



SurfControl[®]
Web Filter

**Configuring Check Point
FireWall-1 NG**

Notices

Updates to the SurfControl documentation and software as well as Support information are available at www.SurfControl.com/support.

Copyright © 1998-2002 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.

SurfControl USA

100 Enterprise Way, Suite A-110
Scotts Valley
CA 95066
USA

Telephone: +1 831 431 1400
Fax: +1 831 431 1800

SurfControl Europe

Riverside
Mountbatten Way
Congleton
Cheshire
CW12 1DY
England

Telephone: +44 (1) 260 296259
Fax: +44 (1) 260 296251

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 October 2002.

Table of Contents

Notices	iii
Introduction	1
Configuring Check Point FireWall-1 NG	1
Creating a Network Object	2
Creating a UFP Server	3
Creating a URI Resource	5
Inserting a URI Resource into a FireWall-1 Access Policy.....	8

Introduction

The information in this document is relevant only when using Check Point FireWall-1 NG. It is supposed to replace the material from Chapter 3 in the SuperScout Installation and Configuration guide (STWeb UFP Server Install Guide.pdf) as that relates to FireWall-1 v4.1 only.

Configuring Check Point FireWall-1 NG

After installing SuperScout UFP Server, the FireWall-1 product needs to be configured to use the SuperScout URL Filtering protocol. FireWall-1 is configured using the Check Point FireWall-1 Policy Editor. The procedures in this subsection illustrate how to complete this configuration.

In the Check Point FireWall-1 Policy Editor:

1. Create a Network Object to represent the machine on which SuperScout UFP Server is installed.
2. Create a UFP Server object for the SuperScout service.
3. Create a URI Resource containing categories from the SuperScout list of URLs.
4. Insert the URI Resource into FireWall-1 access rules. The following example's Internet Acceptable Use Policy contains only two rules, which FireWall-1 enforces in descending order as follows:
 - Reject and log access to Web sites defined in the URI Resource named 'Block'
 - Allow access to all destinations not covered by the previous rule

Optionally, you can configure Authentication Connection between the FireWall-1 machine and the SuperScout UFP Server machine.

Creating a Network Object

FireWall-1 must have a network object defined for the machine on which SuperScout UFP Server is installed. If one does not already exist, perform the following procedure.

Note: If you have installed SuperScout UFP Server on the same machine as FireWall-1, you can skip this step.

To Create a Network Object

1. Start the Check Point Policy Editor and navigate through the interface until you see the initial rule base policy.
2. From the menu bar select **Manage** and then **Network Objects** to display the **Network Objects** dialog.
3. Once you can see the **Network Objects** dialog, click the **New** button and choose **Workstation** from the pull-down list. You will now see the Workstation Properties dialog.
4. Select the **General** tab in order to enter the details of the Workstation on which you have installed SuperScout.
5. In the **Name** edit field enter the name of your SuperScout UFP Server (this is the name of the workstation on which you have installed SuperScout).
6. In the IP Address edit field enter the IP address of this workstation. Alternatively, click the **Get address** button, which will automatically insert the IP Address of the workstation that you have already named.
7. Click **OK**.

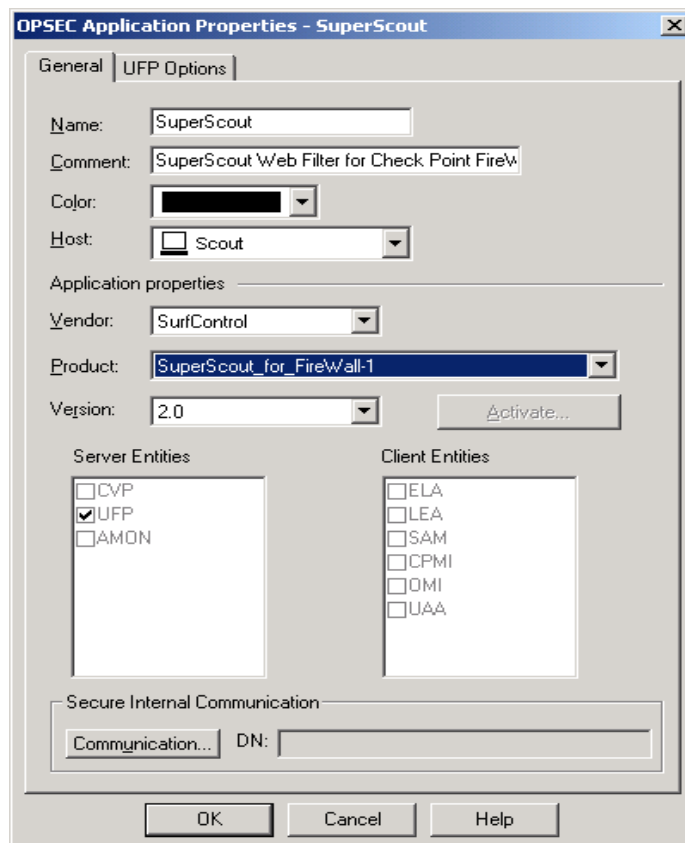
Note: This is the only tab from this dialog that you need to edit.

