GX integration with Symantec Secure Web Gateway (Blue Coat ProxySG) Application note

V1.0 August 2018

Table of Contents

1 Introduction

1.1 Scope

This document outlines how to integrate a Symantec Secure Web Gateway (Blue Coat ProxySG) with Deep Secure's Gateway eXtension (GX) appliance.

GX provides a bi-directional guarding capability for ICAP, as discussed in the *GX Configuration Guide.*

This document details the configuration steps needed for the Blue Coat ProxySG appliance to send data to, and receive data from, GX. This integration guide has been written for the current latest release of SGOS 6.7.1. Whilst previous releases of SGOS are also compatible, however, it should be noted that certain naming conventions may vary in earlier releases.

The integration guide supports both physical appliances and virtual editions of Secure Web Gateway. In addition, the Blue Coat ProxySG can be deployed with the GX in a forward or reverse proxy arrangement.

1.2 Background

A typical deployment is as shown below.

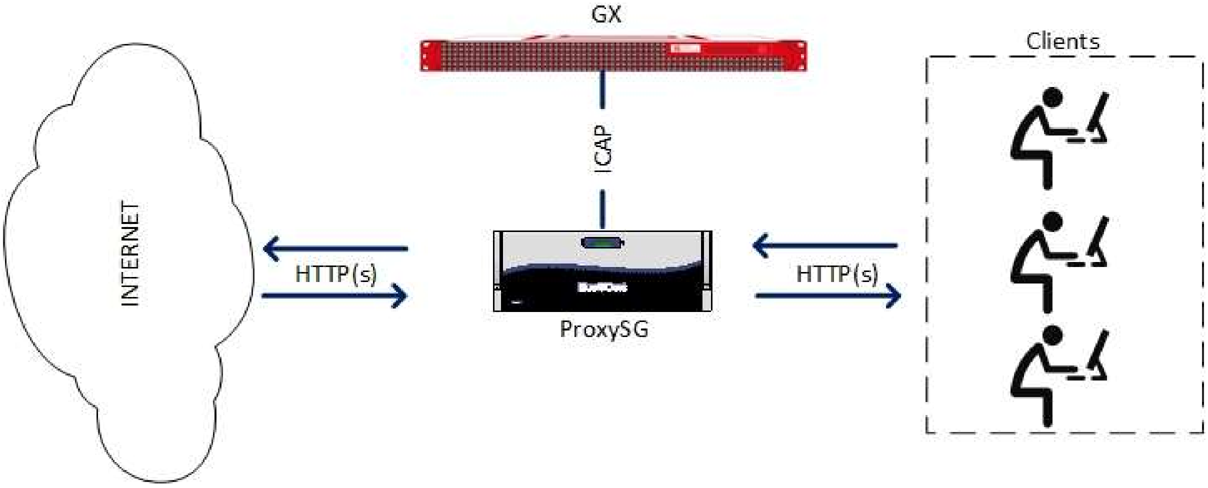


Figure 1-1: GX and ProxySG deployment (Forward Proxy)

1.3 Audience

This guide is for Deep Secure CTR appliance system administrators, who are assumed to have a full understanding of network topology and routing.

1.4 Conventions

This guide uses the conventions shown in Table 1-1 :

Convention	Indicates
Emphasis	Terms in a definition list or emphasis for important introductory words in a paragraph.
`Options`	Menu names, options, buttons, keys and other items from the user interface or the keyboard.
Italics	Cross-reference to related information in another document.
<variable>	A value you must supply, for example in a command line.
[<variable>]	An optional value you can supply, for example, in a command line.
⊗	**Important information that emphasises or supplements points in the text, or that may apply only in special cases.**
⚠	**A caution that alerts you that failure to take or avoid a specified action could result in the loss of data.**
Tip	**A tip that suggests an alternative method for applying a technique or procedure, or helps you to understand the benefits and capability of the product.**

Table 1-1: Conventions in this document

1.5 Purpose

This guide takes you through the steps you need to follow to integrate Symantec Blue Coat ProxySG with a GX CTR appliance.

