



# GX integration with F5 Application note



#### Table of Contents

1	Intro	pduction	3
	1.1	Scope	3
	1.2	Background	3
	1.3	Audience	3
	1.4	Conventions	4
	15	Purpose	4
2	Dro-	requisites	5
2	Inte	aration Stone	5
د ۸	Dofe	gration steps	-
4	Rele	rences	./



## **1** Introduction

#### 1.1 Scope

This document outlines how to integrate an F5 BIG-IP Application Delivery Controller 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 F5 BIG-IP controller to send data to, and receive data from, GX.

#### 1.2 Background

A typical deployment is as shown below.



Figure 1-1: GX and F5 deployment

#### **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.			
Important information that emphasises or supplements points in the text, or that may apply only in special cases.				
A ca loss	aution that alerts you that failure to take or avoid a specified action could result in the s of data.			
<sup>⊺ip</sup> A ti you	p that suggests an alternative method for applying a technique or procedure, or helps 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 F5 with a GX CTR appliance.



## 2 Pre-requisites

Before configuring F5 to work with GX there are a number of pre-requisites that should be set.

Ensure F5 BIG-IP is installed and configured to use either:

- Local Traffic Manager (LTM) functionality
- Application Security Manager (ASM) functionality with Local Traffic

Ensure the F5 Big-IP controller has been configured with, as a minimum, 3 IP addresses that represent:

- a Management interface
- an Internal interface
- an External interface
  - Additional interfaces may be present if more than one network is to be represented by the F5 BIG-IP.

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.

Ensure the GX Data network is configured to be in the same IP range as that of the Internal interface on the F5 BIG-IP.



## **3** Integration Steps

The following steps detail how to configure the F5 BIG-IP controller to receive data and send data to the GX via ICAP.

A For the purpose of the following configuration steps, it is assumed that the F5 is already configured correctly to perform Local Traffic Management. If not, please refer to the appropriate F5 configuration documentation to complete these steps.

It is necessary to first create a node(s) for each GX deployed. To do this, connect to the F5 BIG-IP Web Management Interface.

Locate Local Traffic -> Nodes and within Node settings, select the create button:

When creating a GX Node, fill in the Name as **GX-Node1** and the Description field appropriately. In the Address field type the IP address being used by the GX to receive data. Leave the Health Monitors, Ratio, Connection Limit and Connection Rate Limit settings as default.

Seneral Properties			
Name	GX-Node1		
Description	Node for the GX data connection		
Address	Address      FQDN		
Address	10.20.16.10		
onfiguration			
onfiguration Health Monitors	Node Default		
onfiguration Health Monitors Ratio	Node Default		
onfiguration Health Monitors Ratio Connection Limit	Node Default       1       0		

Figure 3-1: Example GX node configuration

Navigate to **Local Traffic -> Monitors** and create a new Health Monitor with the Name **GX-HM** and an appropriate Description and a Type of TCP. Leave all other settings as default.



-	_				
Local Traffic » Monitors » GX-HM					
Properties Instance			Test		
			<u>,</u>		
General Properties					
Name     O       Partition / Path     O       Description     []       Type     T		GX-HM			
		Common			
		GX health monitor			
		тср			
Parent Monitor		tcp			
Configuration: Basic	•				
Interval		5	seconds		
Timeout		16	seconds		
Send String	Sond String				
Condicating					
	Receive String				
Receive String					
Receive carry					
Receive Dischle String					
The block of the b					
Reverse		○ Yes ● N			
Transparent		○ Yes ● N			
Alias Address		* All Addre	15585		
Alias Service Port		* All Ports			
Adaptive	Adaptive		I		
Update Delete					

Figure 3-2: Example GX health monitor configuration

A pool will need to be created for the GX node(s). Navigate to **Local Traffic -> Pools** and click on the **create** button.

Create the GX Pool with the following settings: give the pool a name of **GX-Pool** and an appropriate **Description** and set the **Health Monitor** to the previously created health monitor. Leave the load balancing method as Round Robin and Ensure Priority Group Activation is disabled. Within the New Members area check the Node List option and select the GX node previously created and use port 1344. Finally click the Add button to add the node member to the pool.



