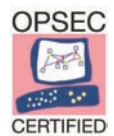




Internet

SurfControl Web Filter for
Check Point™ FireWall-1®

Getting Started Guide



NOTICES

Copyright © 2005 SurfControl plc. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior permission of the copyright owner.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

SurfControl is a registered trademark, and SurfControl and the SurfControl logo are trademarks of SurfControl plc. All other trademarks are property of their respective owners.

Printed September 2005

COMMENTS ON THIS GUIDE?

You can view updated documentation and support information at <http://www.surfcontrol.com>

Was this guide helpful? E-mail us at documentation@surfcontrol.com to suggest changes or make a correction.

TECHNICAL SUPPORT

- For the latest support information on SurfControl products, visit <http://www.surfcontrol.com/support>
- Read the Top Issues - This page has a quick list that covers the most common support issues encountered with SurfControl products.
- Search our Knowledge Base - our new, constantly updated Knowledge Base contains articles, FAQs and glossary items to answer your questions about all SurfControl products.
- If your question or problem cannot be answered by the Top Issues or is not in the Knowledge Base, fill out an Online Support Request Form.
- Telephone Support - If you would like to speak with a Technical Support Representative, our excellent SurfControl Technical Support is just a phone call away.

SURFCONTROL SALES

For product and pricing information, or to place an order, contact SurfControl. To find your nearest SurfControl office, please visit our Website.

<http://www.surfcontrol.com>

CONTENTS

Notices	i
Comments on this Guide?	i
Technical Support	ii
SurfControl Sales	ii
GETTING STARTED	1
SurfControl Web Filter	2
Overview of Web Filter	2
Before You Install	3
Installing Web Filter	4
CHECK POINT FIREWALL-1	5
Configuring Check Point FireWall-1	6
Create a Network Object	7
Create an OPSEC Application	9
Creating an OPSEC Application	9
Set up the sslca authentication	12
Configure the UFP and AMON Server in Web Filter	13
Using the UFP and AMON Server	14
Create a URI Resource	16
Enhanced UFP Performance	18
Insert the URI Resource into an Access Policy	19
What to do next	21
Further Assistance	21

CONTENTS



Chapter 1

Getting Started

SurfControl Web Filter
Before You Install
Installing Web Filter

page 2
page 3
page 4

SURFCONTROL WEB FILTER

In the workplace SurfControl Web Filter can help you to enhance employee productivity, optimize network bandwidth, reduce legal liability and safeguard students by blocking suspect sites. It does this with the following group of components designed to enable you to monitor users' surfing behavior, produce reports on Internet access trends then use rules to manage this access

This guide will give you a quick overview of the program, along with references to where you can find more detailed information in the Installation and Administrator guides. You will also be shown how to set up Web Filter to work with Check Point® FireWall-1™.

OVERVIEW OF WEB FILTER

- **Monitor** - provides a view of activity by user and sites requested. As traffic is generated on the network, information about user activity is recorded in the SurfControl database and then displayed in the Monitor window.
- **Real Time Monitor** - shows activity on the network as it is happening in real time, rather than by displaying past activity as recorded in the SurfControl database. As traffic is generated on the network you will see it appear in the Real-Time Monitor.
- **Rules Administrator** - enables you to create rules that will control the Internet access of the users that you are monitoring. These rules can govern who can access what areas of the Internet at what time of day. Rules can be positive (allowing access to sites or categories) or negative (denying access to sites or categories of sites).
- **Scheduler** - enables you to schedule events at a later date and time. This is a convenient way to update the URL Categories database or perform other tasks on a regular basis.
- **Virtual Control Agent (VCA)** - evaluates unknown web sites, reading and analyzing content page by page. It then uses artificial intelligence algorithms to study and classify each Web page into one of the SurfControl Web Filter categories.
- **Report Central** - SurfControl's powerful reporting tool.
- **Remote Administration** - enables you to use a computer other than the one on which SurfControl Web Filter is installed to control any of the SurfControl services running on a Web Filter machine. It requires a Remote Administration installation of SurfControl Web Filter on the machine that you are going to use remotely along with a full product installation on the machine where the services are running.

