Blue Coat Security First Steps
Solution for Streaming Media
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
# Blue Coat Security First Steps

## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third Party Copyright Notices</td>
<td>2</td>
</tr>
<tr>
<td><strong>Solution: Control Streaming Media</strong></td>
<td>4</td>
</tr>
<tr>
<td>Solution: Improve Quality of Streaming Media</td>
<td>4</td>
</tr>
<tr>
<td>Set Services to Intercept</td>
<td>5</td>
</tr>
<tr>
<td>Transparent Proxy Services</td>
<td>6</td>
</tr>
<tr>
<td>Explicit Proxy Services</td>
<td>8</td>
</tr>
<tr>
<td>Configure Media Players for Explicit Proxy</td>
<td>9</td>
</tr>
<tr>
<td>Configure Windows Media Player</td>
<td>10</td>
</tr>
<tr>
<td>Configure QuickTime Player</td>
<td>11</td>
</tr>
<tr>
<td>Configure RealPlayer</td>
<td>12</td>
</tr>
<tr>
<td>Fine Tune Streaming Proxy Settings</td>
<td>14</td>
</tr>
<tr>
<td>View Bandwidth Savings</td>
<td>15</td>
</tr>
<tr>
<td>List Active Sessions</td>
<td>16</td>
</tr>
<tr>
<td>Solution: Restrict Streaming Media Traffic</td>
<td>17</td>
</tr>
<tr>
<td>Set Services to Intercept</td>
<td>19</td>
</tr>
<tr>
<td>Transparent Proxy Services</td>
<td>19</td>
</tr>
<tr>
<td>Explicit Proxy Services</td>
<td>21</td>
</tr>
<tr>
<td>Limit Bandwidth of Streaming Media</td>
<td>22</td>
</tr>
<tr>
<td>Monitor Bandwidth Utilization</td>
<td>23</td>
</tr>
<tr>
<td>View Bandwidth Savings</td>
<td>24</td>
</tr>
<tr>
<td><strong>Streaming Media Troubleshooting</strong></td>
<td>26</td>
</tr>
<tr>
<td>Why can't users view streaming videos?</td>
<td>26</td>
</tr>
<tr>
<td>Why do Flash videos stop streaming in the middle?</td>
<td>26</td>
</tr>
<tr>
<td>Why won't Flash videos play?</td>
<td>26</td>
</tr>
<tr>
<td>Why aren't Ustream videos playing in Safari?</td>
<td>27</td>
</tr>
</tbody>
</table>
Solution: Control Streaming Media

The ProxySG offers a number of proxies for streaming media:

- Adobe HDS (HTTP Dynamic Streaming)
- Apple HLS (HTTP Live Streaming)
- Flash
- MS Smooth
- Windows Media
- QuickTime
- Real Media

When the native streaming proxies are being used, the ProxySG makes sure that the protocol behavior is standard compliant, allowing it to filter out buffer overflow attacks on the protocol level. This security feature is not configurable—it happens automatically.

In addition to providing a level of security, the streaming proxies offer other benefits, as described in the following solutions:

Solution: Improve Quality of Streaming Media
Solution: Restrict Streaming Media Traffic

Tip Download the Streaming Media solution (PDF).

Solution: Improve Quality of Streaming Media

The ProxySG's streaming proxies are able to improve the quality of streaming media, reducing artifacts such as frozen playback and dropped frames.

These are the basic steps you need to perform to improve the quality of streaming media:

1. To control streaming media traffic, the appliance must be configured to intercept the following services:

   RTMP (for Flash)
   RTSP and MMS (for Windows Media, Real Media, and QuickTime)
   Explicit HTTP, External HTTP, and/or Internal HTTP (for Microsoft Smooth Streaming, Apple HLS, Adobe HDS)

   See Set Services to Intercept; make sure the applicable streaming services are set to intercept.

2. **Explicit Deployments:** The media players on each client system should be configured with the IP address of the ProxySG appliance. See Configure Media Players for Explicit Proxy.

3. The ProxySG appliance is preconfigured to automatically hand off streaming media traffic to the streaming proxies. To verify the HTTP handoff setting is enabled, see Fine Tune Streaming Proxy Settings.

