

Blue Coat[®] Systems

Deployment Guide

Deploying the SSL Proxy

For SGOS 4.2.x



Contact Information

Blue Coat Systems Inc.
420 North Mary Ave
Sunnyvale, CA 94085-4121

<http://www.bluecoat.com/support/index.html>

bcs.info@bluecoat.com
support@bluecoat.com
<http://www.bluecoat.com>

For concerns or feedback about the documentation: documentation@bluecoat.com

Copyright© 1999-2006 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. ProxySG™, ProxyAV™, CacheOS™, SGOS™, Spyware Interceptor™, Scope™, RA Connector™, RA Manager™, Remote Access™ are trademarks of Blue Coat Systems, Inc. and CacheFlow®, Blue Coat®, Accelerating The Internet®, WinProxy®, AccessNow®, Osisis®, Powering Internet Management®, The Ultimate Internet Sharing Solution®, Permeo®, Permeo Technologies, Inc.®, and the Permeo logo 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. DISCLAIMS 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 SYSTEMS, INC., 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.

Document Number: 231-02802

Document Revision: SSL Proxy Deployment Guide—SGOS 4.2x

Table of Contents

Introduction to the Blue Coat SSL Proxy

What the SSL Proxy Does 5

Increasing Control 6

SSL Proxy Overview

Understanding SSL 7

Using an SSL Proxy for Privacy, Authentication, and Data Integrity 8

SSL Proxy Versus HTTPS Reverse Proxy 9

Best Practices and Deployment: An FAQ

Question: What Do I Need to Know Before Deploying the SSL Proxy? 11

Question: How Do I Fix Server Certificate Errors? 12

Question: How Do I Selectively Intercept SSL Traffic? 13

Question: Can the ProxySG Help in Distributing Issuer Certificates to Client Desktops? 15

Question: How Do I Protect End-User Privacy and Avoid Accidental Exposure of Sensitive Information When Intercepting SSL Traffic? 18

Question: How do I set up SSL Proxy in Explicit Mode? 20

Question: How Do I Deploy SSL Proxy in Transparent Mode? 21

Question: How Do I Deploy the SSL Proxy in a Proxy Chain? 21

Question: I am Using a Transparent Proxy Deployment. How Do I Allow Non-SSL Traffic on Port 443 to Certain Servers While Still Enabling the SSL Proxy for the Rest of the Port 443 Traffic? 23

Question: Windows Updates Fail When I Use the SSL Proxy to Intercept all SSL Connections. 24

Question: I have CA Hierarchy in Place in My Enterprise. Can I Use it for Certificate Emulation? 24

Troubleshooting Tips

Upgrading to SGOS 4.2 27

Logging 29

Microsoft 29

Introduction to the Blue Coat SSL Proxy

HTTPS traffic is the same as HTTP traffic except that it is encapsulated so that the content is hidden.

HTTPS traffic poses a major security risk to enterprises. Because SSL (Secure Socket Layer) content is encrypted, it can't be intercepted by normal means. Users can bring in viruses, access forbidden sites, and leak business confidential information over an HTTPS connection, which uses port 443.

Because IT organizations have no visibility into SSL sessions, they are blind to any potential security threats sent over HTTPS.

In addition to the security threat, encrypted traffic makes it difficult for IT to assess bandwidth usage and apply intelligent content control policies to ensure maximum user productivity.

Prior to the SSL Proxy, the only solution for managing HTTPS traffic was to deny HTTPS altogether or severely limit its usage.

What the SSL Proxy Does

The SSL Proxy can be used to tunnel or intercept HTTPS traffic. The SSL Proxy tunnels all HTTPS traffic by default. Some HTTPS traffic, such as financial information, should not be intercepted. The SSL proxy can do the following operations while tunneling HTTPS traffic.

- ❑ Validate server certificates, including revocation checks using Certificate Revocation Lists (CRLs).
- ❑ Check various SSL parameters such as cipher and version.
- ❑ Log useful information about the HTTPS connection.

When the SSL Proxy is used to intercept HTTPS traffic, it can also:

- ❑ Cache HTTPS content.
- ❑ Apply HTTP-based authentication mechanism.
- ❑ Do virus scanning and URL filtering.
- ❑ Apply granular policy (such as validating mime type and filename extension).

The Blue Coat SSL proxy allows you to:

- ❑ Determine what HTTPS traffic to intercept through existing policy conditions, such as destination IP address and port number. You can also use the hostname in the server certificate to make the intercept versus tunnel decision.
- ❑ Validate the server certificate to confirm the identity of the server, and check Certificate Revocation Lists (CRLs) to be sure the server certificate has not been revoked.
- ❑ Apply caching, virus scanning and URL filtering policies to intercepted HTTPS traffic.

Increasing Control

The SSL proxy allows you to increase control by:

- ❑ Distinguishing between SSL and non-SSL traffic on the same port.
- ❑ Distinguishing HTTPS from other protocols over SSL.
- ❑ Categorizing sites by their SSL server certificate hostname.
- ❑ Security is increased through:
 - Server certificate validation, including checking CRLs.
 - Virus scanning and URL filtering of HTTPS content.

Visibility and improved system performance is due to SSL logs and caching (which is enabled by default when using the SSL proxy).

SSL Proxy Overview

.SSL and tunneling protocols are closely tied together. To understand SSL, you must first understand how tunneling applications work.

This chapter discusses:

- ❑ "Understanding SSL"
- ❑ "Using an SSL Proxy for Privacy, Authentication, and Data Integrity"
- ❑ "Digital Certificates and Certificate Authorities"
- ❑ "SSL Proxy Versus HTTPS Reverse Proxy"

Understanding SSL

At the lowest level, SSL is layered on top of TCP/IP. SSL uses the SSL Handshake Protocol to allow the server and client to authenticate each other and to negotiate the encryption cipher before the application protocol transmits or receives its first byte of data.