BEFORE YOU INSTALL

You need to know the answers to the following questions in Table 1 before installing SurfControl Web Filter:

Table 1 Pre-installation checks

Question	Where to find out
Does my hardware meet the minimum specifications?	The System Requirements section in Chapter 1 of the Installation Guide.
What Operating software does Web Filter support?	The System Requirements section Chapter 1 of the Installation Guide.
Do I have the right database for my environment?	The Database considerations section in Chapter 2 of the Installation Guide. Note: SurfControl recommends that you install your database before installing Web Filter.
Where is the best place to install Web Filter on my network?	The Installation Decisions Chapter of the Installation Guide.

INSTALLING WEB FILTER

To install SurfControl Web Filter, follow Procedure 3-2 in Chapter 3 of the Installation Guide. Following installation and re-booting your SurfControl Web Filter server, you can then configure your Check Point FireWall -1 to communicate with Web Filter. This is covered in Chapter 2.



Chapter 2

Check Point FireWall-1

Configuring Check Point FireWall-1	page 6
Create a Network Object	page 7
Create an OPSEC Application	page 9
Set up the sslca authentication	page 12
Create a URI Resource	page 16
Insert the URI Resource into an Access Policy	page 19

Configuring Check Point FireWall-1

After installing Web Filter, you need to configure Check Point FireWall-1 to use the Web Filter UFP server. There are three stages to this process:

- 1 Create a Network Object to represent the machine on which the Web Filter URL Filtering Protocol (UFP) Server is installed.
- 2 Create an OPSEC™ Application to establish and monitor the connection between Web Filter and Check Point FireWall-1.
- 3 Create a URI resource and apply it to a Check Point access policy.

CREATE A NETWORK OBJECT

You must create a network object on FireWall-1 for the machine on which the Web Filter UFP Server is installed.

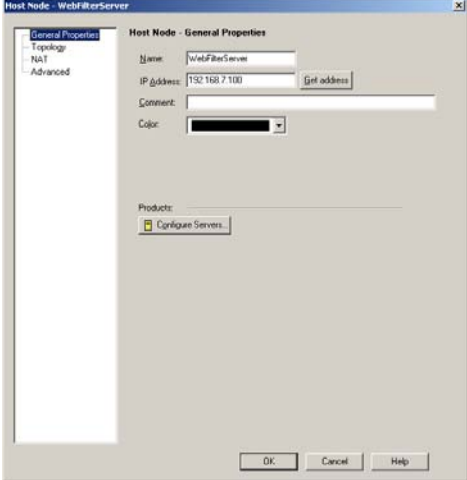


Note: If you have installed the Web Filter UFP Server on the same machine as FireWall-1, skip this procedure.

To Create a Network Object, follow Procedure 2-1:

Procedure 2-1: Creating a Network Object		
Step	Action	Action
1	Launch the Check Point SmartDashboard™.	
2	From the Manage menu select Network Objects . The Network Objects dialog will display.	
3	Click New . Choose Node > Host from the list. The Host Node dialog box will display.	

Procedure 2-1: Creating a Network Object (Continued)

Step	Action	Action
4	<p>Select General Properties. Fill in the fields as follows:</p> <p>Name: enter the name for your Network object, e.g., WebFilterServer.</p> <p>IP Address: enter the name or the IP address of the Web Filter UFP Server.</p>	
5	Click OK .	
6	Close the Network Objects.	

Create an OPSEC Application

You now have to create an OPSEC Application to connect to a UFP and AMON server.

