GX integration with F5
Application note

Table of Contents

1 Introduction 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 Integration Steps 6
4 References 17

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.

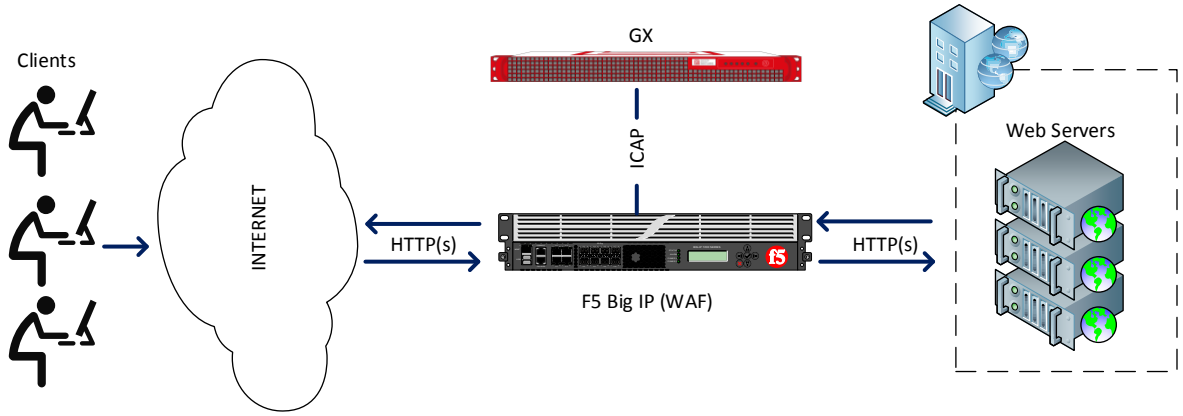

Figure 1-1: GX and F5 deployment

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>	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 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

> Tip 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.

> ⚠ 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.

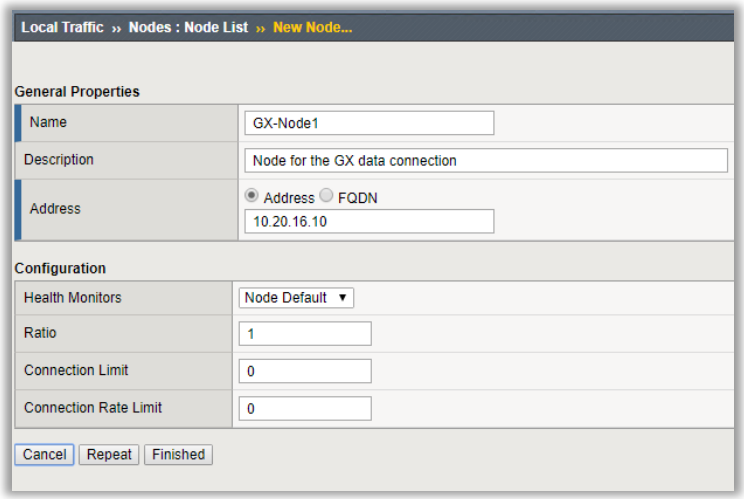

Figure 3-1: Example GX node configuration

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.

