IMPLEMENTATION GUIDE FOR 
GLOBALSCAPE® ENHANCED FILE TRANSFER™ (EFT™) v7.1 
AND F5 BIG-IP® LTM® v11.x INTEGRATION

PROVIDED BY GLOBALSCAPE, INC.

For other versions:
- F5 BIG-IP LTM documentation is available at https://support.f5.com/
<table>
<thead>
<tr>
<th><strong>GlobalSCAPE, Inc. (GSB)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Corporate Headquarters</strong></td>
</tr>
<tr>
<td><strong>Address:</strong> 4500 Lockhill-Selma Road, Suite 150, San Antonio, TX (USA) 78249</td>
</tr>
<tr>
<td><strong>Sales:</strong> (210) 308-8267</td>
</tr>
<tr>
<td><strong>Sales (Toll Free):</strong> (800) 290-5054</td>
</tr>
<tr>
<td><strong>Technical Support:</strong> (210) 366-3993</td>
</tr>
<tr>
<td><strong>Web site:</strong> <a href="http://www.globalscape.com/">http://www.globalscape.com/</a></td>
</tr>
</tbody>
</table>

© 2017 GlobalSCAPE, Inc. All Rights Reserved

**Copying, Use, or Disclosure Without the Express Written Consent of GlobalSCAPE, Inc. is Prohibited.**

_Last saved: January 26, 2017_
_Last saved by: Karla Marsh_
Table of Contents

Introduction ................................................................................................................................................... 4
Test Setup ..................................................................................................................................................... 5
Testing Criteria .............................................................................................................................................. 7
F5 BIG-IP LTM – Required Configuration..................................................................................................... 8
  Create VLANs......................................................................................................................................... 9
  Create Self IPs...................................................................................................................................... 10
  Create Nodes for each DMZ Gateway box .......................................................................................... 11
  HTTP .................................................................................................................................................... 12
  HTTPS .................................................................................................................................................. 13
  SFTP ..................................................................................................................................................... 14
  FTP (and not FTPS Explicit)................................................................................................................. 14
  FTPS Implicit ........................................................................................................................................ 15
  FTP and FTPS Explicit .......................................................................................................................... 15
    iRules® ........................................................................................................................................... 15
    Persistence profile .......................................................................................................................... 16
    Protocol profile ............................................................................................................................... 17
    Virtual servers ................................................................................................................................ 18
    Address Translation SNAT ............................................................................................................... 19
DMZ Gateway – Required Configuration .................................................................................................... 20
EFT – Required Configuration (for external F5 BIG-IP LTM) ........................................................................ 21
  EFT Event Rules Going through DMZ Gateway and F5 BIG-IP LTM .................................................. 21
  EFT Support for External F5 BIG-IP LTM and Internal F5 BIG-IP LTM .................................................. 22
Conclusion .................................................................................................................................................. 23
Introduction

Globalscape’s Quality Assurance team has integrated and tested the F5 BIG-IP Local Traffic Manager™ (LTM) with Globalscape® Enhanced File Transfer™ (EFT™) and DMZ Gateway® in an active-active, high availability cluster. The purpose of the test was to define parameters for and to certify interoperation between the F5 and Globalscape devices to provide load balancing in an active-active, high availability cluster configuration.

This document describes the test setup and testing criteria, then describes specific settings in the F5 BIG-IP LTM and Globalscape Enhanced File Transfer (EFT) and DMZ Gateway devices necessary for successful interoperability.

This document does not describe how to install the software for the F5 BIG-IP LTM, Globalscape EFT, or Globalscape DMZ Gateway. Please refer to the relevant help documentation for those procedures.