2 Pre-requisites

Before configuring Blue Coat ProxySG to work with GX there are a number of pre-requisites that should be set.

Ensure the Blue Coat ProxySG is installed, licensed and configured to:

- Proxy HTTP requests
- Intercept SSL requests
- Enable ICAP

Ensure the Deep Secure GX appliance has been installed and configured to listen for ICAP traffic. Refer to the *GX Configuration Guide* for more information.

The GX Data network interface should be on the same network segment as the interface used to pass ICAP traffic to an external service.

> **Tip** For additional security the GX Data network interface and the Blue Coat ProxySG appliance can reside on a private network or could be connected using a cross-over cable if necessary.

3 Integration Steps

The following steps detail how to configure the Blue Coat ProxySG to receive data and send data to the GX via ICAP.

> ⚠ For the following configuration steps, it is assumed that the Blue Coat ProxySG is already configured correctly to perform as a Secure Web Gateway or Reverse Proxy. If not, please refer to the appropriate Symantec Blue Coat ProxySG configuration documentation to complete these steps.

3.1 Initial configuration

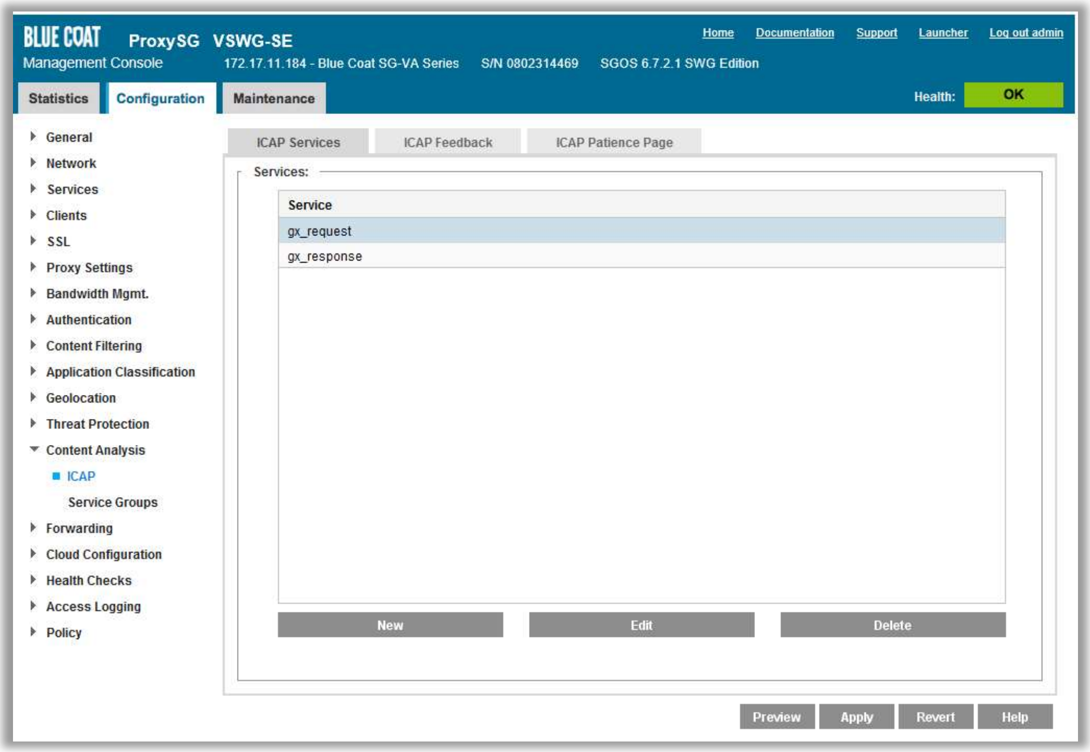
It is necessary to first create the ICAP services for each deployed GX. To do this, connect to the ProxySG Management Interface.

