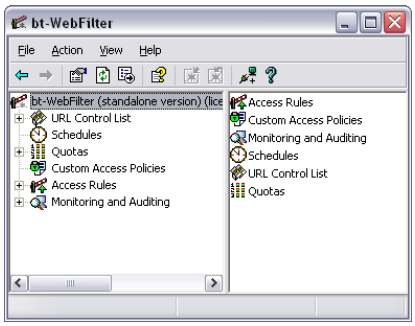
bt-WebFilter for MS ISA/TMG Server
QuickStart Guide

System Requirements

Windows 2003, 2008 or 2008 R2 Server
MS ISA Server 2004, 2006
MS Forefront TMG Server 2010



NOTE: After installation, WebFilter immediately blocks the following categories for unauthenticated (Anonymous) Users of the ISA/TMG server:
Anonymizers, Criminal Skills, Extreme & Violence, Gambling, Hacking, Hate Speech, Malicious Code, Mature, Spyware/Adware and XXX-Sexual Content.

Examples of other categories you may wish to block include:
Chat, File Sharing, Remote Access, and Social Networking

A complete list of categories with definitions can be viewed here:
http://www.burstek.com/products/categories.htm

Quick Setup Procedure

1. To start the installation wizard on a server with ISA or TMG server already installed, unzip and double-click on the **setup.exe** for bt-WebFilter and **reboot** your server as prompted.

2. If you are NOT forcing authentication for the HTTP/HTTPS protocols, the default filtering policy should be blocking access to **"**questionable" categories (i.e. XXX Sexual Content, Gambling, Malicious Code, and more).

Setting Up bt-WebFilter with ISA 2004, 2006 or TMG 2010

1. Install ISA or TMG server.
2. Create an HTTP/HTTPS Access Rule:
   a. Open up the ISA Management Console.
   b. Right-click on Firewall Policy, select "**New" > "Access Rule"**.
   c. Type in the Access Rule Name.
   d. Select **"Allow"** for the Rule Action, and click **"Next."**
   e. Select **"Selected protocols"** for Protocols, and click the **"Add"** button.
   f. Under **"Common Protocols"**, add the **"HTTP"** and **"HTTPS"** protocols, then click **"Close"** and **"Next"**.
   g. Click the **"Add"** button for the Access Rule Sources.
   h. Under **"Networks"** select and add the **"Internal"** Network, then click **"Close"** and **"Next"**. **NOTE: This rule will allow HTTP/HTTPS access for the entire**

"Internal" network. If requiring authentication for another network, or IP range, replace the source as needed.

i. Click the **"Add"** button for the Access Rule Destinations.
j. Under **"Networks"** select and add the **"External"** or **"Internal"** Network, then click **"Close"** and **"Next"**. Depending on the ISA or TMG server's configuration, you will use a different destination network. For ISA or TMG Servers acting as a proxy only (1 NIC), the **"Internal"** network must be used. For ISA or TMG Servers acting as a Firewall (multi-homed server), the **"External"** network must be used.
k. In the **"User Sets"** screen, remove the **"All Users"** user set and add the **"All Authenticated Users"** user set.
l. Click the **"Close"** button, then Proceed to the next page by clicking **"Next"**
m. Click the **"Finish"** button.
n. Apply the settings.

4. Install the bt-WebFilter ISA Server version
   a. Download the latest version of bt-WebFilter ISA Server version
   b. Unzip the file
   c. Double click on **"Setup.exe"**. NOTE: If installing on Server 2008 or later, make sure to use the **"Run as Administrator"** option by right-clicking the **"setup.exe"** file and clicking **"Run as Administrator"**.
   d. Follow the default installation instructions
   e. Once the install is complete, reboot the machine

5. Configure the bt-WebFilter (By default the bt-WebFilter is set to a *Restrictive* policy):
   a. Open up the bt-WebFilter Console.
   b. Right click on **Access Rules**, and select **Register Domain**.
   c. Select the Drop down box and click on your domain name and click the **"OK"** button.
   d. Click on the **Custom Access Policies**.
   e. On the right hand pane, right click on the **Default Custom Policy** and select **Properties**.
   f. Click on the **"Apply to"** tab, and add the user groups (Domain Users, etc.) you want to apply this policy to.

Testing the Software

1. Launch Internet Explorer.
2. Click **Tools> Internet Options> Connections> LAN Settings**.
3. Check the box marked **"Use a proxy server for your LAN"**. **NOTE: Make sure both check boxes are unchecked for "Automatically detect settings" and "Use automatic configuration script". These settings can override the manually entered proxy server.**
4. Enter the IP address of the computer with bt-WebFilter in the **"Address"** field.
5. Set the **"Port"** to port 8080.
6. Click **"OK"** to save, and then close the browser.
7. Re-launch Internet Explorer and try going to www.casino.com

Recommended Filtering Settings

Please visit: http://www.burstek.com/support/btWebFilter/bestPractices.htm

How do I prevent users from bypassing the bt-WebFilter Application?

To prevent internal users from bypassing the bt-WebFilter, direct HTTP/HTTPS access must be restricted to only the proxy server (in this case the ISA or TMG server). If the clients are allowed through the firewall via the HTTP/HTTPS ports, then the client can choose not to use the proxy, and navigate through the firewall as a SecureNAT client.
NOTE: It is recommended to restrict all access via unnecessary ports on the firewall. Excluding the security reasons for this, this will hinder the ability of a client to use an external proxy via a different port to browse the web anonymously.

Technical Support Contacts

Phone: 239.495.5900
E-mail: support@burstek.com
Web: http://www.burstek.com/support/btWebFilter/faq.htm