BLUE COAT

ProxySG Appliance/ SGOS

Blue Coat Security First Steps

Solution for Controlling Users' Access to Web Content

Security Empowers Business

SGOS 6.5

Third Party Copyright Notices

© 2014 Blue Coat Systems, Inc. All rights reserved. BLUE COAT, PROXYSG, PACKETSHAPER, CACHEFLOW, INTELLIGENCECENTER, CACHEOS, CACHEPULSE, CROSSBEAM, K9, DRTR, MACH5, PACKETWISE, POLICYCENTER, PROXYAV, PROXYCLIENT, SGOS, WEBPULSE, SOLERA NETWORKS, DEEPSEE, DS APPLIANCE, SEE EVERYTHING. KNOW EVERYTHING., SECURITY EMPOWERS BUSINESS, BLUETOUCH, the Blue Coat shield, K9, and Solera Networks logos and other Blue Coat logos are registered trademarks or trademarks of Blue Coat Systems, Inc. or its affiliates in the U.S. and certain other countries. This list may not be complete, and the absence of a trademark from this list does not mean it is not a trademark of Blue Coat or that Blue Coat has stopped using the trademark. All other trademarks mentioned in this document owned by third parties are the property of their respective owners. This document is for informational purposes only.

BLUE COAT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. BLUE COAT PRODUCTS, TECHNICAL SERVICES, AND ANY OTHER TECHNICAL DATA REFERENCED IN THIS DOCUMENT ARE SUBJECT TO U.S. EXPORT CONTROL AND SANCTIONS LAWS, REGULATIONS AND REQUIREMENTS, AND MAY BE SUBJECT TO EXPORT OR IMPORT REGULATIONS IN OTHER COUNTRIES. YOU AGREE TO COMPLY STRICTLY WITH THESE LAWS, REGULATIONS AND REQUIREMENTS, AND ACKNOWLEDGE THAT YOU HAVE THE RESPONSIBILITY TO OBTAIN ANY LICENSES, PERMITS OR OTHER APPROVALS THAT MAY BE REQUIRED IN ORDER TO EXPORT, RE-EXPORT, TRANSFER IN COUNTRY OR IMPORT AFTER DELIVERY TO YOU.

Americas:

Blue Coat Systems, Inc.

420 N. Mary Ave.

Sunnyvale, CA 94085

Rest of the World:

Blue Coat Systems International SARL

3a Route des Arsenaux

1700 Fribourg, Switzerland

Contents

Solution: Control Users' Access to Web Content

Web URLs can be grouped into various categories, such as social networking, gambling, pornography, news media, and shopping.The ProxySG is able to analyze URLs that users request, determine what category the website belongs to, and restrict access to the categories that your organization deems inappropriate or a potential threat to your network.

Controlling users' access to Web content involves configuring Blue Coat WebFilter (BCWF), an on-box content filtering database, as well as configuring policy for URL categories.

1. Enable BCWF and download the latest database. See Configure Blue Coat WebFilter.
2. Make sure that the dynamic rating service, WebPulse, is enabled. See Configure WebPulse Services.
3. Determine which categories you want to restrict access to. See View the List of Available Categories.
4. Block "bad" categories. See Restrict Access to Categories.
5. (Optional). See Restrict Category Access by Time of Day.

   Note: This solution assumes that you have HTTP and/or HTTPS set to intercept.