SSL has emerged as the de facto standard protocol for establishing a secure, encrypted link between a remote application server and the client Web browser on the local user's desktop.

SSL is a proven technology with strong appeal to IT organizations because each secure session link is automatically established "on demand" using standards-based protocols, encryption techniques, and certificate exchange – all without the need for any IT administration.

The process of setting up the private connection is automatically initiated by the server communicating directly with the browser. The result is a private, encrypted tunnel used to move information between the server and client desktop. When the session is over, the connection is automatically terminated.

However, SSL sessions are rapidly becoming a conduit for a variety of enterprise security threats – including spyware, viruses, worms, phishing, and other malware.

Using an SSL Proxy for Privacy, Authentication, and Data Integrity

The SSL proxy can manage the SSL sessions in such a way as to prevent enterprise security threats while at the same time allowing you to determine the level of control.

If the HTTPS traffic contains financial information, you probably do not want to intercept that traffic.

However, many other kinds of traffic should and can be intercepted by the SSL proxy.

Determining What HTTPS Traffic to Intercept

The SSL proxy tunnels HTTPS traffic by default; it does not intercept HTTPS traffic.

Many existing policy conditions, such as destination IP address and port number can be used to decide which HTTPS connections to intercept.

Additionally, the SSL proxy allows the hostname in the server certificate to be used to make the decision to intercept or tunnel the traffic. The server certificate hostname can be used as is to make intercept decisions for individual sites, or it can be categorized using any of the various URL databases supported by Blue Coat. Categorization of server certificate hostnames can help place the intercept decision for various sites into a single policy rule.

Recommendations for intercepting traffic include:

- ❑ Intercept Intranet traffic.
- ❑ Intercept suspicious Internet sites, particularly those that are categorized as *none* in the server certificate.
- ❑ Intercept sites that provide secure web based e-mail, such as Gmail over HTTPS.

Managing Decrypted Traffic

Once the HTTPS connection is intercepted, you can do:

- ❑ anti-virus scanning over ICAP.
- ❑ URL filtering (on box and off-box). Blue Coat recommends on box URL/Content filtering if you use transparent proxy. When the URL is sent off-box for filtering, only the hostname or IP address of the URL (not the full path) is sent for security reasons.
- ❑ Filtering based on the server certificate hostname.
- ❑ Caching.

HTTPS applications that require browsers to present client certificates to secure web servers do not work if you are intercepting traffic. Such applications should not be intercepted by creating a policy rule.

If you intercept HTTPS traffic, be aware that local privacy laws might require you to notify the user about interception or obtain consent prior to interception. You can use the HTML Notify User object to notify users after interception. You can use consent certificates to obtain consent prior to interception. The HTML Notify User is easier; however, note that the ProxySG has to decrypt the first request from the user before it can issue an HTML notification page.

Digital Certificates and Certificate Authorities

Server certificates are used to authenticate the identity of a server. A certificate is electronic confirmation that the owner of a public key is who he or she really claims to be and thus holds the private key corresponding to the public key in the certificate. The certificate contains other information, such as its expiration date.

The association between a public key and a particular server is done by generating a certificate signing request using the server's public key. A certificate signing authority verifies the identity of the server and generates a signed certificate. The resulting certificate can then be offered by the server to clients who can recognize the CA's signature and trust that the server is who it claims to be. Such use of certificates issued by CAs has become the primary infrastructure for authentication of communications over the Internet.

ProxySG Appliances come with many popular CA certificates already installed. You can review these certificates using the Management Console or the CLI. You can also add certificates for your own internal certificate authorities.

The ProxySG trusts all root CA certificates trusted by Internet Explorer and Firefox. The list is updated periodically to be in sync with the latest versions of IE and Firefox.

CA certificates installed on the ProxySG are used to verify the certificates presented by HTTPS servers and the client certificates presented by browsers (when browsers are configured to do so).

Certificate Revocation Lists (CRLs) allow checking server certificates against lists provided and maintained by CAs that show certificates that have been revoked.

SSL Proxy Versus HTTPS Reverse Proxy

Depending on your needs, you can use the ProxySG as either an SSL proxy or an HTTPS reverse proxy. SSL proxy functionality enables the ProxySG to act as forward proxy for HTTPS requests.

This deployment guide discusses the HTTPS forward proxy. To configure the ProxySG as an HTTPS reverse proxy, refer to the *Blue Coat ProxySG Configuration and Management Guide*.

- ❑ An SSL proxy is a client-side proxy typically used for applying security and performance features such as authentication, URL filtering, and caching.
- ❑ An HTTPS reverse proxy is a server-side proxy typically used to offload SSL processing from server to the proxy. Reverse proxies are deployed in proximity to the server. The communication between the HTTPS reverse proxy and server might or might not use SSL. The ProxySG can be used as an HTTPS reverse proxy with the help of the existing HTTPS Reverse Proxy service. Performance is usually the only objective.

Best Practices and Deployment: An FAQ

Question: What Do I Need to Know Before Deploying the SSL Proxy?

A: If you have an SSL Termination license, the SSL proxy functionality is enabled by default when you upgrade your ProxySG to SGOS 4.2.x. However, all HTTPS traffic is tunneled until you create a policy that intercepts HTTPS traffic.

Even when the SSL proxy tunnels HTTPS traffic, server certificates are validated. Servers presenting certificates that have errors are denied data exchange. The SSL proxy detects the following certificate errors when tunneling HTTPS traffic:

- ❑ The certificate has expired (or is valid at a future date)
- ❑ The certificate issuer is untrusted; that is, the ProxySG does not recognize or trust the issuer of the certificate.
- ❑ The certificate has been revoked. The ProxySG does a revocation check using Certificate Revocation Lists (CRLs) to determine if the issuer of the certificate has revoked the certificate.