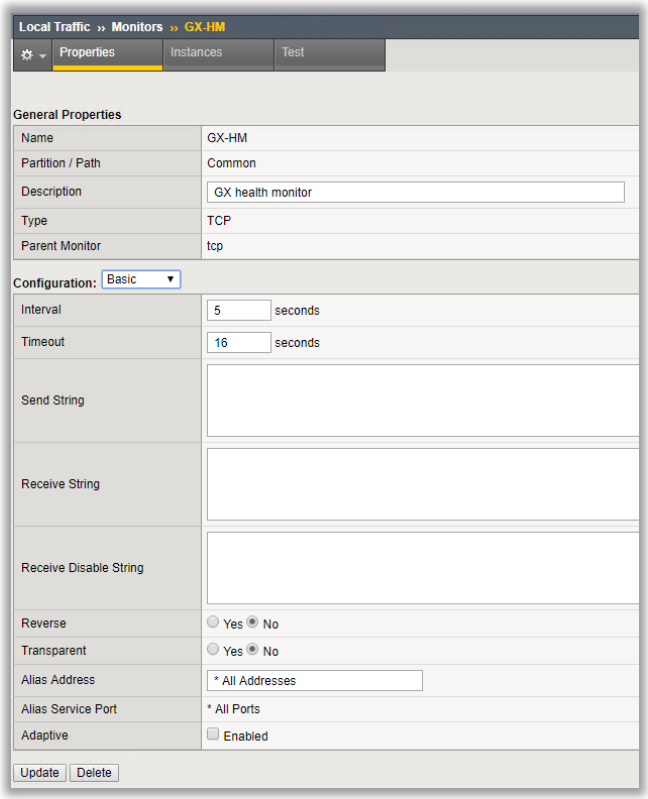

Figure 3-2: Example GX health monitor configuration

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.

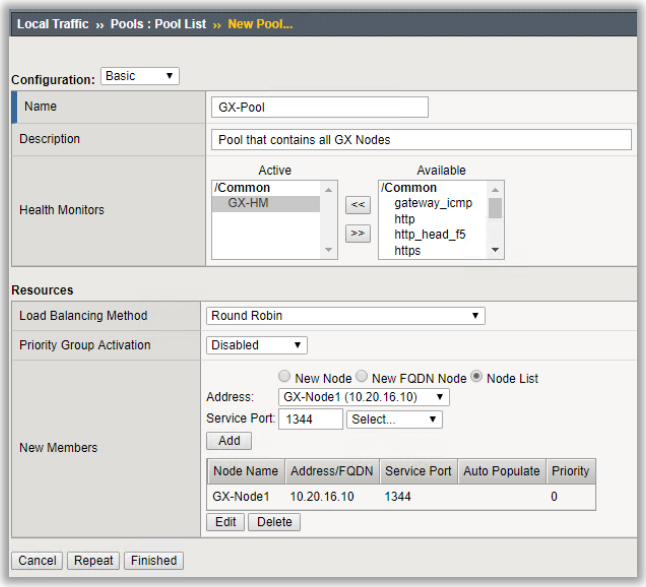

Figure 3-3: Example Pool

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

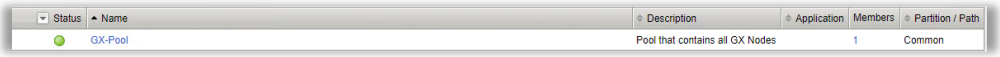

Figure 3-4: Healthy pool containing GX node

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
- Preview Length 0

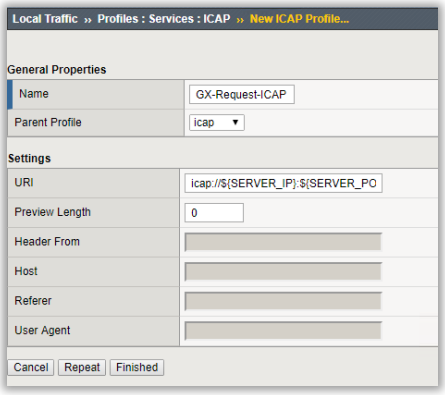

Figure 3-5: Example ICAP GX request service

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
- URI icap://${SERVER_IP}:${SERVER_PORT}/respmod
- Preview Length 0

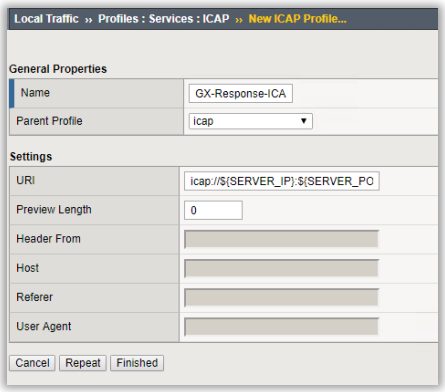

Figure 3-6: Example ICAP GX response service

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

Configure the GX-Request-VS with these settings:

- Description Appropriate description
- Type Internal
- Source address 0.0.0.0/32
- State Enabled
- Configuration Advanced
- 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.

