Deploying BIG-IP GTM with APM for Global Remote Access

Welcome to the F5® deployment guide for BIG-IP® Global Traffic Manager® (GTM) and BIG-IP Access Policy Manager (APM). This guide shows administrators how to configure the BIG-IP GTM and APM together to provide high availability and secure remote access to corporate resources from anywhere in the world.

In this solution, the BIG-IP GTM intelligently directs traffic to the closest available branch office to the user. The BIG-IP APM uses one of several options to authenticate the user, and then creates a secure session between the user and the remote office.

For more information on the F5 BIG-IP system and the modules described in this guide, see *http://www.f5.com/products/big-ip/*.

Products and versions

Product	Version
BIG-IP GTM, APM	11.2, 11.3, 11.4, 11.5, 11.6

Important: *Make sure you are using the most recent version of this deployment guide, available at http://www.f5.com/pdf/deployment-guides/f5-apm-gtm-dg.pdf.*

Contents

Prerequisites and configuration notes

The following are general prerequisites and configuration notes for this guide:

- A minimum of two BIG-IP APM devices and a BIG-IP GTM
- This guide does not cover the deployment or guidance for any specific application, as such we strongly recommend deploying your application prior to proceeding.
- All routes between the GTM and the data centers should be in place before performing the configuration in this guide. See the BIG-IP documentation for more information on configuring routes.
- If one ore more data centers contain multiple APM devices performing the same function, please refer to Appendix A for additional configuration.

Configuration examples

This guide contains two ways of configuring this deployment, a high availability configuration, and a topology-based configuration.

High availability configuration

The high availability configuration is for deployments using multiple BIG-IP APM devices in a single data center. This scenario allows for handling a larger number of concurrent sessions by distributing users by observed connection levels on multiple APM instances by redirecting the connection once the it arrives. In our example, we are configuring two APM devices per Data Center and allowing the GTM health monitors to track the change to a different APM system at the Data Center.

