

Blue Coat® Systems

Transproxy Deployment

*Accelerating Backhauled Explicit
Proxy Internet Traffic*



Copyright© 1999-2013 Blue Coat Systems, Inc. All rights reserved worldwide. No part of this document may be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the written consent of Blue Coat Systems, Inc. All right, title and interest in and to the Software and documentation are and shall remain the exclusive property of Blue Coat Systems, Inc. and its licensors. ProxyAV™, ProxyOne™, CacheOS™, SGOS™, SG™, Spyware Interceptor™, Scope™, ProxyRA Connector™, ProxyRA Manager™, Remote Access™ and MACH5™ are trademarks of Blue Coat Systems, Inc. and CacheFlow®, Blue Coat®, Accelerating The Internet®, ProxySG®, WinProxy®, PacketShaper®, PacketShaper Xpress®, PolicyCenter®, PacketWise®, AccessNow®, Ositis®, Powering Internet Management®, The Ultimate Internet Sharing Solution®, Cerberian®, Permeo®, Permeo Technologies, Inc.®, and the Cerberian and Permeo logos are registered trademarks of Blue Coat Systems, Inc. All other trademarks contained in this document and in the Software are the property of their respective owners.

BLUE COAT SYSTEMS, INC. AND BLUE COAT SYSTEMS INTERNATIONAL SARL (COLLECTIVELY "BLUE COAT") DISCLAIM ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL BLUE COAT, ITS SUPPLIERS OR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF BLUE COAT SYSTEMS, INC. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

Document History

Date	Version	Note
January 15, 2013	v0.1	Initial release

Contents

- Introduction 1
- Scenario 1
 - Application-Level Acceleration..... 2
 - Data-Level Acceleration 2
- Requirements 3
- Configuring a Transproxy 3
- Enabling HTTPS Acceleration..... 6
- Advanced Features and Caveats 8
 - Caching of YouTube Videos 9
 - Caching and Splitting of Flash Streams 9
 - Bandwidth Management..... 10
- Summary 10
- Appendix: HTTP Proxy Settings 11
 - Acceleration Profile..... 11
 - Always Check with Source Before Serving Object..... 12
- About Technical Briefs 12

List of Figures

Exemplary transproxy deployment	1
SWG explicit proxy settings	3
SWG active sessions	3
Edge active sessions	3
Edge Add new service dialog - Application level	4
Edge Add new service dialog - Data level	5
Edge active sessions settings	5
Edge Traffic Summary report	6
Edge/Core Security Settings dialog	6
Edge device - Proxy settings	7
Edge SSL Intercept Layer table	7
Edge Active Sessions report - HTTPS acceleration working	7
Edge Active Sessions report - HTTPS acceleration not working	8
Traffic Summary report	8
License Information dialog	9
Acceleration profile	11
HTTP Proxy Policy dialog	12

Introduction

Many companies backhaul their Internet traffic across the WAN to central or regional Internet access hubs. A vast majority of companies use a Secure Web Gateway (SWG) at these hubs. The prevalent access method is to connect explicitly, for example, configuring the clients to use a specific proxy.

If a company has also deployed WAN optimization technology, the SWG and WAN optimizers must work together, allowing the Internet traffic to achieve maximum optimization. Not only is Internet access at the remote office faster, but because the bandwidth usage of the Internet traffic is reduced significantly, more bandwidth is available for mission-critical traffic (for example, SAP, CRM, VoIP, and so on).

Let's assume that a client in a remote office is configured to use a central corporate proxy, while WAN optimizers are being used on each side of the WAN link. The traffic will be intercepted on the central proxy (to which the client is pointing), but it will be intercepted even before then on the WAN optimizer, (which technically, is also a proxy). Because the client does not know about the existence of the WAN optimizer, the latter must intercept the traffic transparently.

In scenarios such as this, we refer to the downstream transparent proxy as the *transproxy*. This technical brief explains the applications of the transproxy, describes its configuration, and mentions some caveats.

