

**IMPORTANT:** This guide has been archived. While the content in this guide is still valid for the products and version listed in the document, it is no longer being updated and may refer to F5 or 3rd party products or versions that have reached end-of-life or end-of-support. See <https://support.f5.com/csp/article/K11163> for more information.



## 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	3
Configuration examples	3
<hr/>	
<b>Preparation Worksheet</b>	<b>5</b>
<hr/>	
<b>Configuring the BIG-IP APM</b>	<b>6</b>
Configuring BIG-IP APM using the Network Access Setup Wizard	6
<hr/>	
<b>Configuring the BIG-IP system</b>	<b>7</b>
Configuring the BIG-IP APM virtual servers	7
Configuring the BIG-IP LTM virtual server	8
<hr/>	
<b>Configuring the BIG-IP GTM</b>	<b>9</b>
<hr/>	
<b>Appendix: About VS Score load balancing</b>	<b>10</b>
Example calculation	10
<hr/>	
<b>Document Revision History</b>	<b>11</b>

## 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 or 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 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.

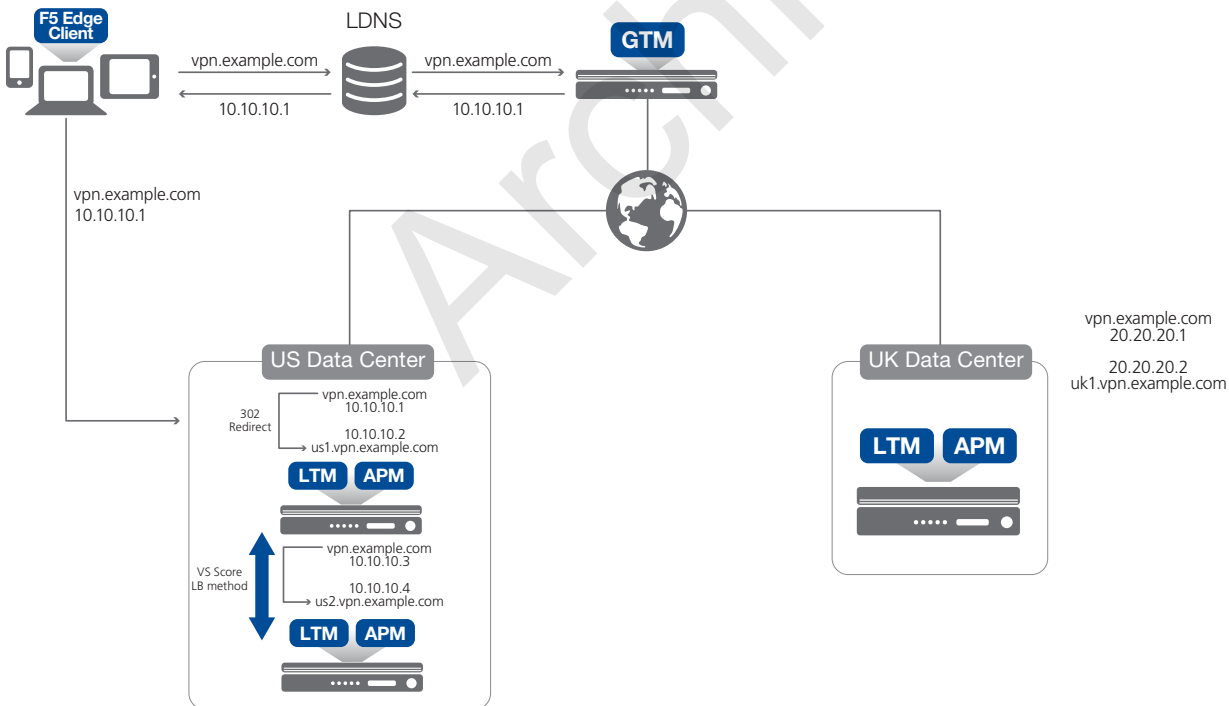


Figure 1: Logical configuration example for high availability

### 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.

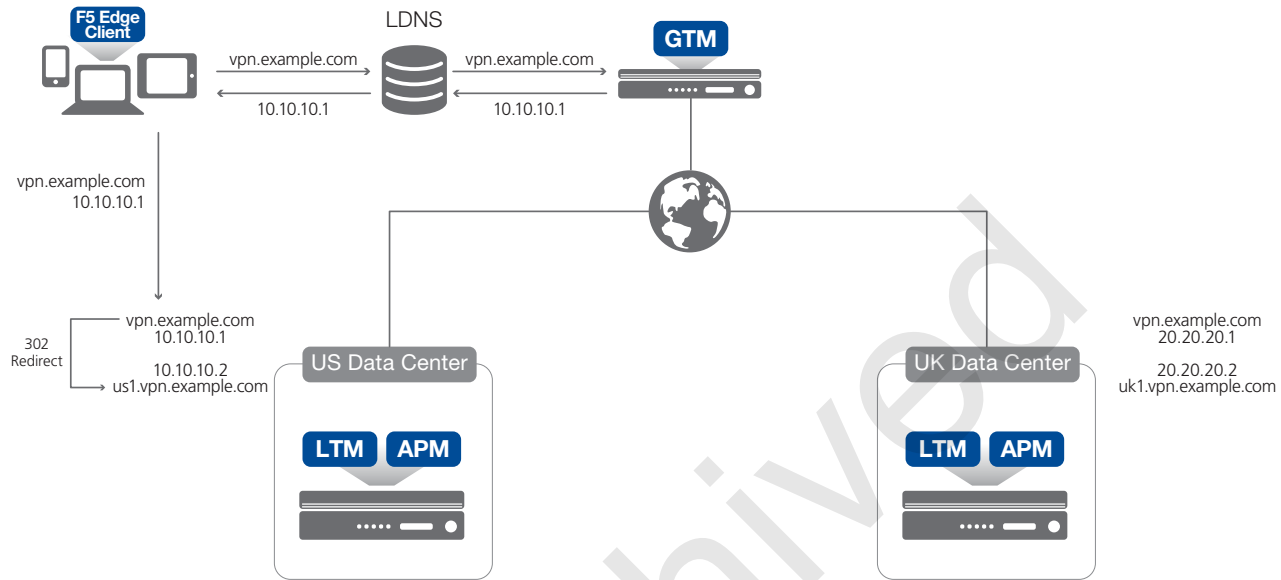


Figure 1: Logical configuration example for topology-based deployments