- F5 BIG-IP LTM documentation is available at https://support.f5.com/
Test Setup

The test setup for the (virtual) devices illustrated below included:

- 12 virtual machine images
- 4 networks
- 2 F5 BIG-IP LTM instances
- 2 EFT servers in active-active HA configuration
- 2 DMZ Gateways, externally facing
- 2 internal clients
- 2 external clients
- 1 HA file server/database server
- 1 external FTP/SFTP server
Once communication between networks was verified, the following tests were run using EFT automation rules:

**Internal Users**
- Files can be uploaded using any supported protocol. The file will be marked with username and eventually archived in a compressed zip file.

**User folders**
- OnUpload

**Processed**
- EVENT RULE (AWE Task):
  1. Rename file to include username
  2. Copy File to Processed folder

**Scheduled Task**
- EVENT RULE (AWE Task):
  1. Get list of all files in Processed folder
  2. Copy to tmp directory
  3. Create a single zip file of all files and move to archive folder

**Archive**

**External Users**
- Files can be uploaded using any supported protocol. The file will be PGP encrypted, sent to an external server and eventually archived in a compressed zip file.
## Testing Criteria

The table below describes the functions that were used to determine solution validation and how success was measured. All tests passed successfully.

<table>
<thead>
<tr>
<th>Function</th>
<th>Success Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 nodes handle client connectivity, connected with the DMZ Gateways</td>
<td>With both EFT/DMZ Gateway nodes up, external clients can upload and download files using any supported EFT protocol. This was confirmed by logging into the EFT Admin UI on one of the nodes, clicking the Report tab and viewing an “Activity – All File Transfers” report, and verifying that the files appear in the transaction log. Additionally, when either EFT node is set to offline in the F5 BIG-IP LTM, the external client can continue to upload/download files just as before.</td>
</tr>
<tr>
<td>2 nodes handle the naturally distributed On File Upload Rules reacting to incoming data</td>
<td>With both nodes up, an internal user can to upload a file and see the file automatically renamed when it is uploaded to the user folder. The file is renamed to include the username prepended to the filename. (The client may need to refresh the directory listing to verify this.)</td>
</tr>
<tr>
<td>2 nodes handle Scheduled Tasks</td>
<td>A scheduled task is configured to create a compressed archive of all processed files. For testing, this is setup to run every minute. After files have been uploaded (by either internal or external clients), a zip file (with a timestamp name) appears in the Archive directory as configured in EFT. This task can always run as long as at least one EFT node is up.</td>
</tr>
<tr>
<td>2 nodes handle Folder Monitors</td>
<td>When an external user uploads a file, a Folder Monitor rule is configured to do OpenPGP encryption on the file and offload a copy of the file to an external SFTP server. This tests whether EFT is able to go out through the F5 BIG-IP LTM using DMZ Gateway as a proxy. This functionality is working; demonstrated by file (with .pgp extension) being successfully copied to the external server.</td>
</tr>
<tr>
<td>2 systems configured to handle AWE tasks</td>
<td>This test environment is setup with two AWE tasks: A Rename task for files sent by internal users. A Scheduled (Timer) task that creates the archive zip files. Successful completion of the Event Rules indicates use of the AWE engine.</td>
</tr>
<tr>
<td>2 systems configured to handle processing the more resource-intensive workflows</td>
<td>The Scheduled (Timer) task for creating the zip archive (see above) in particular is a very resource-intensive operation. When a large file (&gt; 250 MB) is uploaded and compressed into the zip archive, this indicates that the devices can handle resource-intensive workflows.</td>
</tr>
</tbody>
</table>
F5 BIG-IP LTM – Required Configuration

Described below are the necessary configuration steps to configure the F5 BIG-IP LTM to interoperate with Globalscape DMZ Gateway and Enhanced File Transfer (EFT) platform.

