SGOS 5 Series

ProxySG ICAP Integration

Blue Coat's proxies can utilize the Internet Content Adaptation Protocol (ICAP) to hand off HTTP requests and/or responses to an external server for configured processing and transformation.

The most common ICAP integration deployment is a Blue Coat ProxySG appliance and a Blue Coat ProxyAV appliance. This document provides instructions on how to perform generic, third-party appliance ICAP response integration, as well as ProxyAV ICAP integration, and Two-Way response and request ICAP implementation.

What is ICAP Integration?

ICAP is the protocol used by Blue Coat ProxySG appliances to communicate with Blue Coat ProxyAV appliances as well as some third party appliances to perform content scanning. By physically integrating the ProxySG and off-box scanning appliance and including it in the Blue Coat ProxySG configuration, the ProxySG is able to send traffic to the scanning appliance so that it can detect viruses, worms, spyware, malware, Trojans; or, when used for request modification, provide data leak prevention (DLP), also known as information leak prevention (ILP) or information detection and leak prevention (IDLP).

Why Implement ICAP?

The key benefit to a Blue Coat solution consisting of a ProxySG appliance and an ICAP-supported appliance/server is the ability of the ProxySG to cache scanned content. Instead of scanning an object every time it is requested, the ProxySG can cache an object that has been scanned and identified as "clean" and subsequently serve it to users. This ability to immediately serve scanned content to users provides a considerable performance enhancement for networks that require content scanning.

Blue Coat ProxySGs support multiple content-scanning vendors to provide administrators with the flexibility to choose the vendor that best addresses the security concerns of their enterprise. The Blue Coat ICAP implementation currently supports the following vendors:

Scan engines supported on Blue Coat ProxyAV appliances:

- Sophos
- Panda
- McAfee
- Kaspersky

Third party off-box ICAP antivirus appliances/servers supported:

- Finjan Vital Security
- Symantec AntiVirus Scan Engine (SAVSE)
- WebWasher

Third party off-box ICAP DLP/ILP appliances supported:

- Vontu Prevent
- Reconnex iGuard
- Vericept Network Monitor/ Prevention
- Port Authority (now WebSense Data Protection)

NOTE: ICAP is an open publicly available standard, so there may be other 3rd party content scanning devices that are functionally compatible with Proxy SG beyond those listed here. These other devices/integrations have not been tested and certified by Blue Coat and are therefore not supported.

Implementing Response ICAP

To configure and test the Blue Coat ICAP solution for incoming traffic on the ProxySG appliance, you must complete the following tasks:

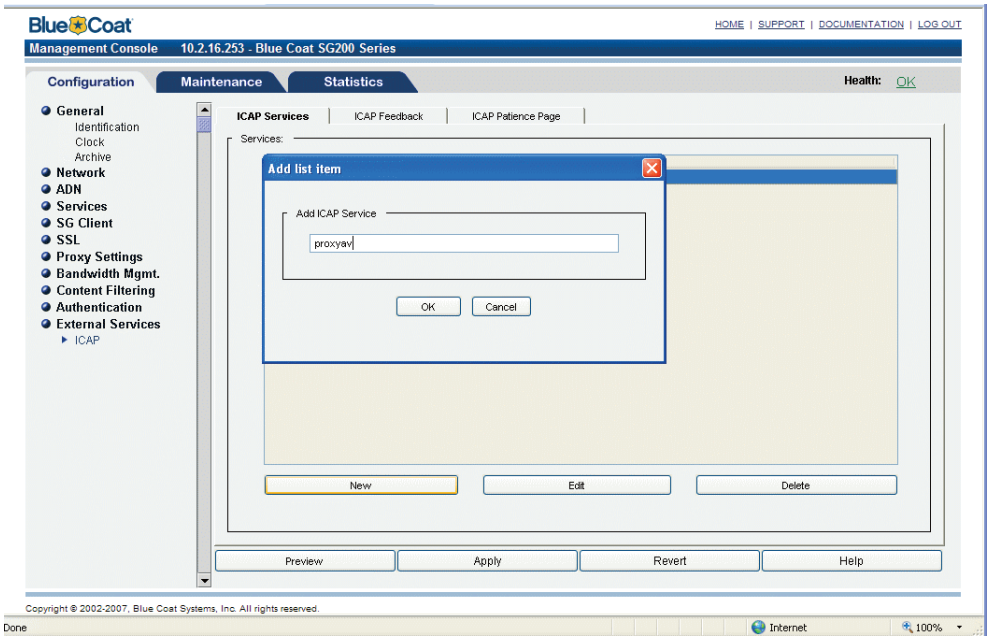
① Configure the ProxySG to communicate with the content-scanning server.