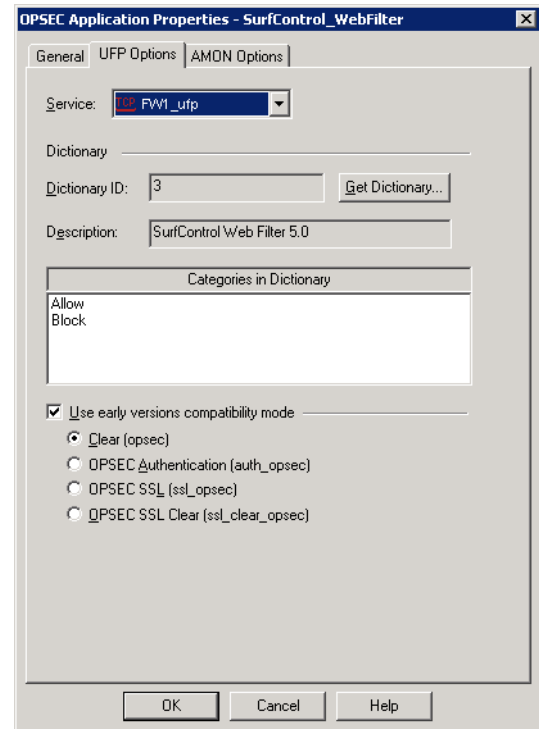
CREATING AN OPSEC APPLICATION

A UFP Server object represents a Network Object that provides URL categorization services. Once you have added the Web Filter network object, you need to create a new Server object. Follow Procedure 2-2:


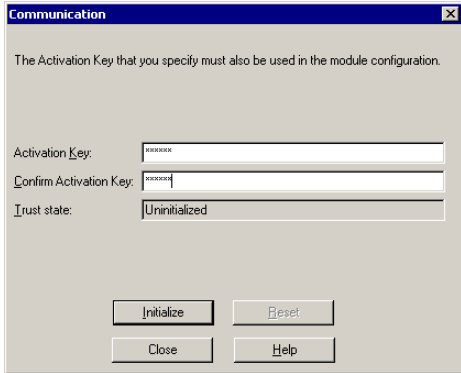
Procedure 2-2: Creating an OPSEC Application	
Step	Action
1	Launch the Check Point SmartDashboard and select Manage > Servers and OPSEC Applications . The OPSEC Applications dialog box will display.
2	Select New then choose OPSEC Application . The OPSEC Application Properties dialog will display.
3	<p>Select the General tab. Fill in the fields as follows:</p> <p>Name: enter the name for your OPSEC Application, e.g., SurfControl_WebFilter.</p> <p>Host: select the network object for your Web Filter Server from the list.</p> <p>Vendor: select User defined.</p> <p>Note: the "Vendor", "Product", and "Version" fields under "Application Properties" do not affect the functioning of this integration product. The values for these fields are updated by Check Point, and these values can get outdated as newer products are released. To avoid any confusion, please set the "Vendor" field to "User Defined".</p> <p>In the Server Entities list, select UFP and AMON.</p>

Procedure 2-2: Creating an OPSEC Application

Step	Action
4	Select the UFP Options tab.
5	Select the Use early versions compatibility mode checkbox.
6	<p>Select Clear (opsec): unauthenticated communication.</p> <p>Note: Only the Clear communication mode is allowed if the URI resource (created later in Procedure 2-4 "Creating a URI Resource" on page 16) is set to "Enhance UFP Performance" instead of the default "Enforce URI Capabilities". However other SIC (Secure Internal Communication) modes like sslca can be used if the URI resource is set to "Enforce URI Capabilities". In that case do not select the "Use early versions compatibility mode" checkbox. The following sections describe how to set up the sslca communication mode for AMON. If one of the SIC modes is used for UFP then appropriate changes will be required for the UFP settings in the ufp.conf file (e.g., use the lines "ufp_server auth_port 18182" and "ufp_server auth_type sslca", instead of "ufp_server port 18182").</p>
7	<p>Click Get Dictionary to retrieve the Web Filter URL Category List and details.</p> <p>Note: if you do not see the list of categories, check that the UFP Server is running and that the host name is correct.</p>
8	Click OK .