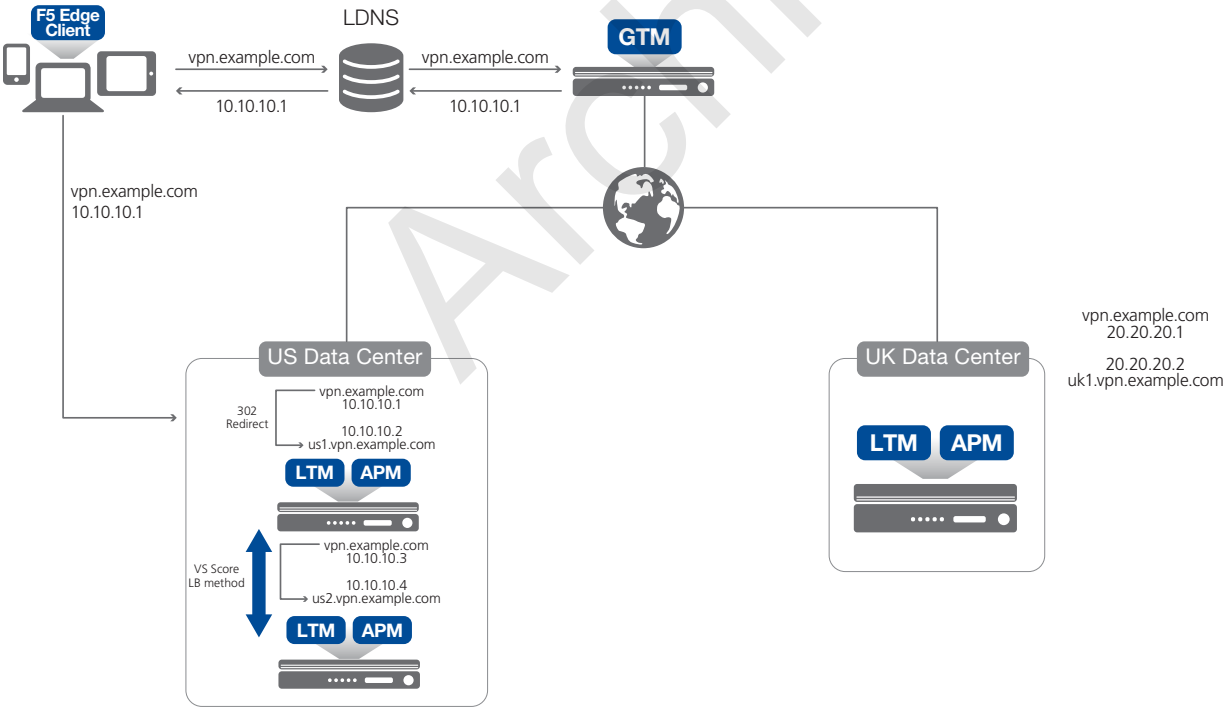

Figure 1: *Logical configuration example for high availability*

Topology-based configuration

With topology-based configuration, the BIG-IP GTM module is used to provide intelligent distribution based on geolocation and application load, providing the highest level of transparency and performance to users. Once connected to the appropriate APM device based on geolocation the BIG-IP APM is able to provide Secure Authentication and SSL VPN access to corporate resources.

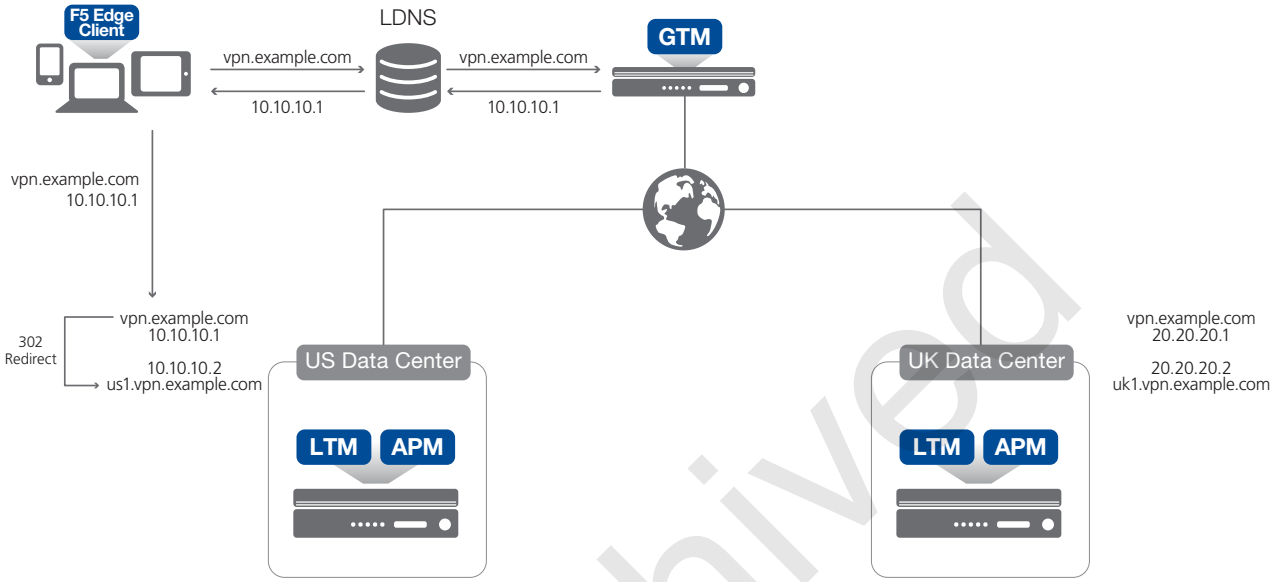

Figure 1: *Logical configuration example for topology-based deployments*

Preparation Worksheet

Before beginning the configuration, it is helpful to gather some information, such as IP addresses and certificate/key information. This worksheets contains the information that is helpful to have in advance. You might find it useful to print the table and then enter the information.

This table shows space to enter your information on top of each cell, and our example on the bottom.

Network	Primary Data Center	Secondary Data Center	Notes
Public WAN			
Network			All public access comes through this network
	60.168.111.0	70.168.111.0	
VLAN + (tag)			
	vlan-public-WAN1 (1192)	vlan-public-WAN2 (1072)	
GTM DNS Listener			
	60.168.111.250		
Application public virtual server			In our example, APM has two virtual servers that provide VPN access, which are on the DMZ / Public WAN
	60.168.111.100	70.168.111.100	
Private WAN			
Network			This network is used for Interconnectivity between APM and GTM. In our example, the private WAN is separated from the public WAN. However this is not required.
	192.168.111.0		
VLAN + (tag)			
	vlan-private-WAN1 (3192)	vlan-private-WAN2 (3072)	
BIG IP GTM Self IP			
	192.168.111.200		
BIG IP APM Self IP			
	192.168.111.200	172.168.111.200	
Private LAN			
Network			This Network is where your clients will be once they access the SSL VPN
	10.10.2.0	10.20.2.0	
BIG IP APM Application VIP			These are the Internal Application virtual servers clients access once connected to the SSL VPN. This is only required in our example use case.
	10.10.2.100	10.20.2.100	
VLAN + (tag)			
	vlan-private-LAN1 (1010)	vlan-private-LAN2 (1020)	
BIG IP APM Application VIP			
	10.10.2.200	10.20.2.200	
Private LAN - Server Layer			
Network			This network contains the application in our example.
	172.10.2.0	172.80.2.0	
VLAN + (tag)			
	vlan-privateApp-LAN1 (7010)	vlan-privateApp-LAN2 (7020)	
BIG-IP APM Self IP			These self IP will be used for access by the application servers.
	172.10.2.200	172.80.2.200	