Scenario

Figure 1-1 shows an example of a possible transproxy scenario. The Internet is backhauled to the SWG at the corporate headquarters. Latency-wise, this can be a large distance (potentially dozens of milliseconds (ms)—even 200 to 300 ms is not uncommon if the traffic is backhauled to another continent). As a result, access to business-critical applications and cloud services can be slow. Additionally, since there is no optimization of Web traffic at the remote office, bandwidth-hungry Web applications, such as YouTube or web TV, can cause network congestion, thus decreasing performance even further.

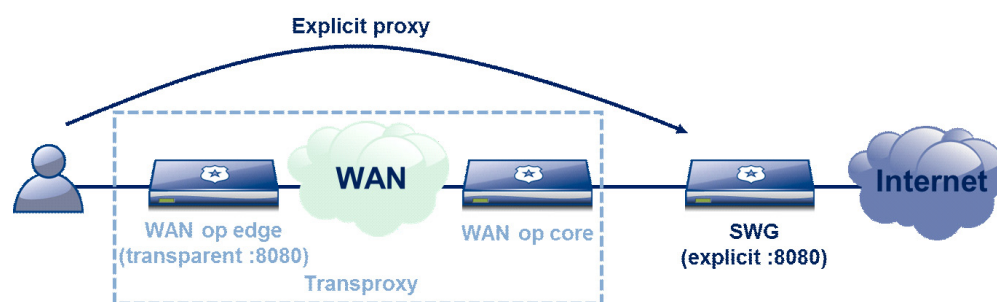


Figure 1-1 Exemplary transproxy deployment

These issues can be effectively mitigated using WAN optimization technology (ProxySG appliances at the edge and at the core) to accelerate the traffic and reduce the bandwidth used. In addition to Web traffic, WAN optimizers typically accelerate internal traffic, such as email (MAPI), file services (CIFS, FTP), intranet (HTTPS), backup/DR and many more. These issues, however, go beyond the scope of this document.

Technically speaking, WAN optimization uses proxy technology to accelerate traffic. Therefore, Web traffic must be intercepted on the edge-side WAN-optimizer ProxySG appliance. This presents us with an interesting situation, since the Web traffic will be intercepted a second time on the SWG ProxySG appliance at the headquarters. Looking at this in more detail, there are two options for transproxy deployments:

- ❑ Client uses explicit proxy (SWG), transproxy uses application-level (HTTP) acceleration. (See "[Application-Level Acceleration](#)".)
- ❑ Client uses explicit proxy (SWG), transproxy uses data-level (TCP) acceleration. (See "[Data-Level Acceleration](#)".)

In general, application-level acceleration should be used, except for sensitive applications (for example, financial or transactional).

Application-Level Acceleration

Application-level acceleration provides the best possible traffic optimization using a maximum of optimization techniques, such as object and byte caching, HTTP-specific optimization, and compression. The result is that Internet access is as fast as possible, while using the least amount of WAN bandwidth. HTTP object caching significantly decreases page load times, as cacheable objects can be served without having WAN latency. Furthermore, HTTP-embedded streaming protocols (for example, tunneled Adobe Flash RTMP streaming, and RTMPT) can be accelerated with help from the ProxySG appliance's streaming proxies. The HTTP proxy does a protocol hand-off to the appropriate streaming proxy (for example, Flash proxy, in this case). Since the transproxy interacts with the traffic at HTTP level, incompatibilities might result if Web servers don't exactly comply with standards.

Another thing to consider is that object caching is used. Although it is the most efficient means for delivering data to the client, in rare cases, it can lead to stale content being delivered. This issue can be resolved by enabling the **Never serve after expiration** and **Always check with source** options globally or through policy. These HTTP proxy options are explained in more detail in the appendix.

Data-Level Acceleration

Data-level acceleration provides maximum data transparency, while still providing good traffic optimization. In this case, the three optimization techniques used are: byte-caching, TCP optimization, and compression. The result is fast Internet access with a significant reduction of WAN bandwidth usage. Its main advantage however, is complete data transparency; the data is bit-by-bit identical on both sides of the transproxy, which ensures maximum compatibility between the WAN optimizers and Web applications. (If it does not work *with* the

WAN optimizers, it does not work *without* them, either.) Also, data always comes from the original server and never from a local cache, thereby ensuring perfect data integrity.