Procedure 2-2: Creating an OPSEC Application

Step	Action
9	Select the AMON Options tab.
10	Leave Service and AMON identifier set to their default settings.
	
11	Select the General tab and click Communication . The Communication dialog box will display.
	
12	Enter an Activation Key (password), and confirm it.
13	Click Initialize . The Trust state will change from Uninitialized to Initialized but trust not established .
14	Click Close . Click OK from the General tab

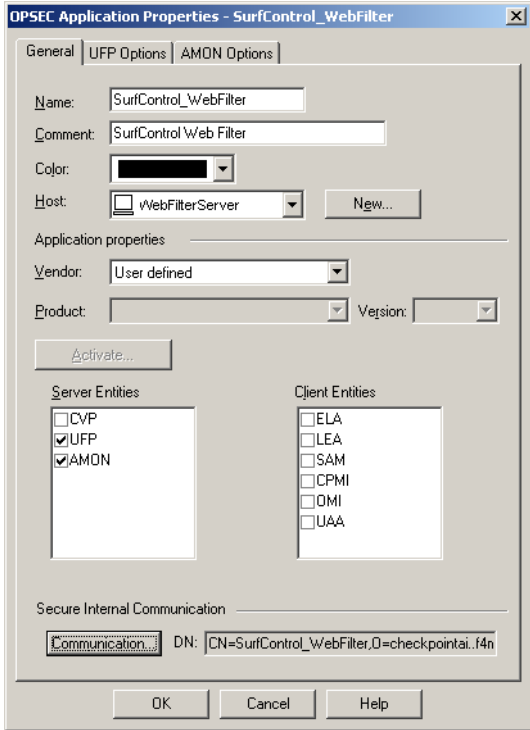
SET UP THE SSLCA AUTHENTICATION

You now have to set up the sslca authentication on the AMON server. To set this up follow Procedure 2-3:

Procedure 2-3: Setting up sslca authentication

Step	Action
1	<p>Locate the <code>opsec_pull_cert.exe</code> file. In a default SurfControl Web Filter installation this will be located in:</p> <p><code>C:\Program Files\SurfControl\Web Filter\OPSEC</code></p>
2	<p>Open a Command prompt from within this folder and type the following command.</p> <pre>opsec_pull_cert -h host -n object_name -p password [-o cert_file] [-od dn_file]</pre> <p>Key:</p> <p><code>host</code> - the resolvable name or IP address of computer on which the Check Point FireWall-1 Server is installed.</p> <p><code>object_name</code> - name of the OPSEC Application object you created in Procedure 2-2.</p> <p><code>password</code> - the Activation Key used in Procedure 2-2.</p> <p><code>cert_file</code> - the name of the output file (default is <code>opsec.p12</code>).</p> <p><code>dn_file</code> - the name of the file containing the Secure Internal Communication (SIC) name of the object. If not specified, the object's SIC name is printed to stdout.</p>
3	<p>Launch the Check Point SmartDashboard and select Manage > Servers and OPSEC Applications. The OPSEC Applications dialog box will display</p>

Procedure 2-3: Setting up sslca authentication (Continued)

Step	Action
4	Select the UFP server object you created in Procedure 2-1. Click Details .
5	Click Communication . The Trust state will now be set to Trust established . The DN field will also be populated.
	
6	Click OK .
7	Click Save from the Check Point SmartDashboard .

CONFIGURE THE UFP AND AMON SERVER IN WEB FILTER

SurfControl Web Filter is supplied with a configuration file, `ufp.conf`. In a default installation this is found in the following location:

```
C:\Program Files\SurfControl\Web Filter\OPSEC
```

As supplied, the contents of `ufp.conf` will be as below:

```
ufp_server port 18182

amon_server auth_port 18193
amon_server auth_type sslca

# The following lines must be customized for each installation and then uncommented.
Please see SurfControl
# documentation for details on replacing the placeholders
"DN_for_SurfControl_UFP_Server",
# "DN_for_Check_Point_FireWall-1" and "pathname_for_sslca_file".
#opsec_sic_name "DN_for_SurfControl_UFP_Server"
#opsec_entity_sic_name "DN_for_Check_Point_FireWall-1"
#opsec_sslca_file "pathname_for_sslca_file"
```

This supplied file allows the UFP server to communicate to Check Point FireWall-1 using the Clear (opsec) authentication method, as described in Procedure 2-2 - “Creating an OPSEC Application” on page 9.