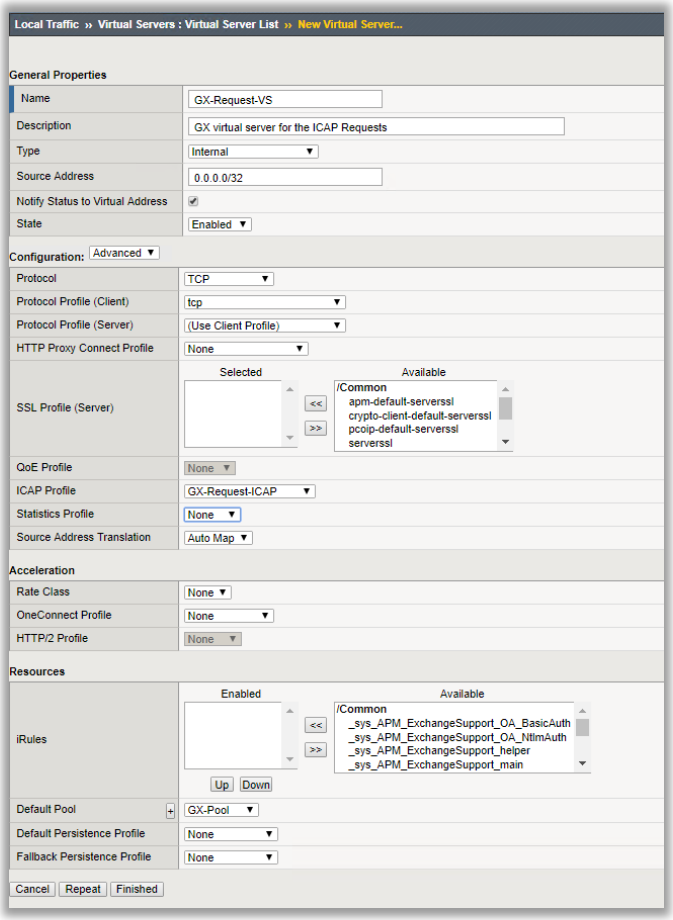

Figure 3-7: Example virtual service for GX Request

Configure the GX-Response-ICAP with these settings:

- Description — Appropriate description
- Type — Internal
- Source address — 0.0.0.0/32
- State — Enabled
- Configuration — Advanced
- Protocol — TCP
- 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.

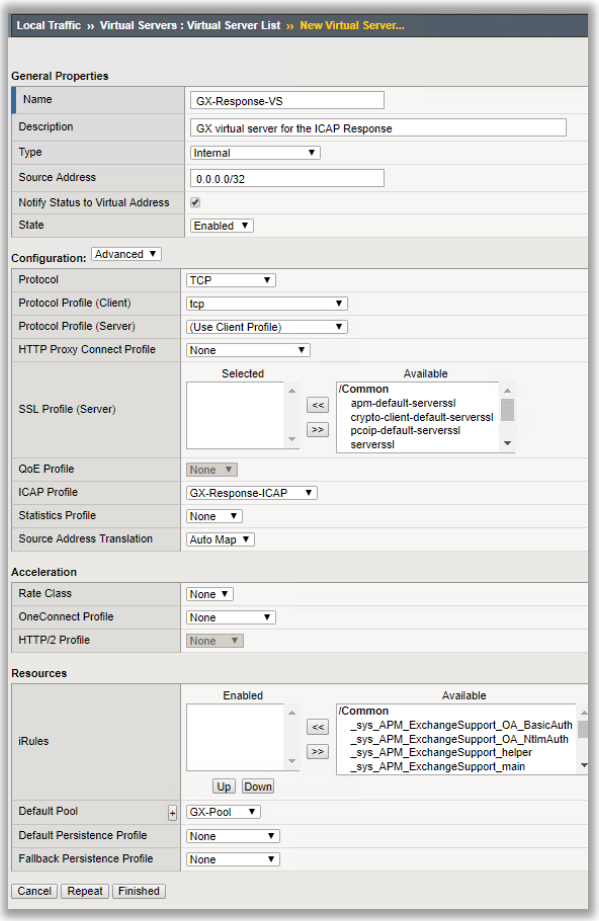

Figure 3-8: Example virtual service for GX Response

- Neither of these Virtual Servers will have a green status, they should be grey.