Recommendation: Do an audit of all internal HTTPS servers and verify that they use valid certificates before upgrading the ProxySG to SGOS 4.2.x. This ensures that internal HTTPS sites accessed through the ProxySG do not break after upgrading the ProxySG.

A: Once SSL proxy starts intercepting traffic, in addition to the certificate validation checks it does in tunnel mode, it also verifies that the common-name (CN) in the certificate matches with the request URL, and denies data exchange between client and server when a mismatch is detected.

A: From the SSL access logs, you can monitor the following fields to know which servers present certificates with errors and what the ProxySG is doing:

- ❑ `x-rs-certificate-observed-errors`: Shows all the actual error(s) detected with the certificate except `hostname-mismatch` error. Detected errors include `untrusted-issuer`, `expired`, and `revoked`.

- ❑ `x-rs-certificate-validate-status`: Shows the certificate validation status after following policy rules. If policy ignores a specific certificate validation error, this field shows the status as `CERT_VALID` although the certificate presented by a server has the error.

Recommendation: Leave the SSL proxy in its default tunneling mode and monitor the SSL access logs until you have a better understanding of the SSL traffic on the network.

Question: How Do I Fix Server Certificate Errors?

A: The most secure way to fix any certificate error is to get a new certificate that does not have the problem. Make exceptions on a case-by-case basis.

The following certificate errors can be detected by SSL Proxy:

- ❑ `untrusted-issuer`
- ❑ `expired`
- ❑ `revoked`
- ❑ `hostname mismatch (intercepted connections only)`

The most secure way to fix any of these errors is to get a new certificate that does not have the detected error. Many times, however, the sites presenting a bad certificate are not in administrative control. In this case, the SSL proxy provides a way to ignore certificate errors for certain sites through policy.

Recommendation: If you have internal HTTPS servers that use certificates issued by an internal Certificate Authority (CA), the SSL proxy flags such certificates with the "untrusted-issuer" error. To avoid such errors, import the internal CA certificate onto the ProxySG as a trusted certificate. Do not ignore untrusted-issuer errors through policy, because an untrusted-issuer error means that nothing from the certificate can be trusted.

Do not disable certificate validation globally. Make the determination of ignorable certificate errors on a case-by-case basis, as discussed below.

Procedure: To ignore certificate errors for specific sites

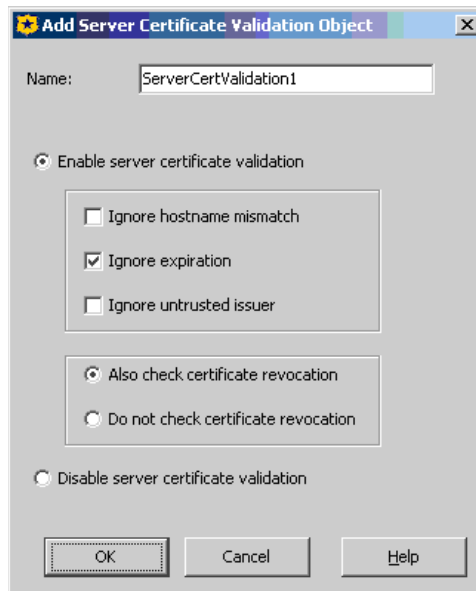
1. Launch the Visual Policy Manager from Configuration>Policy>Visual Policy Manager.
2. Add an SSL Access Layer by selecting Policy>Add SSL Access Layer from the menu bar.

A policy row is added by default when you create a layer.

3. Right click the Destination field; select Set.
4. Click New, then:

For detailed information on using the Visual Policy Manager, refer to the *Blue Coat ProxySG Configuration and Management Guide*.

- a. Add a condition for Destination Host/Port or Server URL.
 - b. Add the IP address and the port.
 - c. Click Close.
 - d. Click OK.
5. Right click the Action field; select Set.
 6. Click New.



7. Select Set Server Certificate Validation.
 - a. Select the certificate errors to ignore for the specific destination selected in Step 4.
 - b. Click OK.
8. Click OK.
9. Apply the policy by clicking Install Policy in the upper-right-hand corner.

Question: How Do I Selectively Intercept SSL Traffic?

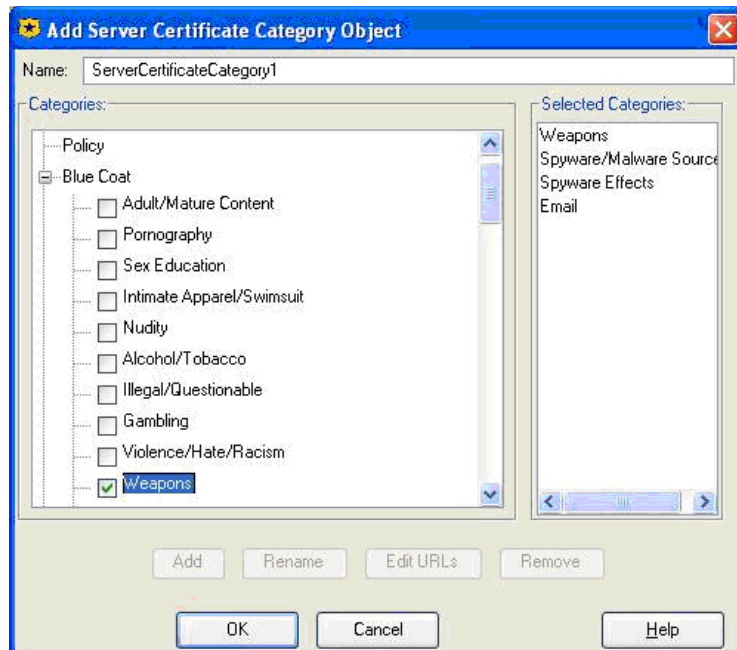
A: In order to selectively intercept SSL traffic using the most preferred method, you must configure a URL filter database.

Using the Blue Coat Web Filter as an example, the following steps illustrate setting up a rule to intercept selected categories.