Other communication modes are available within Check Point FireWall-1. For details on all communication modes, consult the following Check Point documentation:

http://www.opsec.com/developer/gw_comm_mode.html

USING THE UFP AND AMON SERVER

when configuring the UFP server using Clear authentication, and the AMON server with sslca authentication, the `ufp.conf` file is modified as part of the certification process. An example of a modified `ufp.conf` file may look as below:

```
ufp_server port 18182

amon_server auth_port 18193
amon_server auth_type sslca

# The following lines must be customized for each installation and then uncommented.
Please see SurfControl
# documentation for details on replacing the placeholders
"DN_for_SurfControl_UFP_Server",
# "DN_for_Check_Point_FireWall-1" and "pathname_for_sslca_file".
opsec_sic_name CN=SurfControl_WebFilter,O=checkpointai..f4m2sd"
opsec_entity_sic_name cn=cp_mgmt,o=checkpointai..f4m2sd"
opsec_sslca_file "C:\Program Files\SurfControl\Web Filter\OPSEC\opsec.p12"
```

The additional entries are as follows:



Note: the entries below are for illustration purposes only.

```
opsec_sic_name "CN=SurfControl_WebFilter,O=checkpointai..f4m2sd"
```

This entry specifies the distinguished name (DN) of the SurfControl Web Filter UFP server. The value for this entry can be obtained from the properties of the OPSEC Application object. See step 5 of "Procedure 2-3: Setting up sslca authentication" for more details.

```
opsec_entity_sic_name "cn=cp_mgmt,o=checkpointai..f4m2sd"
```

This entry specifies the distinguished name (DN) of the Check Point FireWall-1. The value for this entry can be obtained from the General Properties of the Check Point Gateway object. Alternatively, this value can be easily derived from the value for opsec_sic_name. In the above example, this can be achieved by replacing the name of the OPSEC Application object (i.e., "SurfControl_WebFilter") with "cp_mgmt".

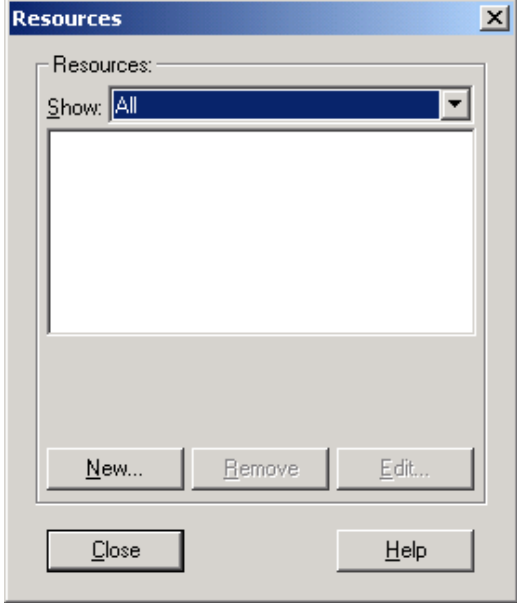
```
opsec_sslca_file "C:\Program Files\SurfControl\Web Filter\OPSEC\opsec.p12"
```

This entry specifies the location of the certificate file - opsec.p12.