Creating a UFP Server

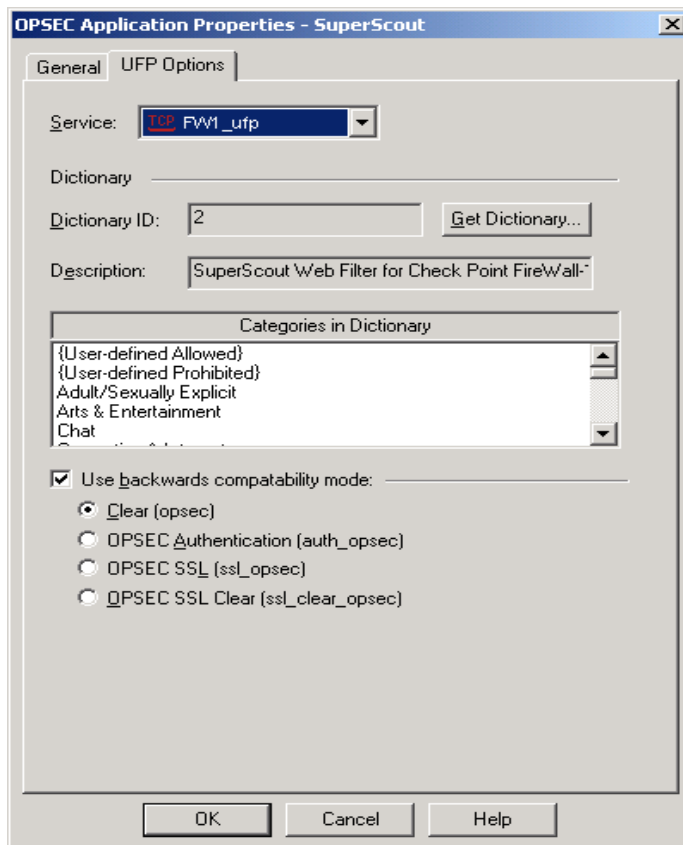
A UFP Server object represents a Network Object that provides URL categorization services. Once you have added the SuperScout network object, you need to create a new Server object.

To create a UFP Server Object

1. From the menu bar of the Check Point Policy Editor select **Manage** and then **OPSEC Applications**.
2. In the **OPSEC Applications** dialog that follows, select **New** then choose **OPSEC Application** from the drop-down menu to display the following dialog:



3. In the General Tab, in the Name edit field of this OPSEC Application Properties dialog enter the name of the SuperScout Server. There is a Comment edit field available if you wish to enter any more details.
4. Next select your SuperScout Server from the list box entitled Host.
5. From the Vendor list box, select **SurfControl**.
6. Go to the UFP Options tab. Click the **Dictionary** tab and then click **Get Dictionary** to retrieve the SuperScout URL Category List and details.
7. Enable the check box for **Use backwards compatibility mode**. For Normal/Unauthenticated communication between the FireWall-1 and the SuperScout UFP Server, select the radio button for **Clear (opsec)**. For authenticated connection, select **OPSEC Authentication (auth_opsec)**. For further details on using authenticated communication, please refer to chapter 2 in the SuperScout Installation and Configuration guide (STWeb UFP Server Install Guide.pdf).



