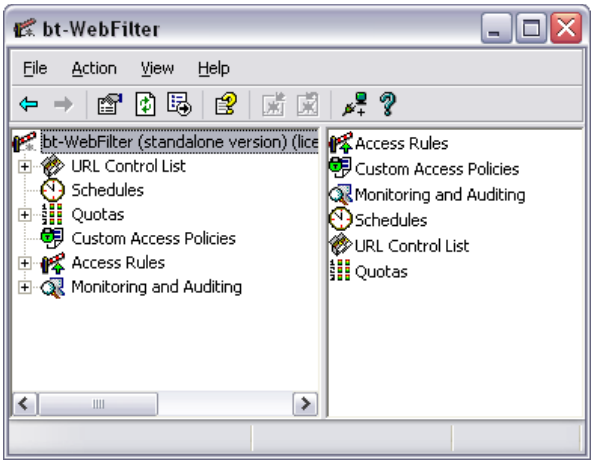
bt-WebFilter Versión para Servidor de MS ISA
Guía de Inicio Rápido

Requisitos del Sistema

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



NOTA: Después de la instalación WebFilter bloquea las siguientes categorías inmediatamente para los usuarios que no estan autenticado (Anonymous):
Anonymizers, Criminal Skills, Extreme & Violence, Gambling, Hacking, Hate Speech, Malicious Code, Mature, Spyware/Adware y XXX-Sexual Content.

Entre los ejemplos de otras categorías que usted puede desear bloquear incluyen:
Chat, File Sharing, Remote Access, y Social Networking

Una lista completa de categorías con las definiciones y los ejemplos se pueden ver en nuestro sitio de web: **http://www.burstek.com/products/categories.htm**

Procedimiento de Rápida Instalación

1. Para iniciar el asistente de instalación descomprima y haga doble click sobre el archivo **setup.exe** para bt-WebFilter y **re-inicie** el servidor.
2. Si usted NO está realizando autenticación de usuarios, la política pre-determinada de filtrado debe estar bloqueando el acceso a categorías "cuestionables" (por ejemplo: XXX Sexual Content, Gambling, Malicious Code, y más).

Configuración de bt-WebFilter con ISA 2004 y 2006 o TMG 2010

1. Instalar Servidor ISA o TMG.

2. Crear una regla de acceso para HTTP/HTTPS:
   a. Abra la consola de adminstración de ISA
   b. Haga click derecho sobre "**Firewall Policy"**, seleccione "**New" > "Access Rule"**
   c. Escriba el nombre de la regla de acceso
   d. Seleccione **"Allow"** para la acción de la regla, y haga click en **"Next"**
   e. Seleccione **"Selected Protocols"** para los protocolos, y haga click en el boton de **"Add"**
   f. Bajo de **"Common Protocols"**, agrega los protocolos de **"HTTP"** y **"HTTPS"** y haga click en **"Close"** y **"Next"**
   g. Haga click en el botón **"Add"** para los Fuentes de las reglas de acceso
   h. Bajo de **"Networks"** selecciona y agrega la red de **"Internal"** y haga click en **"Close"** y **"Next"**. **NOTA: Esta politica permite acceso de HTTP/HTTPS para el red de "Internal". Si requieres autenticacion para otro red o rango de IP, replace el fuente como sea requiere**
   i. Haga click en el boton de **"Add"** para los destinos de la regla de acceso

j. Bajo de **"Networks"** seleccionas y agrega el red de **"External"** o **"Internal"**, y haga click en **"Close"** y **"Next"**. Dependiendo en la configuraccion del servidor de ISA o TMG, vas a usar un destino de red diferente. Para servidores de ISA o TMG que estan configurado como solo un proxy (solo una tarjeta de red), el red de **"Internal"** se usa. Para servidores de ISA o TMG que estan configurado como un firewall (multiples tarjetas de red), el red de **"External"** se usa
k. En la pantalla de **"User Sets"**, eliminas el User Set de **"All Users"** y agregas el User Set de **"All Authenticated Users"**
l. Haga click en el boton de **"Close"** y haga click en **"Next"** para navegar a la siguente pagina
m. Haga click en el boton de **"Finish"**
n. Applicar los ajustes

4. Instale el bt-WebFilter versión para Servidor ISA
   a. Descargue la ultima versión de bt-WebFilter para Servidor ISA
   b. Descomprimir el archivo
   c. Haga doble click en "**Setup.exe"**. **NOTA: Si estas instalando Servidor 2008 o mas reciente, tienes que usar el opcion de "Run as Administrator". Haga click derecho en el archive de "setup.exe" y haga click en "Run as Administrator".**
   d. Siga las instrucciones de instalación pre-determinadas
   e. Una vez completada la instalación, reinicie el equipo

5. Configure el bt-WebFilter (Pre-determinadamente, el bt-WebFilter esta establecido con una política *Restrictiva*):
   a. Abra la consola del bt-WebFilter
   b. Haga click derecho sobre **"Access Rules"**, y seleccione **"Register Domain"**
   c. Seleccione el **'Drop down box'** y haga click en el nombre de dominio y luego haga click en el botón **"OK"**
   d. Haga click en **"Custom Access Policies"**
   e. En el panel derecho, haga click derecho sobre la **"Default Custom Policy"** y seleccione **"Properties"**
   f. Haga click en la pestaña **"Apply to"**, y marque la casilla junto a los grupos de usuarios (Domain
   Users, etc.) a los cuales usted desea aplicar esta política

Prueba del Software

1. Iniciar el Internet Explorer
2. Haga click en **Tools> Internet Options> Connections> LAN Settings**
3. Marque la casilla marcada **"Use a proxy server for your LAN". NOTA: Tenga seguro que los dos casillas de verificacion no estan seleccionado para "Automatically detect settings" y "Use automatic configuration script". Estos ajustes se pueden anular la configuracion del proxy que se entra manualmente.**
4. Introduzca la dirección IP de la computadora con bt-WebFilter en el campo **"Address"**
5. Establezca el **"Port"** en el puerto 8080
6. Haga click en **'OK'** para guardar, y a continuación cierrre el navegador
7. Re-lanzamiento del Internet Explorer e intente ir a www.casino.com

Configuración Recomendada de Filtros

Por favor, visite:
http://www.burstek.com/support/btWebFilter/bestPractices.htm

Cómo puedo evitar que mis usuarios evadan el bt-WebFilter?

Para evitar los usuarios evadan el bt-WebFilter, accesso directo para los protocolos de HTTP/HTTPS tiene que estar restrigido a solo el servidor de proxy (en este caso, el servidor de ISA o TMG). Si los clientes estan permitido ir por el firewall por los puertos de HTTP/HTTPS, entonce los clientes se pueden pasar por el firewall como clientes de SecureNAT.
NOTA: Es recomendido restringir todo el acceso en el firewall para los puertos que no son necesario. Excluyendo los razones de seguridad, esto se obstaculiza la capacidad de un cliente usar un proxy externo por otro Puerto para accesar el web sin autenticarse.

Contactos de Soporte Técnico

Teléfono: 239.495.5900
Correo: support@burstek.com
Web: http://www.burstek.com/support/btWebFilter/faq.htm