



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



Table of Contents

1	Intro	oduction	3
	1.1	Scope	3
	1.2	Background	3
	1.3	Audience	3
	1.4	Conventions	4
	1.5	Purpose	4
2	Pre-	requisites	5
3	Inte	gration Steps	6
	3.1	Initial configuration	6
	3.2	ICAP Request Configuration	7
	3.3	ICAP Response Configuration	8
	3.4	Configuring the Visual Policy Manager for Forward Proxy	9
4	Refe	erences1	3

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></variable>	A value you must supply, for example in a command line.
[<variable>]</variable>	An optional value you can supply, for example, in a command line.
😳 Imp	ortant information that emphasises or supplements points in the text, or that may
арр	ly only in special cases.
🔺 🔺 A ca	aution that alerts you that failure to take or avoid a specified action could result in
the	loss of data.
Tip Ati	p that suggests an alternative method for applying a technique or procedure, or
helj	os 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.

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.

A 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).

TP 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:

	Mainten	ance				Health:	OK
General Gener	ICAP	Services Ces: Service gx_request gx_response	ICAP Feedback	ICAP Patience Page			

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:

	Ealt ICAP Service gx_request		_		
	ICAP version:	1.0			
https://1/2.17.11.184:8082/5	Service URL:	icap:// <gx address<="" ip="" td=""><td>>/REQMOD</td><td>New tab</td><td>10 23 8</td></gx>	>/REQMOD	New tab	10 23 8
NUE AGAT	Service type:	○ Threat Protection ○	DLP Other		
BLUE CUAI ProxySG VSV	Maximum number of connections:	200			<u>nome</u> Doc
Management Console 172	Connection timeout (seconds):	70			
Statistics Configuration M	Defer scanning at threshold:	80 %		Health:	OK
General	Notify administrator when viru	is detected			
Blue Coat	Use vendor's "virus found" page	ge			
IWF	ICAP Service Ports				_
Local Database	This service supports plat	in ICAP connections			-
Third-Party Databases	Plain ICAP port: 1344				
YouTube	This service supports sec	cure ICAP connections			
Application Classification	Secure ICAP port: 11344	4			
Geolocation	SSL Device Profile: <non< td=""><td>i6></td><td>9</td><td></td><td></td></non<>	i6>	9		
Threat Protection	ICAD of a Optimum				
 Content Analysis 	Method supported:	O response modificatio	8		
ICAP Soprice Croups		request modification			
Forwarding	Preview size (bytes):	1024	enabled		
Cloud Configuration	Sand	Client address	Server address		
Health Checks	John.		Authenticated groups		
Access Logging	ICAP server fag	Authenticated User			
▼ Policy	Sense settings	Get settings from ICAP s	erver	Delete	
Policy Options					
Policy Files	Health Check Options				
Visual Policy Manager	Health check	Perform a health ch	eck on this service	bly Revert	Help
Exceptions 🗸					

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	22	~		>
🗧 🕣 🔝 https://172.17.11.184:	ICAP version:	1.0	-	re 🏈 New tab 🛛 🛱 🛱	63
	Service URL:	icap:// <gx address<="" ip="" td=""><td>>/RESPMOD</td><td></td><td></td></gx>	>/RESPMOD		
BLUE COAT ProxySG	Service type:	O Threat Protection	DLP Other	Home Doc	ume
Management Console	Maximum number of connections:	200			
Statistics Configuration	Connection timeout (seconds):	70		Health: OK	
•	Defer scanning at threshold:	80 %	10		
Clients	Notify administrator when virus	s detected			i.
Proxy Settings	Use vendor's "virus found" pag	ge			
Bandwidth Mgmt.	ICAP Service Ports	reason y f		_	
Authentication	 This service supports plai 	n ICAP connections			
▼ Content Filtering	Plain ICAP port: 1344				
General	This service supports sec	ure ICAP connections			
Blue Coat	Secure ICAP port: 11344				
IWF	SSL Device Profile: «Non	e>	v		
Local Database					
Third-Party Databases	ICAP v1.0 Options	response modification	(j		
You lube	metriod supported.	 response modification 	201		
Geolocation	Draviau size (butas)	O Tequest mounication	d apphied		
Threat Protection	Preview size (bytes):		r enableu		
 Content Analysis 	Send:				
ICAP	ICAD server tea	Autnenticated user	Authenticated groups	Delete	
Service Groups	Sense settings	Set settings from ICAP s	erver		
Forwarding					ł
Cloud Configuration	Health Check Options	K		Apply Revert Help	
Health Checks Copyright © 2017 Blue Cost Systems Inc.	Health check	Perform a health ch	eck on this service		
supplier of the out of stells, in			_		
		OK Cance	21		

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.