Set Services to Intercept

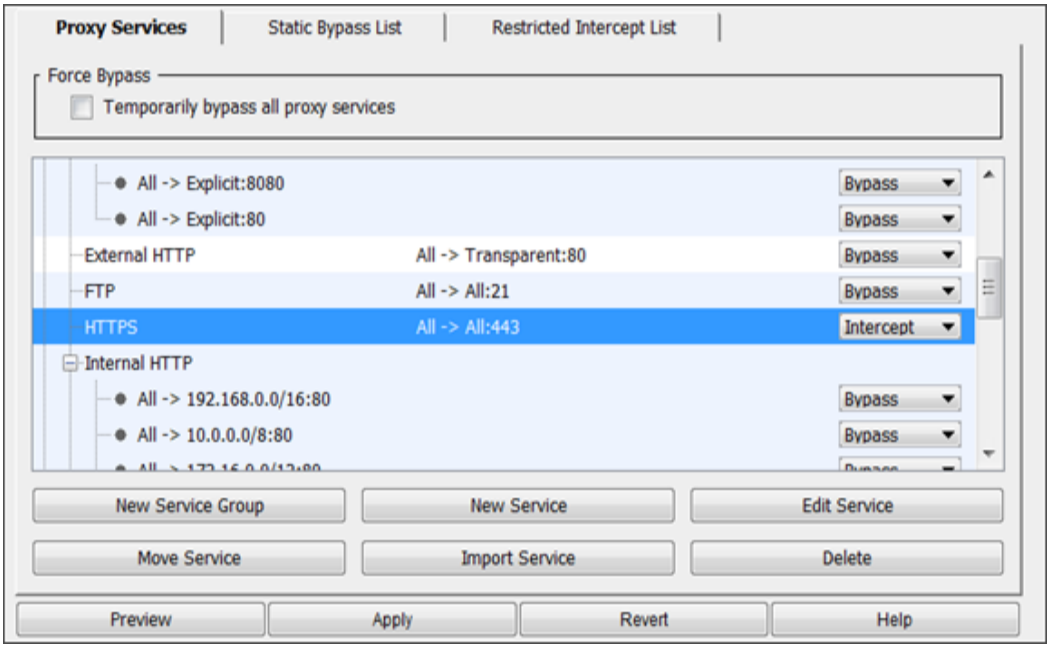
In transparent ProxySG deployments, Internet applications aren't aware that the proxy is in the network, so the ProxySG has to monitor the ports used for their traffic. The most common ports are 80, (HTTP) 443 (HTTPS), and 1935 (RTMP).

> Caution: Any transparent traffic that doesn't have a proxy service set to intercept will pass through the proxy's interfaces unfiltered.

For explicit proxy deployments, client browsers direct all traffic to the appliance on the same port, (typically 80 or 8080). When explicit traffic is intercepted, the appliance uses an advanced protocol detection method to identify the type of traffic (HTTP, HTTPS, RTMP, and so on) and handles it according to the standards for that traffic.

Transparent Proxy Services

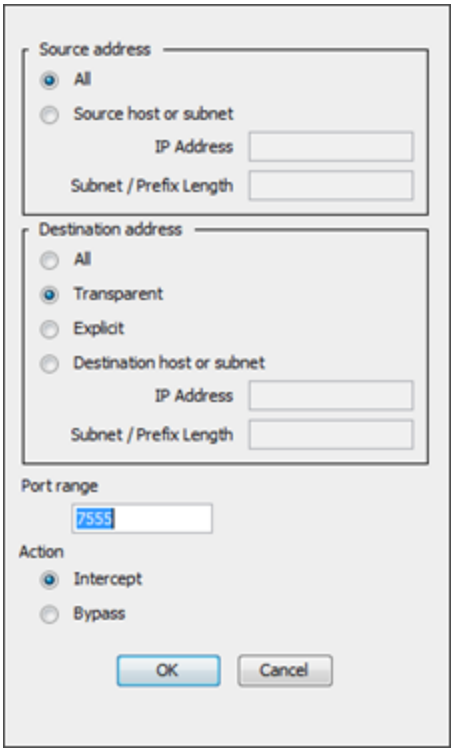
1. In the Management Console, select **Configuration > Services > Proxy Services**.
2. Under Predefined Service Groups, expand the **Standard** group. A list of services displays.
3. Locate the service you want to set to Intercept.
4. From the drop-down menu next to the service, select **Intercept**. In this example, the HTTPS service is set to Intercept.