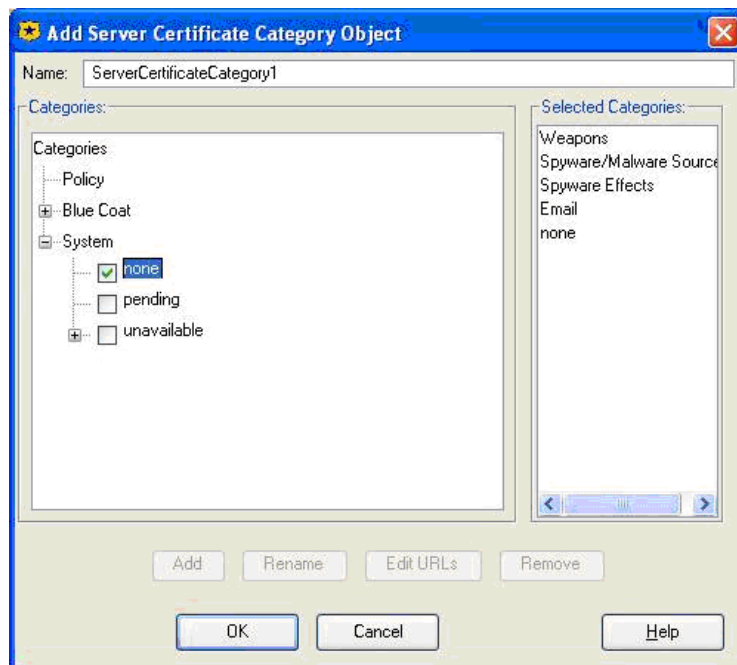
1. Launch the Visual Policy Manager from Configuration>Policy>Visual Policy Manager.
2. Add an SSL Intercept Layer by selecting Policy>Add SSL Intercept Layer from the menu bar.

A policy row is added by default when you create a layer.

3. Right click the Destination field; select Set., then New.



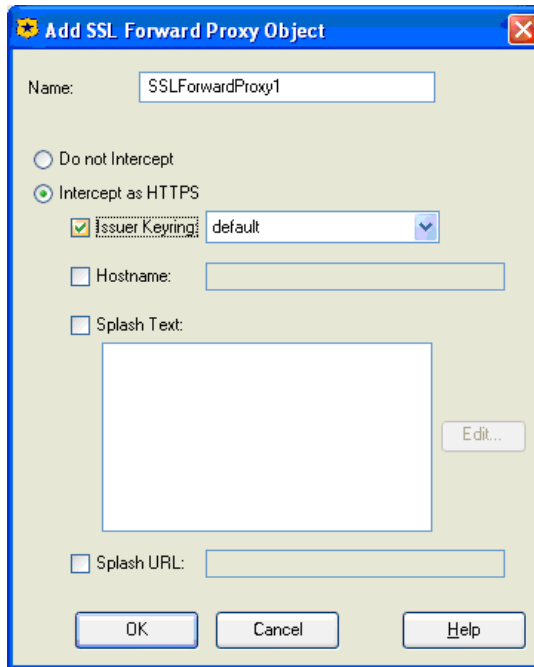
4. Select the Server Certificate Category and expand the Blue Coat category. Select the categories to intercept. Examples include weapons, Spyware/ Malware sources, secure web based e-mail, and the like.



5. Expand the System category; select none to intercept Web sites whose categorization is unknown.

This allows you to treat unrated sites as suspicious and apply security policies to the data transferred to and from such sites.

6. Click OK.
7. Click OK.
8. Right click the Action field; select Set, then New.



For additional details on the SSL Forward Proxy object see Chapter 6 of the *Blue Coat ProxySG Configuration and Management Guide*.

9. Select SSL Forward Proxy Object.
10. Enable Intercept as HTTPS and Issuer Keyring.
11. Click OK.
12. Click OK.
13. Apply the policy by clicking Install Policy in the upper-right-hand corner.

Question: Can the ProxySG Help in Distributing Issuer Certificates to Client Desktops?

A: When the SSL Proxy intercepts an SSL connection, it presents an emulated server certificate to the client browser. The client browser issues a security pop-up to the end-user because the browser does not trust the issuer used by the ProxySG. This pop-up does not occur if the issuer certificate used by SSL Proxy is imported as a trusted root in the client browser's certificate store.

The ProxySG makes all configured certificates available for download via its management console. You can ask end users to download the issuer certificate through Internet Explorer or Firefox and install it as a trusted CA

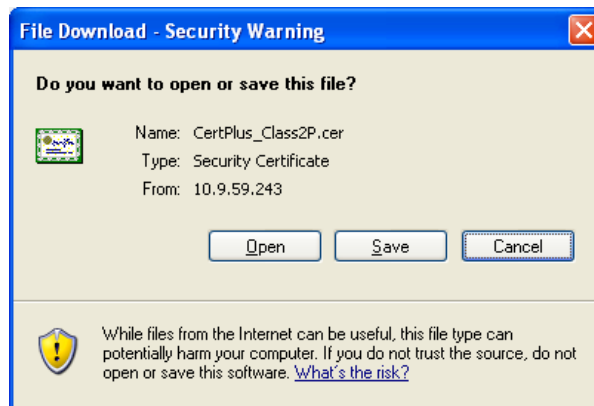
You can e-mail the console URL corresponding to the issuer certificate to end users so that the end-user can install the issuer certificate as a trusted CA.

in their browser of choice. This eliminates the certificate popup for emulated certificates.