Name	GX-Pool				
Description	Pool that contains all GX Nodes				
Health Monitors	Active Available /Common GX-HM				
oad Balancing Method	Round Robin				
Priority Group Activation	Disabled V				
New Members	New Node         New FQDN Node         Node List           Address:         GX-Node1 (10.20.16.10)         ▼           Service Port:         1344         Select         ▼				

Figure 3-3: Example Pool

After the GX-Pool has been created the status should be green showing the pool is available.



Figure 3-4: Healthy pool containing GX node

Navigate to Local Traffic -> Profiles -> Services -> ICAP and create 2 new ICAP services for the Server and Client connections.

Create a new ICAP Service called **GX-Request-ICAP** with the following settings, checking only the URI and Preview Length boxes:

- Parent Profile icap
  - URI icap://\${SERVER\_IP}:\${SERVER\_PORT}/reqmod

0

Preview Length

Local Traffic » Profiles : Services : ICAP » New ICAP Profile					
Seneral Properties					
Name	GX-Request-ICAP				
Parent Profile	icap 🔻				
Settings					
URI	icap://\${SERVER_IP}:\${SERVER_P0				
Preview Length	0				
Header From					
Host					
Referer					
User Agent					
Cancel Repeat Finished					

Figure 3-5: Example ICAP GX request service



Create a second new ICAP Service called **GX-Response-ICAP** with the following settings, checking only the URI and Preview Length boxes:

- Parent Profile icap
  - icap://\${SERVER\_IP}:\${SERVER\_PORT}/respmod
- Preview Length

URI

Constal Proportion				
GX-Response-ICA				
icap 🔻				
icap://\${SERVER_IP}:\${SERVER_PO				
0				

Figure 3-6: Example ICAP GX response service

Internal

Enabled

0.0.0/32

Advanced

Create 2 Virtual Servers called **GX-Request-VS** and **GX-Response-VS**.

Configure the GX-Request-VS with these settings:

0

- Description Appropriate description
- Туре
- Source address
- State
- Configuration
- Protocol TCP
- Protocol Profile (Client) tcp
- Protocol Profile (Server)
   Use Client Profile
- ICAP Profile GX-Request-ICAP
- Source Address Transaction Auto Map
- Default Pool GX-Pool
- VLAN and Tunnel Traffic All VLANs and Tunnels

VLAN and Tunnel Traffic can only be set after the Virtual Server has been created.



Local Traffic » Virtual Servers : Virtual Server List » New Virtual Server						
General Properties						
Name	GX-Request-VS					
Description	GX virtual server for the ICAP Requests					
Туре	Internal					
Source Address	0.0.0/32					
Notify Status to Virtual Address	Ø					
State	Enabled V					
Configuration: Advanced V						
Protocol	TCP V					
Protocol Profile (Client)	tcp v					
Protocol Profile (Server)	(Use Client Profile)					
HTTP Proxy Connect Profile	None					
	Selected Available					
SSL Profile (Server)	apm-default-serverssi					
	pcoip-default-serverssl					
	serverssi					
QoE Profile	None T					
ICAP Profile	GX-Request-ICAP T					
Statistics Profile	None V					
Source Address Translation	Auto Map 🔻					
Acceleration						
Rate Class	None <b>T</b>					
OneConnect Profile	None					
HTTP/2 Profile	None T					
Resources						
	Enabled Available					
	/Common     sys_APM_ExchangeSupport_OA_BasicAuth					
iRules	sys_APM_ExchangeSupport_OA_NtimAuth					
	Up Down					
Default Pool +	GX-Pool V					
Default Persistence Profile	None					
Fallback Persistence Profile	None					
Cancel Repeat Finished						

Figure 3-7: Example virtual service for GX Request

Configure the GX-Response-ICAP with these settings:

Description Appropriate description • Internal Туре • 0.0.0/32 • Source address State Enabled • • Configuration Advanced ТСР Protocol • Protocol Profile (Client) tcp • Protocol Profile (Server) **Use Client Profile** ICAP Profile **GX-Response ICAP** • Source Address Transaction • Auto Map Default Pool GX-Pool • VLAN and Tunnel Traffic All VLANs and Tunnels