Obviously, for all configuration, use the addresses and ports that are used in your network. The following configuration is described:

1. Create VLANS
2. Create Self IPs
3. Create nodes for each DMZ Gateway
4. Define the Pools and virtual servers for the following protocols:
   - HTTP
   - HTTPS
   - SFTP
   - FTP (and not FTPS Explicit)
   - FTPS implicit
   - FTP and FTPS Explicit
Create VLANs

The F5 BIG-IP LTM has multiple physical (or virtual if using the virtual appliance) network adapters. At least one will point internally and one will point externally so that all traffic passing between the two networks goes through the F5 BIG-IP LTM. If VLANs do not already exist for the internal network (EFT/DMZ) and external (e.g. internet) traffic create them by going to Network > VLANs.
Create Self IPs

Next, you can specify the network for each VLAN by creating a Self IP. A Self IP associates an IP Address/mask combination with a VLAN. In our example, our internal VLAN is associated with 172.10.1.1 and mask 255.255.255.0 and our external VLAN is associated with 10.10.10.1 and mask 255.255.255.0.
Create Nodes for each DMZ Gateway box

You can now define nodes for the DMZ Gateway box by going to Local Traffic > Nodes. In our example we have defined two DMZ Gateway nodes named “DMZ1” and “DMZ2” with IP Addresses 172.10.1.101 and 172.10.1.102 respectively.
The last steps in F5 BIG-IP LTM configuration are creating Pools and Virtual Servers for the protocols. Be aware that there are some subtle differences between each protocol.

**HTTP**

To add configuration for handling HTTP traffic:

1. Create a pool named HTTP.
2. Add the two DMZ Gateway nodes and service port 80.
3. Add a health monitor (if you do not know which to select you may use “inband”. See F5 BIG-IP LTM documentation for more information).
4. Create a virtual server named HTTP. A virtual server creates a listening socket on the F5 BIG-IP LTM for a specific port. For this server use port 80.
5. For the Destination Address of the virtual server enter an external IP address the F5 BIG-IP LTM will listen on. This is the IP address that clients will connect to from outside the organization. In our example we have selected 10.10.10.11.
6. For the HTTP Profile select “http” and set the FTP Profile to “None”.
7. For Source Address Translation select “Auto Map”.
8. For the Default Pool select “HTTP”.
9. For the Persistence profile select source_addr.
10. All other default settings are OK.
To add configuration for handling HTTPS traffic:

1. Create a pool named HTTPS.
2. Add the two DMZ Gateway nodes and service port 443.
3. Add a health monitor (if you do not know which to select you may use “inband”. See F5 BIG-IP LTM documentation for more information).
4. Create a virtual server named HTTPS.
5. For the Destination Address of the virtual server enter an external IP address the F5 BIG-IP LTM will listen on. This is the IP address that clients will connect to from outside the organization. In our example we have selected 10.10.10.11. For this server use port 443.
6. Make sure the HTTP and FTP profiles are set to “None”.
7. For Source Address Translation select “Auto Map”.
8. For the Default Pool select “HTTPS”.
9. For the Persistence profile select source_addr.
10. All other default settings are OK as is.
SFTP

To add configuration for handling SFTP traffic:

1. Create a pool named SFTP.
2. Add the two DMZ Gateway nodes and service port 22.
3. Add a health monitor (if you do not know which to select you may use “inband”. See F5 BIG-IP LTM documentation for more information).
4. Create a virtual server named SFTP.
5. For the Destination Address of the virtual server enter an external IP address the F5 BIG-IP LTM will listen on. This is the IP address that clients will connect to from outside the organization. In our example we have selected 10.10.10.11. For this server use port 22.
6. Make sure the HTTP and FTP profiles are set to “None”.
7. For Source Address Translation select “Auto Map”.
8. For the Default Pool select “SFTP”.
9. For the Persistence profile select “None”.
10. All other default settings are OK.

FTP (and not FTPS Explicit)

If the F5 BIG-IP LTM will only handle FTP and not FTPS Explicit traffic then you can use the built-in FTP profile for the Virtual Server. If you need to handle both FTP AND FTPS traffic, see below.