Requirements

All examples in this document use the latest SGOS 6.2 (SWG) and 6.3 (WAN optimizers) releases. While the configuration of SWG uses the Java-based graphical user interface, the WAN optimizers use the more dynamic Sky graphical user interface, which was optimized for this purpose (based on Adobe Flex).

Configuring a Transproxy

Before configuring the transproxy, you will need a working central explicit proxy (SWG).

1. Clients must be properly configured to use this proxy. From the SWG Management Console, select **SWG > Configuration > Services > Proxy Services**. Note the port used for client-to-proxy connections. The example in [Figure 1–2](#) is using TCP/8080.

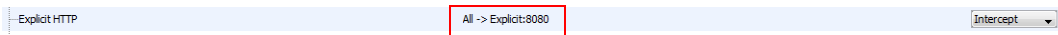


Figure 1–2 SWG explicit proxy settings

2. (Optional) Activate SSL interception on the central SWG proxy, then verify it has been done correctly by selecting **SWG > Statistics > Sessions > Active Sessions** from the SWG Management Console.

[Figure 1–3](#) shows sessions with **HTTPS Fwd** proxy type used when visiting an encrypted Web site. In the example, clients are using central proxy for HTTP (first two sessions) and HTTPS (last two sessions).

▶ 192.168.3.21:52361	svcs.cnn.com:80	8 sec	16,809	16,966	0%	Explicit HTTP	HTTP
▶ 192.168.3.21:52362	cdn.api.twitter.com:80	8 sec	3,110	3,149	0%	Explicit HTTP	HTTP
● 192.168.3.21:52366	www.facebook.com:443	6 sec	1,509	1,356	9.91%	Explicit HTTP	HTTPS Fwd
▶ 192.168.3.21:52367	www.css.ch:443	6 sec	91,137	91,478	0%	Explicit HTTP	HTTPS Fwd

Figure 1–3 SWG active sessions

3. Basic WAN optimization must be working between the edge and core ProxySG appliances. To verify the status, check the active sessions on the edge device by selecting **Edge > Report > Active Sessions** from the Edge Management Console. (See [Figure 1–4](#).)

Client	Server	Connection type	Savings	Service name	Proxy type	ADN	ADN peer	LAN bytes	WAN bytes
192.168.3.188:54010	edition.cnn.com:80	Outbound ADN	48%	External HTTP	HTTP		157.166.255.32	12.7 KB	6.6 KB
192.168.3.188:54009	edition.cnn.com:80	Outbound ADN	28%	External HTTP	HTTP		157.166.255.32	1.6 KB	1.1 KB

Figure 1–4 Edge active sessions

The symbol in the **ADN** column indicates that WAN optimization is being used. Note that the accelerated traffic is **External HTTP** (for example, standard HTTP traffic not going to an explicit proxy).

4. Determine whether to use application-level or data-level acceleration on the transproxy. The advantages and disadvantages for each method are discussed earlier in this document.

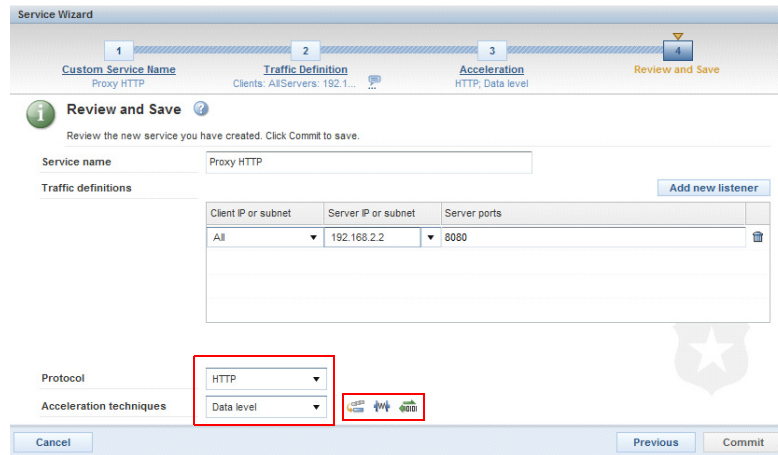
Do one of the following:

- Configure Proxy HTTP service with application-level acceleration on the edge device. From the Management Console, select **Edge > Configure > Acceleration > Traffic Management > Add new service**. (See [Figure 1–5](#).)
- Configure Proxy HTTP service with data-level acceleration on the edge device. From the Management Console, select **Edge > Configure > Acceleration > Traffic Management > Add new service**. (See [Figure 1–6](#).)

The screenshot shows the 'Service Wizard' interface with four steps: 1. Custom Service Name, 2. Traffic Definition, 3. Acceleration, and 4. Review and Save. The 'Review and Save' step is active. It displays the service name 'Proxy HTTP', traffic definitions (Client IP or subnet: All, Server IP or subnet: 192.168.2.2, Server ports: 8080), protocol 'HTTP', and acceleration techniques 'Application level'. A red box highlights the 'HTTP' protocol dropdown and the 'Application level' acceleration techniques dropdown. Below these, five icons represent different acceleration techniques: a star, a gear, a network diagram, a document, and a server. The 'Commit' button is visible at the bottom right.

Figure 1–5 Edge Add new service dialog - Application level

The five icons at the bottom of [Figure 1–5](#) show the acceleration techniques being used in this case. The **Server IP** can be set to the central proxy's IP address or to transparent. If set to transparent, all traffic for the port noted in Step 1 is intercepted and optimized.

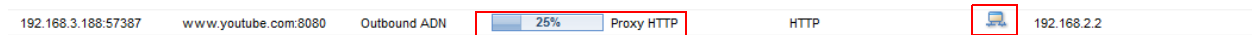


The image shows the 'Service Wizard' dialog in the Edge Management Console, specifically the 'Review and Save' step. The wizard has four steps: 1. Custom Service Name (Proxy HTTP), 2. Traffic Definition (Clients: All Servers: 192.168.2.2), 3. Acceleration (HTTP, Data level), and 4. Review and Save. The 'Review and Save' step shows the service name 'Proxy HTTP' and a table for traffic definitions. The table has columns for Client IP or subnet, Server IP or subnet, and Server ports. The first row shows 'All' for Client IP, '192.168.2.2' for Server IP, and '8080' for Server ports. Below the table, the 'Protocol' is set to 'HTTP' and 'Acceleration techniques' is set to 'Data level'. At the bottom, there are 'Cancel', 'Previous', and 'Commit' buttons. Three icons (a shield, a star, and a gear) are visible at the bottom right of the dialog.

Figure 1–6 Edge Add new service dialog - Data level

The three icons at the bottom of [Figure 1–6](#) show the acceleration techniques being used in this case. Please note that **Server IP** can be set to the central proxy's IP address or to transparent. If set to transparent, all traffic for the port noted in Step 1 is intercepted and optimized.

5. Verify the newly created Proxy HTTP service is working properly and traffic is accelerated.
 - a. From the Edge Management Console, select **Edge > Report > Active Sessions**. (See [Figure 1–7](#).)



192.168.3.188:57387	www.youtube.com:8080	Outbound ADN	25%	Proxy HTTP	HTTP	192.168.2.2
---------------------	----------------------	--------------	-----	------------	------	-------------

Figure 1–7 Edge active sessions settings

- b. Check that the ADN symbol is active. In addition, you can see the bandwidth savings for the accelerated sessions, which is shown as 25% in this exemplary case. (If you selected **Data level** acceleration in Step 4, the **Proxy type** column will list **TCP-tunnel**.)
- c. For a more global view, check the Traffic Summary report by selecting **Edge > Report > Traffic Summary** from the Edge Management Console. The report shows an overview of the network traffic distribution, bandwidth savings, and WAN and LAN bandwidth usage. Verify the bandwidth savings is greater than 0% for the proxied HTTP traffic. (See [Figure 1–8](#).)