② Create a Blue Coat policy to implement the desired content scanning.

③ Test the Blue Coat policy.

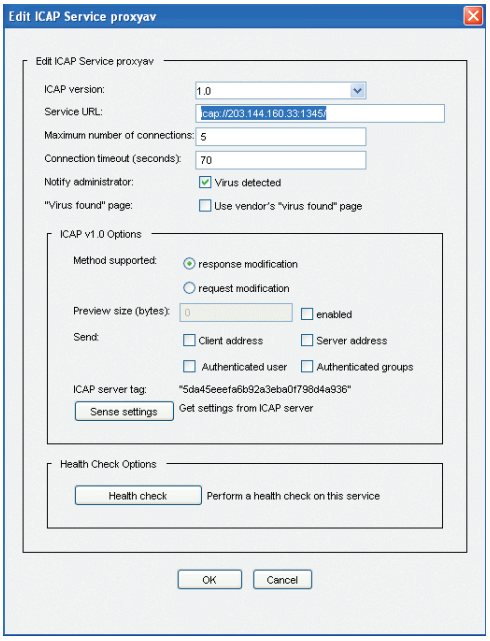
Configuring the ProxySG to Communicate with the Content-Scanning Server Using ICAP

To configure communication between the ProxySG and the ICAP server:



❶ Begin by going to **External Services > ICAP** in the Management Console. Click **New** and create an ICAP service; this example names the service **proxyav**. Click **Apply** to finish. **Note:** If you are using a Blue Coat ProxyAV appliance, check the ICAP Settings page for information on correctly configuring ICAP on the ProxySG.

2. Configure the ICAP service:



   a. Select the new service and click **Edit**.

   b. For the **Service URL**, enter the appropriate content-scanning server URL and port. The port must be included in the URL only if the content-scanning server is not using the default ICAP port, 1344. A list of appropriate content scanning URLs includes the following:

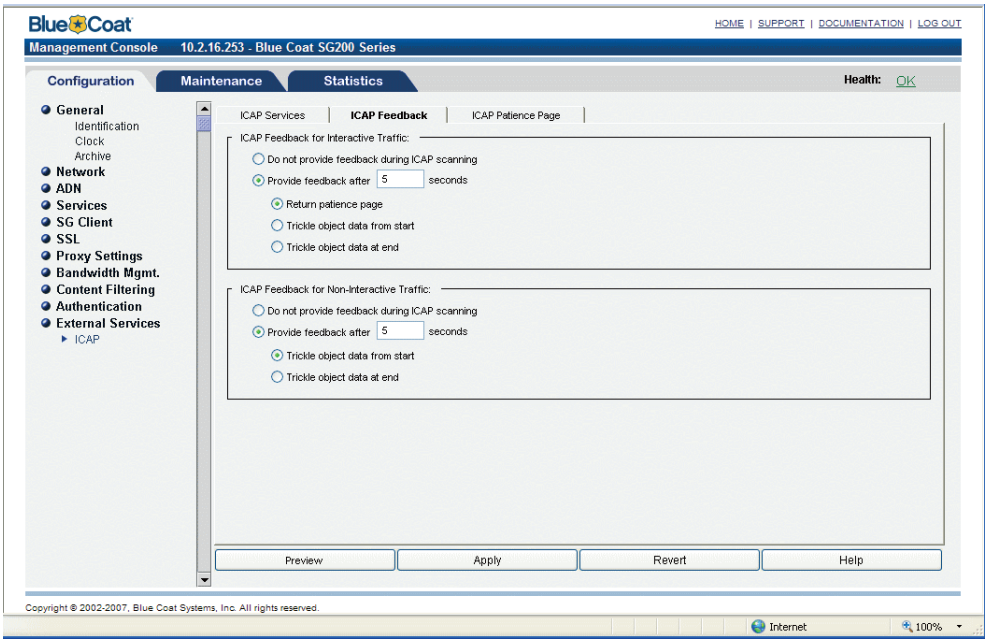
      - ProxyAV: icap://<ipaddress-of-server>:<port>/avscan
      - Symantec SAVSE: icap://<ipaddress-of-server>:<port>/avscan
      - Finjan Vital Security: icap://<ipaddress-of-server>:<port>
      - WebWasher: icap://<ipaddress-of-server>:<port>/wwrespmod

   c. In the **ICAP v1.0 Options** area, select the appropriate **Method supported** option, either **response modification** or **request modification**. Most vendors support only one type of modification; check the vendor documentation to determine the appropriate selection.

   d. Click **Sense Settings** to automatically retrieve IS-TAG settings from the content-scanning server. This automatically populates the preferred ICAP service settings for this particular vendor.

   e. Click **OK** to confirm the sense settings selection.