Blue Coat SG-VA S	Series)	- D Install policy AP REQ Comment	X () () () () () () () () () () () () ()	Health:	ок
Move up ICAP RESP Web Track Request None	✔ Move down eb Content Layer - ICA k	Install polic AP REQ Comment		Health:	OK
Move up ICAP RESP Veb Track Request None	✓ Move <u>down</u> eb Content Layer - ICA k	Install policy	y () () () () () () () () () () () () ()		
ICAP RESP Web Track Request None	eb Content Layer - ICA k	AP REQ Comment	4.12		
Track Request None	k	Comment			
Request None	9				
		.184	.184	.184	.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



BLUE COAT ProxySG	VSWG-SE		Home	Documentation	Support	Launcher	Log out admin
Management Console	BC Blue Coat Visual F	olicy Manager (172.17.11.184 - Blue Coat SG-VA Series)		- 0	×		
Statistics Configuration	<u>File Edit Policy (</u>	Configuration View Help				Health:	ок
General	🗣 🖬 Add rule	🖬 Delete rule(s) 🛛 Move 💷 Move down		😫 Install policy	7		
Network	Corporate Web Ad	80 Set Action Object	Хр	REQ	4 4		
Services	No. Destination	Existing Action Objects	co	omment			
Clients	1 Any	Show: All (sort by object-name)					
▶ SSL		Always Verify					
Proxy Settings		Check Authorization					
Bandwidth Mgmt.		Do Not Cache					
Authentication		Do not Check Authorization	- 7.0				
Content Filtering	-	Do Not Mark as Advertisement					
Application Classification		DSGXICAPRequest					
Geolocation		DSGXICAPResponse	-		-		
Threat Protection		<u>N</u> ew <u>R</u> emove <u>E</u> dit					
Content Analysis	L	Set Dynamic Categorization					
Forwarding		Set External Filter Service					
Cloud Configuration		Set Client HTTP Compression					
Health Checks		Set Server HTTP Compression					
Access Logging		Set HTTP Compression Level					
 Policy 		Set Force Cache Reasons					
Policy Options		Manage Bandwidth					
Policy Files		Perform Request Analysis					
Visual Policy Manager		Perform Response Analysis					
Exceptions	Settings retrieved fro	Set Malware Scanning	77.	17.85			0
		Set TTL		Preview	Apply	Revert	Help
		Modify Access Logging					
opyright © 2017 Blue Coat Systems, Inc	. All rights reserved.	Override Access Log Field					

Figure 3-5: Set Action

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



BLUE COAT ProxySG Management Console	VSWG-SE	Edit Request Analysis Service Object	< ^{cumentatio}	on <u>Support</u>	<u>Launcher</u>	Log out admin
Statistics Configuration	<u>File Edit P</u>	Name: DSGXICAPRequest		~	Health:	ок
General	Cornorate V	O Do not perform request analysis	istall poli	icy		
P Network	Corporate v	Use the following external request analysis services		4 6		
Services	No. Desti	1 ICAP request services configured on SG	ent			
Clients	1 Any	Available services: Selected failover sequence:				
Proxy SettingsBandwidth Mgmt.		Add >> gx_request				
 Authentication Content Filtering 		Move Down				
 Application Classification Geolocation 		< <remove< td=""><td></td><td></td><td></td><td></td></remove<>				
 Threat Protection Content Analysis 		Connection Security O If available use secure ICAP connections for encrypted r		_		
Forwarding Cloud Configuration		○ Always use secure ICAP connections				
 Health Checks 		Always use plain ICAP connections				
 Access Logging Policy Policy Options 		If the request analysis service is not available: Deny the client request (recommended)				
Policy Files		Continue without further request processing				
Exceptions	Settings retrie	OK Cancel <u>H</u> elp				
			Preview	Apply	Revert	Help

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