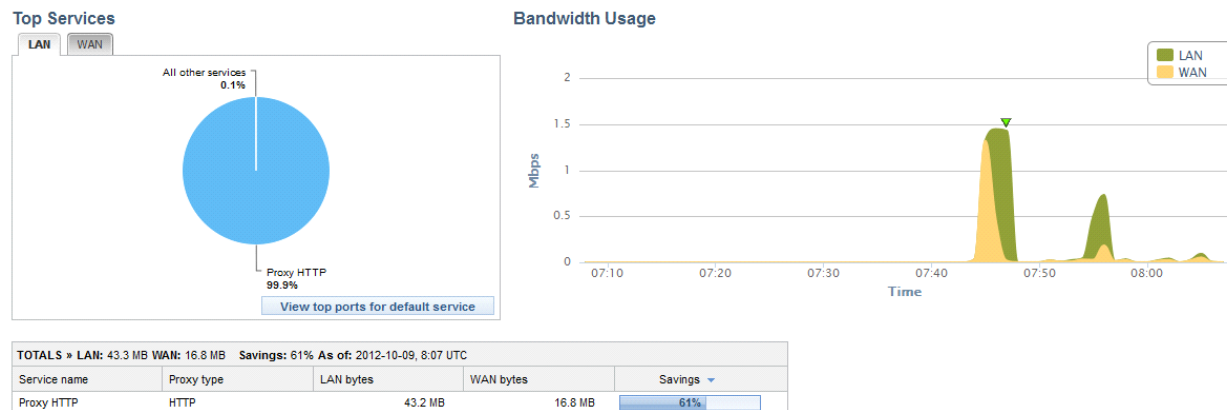


Figure 1-8 Edge Traffic Summary report

6. Consider the following:

- If SSL interception is not configured on the central proxy, or you are using data-level acceleration, you are done at this point.
- If you are using application-layer acceleration, you might consider enabling HTTPS acceleration on the transproxy to obtain the best acceleration results. See ["Enabling HTTPS Acceleration"](#).

Note: If the central proxy uses proxy authentication (HTTP 407 response), SSL interception must not be used on the transproxy, as it breaks connectivity.

Enabling HTTPS Acceleration

The first step towards accelerating HTTPS traffic is to configure secure ADN to encrypt accelerated traffic between the edge and the core device. To do this, you must configure both devices.

1. From the Management Console of each device, select **Edge/Core > Configure > ADN > General > Security Settings**. (See [Figure 1-9](#).)

Security Settings

☒ Enable secure ADN using the following SSL device profile: passive-attack-protection-only ▼

Secure-Outbound Mode

☐ Do not secure outbound ADN connections

☒ Secure ADN routing and outbound tunnel connections made by secure proxies

☐ Secure all ADN routing and outbound tunnel connections

Figure 1-9 Edge/Core Security Settings dialog

- 2. Select an SSL device profile (for each device) to be used for encrypting traffic. The profile in the example provides only encryption and not mutual device authorization. Other SSL profiles are available, which might require additional configuration steps.
- 3. Configure HTTPS acceleration on the edge device.
 - a. From the Edge Management Console, select **Advanced Configuration > Services > Proxy Services > Edit Service**, then enable **Detect Protocol** for the Proxy HTTP service. (See [Figure 1–10](#).)

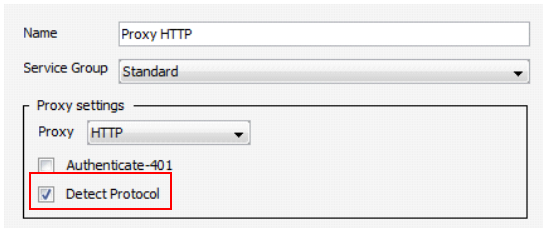


Figure 1–10 Edge device - Proxy settings

- b. Select **Advanced Configuration > Policy > Visual Policy Manager** to create an SSL Intercept Layer and one or more interception rules.