4. To monitor streaming media traffic on your network:
   - Display the Traffic Mix report and locate the streaming proxy you are interested in (such as Flash or Windows Media). Observe the amount of Client Bytes, Server Bytes, and Savings. See View Bandwidth
Display active connections and filter the list for the streaming proxy you are interested in (Adobe HDS, Apple HLS, Flash, MS Smooth, Windows Media, Real Media, or QuickTime). See List Active Sessions.

5. Although not a scientific measurement, talk to users to find out anecdotal information about the quality of streaming traffic after deploying the ProxySG.

Set Services to Intercept

Before you can control or take advantage of the caching and optimization features for streaming media, your ProxySG appliance has to be configured to intercept that traffic.

If your appliance is deployed explicitly, ensure that the explicit proxy service, (typically on port 8080) has Detect Protocol enabled. When streaming media is requested by an explicit user, the appliance will identify it as such. It can then make use of advanced Flash streaming optimization, caching, and reporting features.

If your appliance is deployed transparently, it is important to capture the traffic on all of the various ports each streaming media protocol uses. Specifically:
Controlling Streaming Media

- Flash media (RTMP) uses port 1935.
- Real Time Streaming Protocol (RTSP) uses port 554.
- Microsoft Media Server (MMS) uses port 1755.

To intercept this traffic, follow either the transparent or explicit instructions below, depending on your deployment.

**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.

![Proxy Services](image)

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.
Blue Coat Security First Steps

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.
7. Click **OK**. 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.

Next Step: Return to **Solution: Improve Quality of Streaming Media** (step 2).

**Configure Media Players for Explicit Proxy**

When the ProxySG is deployed explicitly and you want to optimize and control streaming media, you need to configure the browsers and media players on each client system to use the ProxySG as an explicit proxy. After you have configured the media players, the appliance controls the traffic with the appropriate streaming proxy (Windows Media, QuickTime, or Real Media).

Note: Streaming media that is embedded in a Web page, and plays in the browser, is handed off to the streaming proxies.

Configure Windows Media Player

Configure QuickTime Player

Configure RealPlayer
Controlling Streaming Media

Configure Windows Media Player

When the ProxySG is deployed explicitly and you want to secure and optimize streaming media, you need to configure the media players on each client system to use the ProxySG as an explicit proxy. For transparent deployments, you do not need to do any special configuration in the media player.

Note: This procedure features Windows Media Player series 9. Installation and setup menus may vary with different versions of Media Player.

1. Start Windows Media Player.
2. Select Tools > Options.
3. Select the Network tab.
4. In the list of streaming protocols, disable the following protocols: Multicast, UDP, and TCP. The only protocol that should be selected is HTTP; this forces the player to use HTTP as the protocol for streaming.
5. In the Streaming Proxy Settings section, select the HTTP protocol and click Configure.

6. In the Configure Protocol dialog, configure the proxy settings:
   a. Select Use the following proxy server.
   b. Enter the IP address of the ProxySG and the port number used for the explicit proxy (8080).
c. These settings must match the settings configured on the appliance. If you change the explicit proxy configuration, you must also reconfigure Windows Media Player.

7. Click OK in both dialogs.

Windows Media Player now proxies through the ProxySG and content will be cached and controlled according to the streaming proxy settings configured on the appliance.

**Configure QuickTime Player**

When the ProxySG is deployed explicitly and you want to secure and optimize streaming media, you need to configure the browser and media players on each client system to use the ProxySG as an explicit proxy. For transparent deployments, you do not need to do any special configuration in the media player.

Note: This procedure features QuickTime Player version 7.7.4. Installation and setup menus may vary with different versions of QuickTime.

1. Start QuickTime Player.
2. Select **Edit > Preferences > QuickTime Preferences**.
3. Configure the protocol settings:
   a. Click the **Advanced** tab.
   b. Select **RTSP Proxy Server**.
   c. Enter the IP address of the ProxySG and the port number used for the explicit proxy (8080).
d. Click **OK**.

QuickTime now proxies (in pass-through mode) through the ProxySG.

These settings must match the settings configured on the appliance. If you change the ProxySG explicit proxy configuration, you must also reconfigure QuickTime Player.

### Configure RealPlayer

When the ProxySG is deployed explicitly and you want to optimize and control streaming media, you need to configure the browser and media players on each client system to send streaming requests through the ProxySG. For transparent deployments, you do not need to do any special configuration in the media player.

Note: This procedure features RealPlayer SP version 1.1.5. Installation and setup menus may vary with different versions of RealPlayer.