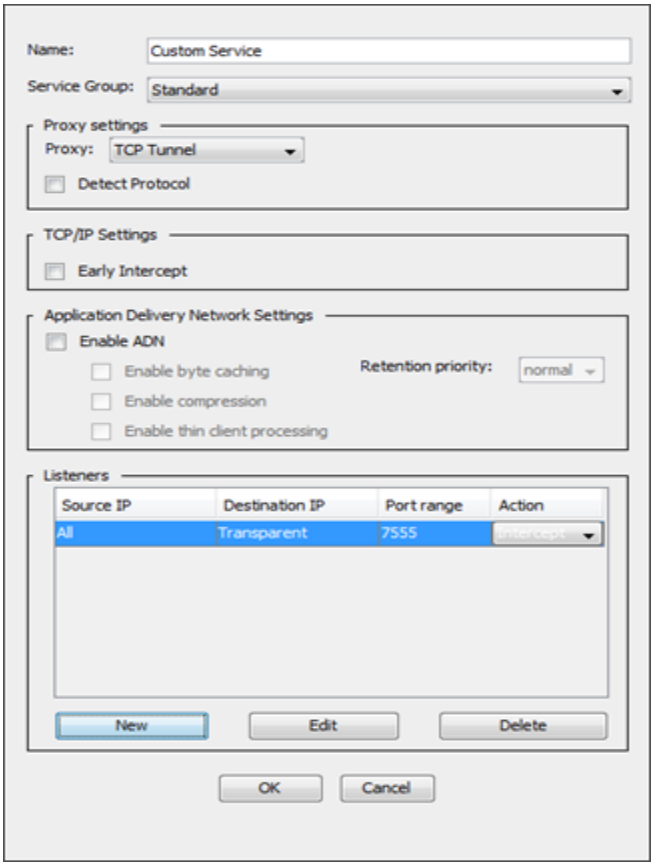
5. Repeat steps 3 and 4 for each additional service you want to intercept.
6. (Optional) To intercept traffic types that are not predefined:
   a. Click **New Service**.
   b. Enter a name for the service and select the service group, under which the new service will be listed.
   c. Select a proxy type from the **Proxy** drop-down menu. This menu lists all of the types of traffic the ProxySG understands. If the type of traffic you are intercepting is not listed, select **TCP Tunnel**.

      Caution: Tunneled traffic can only be controlled based on the information contained in the TCP header of the request: client IP, destination IP, and source and destination ports.

   d. Click **Edit/Add Listeners**. The New Listener dialog displays.



e. In the **Port range** field, enter the port your application uses to communicate.
f. Ensure that the **Action** field is set to **Intercept** and click **OK**.
g. If enabled, uncheck **Enable ADN**.

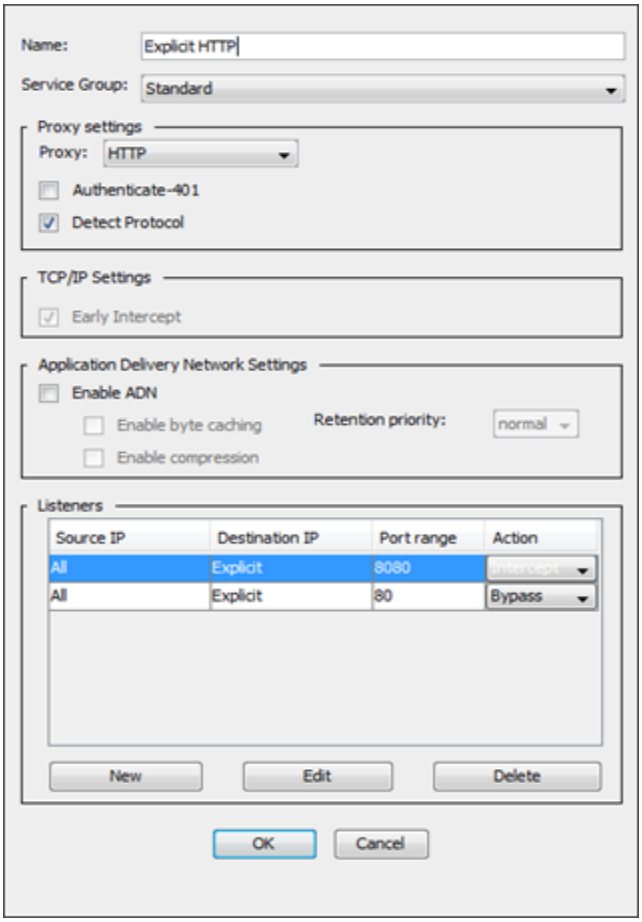


h. Click **OK** .

7. Click **Apply**. The appliance confirms your changes.

Explicit Proxy Services

1. In the Management Console, select **Configuration > Services > Proxy Services**.
2. Under Predefined Service Groups, expand the **Standard** group. A list of services displays.
3. Locate **Explicit HTTP**, select it, and click **Edit Service**.
4. Enable **Detect Protocol**.
5. Under **Listeners**, set the explicit proxy ports (8080 and/or 80) to **Intercept**.