[Figure 1–11](#) shows a very basic setup, in which all HTTPS traffic is intercepted. In reality, technical and regulatory factors determine the traffic that is intercepted (that is, decrypted and accelerated) and the traffic that is tunneled.

SSL Intercept Layer						
No.	Source	Destination	Service	Action	Track	Comment
1	Any	Any	Any	SSL EnableHTTPS...	None	

Figure 1–11 Edge SSL Intercept Layer table

- 4. Verify that HTTPS interception—and hence, acceleration—is working properly on the edge device.
 - a. From the Edge Management Console, select **Edge > Report > Active Sessions**.
 - b. Check that the secure ADN symbol (with the lock) is active. In addition, you will see **HTTPS Fwd** as the proxy type (instead of **HTTP** for non-encrypted traffic). Expected bandwidth savings are as high as that for standard HTTP traffic. [Figure 1–12](#) shows results from the edge device.

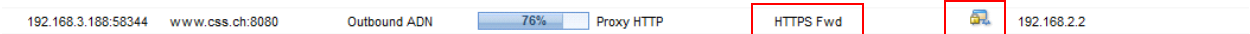


Figure 1–12 Edge Active Sessions report - HTTPS acceleration working

If HTTPS configuration is not properly configured, (for example, no secure ADN), the result looks similar to that shown in [Figure 1–13](#). The proxy type displays as **HTTP** and because the traffic cannot be decrypted, there is no optimization; the bandwidth savings is 0%.



Figure 1–13 Edge Active Sessions report - HTTPS acceleration not working

- 5. For a more global view, access the Traffic Summary report.
 - a. From the Edge Management Console, select **Edge > Report > Traffic Summary**.

The report provides an overview of all traffic, bandwidth savings, and WAN and LAN bandwidth usage, as shown in [Figure 1–14](#). The sample report shows that a bandwidth savings of 51% was achieved for the proxied HTTP traffic, and 44% was achieved for HTTPS.

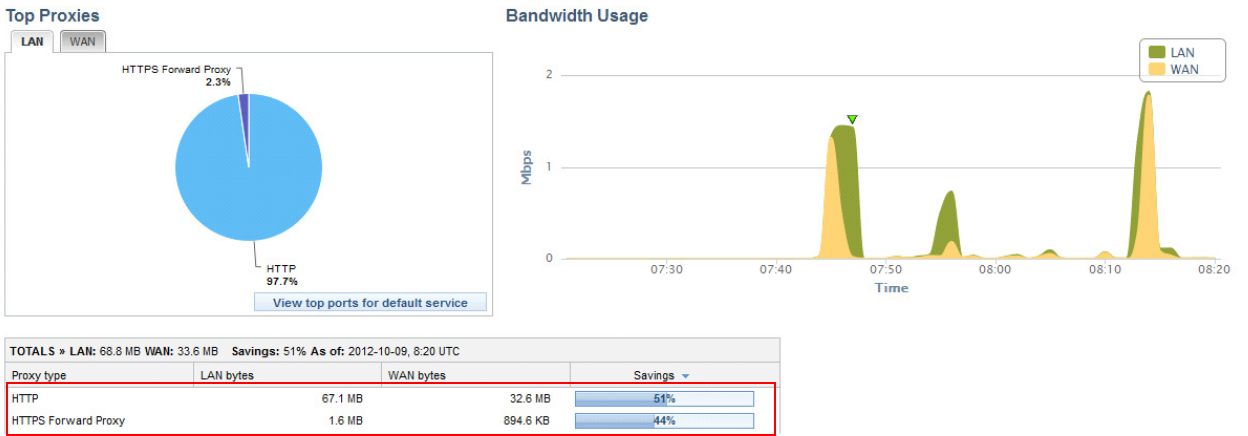


Figure 1–14 Traffic Summary report

Advanced Features and Caveats

The following topics are discussed:

- ❑ "Caching of YouTube Videos" on page 9
- ❑ "Caching and Splitting of Flash Streams" on page 9
- ❑ "Bandwidth Management" on page 10

Caching of YouTube Videos

The volume of YouTube traffic is continuing to grow on corporate networks, so we can expect great bandwidth savings if YouTube content can be efficiently cached at the edge. The configuration should ensure that after a video is cached on the edge device, all subsequent requests for the same video are served from the cache, thereby not using any WAN/Internet bandwidth.