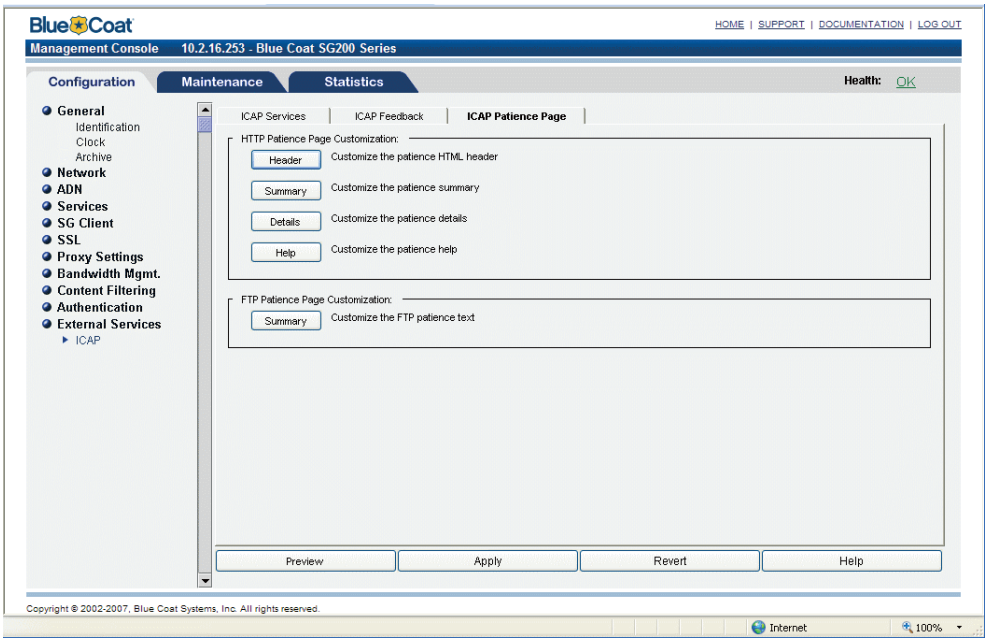
   f. A health check is automatically performed on the service. If the health check and sense settings retrieval are successful, the window closes and the ICAP service settings are saved.



3. Configure the desired feedback type (optional). This example implements patience pages and ICAP data trickling at the start (the default). For information on the available feedback options, click **Help** in the bottom right-hand corner of the screen:

   a. Go to **Configuration > External Services > ICAP > ICAP Feedback**.

   b. Edit any of the selections available to customize the feedback type. Click **Apply** to finish.



4. Customize the HTTP or FTP patience page content (optional):

   a. Go to **Configuration > External Services > ICAP > ICAP Patience Page**.

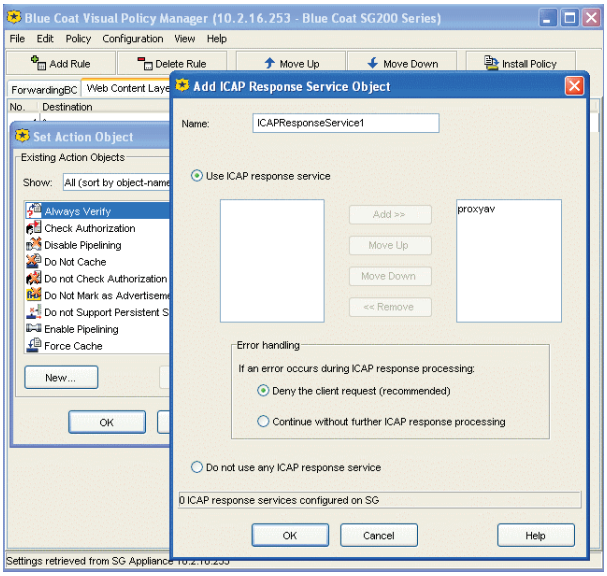
   b. Edit any of the selections available to customize the patience pages. Click **Apply** to finish.

Creating a Blue Coat Policy to Implement the Desired Content Scanning

Blue Coat policy supports request scanning (reqmod) for data leak prevention and response scanning (respmod) for malware scanning. The scanning type selected in policy will depend on the ICAP service(s) created.

If you are scanning both requests and responses, separate ICAP services and policy rules must be created. This procedure describes setting up scanning of responses only. A description of setting up scanning of requests follows in the Implementing Response and Request (Two-Way) ICAP section.