1. Start RealPlayer.
2. Select **Tools > Preferences**.
3. In the Category section in the left pane, select **Connection > Proxy**.
4. Click **Change Settings** in the Streaming Settings section.
5. Configure options:
   a. Select **Use proxies**.
   b. In the **RTSP** field, enter the IP address of the ProxySG and the port number used for the explicit proxy (8080).
c. In the HTTP Proxy section, choose **Use proxy** and enter the IP address of the ProxySG and the port number used for the explicit proxy (8080).

These settings must match the settings configured on the appliance. If you change the ProxySG explicit proxy configuration, you must also reconfigure RealPlayer.

d. To close the Streaming Proxy Settings dialog click **OK**.

To enable the RealPlayer sessions to show up in reports, RealPlayer must be instructed to communicate with the RealServer.

1. In the Category section in the left pane, select **Connection > Internet/Privacy**.
2. In the Privacy Settings section, make sure the **Send connection-quality data to RealServers** is selected, and click **OK**.

RealPlayer now proxies through the ProxySG and content will be cached and controlled according to the streaming proxy settings configured on the appliance.

### Fine Tune Streaming Proxy Settings

You can configure settings for each of the supported streaming media clients: Flash, HTTP (Microsoft Smooth Streaming, Apple HLS, Adobe HDS), Windows Media, Real Media, and QuickTime.
Blue Coat Security First Steps

1. Select Configuration > Proxy Settings > Streaming Proxies.

2. Click the tab of the streaming client you want to configure: Flash, HTTP, Windows Media, Real Media, or QuickTime.

3. The Enable HTTP handoff option is enabled by default. When a streaming client requests a stream from the ProxySG over port 80 (typically the only port that allows traffic through a firewall), the HTTP module passes control to the streaming module so HTTP streaming can be supported through the HTTP proxy port. This is the HTTP handoff.

   Disable this option only if you do not want the appliance to cache on-demand streams or split a live stream to multiple local users; typically there is no reason to do this unless Support requests you to do so for troubleshooting purposes.

4. Configure other options if desired.

5. Click Apply if you made any changes.

Next Step: Return to Solution: Improve Quality of Streaming Media (step 4).

View Bandwidth Savings

To determine how much bandwidth savings you are getting by having the ProxySG manage your traffic, look at the Traffic Mix page. For each service or proxy, this page provides the percentage of bandwidth that has been saved in a specified time period.

1. In the Management Console, select Statistics > Traffic Details > Traffic Mix.

2. Decide whether you want to view services or proxies: select Service or Proxy.

3. Select the time period you are interested in. From the Duration drop-down, select Last Hour, Last Day, Last Week, Last Month, or Last Year.

   The graphs and statistics automatically update to reflect the time period you selected.

4. (Optional) Clear the Include bypassed bytes checkbox if you don't want to include bypassed traffic in the graphs, statistics, and calculations so that you can get a clearer view of intercepted traffic.

5. To view the total bandwidth gain for all services or proxies, click the BW Gain tab under the line graph.
The line graph shows the bandwidth gain from optimization during the specified time period, expressed as a multiple (for example, 2x). The gain is calculated as follows:

\[
\text{Gain} = \frac{\text{client\_bytes}}{\text{server\_bytes}}
\]

6. To view the bandwidth savings per service or proxy, look at the Savings column in the table.

<table>
<thead>
<tr>
<th>Savings</th>
</tr>
</thead>
<tbody>
<tr>
<td>n/a</td>
</tr>
<tr>
<td>96.98%</td>
</tr>
<tr>
<td>0%</td>
</tr>
<tr>
<td>0.99%</td>
</tr>
<tr>
<td>1.96%</td>
</tr>
<tr>
<td>n/a</td>
</tr>
</tbody>
</table>

The savings percentage is the average bandwidth savings due to optimization, during the specified time period. The savings is calculated as follows:

\[
\text{Savings} = \frac{\text{client\_bytes} - \text{server\_bytes}}{\text{client\_bytes}} \times 100
\]

7. To view the total bandwidth savings for all services or proxies, look at the Total Savings value, underneath the table.

**Total Savings:** 18.01%

8. If you are interested in other time periods or other proxies/services, repeat steps 2-7.

**Next Step:** List Active Sessions

**List Active Sessions**

Display active connections and filter the list for the streaming proxy you are interested in (Adobe HDS, Apple HLS, Flash,
Blue Coat Security First Steps

MS Smooth, Windows Media, Real Media, or QuickTime).