1. Create a pool named FTP.
2. Add the two DMZ Gateway nodes and service port 21.
3. Add a health monitor (if you do not know which to select you may use “inband”. See F5 BIG-IP LTM documentation for more information).
4. Create a virtual server named FTP.
5. For the Destination Address of the virtual server enter an external IP address the F5 BIG-IP LTM will listen on. This is the IP address that clients will connect to from outside the organization. In our example we have selected 10.10.10.11. For this server use port 21.
6. Set the FTP profile to “ftp” and the HTTP profile to “None”.
7. For Source Address Translation select “Auto Map”.
8. For the Default Pool select “FTP”.
9. For the Persistence profile select “None”.
10. All other default settings are OK.
**FTPS Implicit**

FTPS Implicit typically runs on port 990 rather than the standard FTP port 21.

1. Create a pool named FTPS-IMPLICIT.
2. Add the two DMZ Gateway nodes and service port 990.
3. Add a health monitor (if you do not know which to select you may use "inband". See F5 BIG-IP LTM documentation for more information).
4. Create a virtual server named FTPS-IMPLICIT.
5. For the Destination Address of the virtual server enter an external IP address the F5 BIG-IP LTM will listen on. This is the IP address that clients will connect to from outside the organization. In our example we have selected 10.10.10.11. For this server use port 990.
6. Make sure the HTTP and FTP profiles are set to “None”.
7. For Source Address Translation select “None”.
8. For the Default Pool select “FTP-IMPLICIT”.
9. For the Persistence profile select “None”.
10. All other default settings are OK.

**FTP and FTPS Explicit**

If the F5 BIG-IP LTM will handle FTP and FTPS Explicit traffic then you cannot use the built-in FTP profile for the Virtual Server. FTP and FTPS Explicit use the same port (21 by default) and if you use the built-in FTP profile the F5 BIG-IP LTM cannot inspect the FTPS traffic because it is encrypted and it will be blocked. To make this work requires another way of handling both types of traffic.

1. Create a pool named FTP.
2. Add the two DMZ Gateway nodes and service port 21.
3. Add a health monitor (if you do not know which to select you may use “inband”. See F5 BIG-IP LTM documentation for more information).
4. Create another pool named FTPS_EXPLICIT.
5. Add the two DMZ Gateway nodes but with a service port of 0. This creates a “wildcard” pool that can service traffic on whatever data port FTP needs.

**iRules®**

Create a new iRule (Local Traffic > iRules > iRule List) named “WILDCARD_PROTECT” with the following script:

```bash
when CLIENT_ACCEPTED {
    if {([TCP::local_port] >= 28005) && ([TCP::local_port] <= 28010)} { pool FTPS_EXPLICIT
}
```

In the iRule 28005 and 28010 represent the port range configured for PASV connections in EFT. This rule will be attached to the Virtual Server we will create.
1. Create a new persistence profile (Local Traffic > Profiles > Persistence) named “FTPS_EXPLICIT”.
2. Create it as type “Source Address Affinity” with a parent profile “source_addr”.
3. Select a custom configuration and enable “Match Across Services” and “Match Across Virtual Servers.”
1. Create a new protocol profile (Local Traffic > Profiles > Protocol > FastL4) named “FTPS_EXPLICIT”.
2. Select fastL4 as the parent profile.
Virtual servers

1. Create a virtual server named “FTP-FTPS_EXPLICIT”.
2. For the Destination Address of the virtual server enter an external IP address the F5 BIG-IP LTM will listen on. This is the IP address that clients will connect to from outside the organization. In our example, we have selected 10.10.10.11. For this server use port 21.
3. Make sure the HTTP and FTP profiles are set to “None”.
4. For Source Address Translation select “None”.
5. For the Default Pool select “FTP”.
6. For the Persistence Profile, select “FTPS_EXPLICIT”.
7. All other default settings are OK.
8. Create another virtual server named “FTP-FTPS-PASV”
9. Make the type “Performance (Layer 4)”
10. Again, make the Destination address 10.10.10.11 (same as previous virtual server) and make the port 0 (for all ports).
11. For the Protocol Profile (Client) select the FTPS_EXPLICIT Protocol profile previous created.
12. For Source Address Translation select “None”.
13. For the Default Pool select “None”.
14. For the Persistence Profile, select “FTPS_EXPLICIT.”
15. Add the “WILDCARD_PROTECT” iRule (see image).
16. All other default settings are OK as is.
Address Translation SNAT