Using the Visual Policy Manager (VPM):

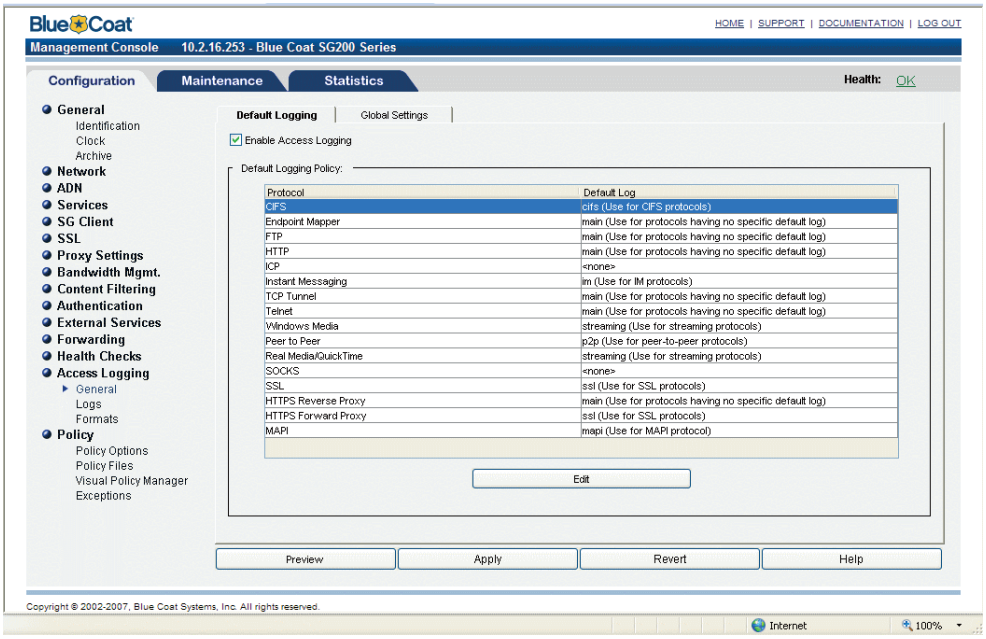


1. Click **Policy** and select **Add Web Content Layer** from the pull-down menu. A new Web Content Layer dialog opens.
2. Name the Web Content Layer (optional) and click **OK**. A new Web Content Layer appears in the VPM.
3. Right-click the **Action** setting and select **Set**. A Set Action Object dialog opens.
4. Click **New** and select **Set ICAP Response Service**. An Add ICAP Response Service Object dialog opens.
5. Name the new ICAP Response Service action object (optional). Select the new ICAP service and click **Add** to apply it to the object. **Note:** Additional configured ICAP services can also be added if failover is desired. Click **OK** to create the ICAP Response Service object and dismiss the dialog.
6. Click **OK** to set the ICAP Response Service object and dismiss the dialog.
7. Click **Install Policy** in the VPM to finish.

Testing the Blue Coat Policy

Appropriate testing depends on the type of scanning solution deployed. For this document, an anti-virus content-scanning solution is described.

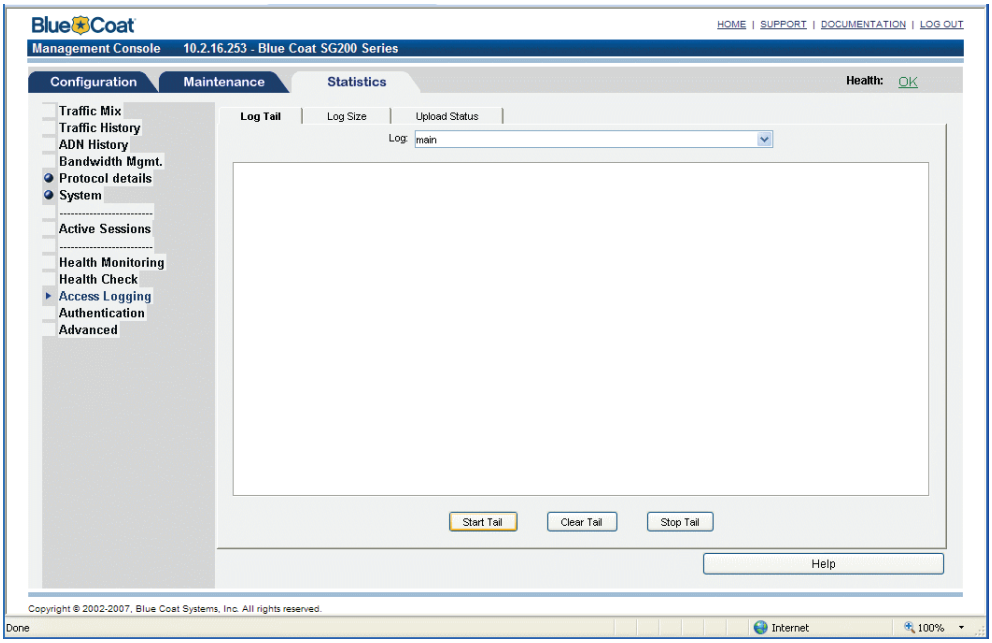
1. Prepare the content-scanning server for test validation:
   a. Verify that the content-scanning service is up and running on the content-scanning server.
   b. Verify that the content-scanning service is configured to log events to the system (if required).
   c. If possible, open the content-scanning server application event viewer (for example, in Windows this may be located at **Control Panel > Administrative Tools > Event Viewer**) and clear the events. Leave the event viewer on the content-scanning server open so that events can be viewed during testing.