Configuring the BIG-IP APM

In this section, we configure the BIG-IP Access Policy Manager (APM) using the Network Access Setup Wizard on the BIG-IP system.

SSL Configuration

You must import and use SSL certificates that match all names in use. If you choose to use one certificate per site, (e.g., *us1.vpn.example.com* and *uk1.vpn.example.com*), you must ensure that both generated certificates contain the Subject Alternative Name matching the main site name – in this case, *vpn.example.com*. It is acceptable to generate one certificate with all names in the Subject Alternative Name field if this is acceptable under your organization's security guidelines.

Wildcard certificates can also be used provided the wildcard matches ALL possible names. Please note that wildcard certificates only match the first subdomain from the wildcard: **.vpn.example.com* will match *uk1.vpn.example.com* or *us1.vpn.example.com*, but will **not** match *vpn.example.com*.

You will need to import the certificates before moving forward with the BIG-IP APM wizard as these objects will be requested during the configuration. To import SSL certificates, on the Main tab, click **System > File Management > SSL Certificate List > Import**. For specific information on how to import SSL certificates, see the online help or product manuals.

Configuring BIG-IP APM using the Network Access Setup Wizard

This table contains guidance on using the Network Access Setup Wizard for Remote Access to configure the BIG-IP APM.

To start the wizard, from the Main tab of the Configuration utility, click **Wizards**, and then click **Device Wizards**. In the Wizard section, click the **Network Access Setup Wizard for Remote Access** option button.

Wizard section	Non-default settings/Notes	
Basic Properties	***Policy Name***	Type a unique name. We use **apm-access**.
	Default Language	Select a language. We leave the default, **en**.
	Full Webtop	Check this box.
	Client Side Checks	Leave this box checked.
Authentication	***Domain Name***	Click the appropriate button. In our example, we the click RADIUS option button.
AAA Server	*The options in this section depend on the authentication method you choose. Configure the AAA Server options as appropriate for your environment and authentication method. Use the Help tab for assistance.*	
Lease Pool	***Type***	Click the option button for a single IP address or an address range. We click **IP Address Range**.
	Address(es)	Type an IP address. If you selected a range, type both the start and end IP addresses. We recommend using enough addresses for the highest number of concurrent network access connections you anticipate. You must ensure the network the lease pool members reside in provide access to the application.
Network Access	***Compression***	Select **GZIP Compression** (strongly recommended)
	Client Settings	Click the button for Forcing all traffic through the tunnel or split tunneling. If you chose split tunneling, configure the split tunneling options as applicable for your configuration. We click **Force all traffic through tunnel**.
	DTLS	Check this box to **enable DTLS**. Leave the default port of **4443** unless you have changed the DTLS port.
DNS Hosts	***Primary Name Server***	Type the IP address of the Active Directory Server in the network; all other settings are optional.
Virtual Server	***Virtual Server IP address***	Type the IP address to use for this virtual server. This address must be in the Public WAN network .
	Redirect Server	Leave this box checked. This redirects users who attempt to connect to the virtual server address using http:// to the correct https:// IP address.

Repeat this configuration on each BIG-IP APM that is a part of this configuration.

The wizard creates three virtual servers, one on port 443 that contains the Access Policy, one on port 80 that redirects users to the port 443 virtual server, and one on port 4443 for DTLS.

Configuring the BIG-IP system

In this section, we configure the local traffic management components of the BIG-IP systems. We will be configuring two virtual servers in this section. The first virtual server created will be used by GTM as a member of the Wide IP group.

Configuring the BIG-IP APM virtual servers

The following table contains a list of BIG-IP configuration objects, along with any non-default settings you should configure as a part of this deployment. Unless otherwise specified, settings not mentioned in the table can be configured as applicable for your configuration. For specific instructions on configuring individual objects, see the online help or product manuals.