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.

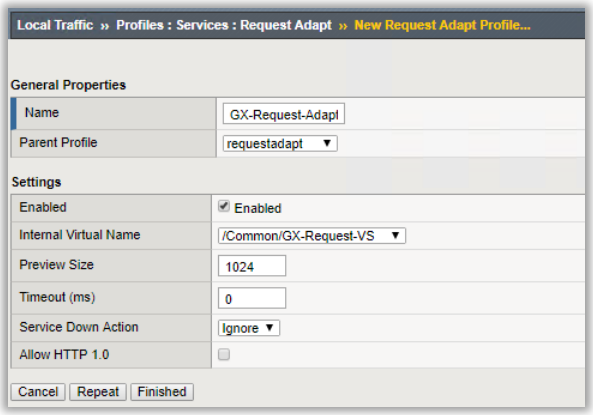

Figure 3-10: Example GX Request adapt profile

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.

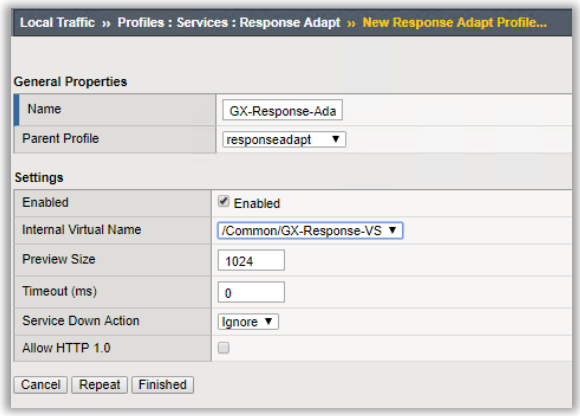

Figure 3-11: Example GX Response adapt profile

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.

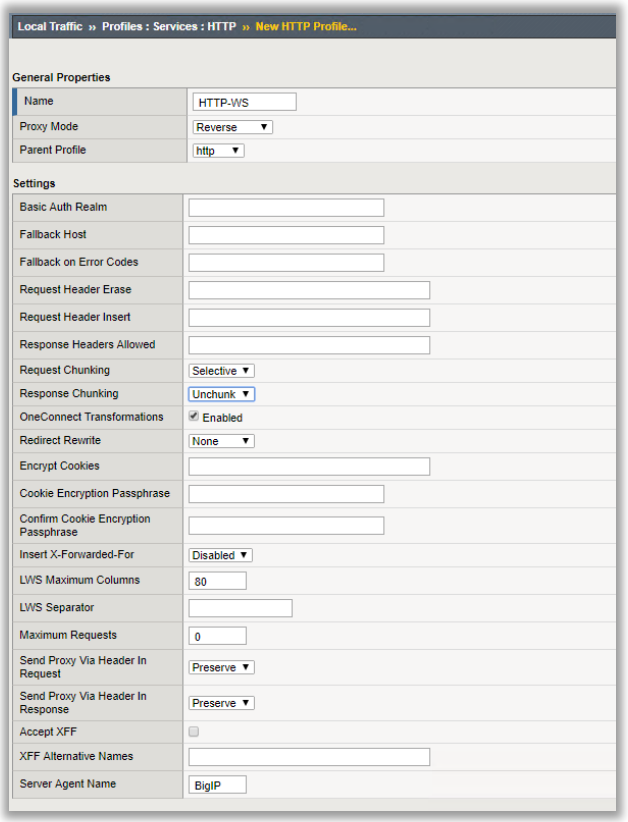

Figure 3-12: Example HTTP profile

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:

- Type — Standard
- Source address — 0.0.0.0/0
- Destination Address — IP address on the same range as the Client connecting to the Web Server
- Server Port — HTTP/80 or HTTPS/443
- Configuration — Advanced
- Protocol — TCP
- Protocol Profile (Client) — tcp
- Protocol Profile (Server) — User Client Profile
- HTTP 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

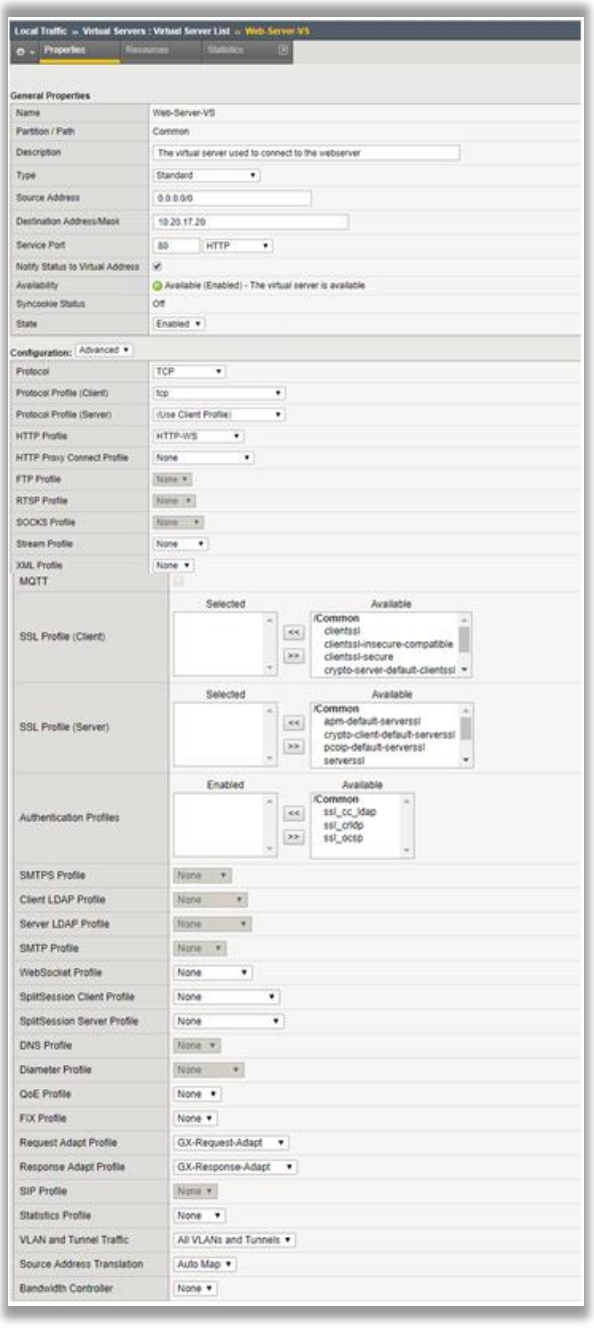

Figure 3-13: Example Web Server virtual server

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

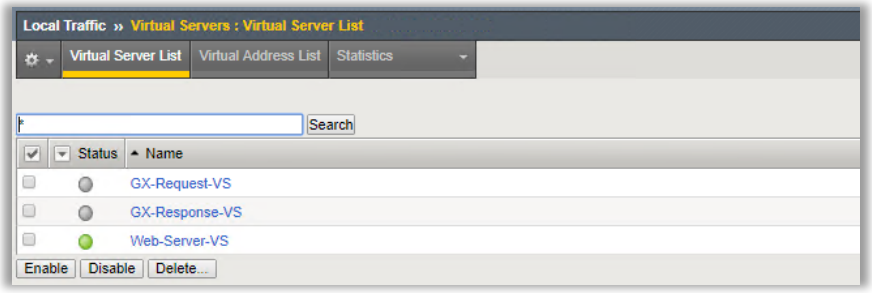

Figure 3-14: Example Virtual Service Status list

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