Locate **Configuration -> Content Analysis -> ICAP -> ICAP Services** and within this window, select the **new** button.

It is necessary to create a new ICAP service for both the ICAP Request and the ICAP Response mode. This allows the Deep Secure GX to support web download (ICAP Response) and web upload (ICAP Request).

> Tip Earlier versions of SGOS may refer to the following: **Configuration -> External Services -> ICAP -> ICAP Services**

Create two new ICAP services, one for ICAP Request and one for ICAP Response, as shown below:



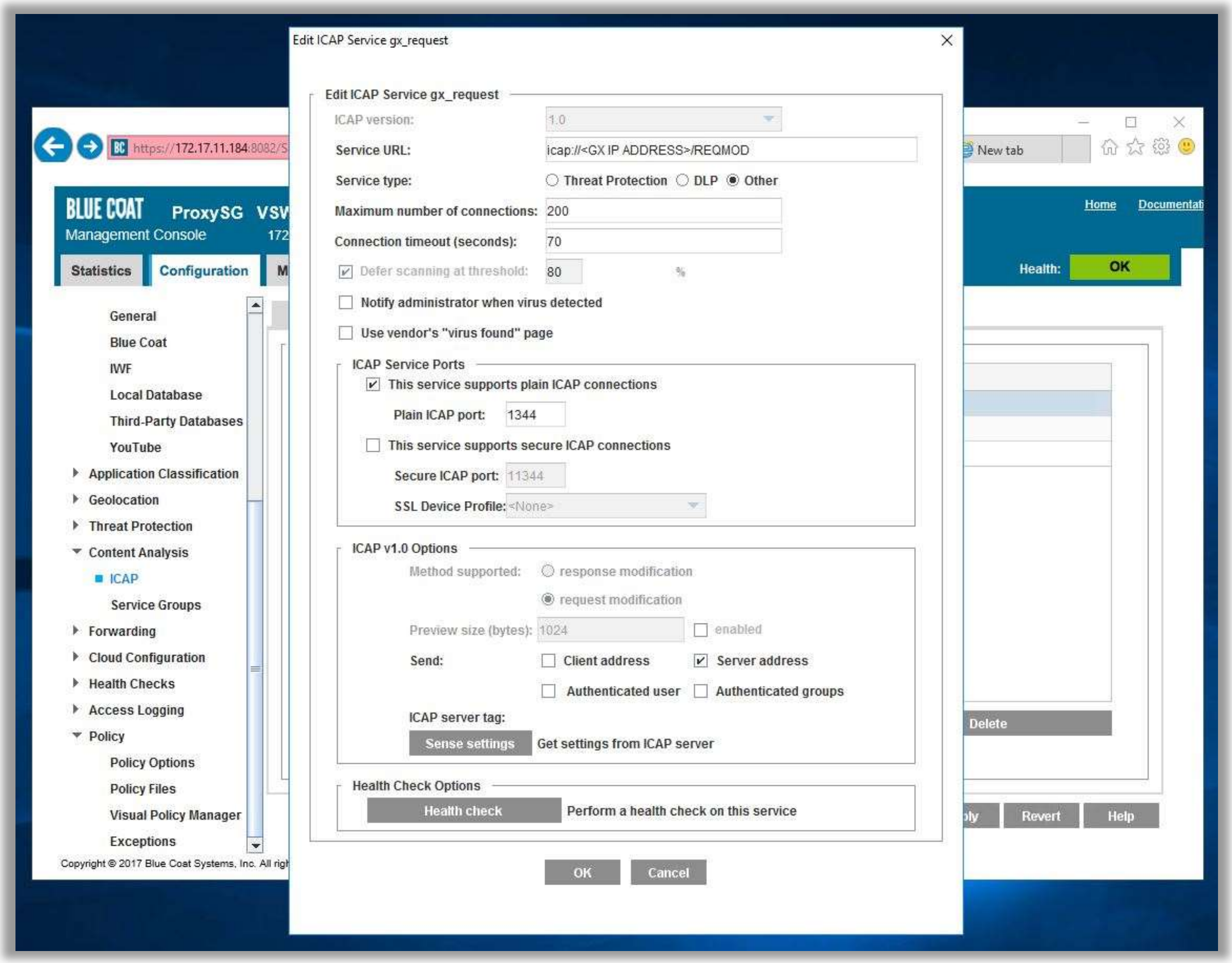
Service
gx_request
gx_response

Figure 3-1: Example GX ICAP Request and Response configuration

Once each ICAP service is created you are required to edit the configuration, as guided below.