The Active Sessions report provides an immediate picture of the client-server sessions and the associated protocols, services, bytes, savings, and other statistics.

1. In the Management Console, select **Statistics > Sessions > Active Sessions > Proxied Sessions**.
2. From the **Filter** drop-down list, select **Proxy**.
3. Select a proxy name from the drop-down list.
4. Click **Show** to see the list of connections for the selected proxy.

Next Step: Return to **Solution: Improve Quality of Streaming Media** (step 5).

Solution: Restrict Streaming Media Traffic

Without bandwidth limiting controls, streaming media can easily cause congestion on your network and disrupt mission-critical traffic.

These are the basic steps you need to perform to limit the bandwidth of streaming media:

1. To control streaming media traffic, the appliance must be configured to intercept the following services:
   
   RTSP and MMS (for Windows Media, Real Media, and QuickTime)
   
   Explicit HTTP, External HTTP, and/or Internal HTTP (for protocols that stream over HTTP)

   See **Set Services to Intercept**; make sure the applicable streaming services are set to intercept.

2. **Explicit Deployments**: The media players on each client system must be configured with the IP address of the ProxySG appliance. See **Configure Media Players for Explicit Proxy**.

3. **Limit Bandwidth of Streaming Media**.

4. To verify that the bandwidth limits are being enforced, you can look at Traffic History utilization graphs for the streaming proxies. See **Monitor Bandwidth Utilization** and select the service or proxy you are interested in.
5. If the appliance is caching video and audio files and optimizing the delivery of streaming media, you will see an increase in bandwidth savings for the streaming services and proxies. See View Bandwidth Savings.
Blue Coat Security First Steps

Set Services to Intercept

Before you can control or take advantage of the caching and optimization features for streaming media, your ProxySG appliance has to be configured to intercept that traffic.

If your appliance is deployed *explicitly*, ensure that the explicit proxy service, (typically on port 8080) has **Detect Protocol** enabled. When streaming media is requested by an explicit user, the appliance will identify it as such. It can then make use of advanced Flash streaming optimization, caching, and reporting features.

If your appliance is deployed *transparently*, it is important to capture the traffic on all of the various ports each streaming media protocol uses. Specifically:

- Flash media (RTMP) uses port 1935.
- Real Time Streaming Protocol (RTSP) uses port 554.
- Microsoft Media Server (MMS) uses port 1755.

To intercept this traffic, follow either the transparent or explicit instructions below, depending on your deployment.

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
Controlling Streaming Media

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**.
Blue Coat Security First Steps

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.
5. Under Listeners, set the explicit proxy ports (8080 and/or 80) to Intercept.

Explicit Proxy Services

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

**Next Step: Return to Solution: Improve Quality of Streaming Media** (step 2).

**Limit Bandwidth of Streaming Media**

So that your network doesn't get overloaded with users watching recreational streaming videos, you may want to limit bandwidth from the streaming media clients to the ProxySG or from the appliance to the servers that contain streaming content. The ProxySG Management Console has settings for limiting bandwidth of Windows Media, QuickTime, and RealMedia. For protocols that stream over HTTP, you can write policy in CPL.

Note: This solution does not apply to Flash streaming.

**Windows Media, QuickTime, and Real Media**

1. Decide how much of your WAN bandwidth you are willing to set aside for streaming media traffic; this number (in kilobits per second) is the gateway bandwidth limit.

Suppose you have a 10 Gbps link and you know that you regularly have 7 Gbps of business-related traffic; you may
Blue Coat Security First Steps

then decide that it’s acceptable to have up to 3 Gbps of streaming traffic without disrupting business traffic.

2. In the Management Console, select Configuration > Proxy Settings > Streaming Proxies > General.

3. To limit the bandwidth for streaming client connections, select Client bandwidth limit and enter the maximum number of kilobits per second that the appliance allows for all streaming client connections.

4. Using the value determined in step 1, specify the gateway bandwidth limit for connections to streaming servers. Select Gateway bandwidth limit, and enter the maximum number of kilobits per second that the appliance allows for all streaming connections to media servers.