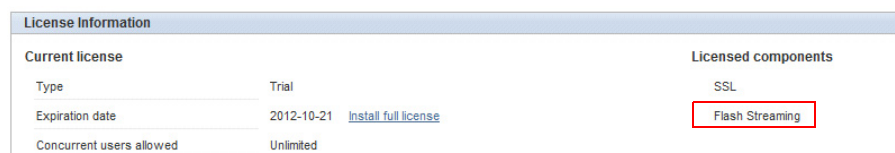
The policy for caching YouTube can be found at:

<https://kb.bluecoat.com/index?page=content&id=KB5121>

Note: Caching of YouTube videos only works as described when using application-level acceleration (for example, HTTP), since object caching is only available in this mode.

Caching and Splitting of Flash Streams

Many Web sites today contain streaming video content. The prevalent streaming protocols are RTMP and RTMPS (commonly referred to as Flash streaming and encrypted Flash streaming). To optimize this traffic, a valid Flash Streaming license is needed. (See [Figure 1–15](#).) After the license is installed, configuration is straightforward.



License Information		
Current license		Licensed components
Type	Trial	SSL
Expiration date	2012-10-21 Install full license	Flash Streaming
Concurrent users allowed	Unlimited	

Figure 1–15 License Information dialog

The following procedure assumes the Flash Streaming license has already been installed. You can verify the Flash Streaming license was installed successfully by selecting **System Settings > Software > Licensing** from the Management Console.

Procedure:

1. Select **Advanced Configuration > Proxy Settings > Streaming Proxies > Flash**. Verify the **HTTP handoff** option is enabled.
2. Select **Advanced Configuration > Services > Proxy Services > Edit Service**. Enable **Detect Protocol** for the Proxy HTTP service.

Flash Streaming should display **RTMP** in the active sessions. Flash players do not always respect the browser's proxy settings, so you might also need to intercept RTMP transparently.

The two mechanisms used to optimize Flash streaming are: video-on-demand (VOD) caching and stream splitting (for live streams). The latter is of great importance during large events (for example, Olympic Games, Presidential Elections, etc.) as it retrieves a stream from the server only once and serves it to many users, thereby preventing potential network congestion.

Note: VOD caching and live stream splitting only works as described when using application-level acceleration (such as HTTP), since this is required to hand off the traffic to the respective streaming proxy (such as RTMP).

Bandwidth Management

On the edge device, policy can be created to manage bandwidth, for example, to guarantee, limit, or prioritize certain traffic. This mechanism can be used to protect mission-critical traffic or to confine recreational traffic.

Summary

This document provides an overview of how to efficiently combine a central Internet backhaul with WAN optimization technology. Configuration options are discussed for normal and encrypted traffic. As a general rule, application-level (for example, HTTP) optimization should be used in transproxy deployments. Scenarios in which it makes sense to use data-level optimization include the following:

- ❑ Internal, non-standard Web applications
- ❑ Sensitive data that must not be altered (for example, financial or transactional)
- ❑ SSL applications that break

Appendix: HTTP Proxy Settings

Acceleration Profile

This section discusses some of the Acceleration Profile feature settings, mainly **Never serve after expiration** and **Enable Bandwidth Gain Mode**. To access the Acceleration Profile dialog, from the Management Console, select **Configuration > Proxy Settings > HTTP Proxy > Acceleration Profile**. (See [Figure 1–16](#).)