Before beginning this part of the configuration, make sure you know the FQDN for the IP address of the local BIG-IP APM virtual server on port 443 that was created by the wizard in the previous section. Your DNS administrator may need to add a record for this IP address.

BIG-IP Object	Non-default settings/Notes		
Profiles *(Main tab--> Local Traffic-->Profiles)*	***HTTP*** *(Profiles-->Services)*	Name	Type a unique name
		Parent Profile	**http**
	TCP WAN *(Profiles-->Protocol)*	Name	Type a unique name
		Parent Profile	**tcp-wan-optimized**
	TCP LAN *(Profiles-->Protocol)*	Name	Type a unique name
		Parent Profile	**tcp-lan-optimized**
iRules (*Local Traffic-->Rules*) Create one of these iRules, depending on which scenario you are deploying.	***If deploying the High Availability configuration (default)***		
	Name	Type a unique name	

	Definition	`when CLIENT_ACCEPTED {`
		`  ACCESS::restrict_irule_events disable`
		`}`
		`when HTTP_REQUEST {`
		`  HTTP::respond 302 Location "https://<FQDN of the local name of the APM instance>[HTTP::uri]"`
		`}`	

	If deploying the Topology-based configuration		
	Name	Type a unique name	

	Definition	`when HTTP_REQUEST {`
		`  HTTP::respond 302 Location "https://<FQDN for the IP address of the local APM virtual server created by the wizard[2]>[HTTP::uri]"`
		`}`	

Virtual Server *(Main tab-->Local Traffic -->Virtual Servers)*	***Name***	Type a unique name.	
	Address	Type the IP Address for this virtual Server.	
	Service Port	Type the appropriate port. In our example, we use 80.	
	Protocol Profile (client)[3]	Select the WAN optimized TCP profile you created	
	Protocol Profile (server)[3]	Select the LAN optimized TCP profile you created	
	HTTP Profile	Select the HTTP profile you created	
	Source Address Translation	**Auto Map**	
	Access Profile	*High Availability configuration (default):* Select the Access Profile created by the wizard in *Configuring BIG-IP APM using the Network Access Setup Wizard on page 6*	
		Topology-based configuration: If deploying a Topology-based configuration, do not select the Access Profile.	
	Default Pool	Select the pool you created	

[2] This is the fully qualified domain name that resolves to the IP address of the BIG-IP APM virtual server created by the wizard. Your DNS administrator may have to add this record
[3] You must select **Advanced** from the **Configuration** list for these options to appear

Repeat this configuration on the BIG-IP system in the secondary data center

Configuring the BIG-IP LTM virtual server

The next task is to create the virtual server for your internal application server. This part of the configuration depends on which application you are using. For a list of BIG-IP deployment guides for specific applications, see *https://f5.com/solutions/deployment-guides*.

You can also use iApp templates to configure the BIG-IP system for your application. From the main tab of the Configuration utility, go to **iApps > Templates** to see a list of the iApp Templates on the box (click **iApps > Application Services > Create** to start configuring a template. For a list of F5 contributed iApps, release candidate iApps, and community contributed iApps, see *https://devcentral.f5.com/wiki/iApp.Codeshare.ashx*.

Configure an application virtual server on the BIG-IP system in each data center.

Important

The IP address you use for this internal application virtual server must be accessible by the Lease Pool members (the IP addresses or range you specified in the Lease Pool section while running the BIG-IP APM Network Access Wizard). It can either be on the same network or on a routed network.

Configuring the BIG-IP GTM

Use the following procedures to configure the BIG-IP Global Traffic Manager for Global Server Load Balancing using the VS Score load balancing method. For a description of VS Score, see *Appendix: About VS Score load balancing on page 10*.

For specific instructions on configuring individual objects, see the online help available from the Help tab, or the BIG-IP GTM documentation.