2. Prepare the ProxySG appliance for test validation:

   a. Go to **Configuration > Access Logging > General > Default Logging**.

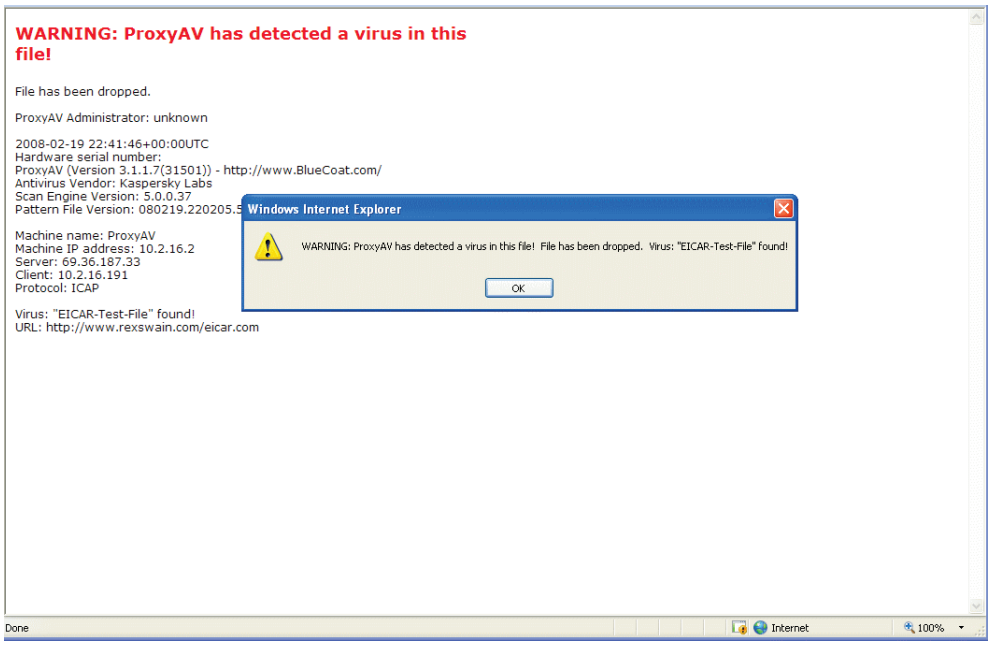
   b. Check the **Enable Access Logging** checkbox in the upper left-hand corner. Click **Apply**.



   c. Go to **Statistics > Access Logging > Log Tail**. From the pull-down menu at the top, select log type **main**. Click **Start Tail**.

   d. Leave the Log Tail page on the ProxySG open so that log entries can be viewed during testing.

3. Request an "infected" test file. **Note:** The file provided below is not actually an infected file but has a virus signature that identifies it as infected for testing purposes: From a browser either explicitly or transparently redirected to the ProxySG appliance, go to: http://www.eicar.org/download/eicar.com.



4. Confirm that you were not provided with the "infected" file: You should have been presented with a page (from the ProxySG or the content-scanning server, depending on your configuration) indicating that the file could not be served because it contained a virus (or virus signature).

5. Verify that the ProxySG appliance requested the content from the origin content server (and not from cache): On the open Access Log Tail screen, verify that the access log entry for the **eicar** file contains a **TCP_MISS**.

6. If possible, verify that the content-scanning server has scanned the file and detected the virus: In the open event viewer, refresh the event log and verify that event messages indicate that the file was scanned.