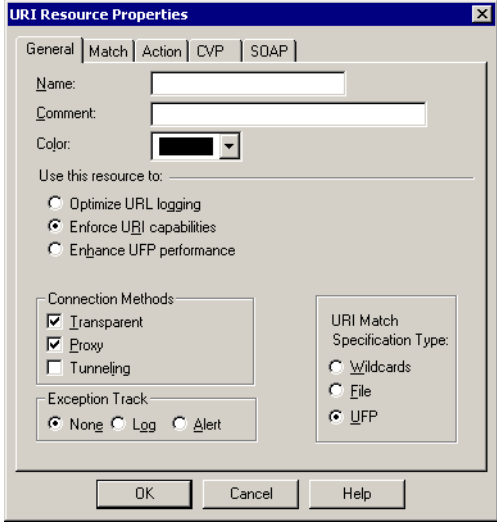
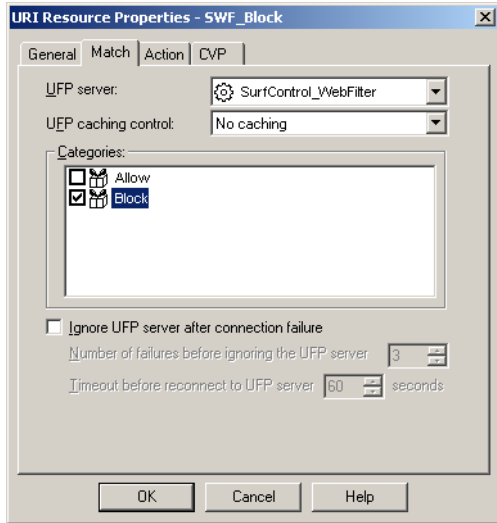
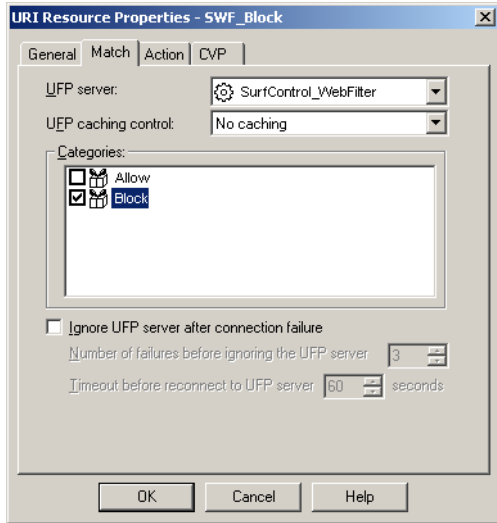
Create a URI Resource

A URI is a Uniform Resource Identifier, of which the familiar URL (Uniform Resource Locator) is a specific case. URI Resources can define schemes (HTTP, FTP, GOPHER, etc.), methods, (GET, POST, etc.), hosts (for example “*.com”), paths and queries. In addition, the Security Administrator can define how to handle responses to allowed resources:¹

Procedure 2-4: Creating a URI Resource

Step	Action	
1	From the Check Point SmartDashboard , select Resources from the Manage menu. The Resources dialog box will display.	
2	Click New and select URI from the drop-down menu. The URI Resource Properties dialog will display.	