8. Click OK to exit and save the object.

Note: If you do not see the list of categories then this is an indication that there is a problem in the communication between FireWall-1 and the UFP Server. Common causes of this are that the UFP Server is not running or that the wrong host has been defined.

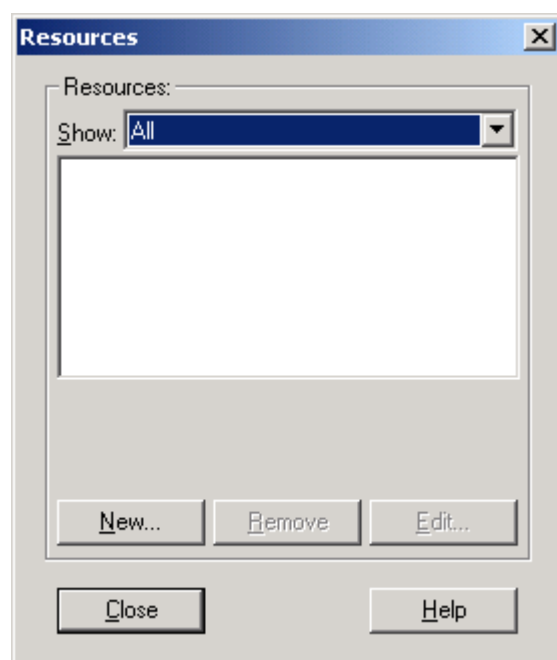
Creating a URI Resource

A URI is a Uniform Resource Identifier, of which the familiar URL (Uniform Resource Locator) is a specific class. A URI Resource is a collection of URIs. In the following example, the URI Resource contains the URLs within specified SuperScout categories.

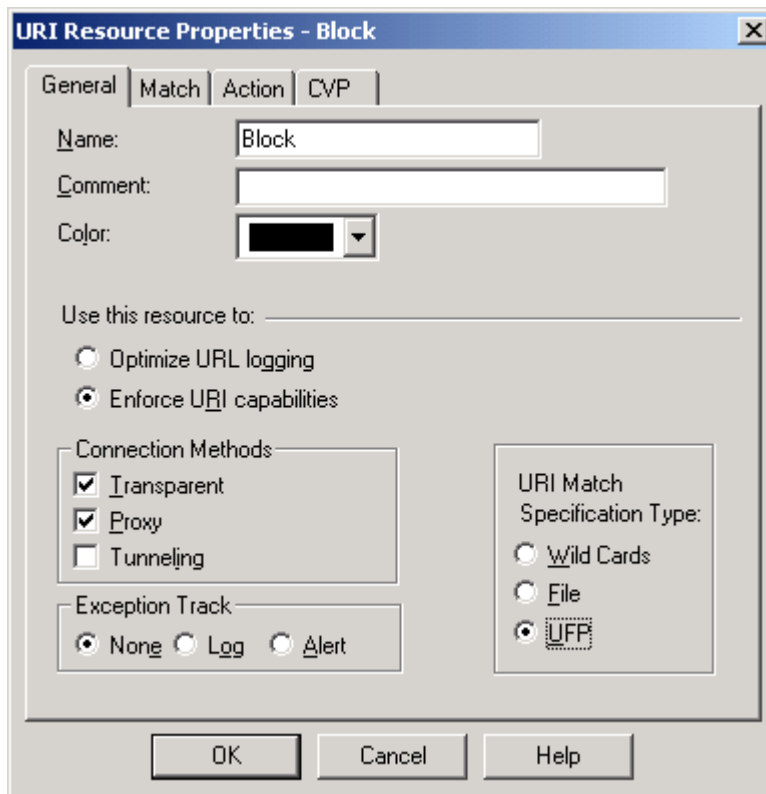
In the following procedure, a single URI resource is created for the SuperScout UFP Server.