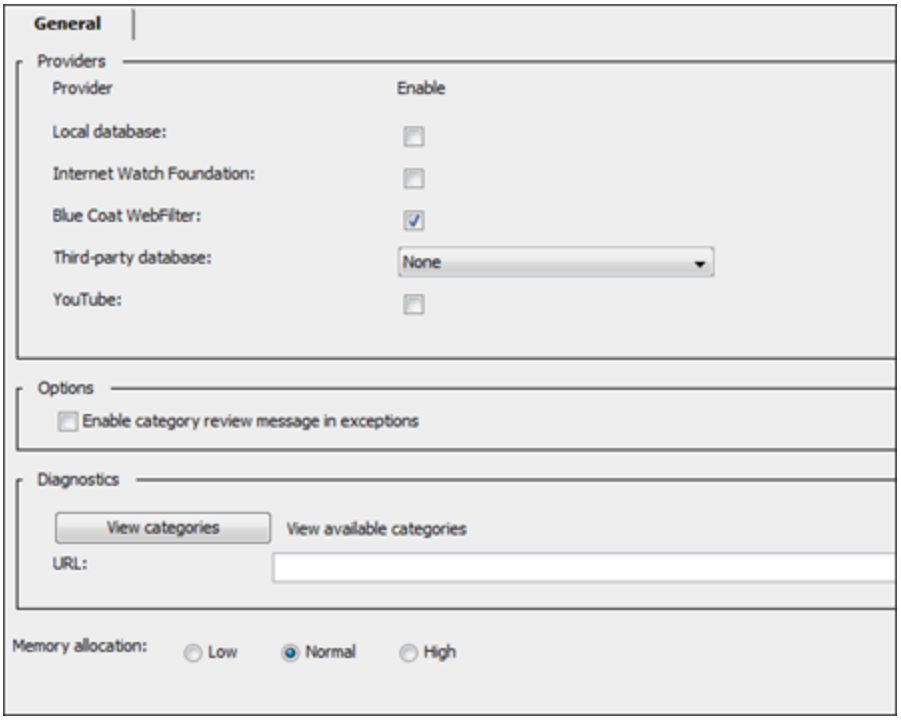


6. Click **OK** and **Apply** . The appliance confirms your changes.

Configure Blue Coat WebFilter

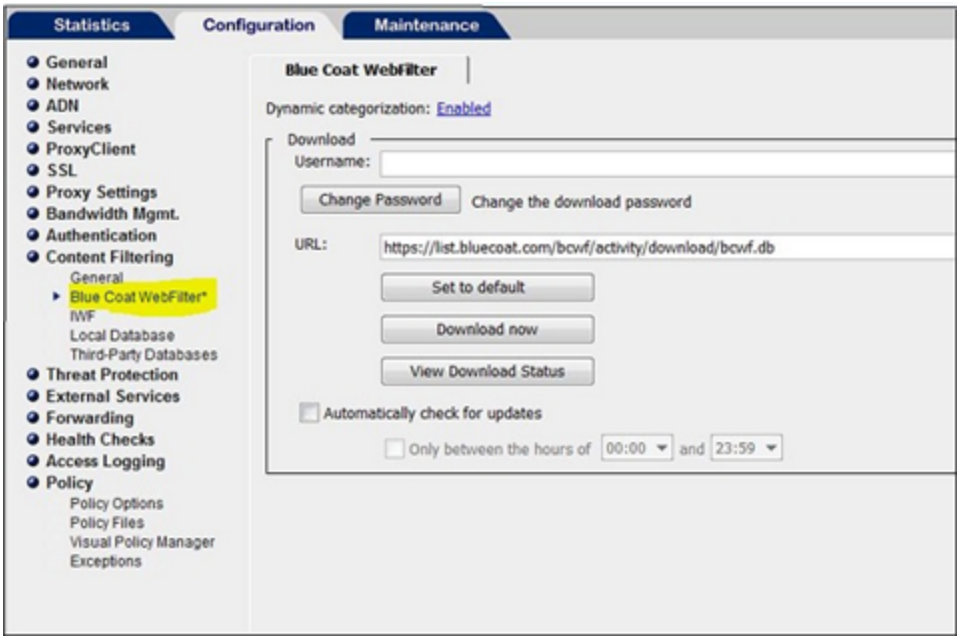
Blue Coat WebFilter (BCWF) is an on-box content filtering database. To control access to websites and web applications, you need to enable BCWF and download the latest database.

1. Confirm that you have a Proxy Edition license (not a MACH5 license). The license name appears in the banner of the Management Console banner.
2. Enable Blue Coat WebFilter:
    a. Select **Configuration > Content Filtering > General**.
    b. For **Blue Coat WebFilter**, select the checkbox in the Enable column.



c. Click **Apply**.