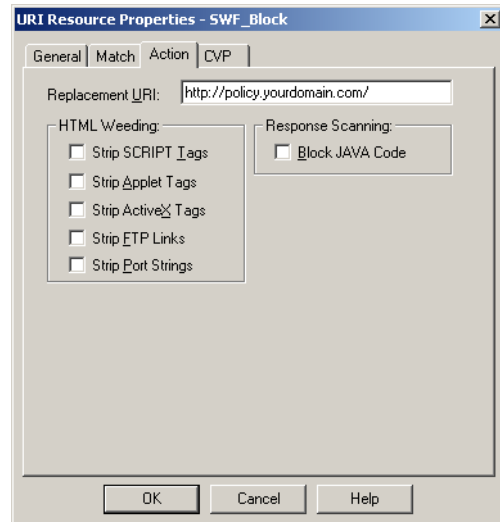
Procedure 2-4: Creating a URI Resource

Step	Action	
3	<p>From the General tab:</p> <p>Give the URI Resource a name, for example SWF_Block.</p> <p>Note: The name must not contain any spaces.</p> <p>In the Use this resource to: section, the default selection is Enforce URI Capabilities. You can alternatively select Enhance UFP Performance.</p> <p>For an explanation of Enhance UFP Performance, see "Enhanced UFP Performance" on page 18.</p> <p>In the URI Match Specification Type section, select UFP.</p>	
4	<p>Select the Match tab:</p>	
5	<p>From the UFP Server drop-down list box, select your UFP Server, as set up in Procedure 1.</p> <p>From the UFP caching control drop-down list box, select No caching.</p> <p>Note: No caching allows all HTTP requests to be submitted to the SurfControl Web Filter UFP server. This will give you the most accurate filtering, monitoring and reporting from Web Filter.</p> <p>From the Categories, select Block.</p>	

1. Taken from the following Check Point document:
http://www.checkpoint.com/support/downloads/docs/firewall1/ng/fp3/SmartCenter_NG_FP3.pdf

Procedure 2-4: Creating a URI Resource

Step	Action
6	<p>Select the Action tab.</p> <p>Note: The Action tab will not be available if you have configured the URI resource as "Enhance UFP Performance" in Step 3.</p>
7	<p>You can specify a Replacement URI which will launch when a user tries to access a blocked site.</p> <p>In the Replacement URI field, enter the URL to which user will be redirected.</p> <p>Note: If you have specified a Redirect URL in the Web Filter Rules Administrator, this will override the Replacement URI.</p>
8	<p>Click OK. The next time that you access the Resources tab, you will see this resource listed.</p>



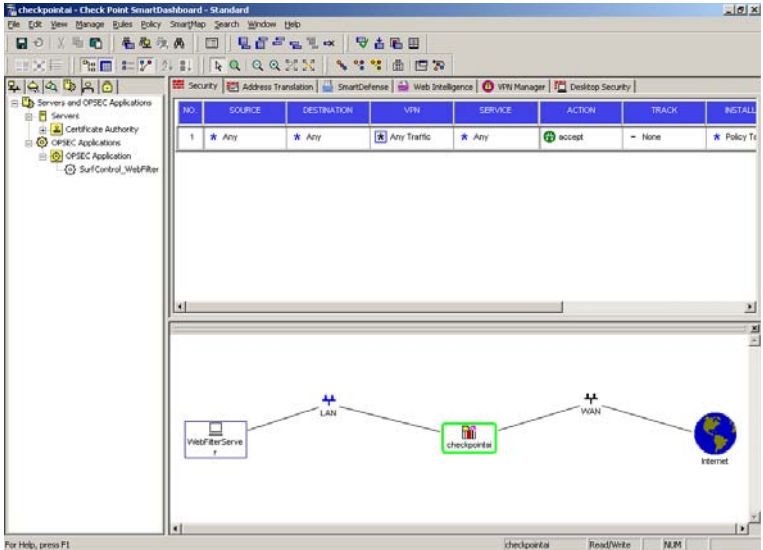
ENHANCED UFP PERFORMANCE

You can use **Enhanced UFP Performance** instead of **Enforce URI Capabilities**. This uses FireWall-1 kernel inspection together with a dedicated UFP daemon (aufpd) to increase the performance of the UFP. UFP caching, Content Vectoring Protocol (CVP) checking and authentication are not available in this mode, as well as HTTP Header method and length verifications.