## 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
<b>Public WAN</b>			
Network	60.168.111.0	70.168.111.0	All public access comes through this network
VLAN + (tag)	vlan-public-WAN1 (1192)	vlan-public-WAN2 (1072)	
GTM DNS Listener	60.168.111.250		
Application public virtual server	60.168.111.100	70.168.111.100	In our example, APM has two virtual servers that provide VPN access, which are on the DMZ / Public WAN
<b>Private WAN</b>			
Network	192.168.111.0		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.
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	
<b>Private LAN</b>			
Network	10.10.2.0	10.20.2.0	This Network is where your clients will be once they access the SSL VPN
BIG IP APM Application VIP	10.10.2.100	10.20.2.100	These are the Internal Application virtual servers clients access once connected to the SSL VPN. This is only required in our example use case.
VLAN + (tag)	vlan-private-LAN1 (1010)	vlan-private-LAN2 (1020)	
BIG IP APM Application VIP	10.10.2.200	10.20.2.200	
<b>Private LAN - Server Layer</b>			
Network	172.10.2.0	172.80.2.0	This network contains the application in our example.
VLAN + (tag)	vlan-privateApp-LAN1 (7010)	vlan-privateApp-LAN2 (7020)	
BIG-IP APM Self IP	172.10.2.200	172.80.2.200	These self IP will be used for access by the application servers.