3. Download a current BCWF database:
   a. Select **Configuration > Content Filtering > Blue Coat WebFilter.**



   b. Click **Download now**.
   c. Click **Apply**.

Note: In addition to BCWF, ProxySG also supports third-party or local content filtering databases.

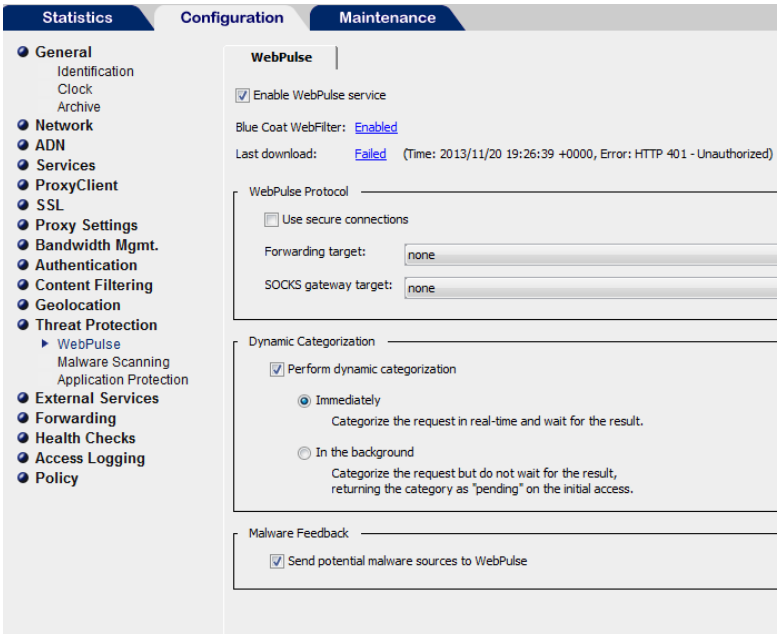
Next Step: Configure WebPulse Services

Configure WebPulse Services

WebPulse provides an off-box dynamic categorization service for real-time categorization of URLs that are not rated or categorized in the on-box BCWF database. This cloud service blocks malware hosts, rates web content, and provides dynamic categorization. The WebPulse cloud service is enabled by default when you use BCWF.

1. In the ProxySG Management Console, select **Configuration > Threat Protection > WebPulse**.
2. Ensure the **WebPulse Service** check box is selected.
3. Ensure the **Perform Dynamic Categorization** check box is selected.
4. Select your preference for performing dynamic categorization:
   Immediately - Categorize in real time and wait for the result before proceeding to a requested URL.
   In the background - WebPulse runs in the background without waiting for a response when a URL is requested. The response from WebPulse is placed into the categorization cache so that when another user requests the same URL, WebPulse will not process the URL again.

Below is an example configuration.



Next Step: View the List of Available Categories

View the List of Available Categories

The BCWF database contains a read-only list of available categories. Before setting polices to block categories, you should review the list to determine which categories you want to restrict.

1. Select **Configuration > Content Filtering > General**.
2. Click **View Categories**. The list displays in a new window.

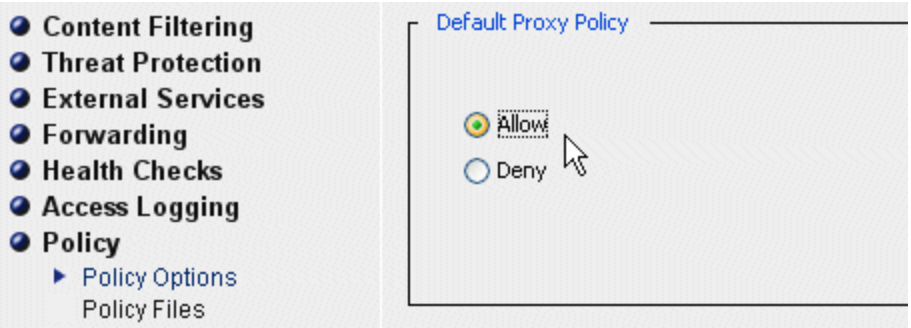
   Tip If you want to find out which category a URL belongs to, you can test the URL. The Test option is in the Diagnostics section of the Management Console. Select **Configuration > Content Filtering > General** .