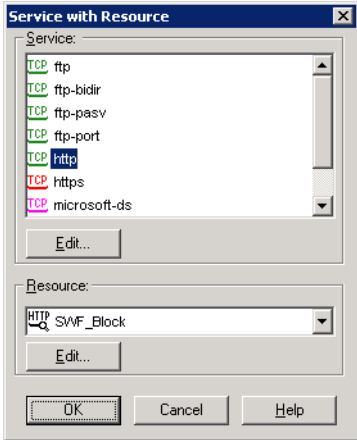
INSERT THE URI RESOURCE INTO AN ACCESS POLICY

You now need to define two rules for HTTP traffic that should be checked by Web Filter. To insert the Web Filter URI Resource into the FireWall-1 access policy, follow Procedure 2-5:

Procedure 2-5: Inserting the URI Resource into a FireWall-1 Access Policy

Step	Action																
1	<p>Launch the Check Point SmartDashboard:</p>  <p>The screenshot shows the Check Point SmartDashboard interface. On the left is a tree view with 'SurfControl_WebFilter' selected. The main window displays a table with the following data:</p> <table border="1"> <thead> <tr> <th>NO.</th> <th>SOURCE</th> <th>DESTINATION</th> <th>VPN</th> <th>SERVICE</th> <th>ACTION</th> <th>TRACK</th> <th>INSTALL</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Any</td> <td>Any</td> <td>Any Traffic</td> <td>Any</td> <td>accept</td> <td>None</td> <td>Policy Tr</td> </tr> </tbody> </table> <p>Below the table is a network diagram showing a 'WebFilter Server' connected to a 'LAN' interface, which is connected to a 'WAN' interface, which is connected to the 'Internet'.</p>	NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL	1	Any	Any	Any Traffic	Any	accept	None	Policy Tr
NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL										
1	Any	Any	Any Traffic	Any	accept	None	Policy Tr										
2	<p>From the Rules menu, select Add Rule and select where you want the rule to appear in the list. The options are:</p> <ul style="list-style-type: none"> • Bottom • Top • Below • Above 																
3	<p>Right-click on the Service column. From the menu that displays, select Add With Resource.</p>																

Procedure 2-5: Inserting the URI Resource into a FireWall-1 Access Policy

Step	Action
4	<p>The Add With Resource dialog will display.</p> <p>From the Service: section, select http.</p> <p>From the Resource: section, select the resource created in Procedure 2-4, for example, SWF_Block.</p> <p>Click OK.</p>
	
5	<p>Right-click on the Action column. From the menu, select how FireWall-1 will respond to requests to access URLs in this URI resource. The options are:</p> <ul style="list-style-type: none"> • accept • drop • reject • User auth • Client auth • Session auth <p>SurfControl recommend using the reject action.</p>
6	<p>Right-click in the Track column and choose the level of logging required. The options are:</p> <ul style="list-style-type: none"> • None • Log • Account • Alert • Snmp Trap • Mail <p>You can also set up user defined logging options.</p>
7	<p>Create another rule that will allow all HTTP traffic. Create this rule with the following parameters:</p> <ul style="list-style-type: none"> • Service - select Add then select http from the Service: list box. • Action - accept. <p>Set this rule to appear below the rule with the SWF_Block resource.</p>
8	<p>From the Policy menu, select Install to install the policy.</p>
9	<p>Click OK to exit.</p>

WHAT TO DO NEXT

SurfControl recommends the following to help you get the most from Web Filter:

- Check that you have a Category List update scheduled event listed in the SurfControl Scheduler. This list is updated daily by the SurfControl content team. See Available Events in Chapter 9 of the Administrator's Guide for more details.
- Configure SurfControl Report Central to enable you to run reports on your network's Internet activity. See Chapter 11 of the Administrator's Guide for more details.
- Consideration should also be given to basic database administration tasks such as purging, archiving and compacting. See the Database Chapter of the Administrator's Guide for more details.

FURTHER ASSISTANCE

- **SurfControl's Knowledge base** - SurfControl have an extensive knowledge base covering all areas of SurfControl Web Filter. It can be found at:
<http://kb.surfcontrol.com>
- **Technical Support** - details of how to contact SurfControl's Technical Support teams for your location can be found at:
www.surfcontrol.com/support/



CHECK POINT FIREWALL-1 *Further Assistance*