3.2 ICAP Request Configuration

Navigate to **Configuration -> Content Analysis -> ICAP** and select **GX_Request** then select **Edit**:



Edit ICAP Service gx_request

Edit ICAP Service gx_request

ICAP version: 1.0

Service URL: icap://<GX IP ADDRESS>/REQMOD

Service type: ○ Threat Protection ○ DLP ● Other

Maximum number of connections: 200

Connection timeout (seconds): 70

☑ Defer scanning at threshold: 80 %

□ Notify administrator when virus detected

□ Use vendor's "virus found" page

ICAP Service Ports

☑ This service supports plain ICAP connections

Plain ICAP port: 1344

□ This service supports secure ICAP connections

Secure ICAP port: 11344

SSL Device Profile: <None>

ICAP v1.0 Options

Method supported: ○ response modification ● request modification

Preview size (bytes): 1024 □ enabled

Send: □ Client address ☑ Server address □ Authenticated user □ Authenticated groups

ICAP server tag:

Sense settings — Get settings from ICAP server

Health Check Options

Health check — Perform a health check on this service

Figure 3-2: Edit GX Request Configuration

The following general settings, only, should be specified:

ICAP version	1.0
Service URL	`icap://`**`<ip address of your GX>`**`/REQMOD`
Service Type	Other

Under the heading **ICAP Service Ports** ensure **This service supports plain ICAP connections** is ticked

Under **ICAP v1.0 Options**:

- Method supported request modification
- Preview size (bytes) 1024 (and **enabled** is ticked)