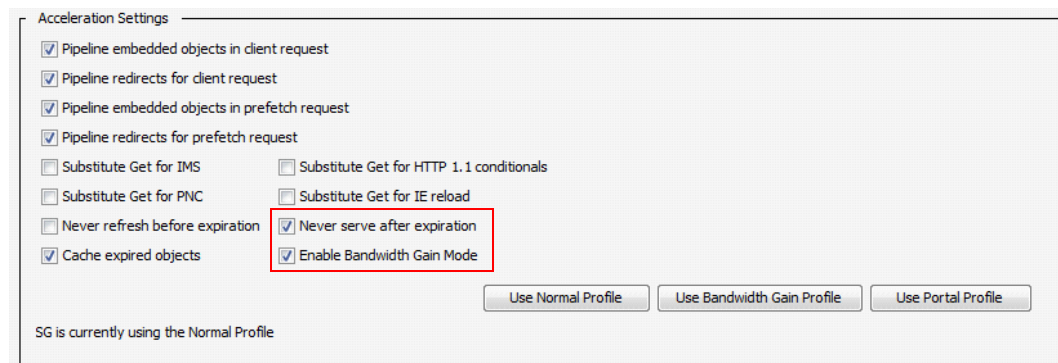


Figure 1–16 Acceleration profile

Never Serve After Expiration

The **Never serve after expiration** option applies only to cached type-T objects (for example, objects for which the server specifies an explicit expiration time).

- ❑ When **Never serve after expiration** is *selected*, an object is synchronously revalidated before being served to a client, if the client accesses the object after its expiration time.
- ❑ When **Never serve after expiration** is *cleared*, the object is served to the client and, depending on its relative popularity, may be asynchronously revalidated before it is accessed again.

Enable Bandwidth Gain Mode

The **Enable Bandwidth Gain Mode** setting controls both the download of HTTP objects after client-side abandonment and AAR (asynchronous adaptive refresh) revalidation frequency.

- ❑ HTTP object download
 - When **Enable Bandwidth Gain Mode** is *selected*, if a client requesting a given object abandons its request, HTTP proxy immediately abandons the download of the object from the server, if it is still in progress.
 - When **Enable Bandwidth Gain Mode** is *cleared*, the HTTP proxy continues to download the object from the server for possible future requests for that object.

- ❑ AAR revalidation frequency
 - When **Enable Bandwidth Gain Mode** is *selected*, objects that are asynchronously refreshable are revalidated at most twice during their estimated time of freshness.
 - When **Enable Bandwidth Gain Mode** is *cleared*, objects are revalidated a maximum of three times. Note that not all asynchronously refreshable objects are guaranteed to be revalidated.

Always Check with Source Before Serving Object

The **Always check with source before serving object** option verifies that each object is fresh upon access. This feature is accessed using the **HTTP Proxy Policy** dialog. To access this dialog, from the Management Console, select **Configuration > Proxy Settings > HTTP Proxy > Policies**. (See [Figure 1–17](#).)

Enabling this setting has a significant impact on performance because the HTTP proxy revalidates requested cached objects with the server before serving them to the client. This results in a negative impact on bandwidth gain. Therefore, do not enable this configuration unless it is absolutely necessary.

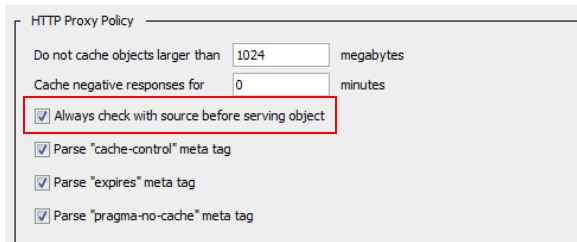


Figure 1–17 HTTP Proxy Policy dialog

About Technical Briefs

Technical briefs are designed to illustrate the features and capabilities of Blue Coat products. By describing generic solutions, technical briefs provide a foundation that Blue Coat customers can use to understand how Blue Coat products can be used to solve specific problems.

These technical briefs are not intended to solve customer-specific requests; if you need a customized solution to address a specific concern, contact Blue Coat Professional Services at Professional.Services@bluecoat.com.