**VLAN** and Tunnel Traffic can only be set after the Virtual Server has been created.



Local Traffic » Virtual Servers :	Virtual Server List » New Virtual Server
General Properties	
Name	GX-Response-VS
Description	GX virtual server for the ICAP Response
Туре	Internal
Source Address	0.0.0.0/32
Notify Status to Virtual Address	8
State	Enabled <b>T</b>
Configuration: Advanced V	
Protocol	TCP V
Protocol Profile (Client)	tcp 🔻
Protocol Profile (Server)	(Use Client Profile)
HTTP Proxy Connect Profile	None
SSL Profile (Server)	Selected Available Common apm-default-serverssl pcoip-default-serverssl pcoip-default-serverssl
QoE Profile	None V
ICAP Profile	GX-Response-ICAP T
Statistics Profile	None <b>T</b>
Source Address Translation	Auto Map 🔻
Acceleration	
Rate Class	None V
OneConnect Profile	None
HTTP/2 Profile	None T
Resources	
iRules	Enabled Available Common _sys_APM_ExchangeSupport_OA_BasicAuth _sys_APM_ExchangeSupport_OA_NtimAuth _sys_APM_ExchangeSupport_helper sys_APM_ExchangeSupport_helper
	Up Down
Default Pool +	GX-Pool V
Default Persistence Profile	None
	New

Figure 3-8: Example virtual service for GX Response

Solution of these Virtual Servers will have a green status, they should be grey.

Virtual Server List     Virtual Address List     Statistics     +						
Search					Create	
Status + Name	Description     Ap	lication / Destination	Service Port	© Type	Resources	Partition / Pa
GX-Request-VS	GX virtual server for the ICAP R	Any IPv4	0 (Any)	Internal	Edit	Common
GX-Response-VS	GX virtual server for the ICAP R	Any IPv4	0 (Any)	Internal	Edt	Common
					-	

Figure 3-9: Example virtual service health monitor status

Navigate to Local Traffic -> Profiles -> Services -> Request Adapt and create a new Request Adapt service.

Configure the Request Adapt with the following settings:



- Name GX-Request-Adapt
- Parent Profile requestadapt
- Check the Custom settings box so that all settings are enabled
- Internal Virtual Name GX-Request-VS
- Leave all other settings as default.

Local Traffic » Profiles : Services : Request Adapt » New Request Adapt Profile					
General Properties					
Name	GX-Request-Adapt				
Parent Profile	requestadapt <b>v</b>				
Settings					
Enabled	C Enabled				
Internal Virtual Name	/Common/GX-Request-VS				
Preview Size	1024				
Timeout (ms)	0				
Service Down Action	Ignore V				
Allow HTTP 1.0					
Cancel ] Repeat ] Finished					



Navigate to Local Traffic -> Profiles -> Services: Response Adapt and create a new Response Adapt service.

Configure the Response Adapt with the following settings:

- Name GX-Response-Adapt
- Parent Profile responseadapt
- Check the Custom settings box so that all settings are enabled
- Internal Virtual Name GX-Response-VS
- Leave all other settings as default.

Local Traffic » Profiles : Services : Response Adapt » New Response Adapt Profile					
General Properties					
Name	GX-Response-Ada				
Parent Profile	responseadapt ▼				
Settings					
Enabled	✓ Enabled				
Internal Virtual Name	/Common/GX-Response-VS ▼				
Preview Size	1024				
Timeout (ms)	0				
Service Down Action	Ignore ▼				
Allow HTTP 1.0					
Cancel Repeat Finished					

Figure 3-11: Example GX Response adapt profile



Navigate to Local Traffic -> Profiles -> Services: HTTP and create a HTTP Service.

Configure the HTTP Service with these setting:

- Name HTTP-WS
- Partition/Path Common
- Proxy Mode Reverse
- Parent Profile HTTP
- Check the Custom check box.
- Request Chunking Selective
- Response Chunking Unchunk
- Leave all other settings as default.