To create a URI Resource

1. From the menu bar of the Check Point initial rule base policy select **Manage** and then **Resources** to display the following dialog:



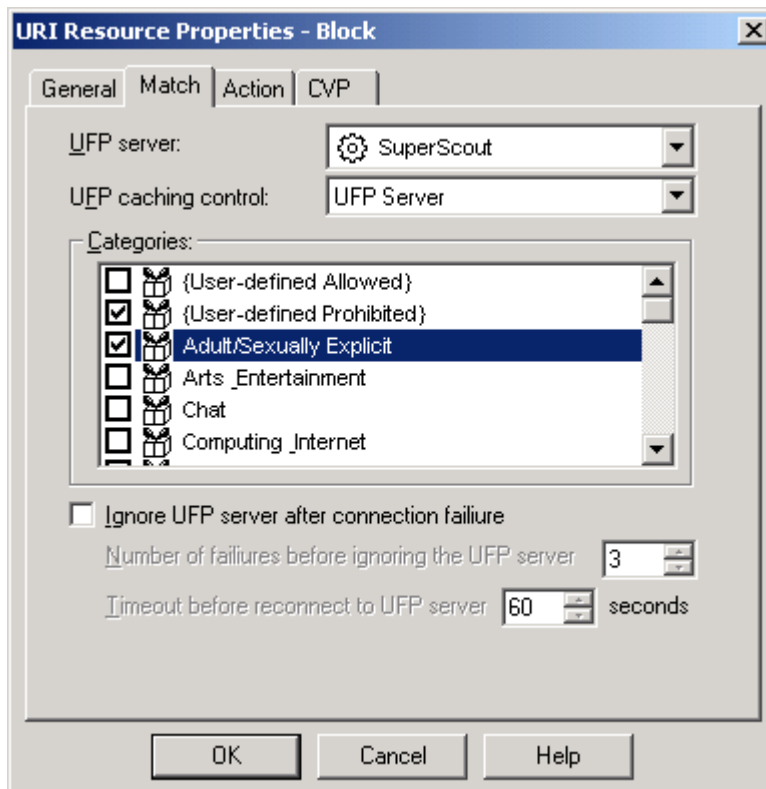
2. Click **New** and select **URI** from the drop-down menu. This will display the following dialog:



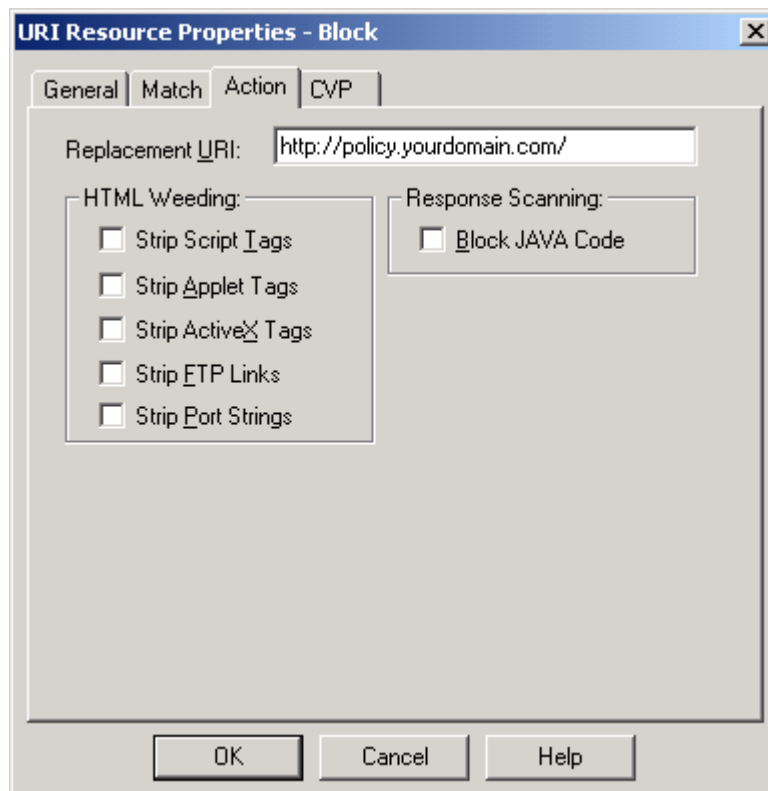
3. In the above example, the URI Resource is named 'Block' as we will be using it as an example of a common object contained in Drop or Reject rules.