7. Request the "infected" test file again and verify that the ProxySG serves it from cache. This illustrates the ProxySG's ability to "scan once, serve many". For objects that have already been scanned and found to be "clean", this means that the object originally requested and scanned is served from cache. For objects that were modified in some way by the scanning server, or for those that resulted in the scanning server providing an error page in lieu of the object, the object returned by the scanning server is served from cache.

   a. From a browser either explicitly or transparently redirected to the ProxySG, go to: http://www.eicar.org/download/eicar.com again.

   b. On the open Access Log Tail screen on the ProxySG, verify that the access log entry for the eicar object contains a **TCP_HIT**.

   c. In the open event viewer on the content-scanning server, refresh the event log and verify that there are no new event messages pertaining to this file. (Since the object was served from cache it should not have been sent to the content-scanning server for scanning).

Implementing Response and Request (Two-Way) ICAP

ICAP response modifications for incoming traffic are used for virus protection; ICAP request modifications for outgoing traffic are mostly used for data leak prevention (DLP). The same client request can have request-modification applied before it is forwarded to the origin-content server and response-modification applied as the object data returns.

To set up two-way ICAP on the ProxySG appliance, you must complete the following tasks:

① Configure two ICAP services on the ProxySG; one for Requests and one for Responses.

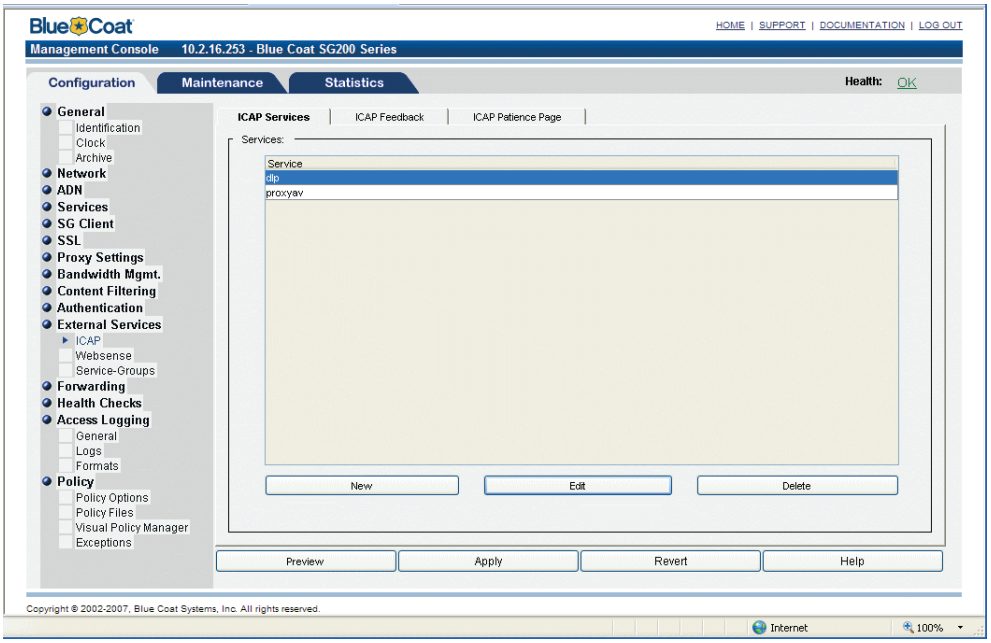
② Create a Blue Coat policy for the ICAP Response service for inbound traffic.

③ Create a Blue Coat policy for the ICAP Request service for outbound traffic.

④ Test the Blue Coat policies.

Configuring the ICAP Services

To configure the ICAP services on the ProxySG:



❶ Create two ICAP services, one in **Response modification** mode for virus scanning on inbound traffic, one in **Request modification** mode for data leak prevention (DLP) on outbound traffic. Name the services appropriately; for example, name the Response modification service "proxyav," the Request modification "DLP."

❷ Configure the ICAP service, for each:

a. Select the new service and click **Edit**.

b. For the **Service URL**, enter the appropriate content-scanning server URL and port. The port must be included in the URL only if the content-scanning server is not using the default ICAP port, 1344. A list of appropriate content scanning URLs includes the following:

- ProxyAV: icap://<ipaddress-of-server>:<port>/avscan
- Symantec SAVSE: icap://<ipaddress-of-server>:<port>/avscan
- Finjan Vital Security: icap://<ipaddress-of-server>:<port>
- WebWasher: icap://<ipaddress-of-server>:<port>/wwrespmod

c. In the **ICAP v1.0 Options** area, select the appropriate **Method supported** option, either **response modification** or **request modification**. Most vendors support only one type of modification; check the vendor documentation to determine the appropriate selection.