Next Step: Restrict Access to Categories

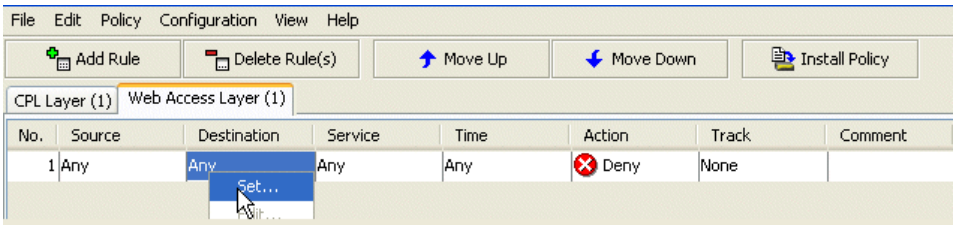
Restrict Access to Categories

You must create policy rules for each category you want to block. Use the Visual Policy Manager(VPM) to create your policy rules.

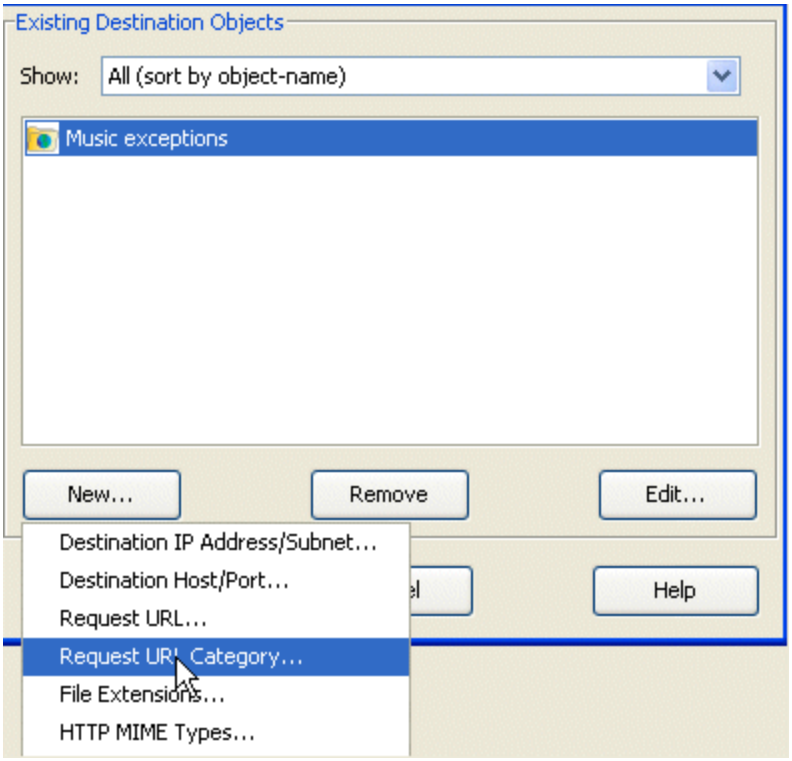
1. Verify that the default proxy policy is set to **Allow** by selecting **Configuration > Policy > Policy Options**.



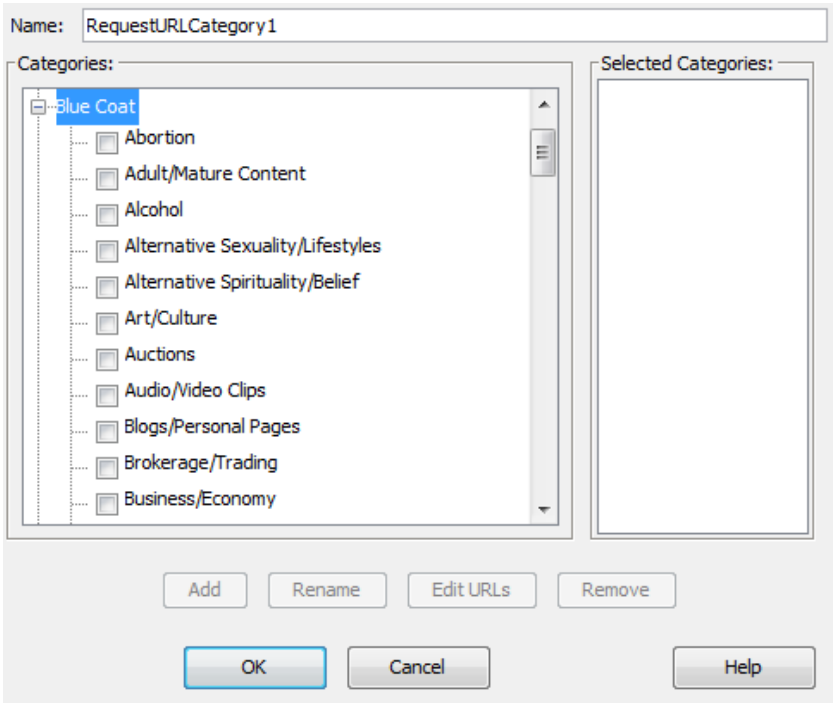
2. To configure policy in the Visual Policy Manager (VPM), select **Configuration > Policy > Visual Policy Manager > Launch**. The VPM opens in a new window.
3. In the Visual Policy Manager (VPM), select **Policy > Add Web Access Layer**.
4. Give the Web Access Layer a unique name, such as Blocked Categories.
5. Click **OK**.
6. If necessary, click **Add Rule**. A new rule displays in the Web Access Layer.
7. In the **Destination** column of the new rule, right-click and select **Set**.