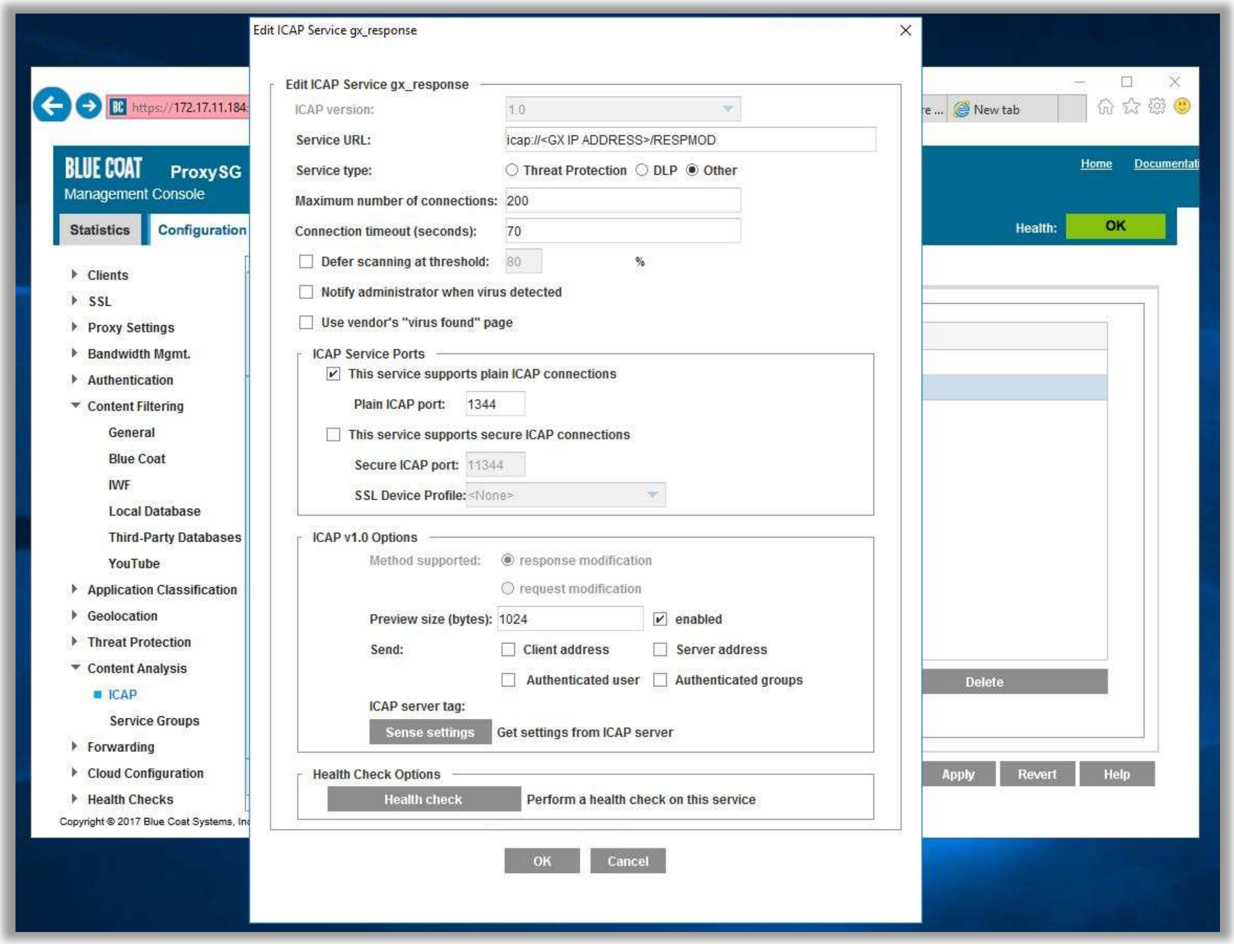
Next, press **Sense settings** to retrieve configuration information from the GX.

Finally, press the **Health check** button to ensure the GX is reachable.

Tip If the health check did not successfully respond, please check network configuration and try the above steps again.

3.3 ICAP Response Configuration

Navigate to **Configuration -> Content Analysis -> ICAP** and select **GX_Response** then select **Edit**:



Edit ICAP Service gx_response

Edit ICAP Service gx_response

ICAP version: 1.0

Service URL: icap://<GX IP ADDRESS>/RESPMOD

Service type: ○ Threat Protection ○ DLP ● Other

Maximum number of connections: 200

Connection timeout (seconds): 70

□ Defer scanning at threshold: 80 %

□ Notify administrator when virus detected

□ Use vendor's "virus found" page

ICAP Service Ports

☑ This service supports plain ICAP connections

Plain ICAP port: 1344

□ This service supports secure ICAP connections

Secure ICAP port: 11344

SSL Device Profile: <None>

ICAP v1.0 Options

Method supported: ● response modification ○ request modification

Preview size (bytes): 1024 ☑ enabled

Send: □ Client address □ Server address □ Authenticated user □ Authenticated groups

ICAP server tag:

Sense settings Get settings from ICAP server

Health Check Options

Health check Perform a health check on this service

OK Cancel

Figure 3-3: Edit GX Response Configuration

The following general settings, only, should be specified:

ICAP version	1.0
Service URL	`icap://`**`<ip address of your GX>`**`/RESPMOD`
Service type	Other

Under the heading **ICAP Service Ports** ensure **This service supports plain ICAP connections** is ticked

Under **ICAP v1.0 Options**:

Method supported	response modification
Preview size (bytes)	1024 (and **enabled** is ticked)

Next, press **Sense Settings** to retrieve configuration information from the GX.

Finally, press the **Health Check** button to ensure the GX is reachable.