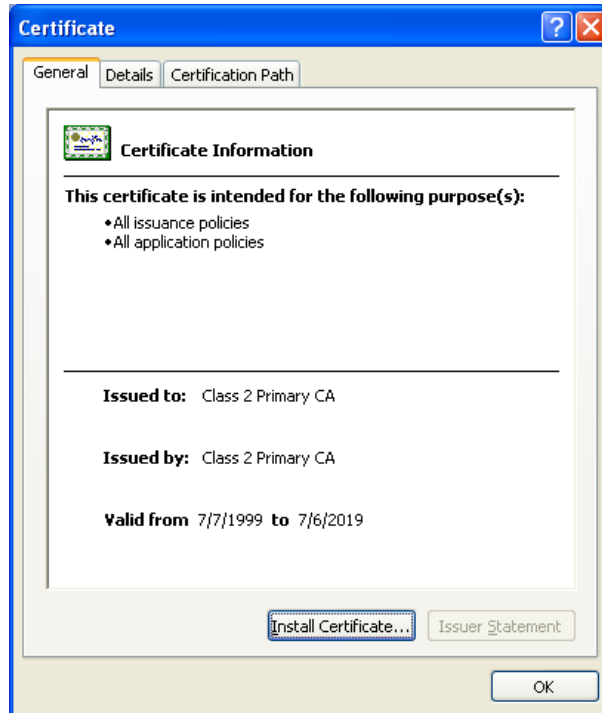
To download the certificate through Internet Explorer, see "To download a certificate through Internet Explorer". To download a certificate through Firefox, see "To download a certificate through Firefox" on page 17.

Procedure: To download a certificate through Internet Explorer

1. Go to Statistics>Advanced.
2. Select SSL.
3. Click Download a ProxySG Certificate as a CA Certificate; the list of certificates on the system display.
4. Click a certificate (it need not be associated with a keyring); the File Download Security Warning displays asking what you want to do with the file.



5. Click Save. When the Save As dialog box displays, click Save; the file downloads.
6. Click Open to view the Certificate properties; the Certificate window displays.



7. Click the Install Certificate button to launch the Certificate Import Wizard.
8. Make sure the Automatically select the certificate store based on the type of certificate radio button is enabled before completing the wizard; the wizard announces when the certificate is imported.
9. (Optional) To view the installed certificate, go to Internet Explorer, Select Tools>Internet Options>Contents>Certificates, and open either the Intermediate Certification Authorities tab or the Trusted Root Certification Authorities tab, depending on the certificate you downloaded.

Procedure: To download a certificate through Firefox

1. Go to Statistics>Advanced.
2. Select SSL.
3. Click Download a ProxySG Certificate as a CA Certificate; the list of certificates on the system display.
4. Click a certificate (it need not be associated with a keyring); the Download Certificate dialog displays.

You can e-mail the console URL corresponding to the issuer certificate to end users so that the end-user can install the issuer certificate as a trusted CA.



5. Enable the checkboxes needed. Note that you should view the certificate before trusting it for any purpose.
6. Click OK; close the Advanced Statistics window.

Question: How Do I Protect End-User Privacy and Avoid Accidental Exposure of Sensitive Information When Intercepting SSL Traffic?

A: For intercepted SSL traffic, potentially sensitive information is available in cleartext in the following locations:

- ❑ If ICAP scanning is enabled for intercepted HTTPS traffic, such data is sent without encryption to the ICAP server.
- ❑ You can log request and response headers containing sensitive information to the access log and event log.
- ❑ If you use an off-box URL filtering solution, part of the URL may be sent in cleartext to the URL database service point. Note that such a service point can be located on the internet.

Recommendation: Take the following measures to avoid accidental exposure of sensitive information:

- Be smart about what sites to intercept. Avoid intercepting well-known banking and financial sites. On-box URL databases and server certificate categories can be used in determining which sites to intercept.
- Use on-box URL databases, such as Blue Coat Web Filter or a third-part content filtering vendor, to avoid transmitting URLs in cleartext.
- Implement HTML notification for intercepted sites. This can be used to inform end-users that their HTTPS traffic will be monitored and that they can opt-out if they do not want their traffic to be

For information on HTML Notification, refer to Chapter 6 of the *Blue Coat ProxySG Configuration and Management Guide*.

For information on Client Consent Certificates, refer to Chapter 6 of the *Blue Coat ProxySG Configuration and Management Guide*.

intercepted. HTML notification is also helpful if a site is accidentally intercepted.

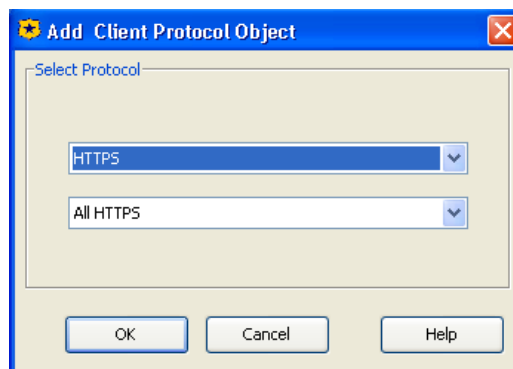
- If you use ICAP scanning for intercepted HTTPS content, make sure the network link between the ProxySG and the ICAP server cannot be snooped.
- Do not log URL or header information for intercepted HTTPS traffic. (By default, the SSL log does not log this information.)

The ProxySG allows you to set up notification two ways, HTML notification and client consent certificates

Setting up HTML Notification

Procedure: Set up HTML notification only for HTTPS sites

1. Launch the Visual Policy Manager from Configuration>Policy>Visual Policy Manager.
2. Add a new rule to the Web Access layer.
 - a. Right click the Action field; select Set.
 - b. Click New, then select the Notify User object.
 - c. Customize the Notify User object as needed.
 - d. Click OK.
 - e. Click OK.
 - f. Right click the Service field; select Set.
 - g. Click New, then select the Client Protocol object.