5. Click Apply.

Protocols that Stream over HTTP

The global bandwidth limits for streaming protocols do not apply to MS Smooth Streaming, Apple HLS, and Adobe HDS because they are essentially treated just like HTTP traffic. However, you can write policy to limit bandwidth of these clients. For example:

<proxy>
streaming.client=ms_smooth  limit_bandwidth.client.outbound(bw_class)

The streaming.client condition can also be adobe_hds or apple.hls. Note that “bw_class” needs to be defined in the Management Console for this policy to work.

Additional Information:

- Once a limit is reached, any additional streaming connections will be denied. Clients attempting to connect may receive an error message, depending on the media player they are using. They will not be able to make a streaming media connection until the total streaming bandwidth is under the maximum limit.
- You can also specify bandwidth limits for a particular streaming client: Windows Media, Real Media, or QuickTime. However, it typically is sufficient to limit bandwidth for all types of streaming clients, as described in the above procedure.
- If you want even more granularity, you can reserve bandwidth for business-related streaming and limit recreational streaming. This can be done on a URL, IP address, or user name basis. For more information on configuring this feature, see the Bandwidth Management chapter in the SGOS Administration Guide.

Next Step: Monitor Bandwidth Utilization

Monitor Bandwidth Utilization

As you use proxies and policies to exercise control over traffic on your network, you will want to verify their effectiveness. Using various built-in charts, you can see how much traffic is going through the ProxySG as well as the utilization of each proxy or service, during a specified time period.

2. From the Service or Proxy drop-down list, select the type of traffic for which you want to analyze bandwidth utilization. For example, you can select the RTSP service or the Windows Media proxy.
3. Select the time period you are interested in: From the Duration drop-down, select Last Hour, Last Day, Last Week, Last Month, or Last Year. The graphs and statistics automatically update to reflect the time period you
selected. The **BW Usage** tab displays an area graph showing the rate (in kilobits per second) of client, server, and bypassed traffic in the selected service/proxy during the time period.

4. (Optional) Clear the **Include bypassed bytes** checkbox if you don’t want to include bypassed traffic in the graphs, statistics, and calculations; this would allow you to get a clearer view of traffic that is intercepted.

5. If you are interested in other time periods or other services/proxies, repeat steps 1-4.

**View Bandwidth Savings**

To determine how much bandwidth savings you are getting by having the ProxySG manage your traffic, look at the Traffic Mix page. For each service or proxy, this page provides the percentage of bandwidth that has been saved in a specified time period.

1. In the Management Console, select **Statistics > Traffic Details > Traffic Mix**.
2. Decide whether you want to view services or proxies: select **Service** or **Proxy**.
3. Select the time period you are interested in. From the **Duration** drop-down, select **Last Hour**, **Last Day**, **Last Week**, **Last Month**, or **Last Year**.
   
   The graphs and statistics automatically update to reflect the time period you selected.
4. (Optional) Clear the **Include bypassed bytes** checkbox if you don’t want to include bypassed traffic in the graphs, statistics, and calculations so that you can get a clearer view of intercepted traffic.
5. To view the total bandwidth gain for all services or proxies, click the **BW Gain** tab under the line graph.
The line graph shows the bandwidth gain from optimization during the specified time period, expressed as a multiple (for example, 2x). The gain is calculated as follows:
\[
\text{Gain} = \frac{\text{client} \_ \text{bytes}}{\text{server} \_ \text{bytes}}
\]

6. To view the bandwidth savings per service or proxy, look at the Savings column in the table.

<table>
<thead>
<tr>
<th>Savings</th>
</tr>
</thead>
<tbody>
<tr>
<td>n/a</td>
</tr>
<tr>
<td>96.98%</td>
</tr>
<tr>
<td>0%</td>
</tr>
<tr>
<td>0.99%</td>
</tr>
<tr>
<td>1.96%</td>
</tr>
<tr>
<td>n/a</td>
</tr>
</tbody>
</table>

The savings percentage is the average bandwidth savings due to optimization, during the specified time period. The savings is calculated as follows:
\[
\text{Savings} = \frac{\text{client} \_ \text{bytes} - \text{server} \_ \text{bytes}}{\text{client} \_ \text{bytes}} \times 100
\]

7. To view the total bandwidth savings for all services or proxies, look at the Total Savings value, underneath the table.

| Total Savings: 18.03% |

8. If you are interested in other time periods or other proxies/services, repeat steps 2-7.
Streaming Media Troubleshooting

Why can't users view streaming videos?