Note: The name cannot have any spaces.

4. Fill in the details on the **General** tab.
5. In the section titled URI Match Specification Type, click the radio button for UFP.
6. Next select the **Match** tab to display the following dialog:



7. Choose your UFP Server from the drop-down list. The category list associated with this Server will be displayed.
 8. For UFP caching control select **UFP Server**. By Setting the UFP Caching Control to **UFP Server** the categorizations returned from SuperScout will be cached by FireWall-1 for a time period specified in the SuperScout Administrator UI.
 9. Check all categories associated with this resource, i.e. any URL categories that you would like to have blocked. These include specific categories such as Arts & Entertainment or non specific ones such as {User-defined Prohibited} and {User-defined Allowed}. You define the contents of these two User-defined categories by using the URL Exception List in the Administrator.
- Note: Once you have done this, all URLs that fit into these categories will be grouped into a single resource bearing the name that you entered in the Name edit field of the General tab.**
10. Finally select the **Action** tab in the URI Definition dialog:



11. If you want to specify a Replacement URI, type the URL to which the user will be redirected if they try to connect to a forbidden site. This would normally be the URL containing a message that explains your company's Acceptable Usage Policy.

The Replacement URI field here is similar to the Redirection URL field in the SuperScout Administrator. The only difference is that the Redirection URL works on a global level, while the Replacement URI can be different for each URI resource. If both the Replacement URI and the Redirection URL are specified, then the Redirection URL will override the Replacement URI.

12. Click **OK**. The next time that you access the **Resources** tab, you will see this resource already listed.

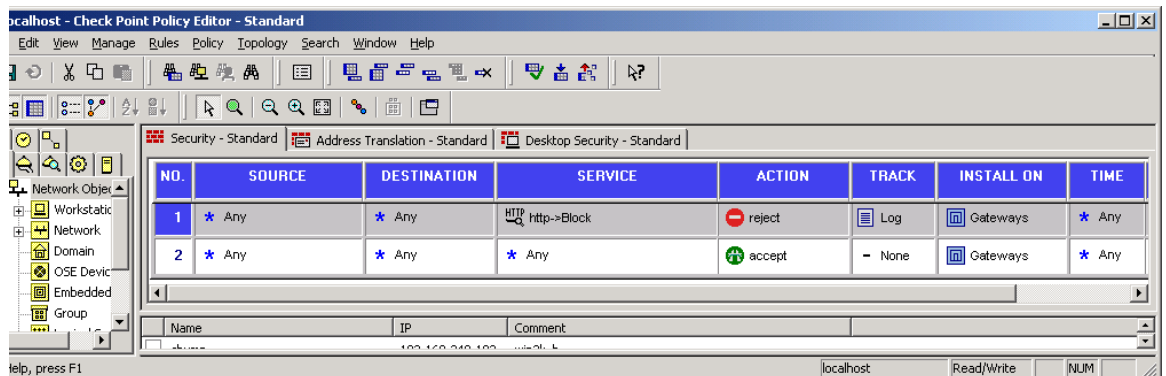
Inserting a URI Resource into a FireWall-1 Access Policy

You next need to define a rule for the HTTP traffic that should be checked by SuperScout. Go back to the rule base policy and add a new Accept rule (a rule that allows anyone access to anywhere at any time. Above this rule insert a new one that defines how you wish HTTP traffic to be blocked.

URI Resources are added to the FireWall-1 access policy by clicking the right mouse button over a rule's **Service** column. Place the URI Resource in the proper sequence to support your Internet Acceptable Use Policy.

To insert the SuperScout URI Resource into the FireWall-1 access policy

1. Access the **Check Point Policy Editor**:



2. Place the mouse cursor over the **Service** column and right click.
3. In the popup menu select **Add With Resource** to display a dialog that allows you to enter the URI Resource that you configured earlier.
4. In the **Action** column right-click and choose how you wish FireWall-1 to respond to any requests for access to the URLs grouped together under this URI resource.
5. Right-click in the **Track** column and choose the level of logging required.
6. Click the **Install Policies** button to install the policy.
7. Click **OK** to exit.