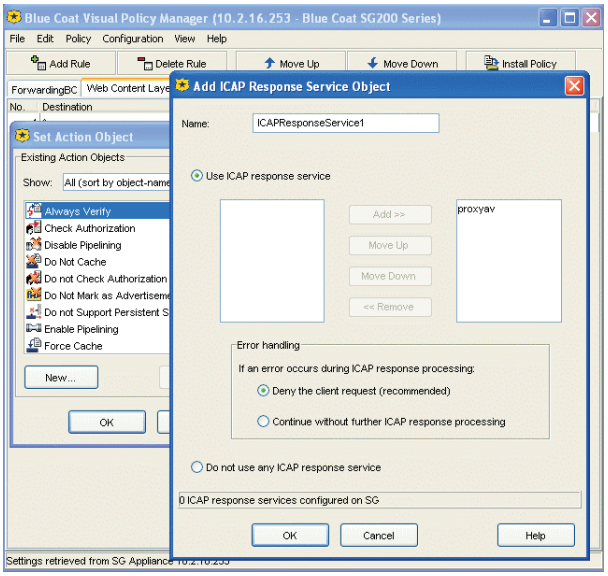
d. Click **Sense Settings** to automatically retrieve IS-TAG settings from the content-scanning server. This automatically populates the preferred ICAP service settings for this particular vendor.

e. Click **OK** to confirm the sense settings selection.

f. A health check is automatically performed on the service. If the health check and sense settings retrieval are successful, the window closes and the ICAP service settings are saved.

Creating the ICAP Response Policy

You'll create a separate policy for each ICAP service; for the Response policy:



1. Using VPM, create a Web Content Layer for the ICAP Response Service, all inbound traffic comes through the Web Content Layer: Click **Policy** at the top and select **Web Content Layer**. A new layer displays.
2. Set the action for the Response policy:
   a. Right-click the **Action** setting and select **Set**. A Set Action Object dialog opens.
   b. Click **New** and select **Set ICAP Response Service**. An Add ICAP Response Service Object dialog opens.
   c. Name the new ICAP Service action (optional). Select the new ICAP Response service and click **Add** to apply it to the object. Click **OK** to create the ICAP Response Service object and dismiss the dialog.
   d. Click **OK** to set the ICAP Response Service object and dismiss the dialog.
3. Click **Install Policy** to finish.

Creating the ICAP Request Policy

To create the Request policy:

1. Create a Web Access Layer for the ICAP Request Service: Click **Policy** at the top and select **Web Access Layer**. A new layer displays.

2. Create a combined service object for the Request policy:

   a. Right-click the **Service** setting and select **Set**. A Set Service Object dialog opens.

   b. Click **New** and select **Protocol Methods**. The Add Methods dialog opens.

   c. Name the new protocol method (optional) and select **HTTP/HTTPS** from the **Protocol** drop-down menu. Options display for selecting HTTP/HTTPS methods.

   d. Select the **Common methods (HTTP 1.1 / RFC 2616)** checkbox and the **Post** and **Put** checkboxes. Click **OK** to set the HTTP/HTTPS Method object and dismiss the dialog.

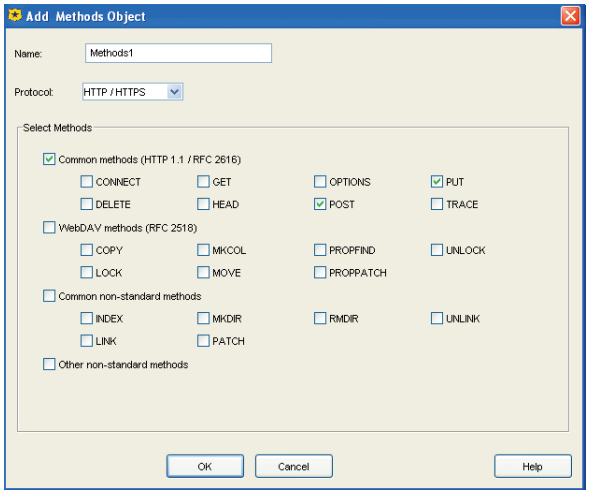
   e. Create another Protocol Method for FTP traffic by clicking **New** and again selecting **Protocol Methods**. The Add Methods dialog opens.