Local Hame // Fromes. Servi	
Name	
name	HTTP-WS
Proxy Mode	Reverse
Parent Profile	nttp •
ettings	
Basic Auth Realm	
Fallback Host	
Fallback on Error Codes	
Request Header Erase	
Request Header Insert	
Response Headers Allowed	
Request Chunking	Selective V
Response Chunking	Unchunk T
OneConnect Transformations	
Redirect Rewrite	None T
Encrypt Cookies	
Cookie Encryption Passphrase	
Confirm Cookie Encryption Passphrase	
Insert X-Forwarded-For	Disabled V
LWS Maximum Columns	80
LWS Separator	
Maximum Requests	0
Send Proxy Via Header In Request	Preserve V
Send Proxy Via Header In Response	Preserve T
Accept XFF	
XFF Alternative Names	
Server Agent Name	RialD

Figure 3-12: Example HTTP profile

Modify the virtual server that GX will be protecting. In this example it is called **Web-Server-VS**. Modify the **Web-Server-VS** with these settings:



• Туре

•

•

•

•

•

Standard 0.0.0.0/0

Advanced

- Source addressDestination Address
- IP address on the same range as the Client connecting to the Web Server
- HTTP/80 or HTTPS/443

тср

tcp

- Configuration
- Protocol

Server Port

**HTTP Profile** 

• Protocol Profile (Client)

Protocol Profile (Server)

- User Client Profile
- Use the HTTP WS Profile previously created
- Request Adapt Profile GX-Request-Adapt
- Response Adapt Profile
   GX-Response-Adapt
- VLAN and Tunnel Traffic All VLANs and Tunnels
- Source Address Transaction Auto Map
- Leave all other settings as default



Local Itaffic - Virtual Server	s : Verhad Server List a Verb Server VS exates Children (P
General Properties	
Name	Web-Server-VS
Partition / Path	Common
Description	The virtual server used to connect to the webserver
Type	Standard
Source Address	0.0.0.00
Destination Address/Mask	10 20 17 20
Service Part	80 HTTP •
Notify Status to Virtual Address	*
Availability	Available (Enabled) - The virtual server is available
Byncookie Status	ot
State	Enabled *
Configuration: Advanced •	
Protocol	TCP •
Protocol Profile (Client)	(8cp +
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile	HTTP-WS •
HTTP Praxy Connect Profile	None
FTP Profile	lune *
KJSP Profile	Autom 1
SOCKS Profile	Name V
Stream Protee	Note
MQTT	Note •
	Selected Available
	- Common -
SSL Profile (Client)	clientssl-insecure-compatible
	Cientssi-secure crypto-server-defaut-cientssi *
	Selected Available
	a Common a
SSL Profile (Server)	crypto-client-default-serverssi
	serverssi *
	Enabled Available
	- Common -
Authentication Profiles	ssi_cridp
	* SSLOCED
SMTPS Profile	None +
Clerit LOAP Profile	None •
Present ID-16 Press	New York Control of Co
Server LUAP Profile	hone •
SMTP Profile	None *
WebSocket Profile	None
SplitSession Client Profile	None •
SplitSession Server Profile	None •
DNS Profile	None *
Diameter Profile	None +
QoE Profile	None •
FIX Profile	None •
Request Adapt Profile	GX-Request-Adapt
Parnanza Adapt Profile	OV Parameter Adapt
Nesponde Adapt Protes	And a second sec
211, h1006	Testin T
Statistics Profile	None •
VLAN and Tunnel Traffic	All VLANs and Tunnels *
Source Address Translation	Auto Map •
Bandwidth Controller	None *

Figure 3-13: Example Web Server virtual server

After the Web-Server-VS has been modified the status of the Virtual Server should be green.



Virtual Server List Virtual Address List Statistics -				
		Search		
	- Status	▲ Name		
	0	GX-Request-VS		
	0	GX-Response-VS		

Figure 3-14: Example Virtual Service Status list

Now you have configured the F5 to communicate to the GX you will now be able to send traffic to the web server and it will be processed by the GX. To confirm data is being processed view the diagnostic logs within the GX to see log messages around traffic flow, or if the GX has been configured to store the data view the content being stored from the GX Content Dashboard.



# **4** References

GX Configuration Guide