GTM Object	Description/Notes	
Listener *(Main tab-->Global Traffic -->Listeners)*	***Name***	Type a unique name
	Destination	Type the IP address on which the Global Traffic Manager listens for network traffic. In our example, this is an IP address on the WAN network.
	VLAN Traffic	Select a VLAN setting appropriate for this Listener.
	Create additional listeners using the same IP address if necessary. If creating an IPv6 listener, be sure to use an IPv6 destination address	
Data Center *(Main tab-->Global Traffic -->Data Centers)*	***Name***	Type a unique name. Configure other options as applicable for your environment.
Servers *(Main tab-->Global Traffic -->Servers)*	***Name***	Type a unique name
	Product	Select the either **BIG-IP System (Single)** or **BIG-IP System (Redundant)**. Redundant is only used when the GTM is also an LTM/GTM combo and specifically configured for LTM failover of the listener. Otherwise use **BIG-IP System (Single**).
	Address List: Address	Type the Self IP address of this GTM.
	Data Center	Select the Data Center you created
	Health monitors	*Optional:* Select **bigip**
	Virtual Server Discovery	**Enabled** (We strongly recommend Enabling Discovery, however you can leave this set to Disabled and manually configure the virtual server information)
	Repeat this procedure to create the GTM Server objects for each of the BIG-IP APMs	
Enabling connectivity with remote BIG-IP systems *(Command line)*	When adding a remote BIG-IP LTM server, you must make sure the ***big3d*** agent is on the same version on the BIG-IP APM and GTM. If you have never registered the BIG-IP APM systems with BIG-IP GTM before, you should perform the following steps from GTM using the management IP address(es) of each of the APM hosts. From the GTM device command line, type: **big3d_install** ***<IP address of target system>*** where the target system is the BIG-IP APM that you want to add as a server on the GTM. This pushes out the newest version of big3d. Next, type: **bigip_add** to exchange SSL keys with the BIG-IP APM. Type the password at the prompt, and then type **iqdump** ***<ip address of remote box>***. If the boxes are communicating over iQuery, you see a list of configuration information from the remote BIG-IP. The **bigip_add** command must be run for every BIG-IP in the configuration. Adding GTM servers to a Sync Group If you have more than one BIG-IP GTM, you must run **gtm_add** on each additional GTM in the sync group as well to ensure the iQuery configuration is working. If not already part of a sync group, this command adds the GTM to the sync group. For more information on sync groups, see the GTM documentation.	
Pools *(Main tab-->Global Traffic -->Wide IPs --> Pools)*	***Name***	Type a unique name
	Health Monitors	You can optionally attach a health monitor, such as the **gateway_icmp** monitor.
	Load Balancing Method	***Preferred:*** **VS Score**[1] (if using Topology-based GTM configuration, select **Topology** here) ***Alternate:*** **VS Capacity** ***Return to DNS:*** **VS Score**
	Member List	**Virtual Server** Select the BIG-IP APM virtual server IP address and port you created in *Configuring the BIG-IP APM virtual servers on page 7* and then click **Add**. Repeat for each BIG-IP APM virtual server you created for use with GTM that is a part of this configuration.
Wide IPs *(Main tab-->Global Traffic -->Wide IPs)*	***Name***	Type a unique name
	Load Balancing Method	**Topology**
	Pool List	Select the pool you created.

[1] For a description of the VS Score load balancing method, see *Appendix: About VS Score load balancing on page 10*

Appendix: About VS Score load balancing

This appendix explains how the BIG-IP GTM load balancing method VS Score works, and how the score is calculated.

After you integrate BIG-IP GTM with BIG-IP APM, the APM calculates virtual server scores and provides them to GTM. The calculation is based on the number of active access sessions. APM calculates two usage scores and assigns the higher of the two to the virtual server:

- One usage score is based on the BIG-IP system licensed maximum access concurrent sessions and the sum of the current active sessions on all the access profiles configured on the system.
- The other usage score is based on the maximum concurrent user sessions configured on the access profile attached to the virtual server and the current active sessions count on the access profile.

A value of 0 indicates no capacity and a value of 100 means full capacity available on the device.

Note

Connectivity sessions do NOT count toward the VS Score.

The GTM global load balancing method VS Score load balances APM users based on the virtual server score only.

Example calculation

The following is an example of how the VS Score is calculated

- ***Score A*** – Compute total number of access sessions used on all access policies configured on the system:
  - You have a BIG-IP licensed for 50,000 sessions.
    - Access policy 1 has 5,000 active concurrent access sessions.
    - Access policy 2 has 2,000 active concurrent access sessions.
    - Access policy 3 has 6,000 active concurrent access sessions.

(1- (13000/50000)) x 100 = 74%

- ***Score B*** – Compute the total number of access sessions used on the access policy for the current virtual server:
  - You have an access policy configured for a maximum number of 10,000 sessions.
    - When attached to the virtual server, you have 5,000 active concurrent access sessions established.

(1 – (5000/10000)) x 100 = 50%

Because 74% is greater than 50%, the VS Score in this example would be 74.

Document Revision History

Version	Description	Date
1.0	New Version	11-03-2014

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com