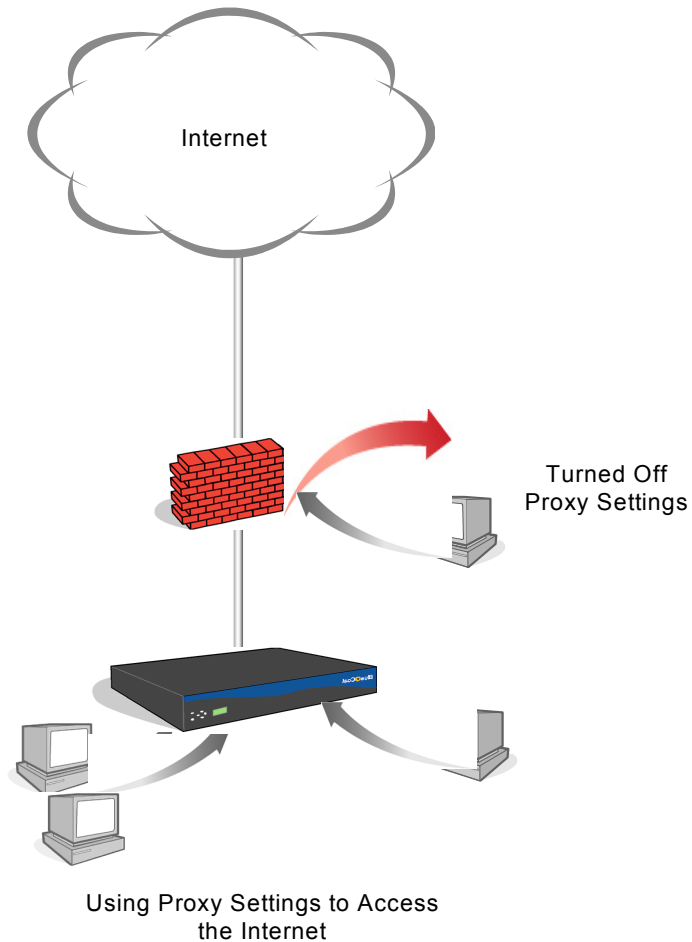
- h. Select HTTPS from the drop-down list in the top field; make sure ALL HTTPS is selected from the drop-down list in the lower field.
 - i. Click OK.
3. Click OK.
 4. Apply the policy by clicking Install Policy in the upper-right-hand corner.

Question: How do I set up SSL Proxy in Explicit Mode?

A: The SSL Proxy can be used in explicit mode in collaboration with the HTTP Proxy or SOCKS Proxy. You must create an HTTP Proxy service or SOCKS Proxy service and use it as the explicit proxy from desktop browsers. When requests for HTTPS content are sent to either a SOCKS proxy or an HTTP proxy, the proxies can detect the use of the SSL protocol on such connections and enable SSL Proxy functionality.

To create an explicit SSL proxy, complete the following steps:

- ❑ Configure the browser on the desktop to use a proxy or point to a PAC file that points to the proxy.
- ❑ Coordinate with other devices, such as a firewall, to prevent users from accessing the internet without a proxy.
- ❑ Create an HTTP proxy service.
- ❑ Create or import an issuer keyring or use the defaults.
- ❑ Configure SSL proxy rules through VPM.



If you want to use an L4 switch, WCCP, or an explicit proxy instead of bridging, disable the bridging Pass-Thru card.

Question: How Do I Deploy SSL Proxy in Transparent Mode?

A: In a transparent proxy configuration, neither the client (browser) nor the desktop knows that the traffic is being processed by a machine other than the origin content server (OCS). The browser believes it is talking to the OCS, so the request is formatted for the OCS; the proxy determines for itself the destination server based on information in the request, such as the destination IP address in the packet, or the Host: header in the request.

A transparent proxy requires one of the following:

- A hardware bridge.
- A WCCP switch.
- An L4 switch.

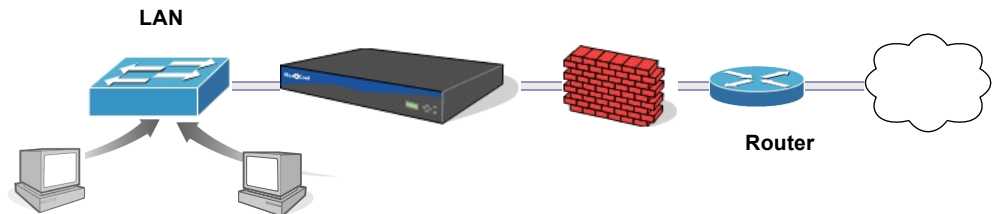
Bridging functionality allows ProxySG Appliances to be deployed in environments where L4 switches, explicit proxies, and WCCP-capable routers are not feasible options.

A branch office that would take advantage of a bridging configuration is likely to be small (from 20 to 50 users); for example, it might have only one router and one firewall in the network, as shown below.

To create a transparent SSL proxy, complete the following steps:

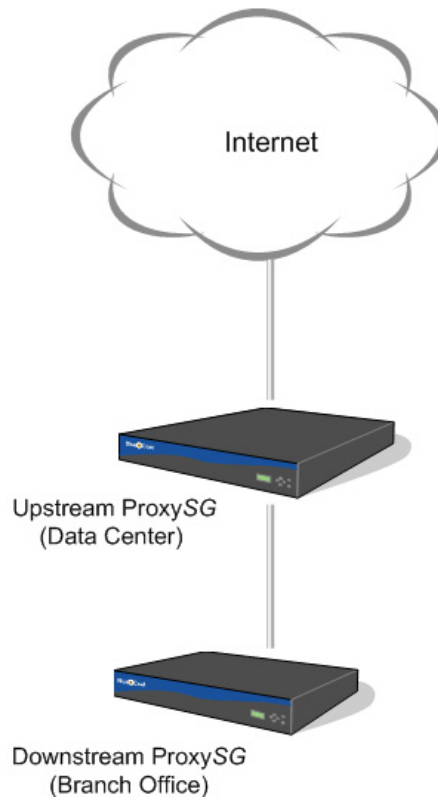
Configure the hardware to use a transparent proxy.