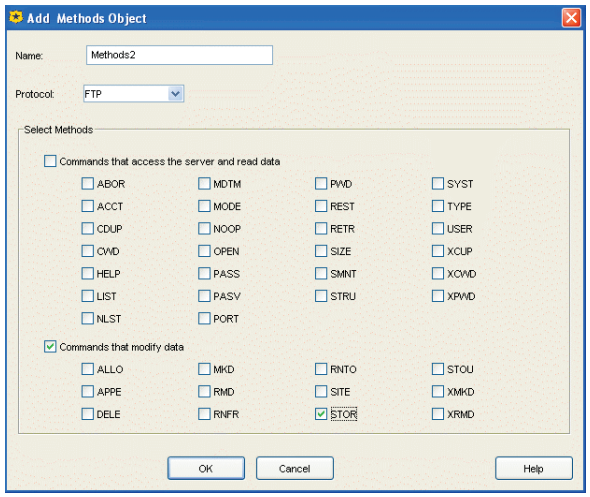
   f. Name the new protocol method (optional) and select **FTP** from the **Protocol** drop-down menu. Options display for selecting FTP methods.

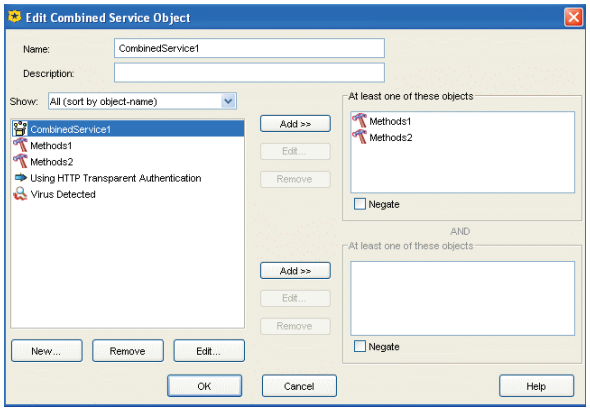
   g. Select the **Commands that modify data** checkbox and the **STOR** checkbox. Click **OK** to set the FTP Method object and dismiss the dialog.

   h. Combine the two method objects by clicking **New** and selecting **Combined Service Object**. The Add Combined Service Object dialog opens.

   i. Select the HTTP/HTTPS and FTP service objects that you created, one at a time, and click **Add** to add them to the combined service object. Click **OK** to finish and dismiss the dialog. Click **OK** again to set the Combined Service object as the Web Access Layer service.







3. Now, set the action for the Request policy:

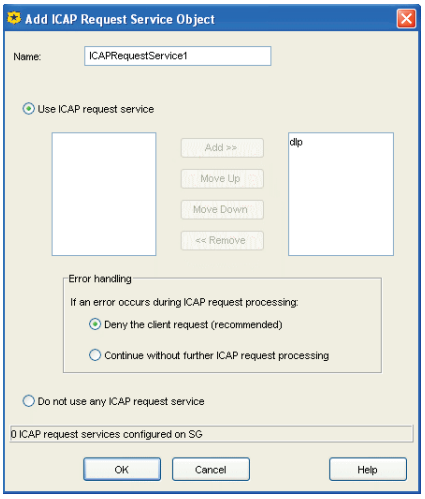
   a. Right-click the **Action** setting and select **Set**. A Set Action Object dialog opens.

   b. Click **New** and select **Set ICAP Request Service**. An Add ICAP Request Service Object dialog opens.

   c. Name the new ICAP Service action (optional). Select the appropriate new ICAP Request service and click **Add** to apply it to the object. Click **OK** to create the ICAP Request Service object and dismiss the dialog.

   d. Click **OK** to set the ICAP Request Service object and dismiss the dialog.

4. Click **Install Policy** in the VPM to finish. Close the VPM window.



Testing the Two-Way ICAP Implementation

This combined layer policy can be tested in a similar manner as the single layer ICAP policy described in Testing the Blue Coat Policy for the ICAP Response policy described previously.

For the ICAP Request policy, make sure that DLP has been configured on the ICAP Request content-scanning server and send a request out to trigger it.

Note: *When testing the FTP request, the request will succeed but ICAP content-scanning server should replace the FTP content with the configured message.*

Conclusion

By implementing Blue Coat ProxySG's ICAP integration functionality, you can offload server requests through the caching of already-scanned objects, and implement malware prevention through the use of an anti-virus scanner or, when used for request modification, provide data leak prevention (DLP), also known as information leak prevention (ILP) or information detection and leak prevention (IDLP).

Blue Coat Systems, Inc.
www.bluecoat.com

Corporate Headquarters
Sunnyvale, CA USA // +1.408.220.2200

EMEA Headquarters
Hampshire, UK // +44.1252.554600

APAC Headquarters
Hong Kong // +852.3476.1000