## 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.*

Archived



## 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
<b>Listener</b> (Main tab-->Global Traffic -->Listeners)	<p><b>Name</b> Type a unique name</p> <p><b>Destination</b> 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.</p> <p><b>VLAN Traffic</b> Select a VLAN setting appropriate for this Listener.</p> <hr/> Create additional listeners using the same IP address if necessary. If creating an IPv6 listener, be sure to use an IPv6 destination address
<b>Data Center</b> (Main tab-->Global Traffic -->Data Centers)	<p><b>Name</b> Type a unique name. Configure other options as applicable for your environment.</p>
<b>Servers</b> (Main tab-->Global Traffic -->Servers)	<p><b>Name</b> Type a unique name</p> <p><b>Product</b> Select the either <b>BIG-IP System (Single)</b> or <b>BIG-IP System (Redundant)</b>. Redundant is only used when the GTM is also an LTM/GTM combo and specifically configured for LTM failover of the listener. Otherwise use <b>BIG-IP System (Single)</b>.</p> <p><b>Address List: Address</b> Type the Self IP address of this GTM.</p> <p><b>Data Center</b> Select the Data Center you created</p> <p><b>Health monitors</b> <i>Optional:</i> Select <b>bigip</b></p> <p><b>Virtual Server Discovery</b> <b>Enabled</b> (We strongly recommend Enabling Discovery, however you can leave this set to Disabled and manually configure the virtual server information)</p> <hr/> Repeat this procedure to create the GTM Server objects for each of the BIG-IP APMs
<b>Enabling connectivity with remote BIG-IP systems</b> (Command line)	<p>When adding a remote BIG-IP LTM server, you must make sure the <b>big3d</b> 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.</p> <p>From the GTM device command line, type: <b>big3d_install &lt;IP address of target system&gt;</b>                      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.</p> <p>Next, type: <b>bigip_add</b>                      to exchange SSL keys with the BIG-IP APM. Type the password at the prompt, and then type <b>iqdump &lt;ip address of remote box&gt;</b>.                      If the boxes are communicating over iQuery, you see a list of configuration information from the remote BIG-IP.</p> <p>The <b>bigip_add</b> command must be run for every BIG-IP in the configuration.</p> <p>Adding GTM servers to a Sync Group</p> <p>If you have more than one BIG-IP GTM, you must run <b>gtm_add</b> 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.</p> <p>For more information on sync groups, see the GTM documentation.</p>
<b>Pools</b> (Main tab-->Global Traffic -->Wide IPs -->Pools)	<p><b>Name</b> Type a unique name</p> <p><b>Health Monitors</b> You can optionally attach a health monitor, such as the <b>gateway_icmp</b> monitor.</p> <p><b>Load Balancing Method</b> <b>Preferred: VS Score<sup>1</sup></b> (if using Topology-based GTM configuration, select <b>Topology</b> here)  <b>Alternate: VS Capacity</b>  <b>Return to DNS: VS Score</b></p> <p><b>Member List</b> <b>Virtual Server</b> Select the BIG-IP APM virtual server IP address and port you created in <i>Configuring the BIG-IP APM virtual servers on page 7</i> and then click <b>Add</b>.                      Repeat for each BIG-IP APM virtual server you created for use with GTM that is a part of this configuration.</p>
<b>Wide IPs</b> (Main tab-->Global Traffic -->Wide IPs)	<p><b>Name</b> Type a unique name</p> <p><b>Load Balancing Method</b> <b>Topology</b></p> <p><b>Pool List</b> Select the pool you created.</p>

<sup>1</sup> 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.

$$(1 - (13000/50000)) \times 100 = 74\%$$

- **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.

$$(1 - (5000/10000)) \times 100 = 50\%$$

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

Archived

**F5 Networks, Inc.** 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 [www.f5.com](http://www.f5.com)

F5 Networks, Inc.  
Corporate Headquarters  
[info@f5.com](mailto:info@f5.com)

F5 Networks  
Asia-Pacific  
[apacinfo@f5.com](mailto:apacinfo@f5.com)

F5 Networks Ltd.  
Europe/Middle-East/Africa  
[emeainfo@f5.com](mailto:emeainfo@f5.com)

F5 Networks  
Japan K.K.  
[f5j-info@f5.com](mailto:f5j-info@f5.com)