Problem: Users can't view streaming videos.

Resolution: Here are several reasons why videos may not stream:

- When a Trend Micro server is installed on the network, the Trend Smart Feedback option can prevent streaming media from playing. To fix the playback problem, disable this option.
- Most videos don't play in Quick Time Player 7.x on Windows 7. (audio does work) This issue has nothing to do with ProxySG.

Why do Flash videos stop streaming in the middle?

Problem: When tunneling Flash/RTMP over the HTTP proxy, content stops playing in the middle of the stream.

Resolution: This problem can occur in some sites that host Flash content. RTMPT (RTMP over HTTP) always uses HTTP between the client and the OCS through the ProxySG. The workaround for this issue is to enable HTTP handoff for Flash proxy on the ProxySG. This workaround is effective because the Flash proxy forces the device to maintain a connection with one server for the duration of the entire stream. Note that this workaround requires that your ProxySG is running SGOS 6.x.x.x or later and has a Flash license installed.

1. To enable HTTP handoff for Flash, see Fine Tune Streaming Proxy Settings.
2. To verify that you have a valid Flash license, select Maintenance > Licensing > View > Licensed Components. If you do not have a Flash license, contact the Blue Coat Customer Care team for help.

Why won't Flash videos play?

Problem: Flash video streaming is not working through the ProxySG. It tries to load for a while and then shows an error "server not found" or "connection timed out." This occurs with embedded flash videos that use RTMP over port 1935.

This problem can appear in an explicit deployment with an explicit IP or a PAC file, or in transparent deployments.

Resolution: First, make sure you have a Flash license. To verify that you have a valid Flash license, select Maintenance > Licensing > View > Licensed Components. If you do not have a Flash license, contact the Blue Coat Customer Care team for help.

Explicit Deployments
Blue Coat Security First Steps

In an explicit deployment, you need to make sure that Flash traffic is passing through the ProxySG. Some websites that have embedded flash streaming video don’t look at the browser’s proxy configuration or PAC file settings. Instead, they try to connect directly over the default gateway configured on the client workstation.

The easiest way to isolate this problem is to take a packet capture on the client workstation that is unable to play Flash video; follow the traffic over port 1935. If Flash traffic is passing through the ProxySG, the packet capture will look similar to the one below. Destination URL: http://www.globaltv.com, Client IP: 10.167.0.138, ProxySG IP: 10.169.3.131.

<table>
<thead>
<tr>
<th>Filter</th>
<th>Port request</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length Info</th>
</tr>
</thead>
</table>

If the browser’s proxy configuration or PAC file settings are not being used, the packet capture will show that it’s taking the default gateway settings on the client workstation and then getting blocked on the firewall. Displaying the filter "tcp.-port==1935" will show this.

Transparent Deployments

In a transparent deployment, you need to make sure:

- port 1935 is intercepted on the ProxySG
- port 1935 is redirected from the WCCP router
- port 1935 is not closed on the firewall/default gateway

Possible Solutions

One way to solve this problem is to open port 1935 and the destination IP on the firewall (assuming the IP is not a random IP address).

Another option is to disable the HTTP handoff for Flash: Configuration > Proxy Settings > Streaming Proxies > Flash.

If videos still are not loading, you can configure static bypass rules as a temporary workaround. You can set up the destination IP (where the Flash content is hosted) to be bypassed by the ProxySG: Configuration > Services > Proxy Services > Static Bypass. Or you can configure a single client IP address as a static bypass for all destinations. If you are able to play the video using the workaround, call Blue Coat Support for further troubleshooting.

Why aren’t Ustream videos playing in Safari?

Problem: When an iPhone or iPad tries to play a Ustream streaming video in the Safari browser, the video does not load when going through a ProxySG.

Resolution: An HTTP request from Safari on an iPhone or iPad contains an HTTP header of WebSocket Protocol (RFC 6455). The ProxySG does not support the WebSocket protocol at this time. When the ProxySG intercepts an HTTP request for Ustream streaming from an iPhone or iPad, the ProxySG will return an HTTP 503 error to the client (Safari).

Workaround:

Add policy to turn off protocol detection for connect requests from iPhone/iPad.
Policy sample:

define condition UstreamRequest
url.host.substring="ustream.tv"
end condition UstreamRequest

<Proxy>

http.method=(CONNECT) condition=UstreamRequest detect_protocol(no)