1. Create a SNAT List entry (Local Traffic > Address Translation > SNAT List) for the IP Address of the Virtual Server (10.10.10.11 in our example).

2. Add the IP addresses of the DMZ Gateway nodes to and address list of the SNAT entry.

Ensure that Address Translation and Port Translation are enabled on every virtual server.
DMZ Gateway – Required Configuration

In order for EFT to use DMZ Gateway as a proxy (useful when using Event Rules to copy/move files), DMZ Gateway must have the F5 BIG-IP LTM configured as its default gateway. This is also required if you want to use FTP/FTPS in Active mode. When EFT needs to get out to the Internet, it goes through DMZ Gateway, which then must go through the F5 BIG-IP LTM.

In our example, the default gateway of our DMZ Gateway box is set to the Internal Network Self IP that we previously created on our F5 BIG-IP LTM.
EFT – Required Configuration (for external F5 BIG-IP LTM)

You must configure EFT to use the DMZ Gateway. Obviously, for all configuration, use the addresses and ports that are used in your network.

If you want to support FTP PASV you must configure the PASV settings for DMZ Gateway and enter the Destination IP Address for the Virtual Server previously created in the F5 BIG-IP LTM for FTP.

Also, the port range previously used in the “WILDCARD_PROTECT” iRule must be the same port range used here:
EFT Event Rules Going through DMZ Gateway and F5 BIG-IP LTM

If your Event Rule has a copy/move offload action and the destination is a server external to your organization, you must configure DMZ Gateway to be used as a proxy. This will ensure that it goes through DMZ Gateway and the F5 BIG-IP LTM.

EFT Support for External F5 BIG-IP LTM and Internal F5 BIG-IP LTM

A single EFT site is able to operate connected to two F5 BIG-IP LTMs on two different networks. This setup may be necessary when one network handles external traffic and another handles internal traffic. For this to work correctly for all protocols, the external traffic must go through DMZ Gateway as shown in the previous section, and the internal traffic cannot go through DMZ Gateway. If you require internal traffic to also go through DMZ Gateway, it will require a separate site.

To use a single site with 2 F5 BIG-IP LTMs, you must configure the internal F5 BIG-IP LTM exactly as the external one. Since this second one exists on an internal network it should be on a different subnet than the external F5 BIG-IP LTM. This means the IP addresses used for the internal F5 BIG-IP LTM (e.g., for nodes, Self IPs, Virtual Servers, etc.) will be different; however, the basic configuration of the internal F5 BIG-IP LTM will be the same as the external F5 BIG-IP LTM.

Another small difference is that the internal F5 BIG-IP LTM nodes will point to the EFT machines themselves rather than DMZ Gateway machines.

Assuming you have a second F5 BIG-IP LTM configured for the internal network:

1. To use FTP/FTPS in Active mode set the default gateway of the EFT machine to point to the internal F5 BIG-IP LTM.
2. In the main site configuration (not the gateway configuration for the site) you must configure the FTP PASV setting. Here you will use the Destination IP Address you configured for your FTP Virtual Server and you must also have the same port range as configured in your internal F5 BIG-IP LTM iRule.

**Conclusion**

If you have configured the F5 BIG-IP LTM, EFT, and DMZ Gateway as described in this document, your system should be able to pass the same testing criteria as used in our testing.

If you need assistance with this configuration, please contact your Globalscape account manager or Globalscape Support at [https://www.globalscape.com/support](https://www.globalscape.com/support).