- Create an SSL service on port 443.
- Create or import an issuer keyring or use the defaults.
- Configure SSL proxy through VPM or CPL.



Question: How Do I Deploy the SSL Proxy in a Proxy Chain?

A: A typical SSL proxy chain is shown below.



The ProxySG at the branch office (the downstream ProxySG) uses the ProxySG at the data center (the upstream ProxySG) as its forwarding host, allowing SSL Proxy functionality to be enabled at both the ProxySG appliances.

Tips on Setting Up SSL Proxy Chaining Functionality

- ❑ The upstream ProxySG is configured as the forwarding host of type "HTTP proxy" for the downstream ProxySG.
- ❑ Both proxies have identical SSL related policy; that is, both should make identical decisions in terms of which SSL connections are intercepted and which SSL connections are tunneled.
- ❑ The issuer certificate used by the upstream ProxySG to sign emulated certificates should be imported as a CA certificate on the downstream ProxySG. This ensures that the downstream ProxySG can successfully verify emulated certificates presented by the upstream ProxySG.

Note that this applies to intercepted SSL connections only. For tunneled SSL connections the downstream ProxySG sees the original server certificate.

Now, when an SSL connection is intercepted at the upstream ProxySG, the ProxySG emulates the server certificate and presents the emulated server certificate to the downstream ProxySG.

For information on using forwarding hosts, refer to Chapter 19 of the *Blue Coat ProxySG Configuration and Management Guide*.

For information on creating TCP-tunnel services, refer to the *Blue Coat ProxySG Configuration and Management Guide*.

Question: I am Using a Transparent Proxy Deployment. How Do I Allow Non-SSL Traffic on Port 443 to Certain Servers While Still Enabling the SSL Proxy for the Rest of the Port 443 Traffic?

A: Some legitimate applications, such as the SOCKS-based VPN clients from Aventail and Permeo, use port 443 to communicate to the VPN gateway. However, the protocol they use is not SSL. An SSL service created on port 443 that transparently terminates such TCP connections breaks these applications. That is because the SSL service enforces the use of the SSL protocol.

Administrators would want to allow such SOCKS-based VPN tunnels to a few trusted partner sites.

Procedure: To enable non-SSL protocols on port 443 for certain applications

1. Create a transparent TCP-tunnel service on port 443. Do not create an SSL service on port 443.
2. Specify the list of servers that can use port 443 for non-SSL protocols in policy:

```
define condition Trusted_non_ssl_servers
  url.address=1.1.1.1
  url.address=2.2.2.2
end condition Trusted_non_ssl_servers
```

3. Write a <proxy> layer that forces all other traffic on port 443 to use the SSL protocol:

```
<proxy>
  proxy.port=443 condition != Trusted_non_ssl_servers
  force_protocol(ssl)
```

These rules ensures that port 443 connections to the list of trusted servers are tunneled without intervention while all other port 443 connections use the SSL protocol.

Question: Windows Updates Fail When I Use the SSL Proxy to Intercept all SSL Connections.

A: SSL connections for Windows updates should always be tunneled.

```
<ssl-intercept>  
server.certificate.hostname=update.microsoft.com \  
ssl.forward_proxy(no)  
ssl.forward_proxy(https)
```

The same policy can be created in VPM using the SSL Intercept Layer, the Server Certificate Object, and the SSL Forward Proxy object.

Note that you only need to do this if the policy intercepts everything. If you do selective interception, as recommended, this issue does not arise.

Question: I have CA Hierarchy in Place in My Enterprise. Can I Use it for Certificate Emulation?

A: Some enterprises have a well-defined CA Certificate hierarchy (chain) in place. For example, Clothing-Max, a retail clothing outlet with 150 stores in the U.S. and Canada, has the following:

The Clothing-Max Root CA Certificate is at the top of the hierarchy and has issued a CA certificate for the Clothing-Max IT department. In turn, the IT department issues a CA certificate for the IT security team. The certificate hierarchy looks like this:

If the security team wants to deploy the SSL proxy using its CA certificate as the issuer for emulated certificates, the team will import this certificate and its private key on the ProxySG.

The ProxySG now signs the emulated certificates using the private key of the Clothing-Max IT Security Team CA Certificate. The certificate chain for an emulated certificate for a Clothing-Max server will be:

Root CA	Intermediate CAs	Emulated Certificate
Clothing-Max	Clothing-Max IT Clothing-Max IT Security Team	Clothing-Max Server

In this case the browser does not show a security pop-up if it is able to verify all certificates in the certificate hierarchy.

If you use Internet Explorer, additional requirements are necessary on the intermediate CA certificates in the certificate chain:

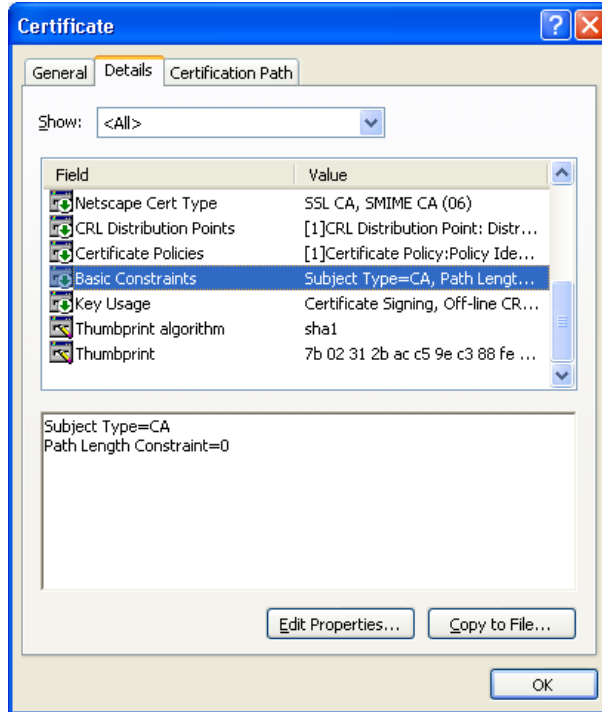
Intermediate CA certificates must contain the basic constraints certificate extension with the Subject Type set to CA.