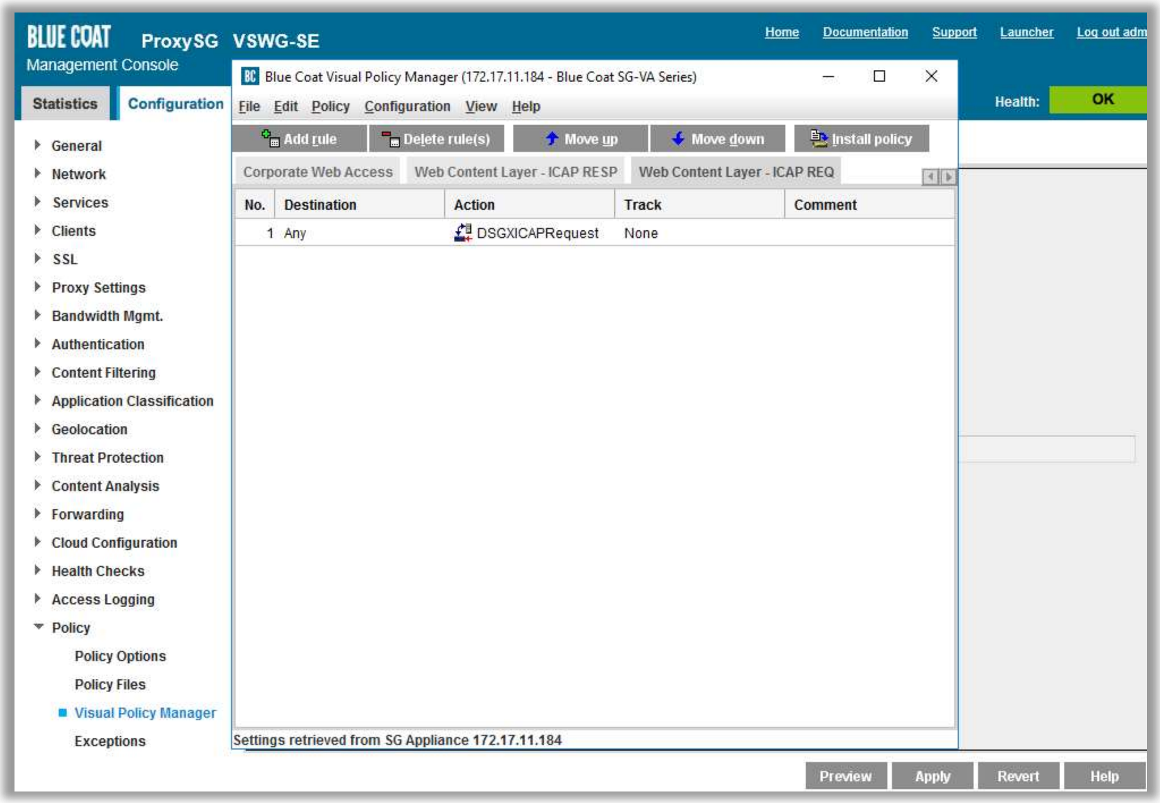
Tip If the health check did not successfully respond, please check network configuration and try the above steps again.

The ProxySG is now configured to communicate with the GX, and is therefore ready for policy implementation.

3.4 Configuring the Visual Policy Manager for Forward Proxy

To apply content transformations for a Secure Web Gateway implementation (forward proxy):

Locate **Configuration -> Policy-> Visual Policy Manager** and select the **Launch** button.



No.	Destination	Action	Track	Comment
1	Any	DSGXICAPRequest	None	

Settings retrieved from SG Appliance 172.17.11.184

Figure 3-4: Launch Visual Policy Manager

It is necessary to create two new **Web Content Layer** policies, one for ICAP Request and one for ICAP Response. To do this, select **Policy** from the **Visual Policy Manager** menu and select **Add Web Content Layer.**

Provide a relevant name in the **Add New Layer** window (for example **Web Content Layer – ICAP REQ**).