8. In the Set Destination Object dialog, click **New**. In the drop down list, select **Request URL Category**.



9. In the Add Request URL Category Object dialog, expand the Blue Coat folder. Select the categories you would like to block.



10. Give the category object a unique name.

11. Click **OK**. The Request URL Category Object dialog closes.
12. Click **OK**. The Set Destination Object dialog closes.
13. Click **Install Policy**.
14. Click **OK**.

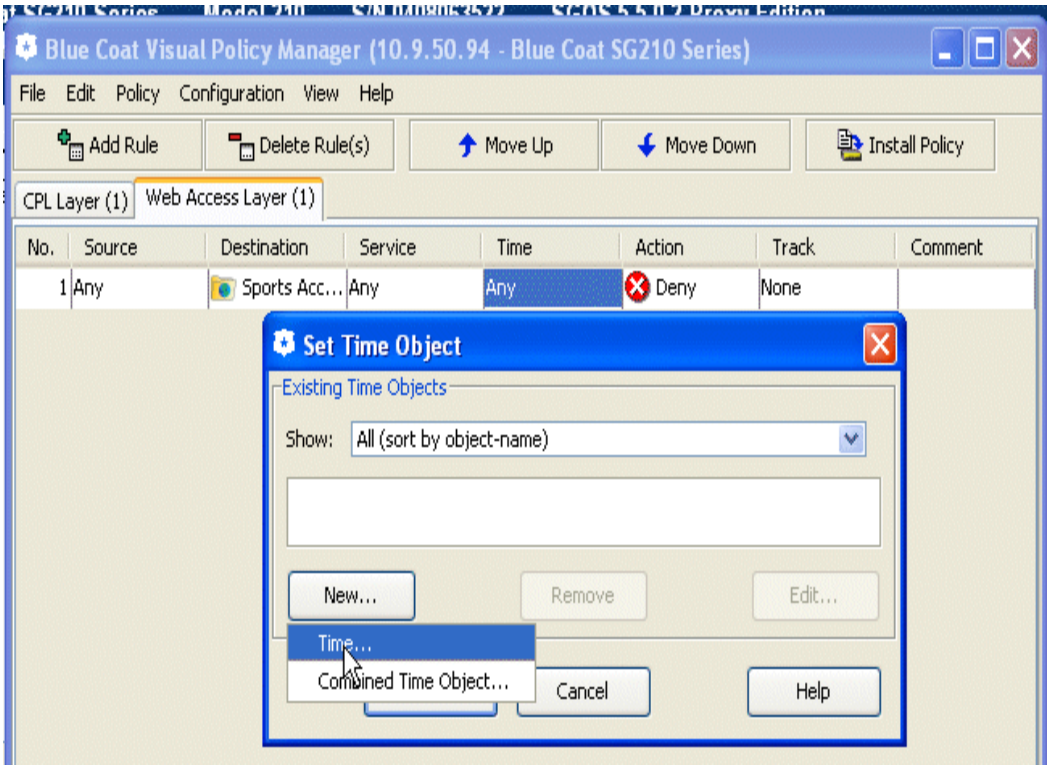
Next Step: Restrict Category Access by Time of Day

Restrict Category Access by Time of Day

Some categories, such as Phishing and Malicious Sources, should be blocked at all times of the day, while less dangerous categories, such as Chat/Instant Messaging and Audio/Video Clips, can be blocked during business hours only.