Root CA certificates are exempt from this requirement

Root CA	Intermediate CA	Intermediate CA
Clothing-Max	Clothing-Max IT	Clothing-Max IT Security Team

The illustration below shows a Verisign Class 2 Intermediate Certificate Basic Constraints Extension.

For detailed information on creating an Intermediate CA using OpenSSL, refer to Chapter 6 of the *Blue Coat ProxySG Configuration and Management Guide*.





Troubleshooting Tips

If a site is rejected by the ProxySG, it does not necessarily mean the certificate is self-signed or not valid.

Certificates not signed by a commercial signing authority, such as those signed by the United States Department of Defense, are rejected until the CA is added to the ProxySG's store.

Upgrading to SGOS 4.2

Upgrading with a Valid SSL Termination/or SSL Proxy Demo License Installed

When upgrading to SGOS 4.2, SSL protocol detection automatically occurs on tunneled connections if you have a valid SSL license installed. In SGOS 4.1, such traffic would just pass through the proxy.

If the proxy detects that the SSL protocol is being used it attempts to validate the server certificate by default. If the server certificate is not signed by a trusted root CA or is expired, the ProxySG aborts the connections. This typically occurs with intranet sites since most of them have certificates not issued by trusted root CAs.

Problem: Can't Reach an HTTPS Site

Description: A request to an HTTPS site results in a failure to reach the site and the browser's default error page will be displayed. In the ProxySG event log, one of the following is displayed:

```
"Server certificate validation failed for support.bluecoat.com at depth 0, reason Untrusted Issuer" 0 310000:1 ../ssl_proxy/sslproxy_worker.cpp:1157
```

```
"Server certificate validation failed for www.etrade.com at depth 0, reason Certificate expired or not valid yet" 0 310000:1 ../ssl_proxy/sslproxy_worker.cpp:1157
```

Solutions:

Option 1 (Most Secure):

- For untrusted issuer errors:

Get the CA certificate from the server administrator and import it to the ProxySG. This is secure only if you can trust the CA's policies when they issue server certificates. When validating the new server certificate, make sure that a new browser instance is used.

- ❑ For expired certificate errors:
 - First check the clock on your proxy. Since the expiration check compares the dates in the certificate against the proxy's clock, make sure that the correct date and time is set.
 - If you still get certificate expired errors, the most secure solution is to get a new certificate with valid dates. This may not possible if you do not control the server.

Option 2 (Less Secure):

Create and install policy to ignore specific errors.

- ❑ To ignore untrusted issuer errors

```
<ssl>
  server_url.host="intranet.company.com"
  server.certificate.validate.ignore.untrusted_issuer (yes)
```

- ❑ To ignore certificate expiration errors

```
<ssl>
  server_url.host="intranet.company.com"
  server.certificate.validate.ignore_expiration (yes)
```

Option 3 (Least Secure):

- ❑ Configure policy to not do protocol detection for SSL. Note that this will disable all SSL Proxy functionality for both internet as well as intranet sites.

```
<proxy>
  detect_protocol.ssl (no)
```

Upgrading and Using SSL Client Certificates with Internet Explorer

After upgrade to SGOS 4.2.x, client certificate authentication can stop working with Internet Explorer if the HTTPS reverse proxy service in question is not using a CA-Certificate List (CCL). This is because IE cannot handle the long list of CAs presented by SG in the handshake messages.

Problem: Client Certificates do not Work with Internet Explorer

Description: When the ProxySG requests a client certificate from the browser, it includes the list of CAs it trusts in the "CertificateRequest" message. The default list of CA certificates configured on the ProxySG has grown and now spans multiple SSL records. Internet Explorer cannot handle SSL handshake messages that span multiple SSL records.

Solutions:

- ❑ For the SSL Proxy, this issue means that the client consent certificate feature that allows the ProxySG to notify users in advance of HTTPS

This problem only affects Internet Explorer. Other browsers do not have this issue.

interception does not work with Internet Explorer. No workaround exists.

- ❑ For the HTTPS Reverse Proxy, you can create a CCL, which reduces the number of CAs trusted by a service to the point where Internet Explorer can handle it.

Problem: Want to Use Client Certificates to Communicate with Server using the SSL Proxy

Description: While client certificates are often used when the SSL proxy is communicating with the client, it is not common for them to be used when communicating with the server.

Solution: You can use client certificates to communicate with the server as long as the SSL proxy is used in tunnel mode. You cannot use client certificates to communicate with the server when the SSL proxy is intercepting traffic.

Logging

Problem: Want to Include other Information in the SSL Access Log

Description: The default access log fields for the SSL log do not contain any sensitive information. Only information that can be seen in the clear on the wire is included in the SSL access log.

Solution: The SSL access log is customizable, meaning that you can add fields that containing sensitive information. For more information on configuring access logs, refer to Chapter 21 in the *Blue Coat ProxySG Configuration and Management Guide*.

Problem: SSL Access Log Contains No Data

Description: When your are intercepting all traffic and logging it, the log remains empty.

Solution: You might be logging all https-forward-proxy connections (that is, intercepted connections) to the main facility instead of the SSL facility.

Microsoft

Problem: Windows Update

Description: The Windows update does not work when the SSL Proxy intercepts windows updates connections. This is because the Windows update client does not trust the emulated certificate presented by the SSL Proxy.

Solution: SSL connections for Windows updates should always be tunneled.

```
<ssl-intercept>  
  server.certificate.hostname=update.microsoft.com \  
  ssl.forward_proxy(no)  
  ssl.forward_proxy(https)
```