In the new content layer right click **Use Default Caching** and select **Set** and then select **New…** button

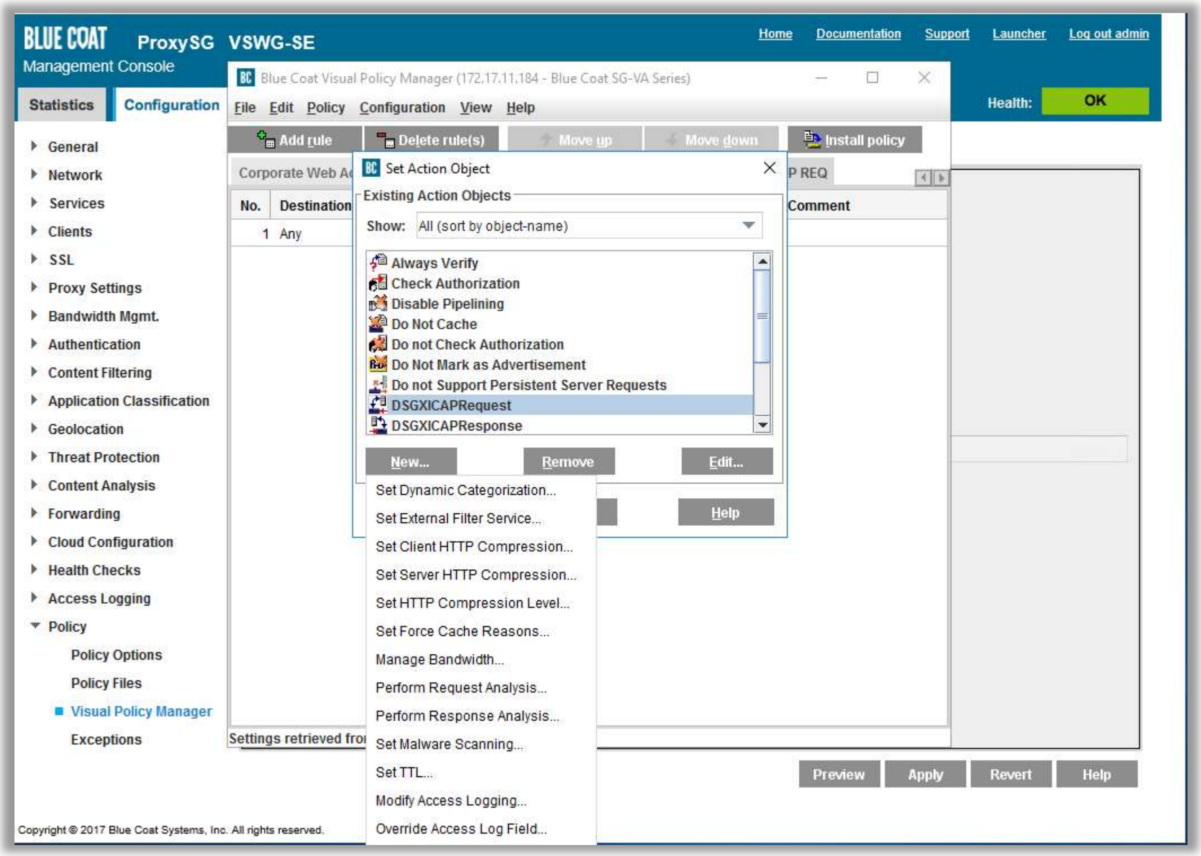
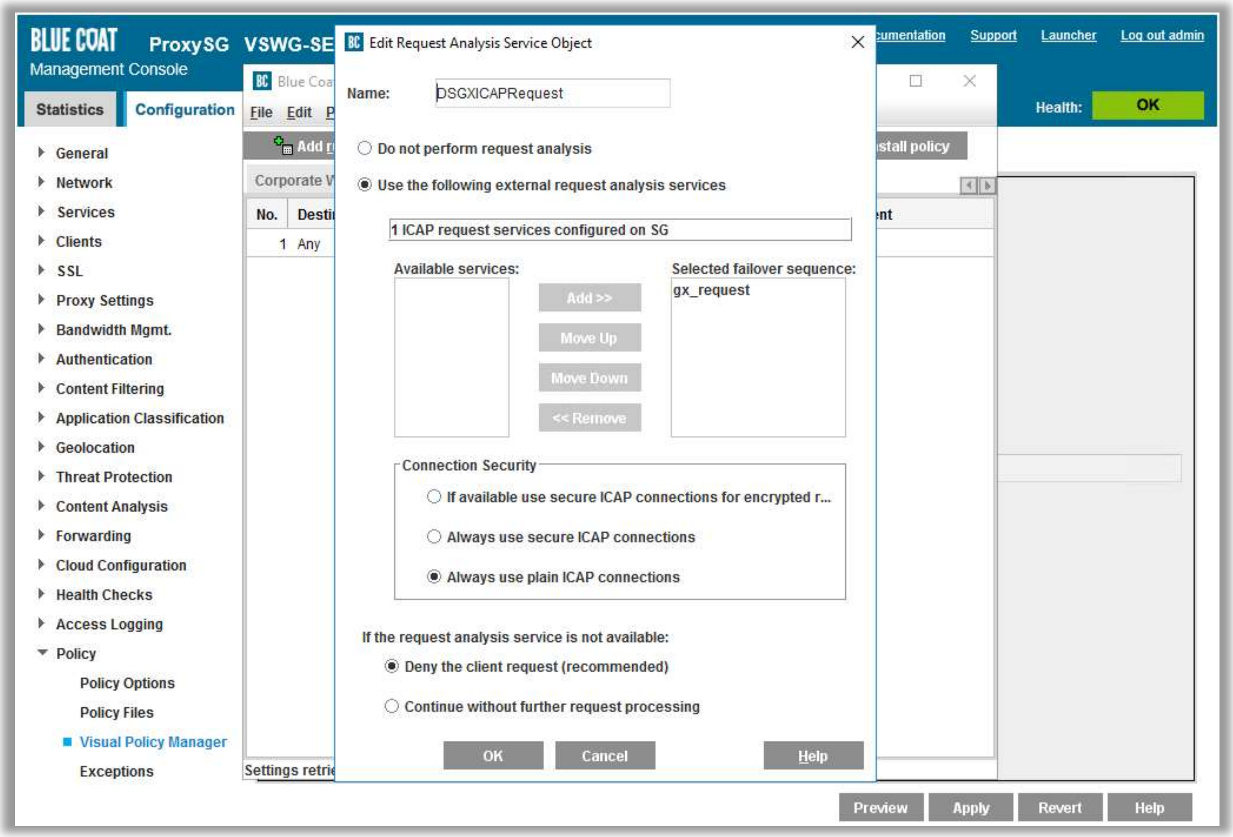


Figure 3-5: Set Action

From the drop-down for **Set Action** select **Perform Request Analysis**.



Edit Request Analysis Service Object

Name: DSGXICAPRequest

○ Do not perform request analysis

● Use the following external request analysis services

1 ICAP request services configured on SG

Available services:

Selected failover sequence: gx_request

Connection Security

○ If available use secure ICAP connections for encrypted r...

○ Always use secure ICAP connections

● Always use plain ICAP connections

If the request analysis service is not available:

● Deny the client request (recommended)

○ Continue without further request processing

Figure 3-6: Edit Request Analysis Service Object

Enter a relevant name for the new object (for example **DSGXICAPRequest**)

Under the **Available Services** select the object created in step 3.2 (e.g. **gx_request**) and move to **Selected failover sequence**.

Change **Connection Security** to **Always use plain ICAP connections**.

Leave all other settings as default.

Repeat the above steps to create a new **Web Content Layer** for the ICAP Response.

On completion of creating the Web Content Layer policies it is necessary to select the **Install Policy** button to apply the new configuration.

4 References

GX Configuration Guide