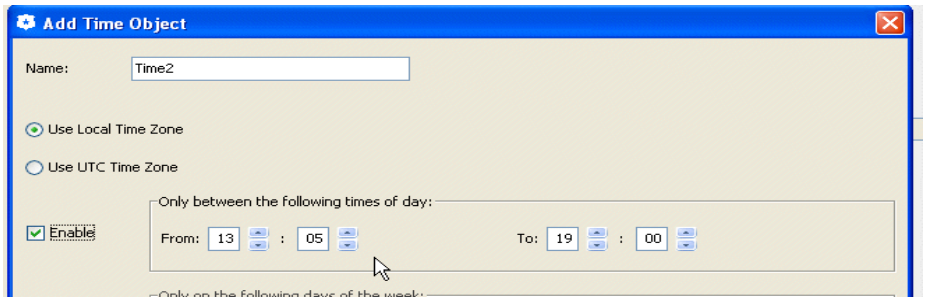
For example, you can block the Radio category from 8am to 5pm, allowing employees to stream radio after business hours.

1. If you have not already done so, create a rule for the category you want to restrict. See Restrict Access to Categories.
2. In the rule you want to restrict by time of day, right click the **Time** column and select **Set**.
3. In the Set Time Object dialog, select **New > Time**.



4. In the Add Time Object dialog, give your time object a descriptive name, such as Business Hours.

5. Enter the time interval you would like to restrict in the **From** and **To** sections of the Add Time Object dialog.



6. Click **OK.**
7. Repeat the above steps for any other rule you want to restrict by time of day.
8. Click **Install Policy**.

Content Filtering Troubleshooting

How do I block uncategorized URLs?

Problem: I would like to block all URLs that are uncategorized.

Resolution: Uncategorized URLs are categorized in the category None. Follow the procedure below to deny all categories in the category None.

1. Open the Visual Policy Manager by selecting **Configuration > Policy > Visual Policy Manager > Launch**. The VPM opens in a new window.
2. Add a new rule in a Web Access Layer. See Restrict Access to Categories.
3. Right-click in the **Destination** column and select **Set > New > Request URL Category**.
4. Name the URL category object.
5. Expand **System** and select **None**.
6. Click **OK** to close the dialogs.
7. Right click the **Set Action** column and select **DENY**.
8. Click **Install policy**.
9. Click **Ok**.

How do I override URL category filtering for a website?

Problem: I would like to allow access to a URL but the category associated with the URL is blocked.

Solution: You can allow access to websites that are denied by your policy by creating a whitelist.

For example, the social media category is blocked, but you would like to allow your employees access to Facebook, you can do that by creating a white list. To create a white list see the topic Create Whitelist .

> Note: You can only create a whitelist if the default proxy policy is set to deny.

Create Whitelist

A whitelist allows you to allow access to specific website while the category the URL represents is unallowed. For example, while pornography is a blocked category, you can use the whitelist to allow access to playboy.com since there are no nude photographs on its front page. You can only create a whitelist if the default proxy policy is set to deny.

1. From the Management Console, select **Configuration > Policy > Visual Policy Manager > Launch**. The visual policy dialogue displays.
2. Select **Policy > Add Web Access Layer**. Give the web access layer a unique name. For example "Web Access Exceptions.

3. Click **OK.**
4. Click **Add a Rule**.
5. Right click the **Destination** column within the rule and select **Set**.
6. Click **New**, and select **Request URL Category**.

   Note: You can only create a whitelist if the default proxy policy is set to deny.

Next Step: Restrict Access to Categories

How can I fix a URL that's been incorrectly categorized?

Problem: Some URLs appear to be in the wrong category.

Resolution: If you believe that a URL is associated with the wrong category, you can make a request to Blue Coat asking to change the category of the URL.

1. Go to http://sitereview.bluecoat.com/sitereview.jsp and enter the valid site for the review process.
2. In the **Filtering Service** drop-down dialog, choose Blue Coat ProxySG.
3. Select the category you suggest the site should belong to.
4. Provide as much detail about the website in the **Comments and Description** dialog.
5. Click **Submit** for Review.

If the URL is accepted for the specified category, it will be updated within 24 to 48 hours.