Deploying the BIG-IP System with SMTP servers

This document contains guidance on configuring the BIG-IP system version 11.4 and later for most SMTP server implementations, resulting in a secure, fast, and available deployment. This guide shows how to quickly and easily configure the BIG-IP LTM (Local Traffic Manager) and AFM (Advanced Firewall Manager) modules.

Products and versions

Product	Version
BIG-IP LTM	11.4 - 13.0
BIG-IP AFM	11.5 - 13.0
SMTP Server	Not generally applicable; see the Monitor section for specifics
iApp version	f5.smtp.v1.0.0rc9
Deployment Guide version	1.9 (see *Document Revision History on page 42*)
Last updated	08-28-2019

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

To provide feedback about this deployment guide or other F5 solution documents, contact us at *solutionsfeedback@f5.com*.

For previous versions of this and other guides, see the Deployment guide Archive tab on f5.com: https://f5.com/solutions/deployment-guides/archive-608

Contents

Terminology

This guide uses the following terminology.

Term	Definition
MSA	Message Submission Agent. Microsoft Exchange's SMTP service is an example of this when used to receive SMTP mail for local mailbox delivery.
MTA	Message Transfer Agent. Common examples include Sendmail and Postfix.
MX record	A DNS resource record type that indicates the SMTP destination(s) for a given domain. MX records typically resolve to A records, which in turn each resolve to an IP address. MX records can also include priorities, indicting the order of preference when sending mail, based on availability.

Supported Configurations

This deployment guide provides guidance on configuring a BIG-IP LTM system to support the following scenarios. All scenarios support the use of the Advanced Firewall Manager (AFM) module.

1. **Standard unencrypted SMTP on the client and server side**
   Most domain-to-domain email transfers over the Internet—from userX@my.example.com to userY@your.example.com—occur on unencrypted TCP port 25; the public-facing DNS MX record for your domain will resolve to the IP address you associate with the virtual server in this scenario. Because the Internet side of the connection is unencrypted, there is usually no requirement to encrypt the traffic between the BIG-IP system and the local SMTP MTAs.

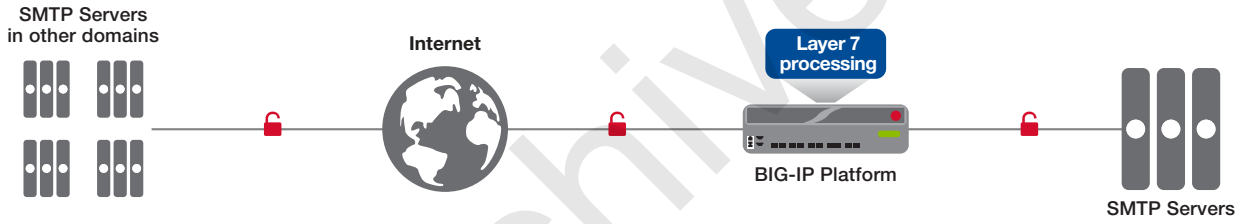

Figure 1: *Standard unencrypted SMTP*

2. **Client-side: SMTP encrypted with TLS/SSL; server-side: unencrypted SMTP**
   We refer to this scenario as *SSL Offload*. Note that encrypted SMTP is often referred to as SMTPS or ESMTPS.
   Clients may send mail using SMTP over an encrypted link, typically on TCP port 587 (or the deprecated port 465), with a BIG-IP system decrypting the traffic before load balancing to SMTP MTAs or MSAs on port 25. Some business-to-business connections may also use encrypted SMTP links over the Internet, and email providers are increasingly encrypting inter-domain email transfers.

   This scenario covers standard SMTP connections encrypted with TLS/SSL only. An alternative and common encryption approach, STARTTLS, is covered in scenario 6.

Figure 2: *SMTP encrypted on the client-side only*

3. **Client-side: SMTP encrypted with TLS/SSL; server-side: SMTP encrypted with TLS/SSL**
   In this scenario (which we refer to as SSL Bridging), the BIG-IP system performs decryption in order to process messages or connections, for instance to use an iRule, and then re-encrypts the connection to the back-end servers.

   SSL Bridging covers many of the same scenarios as example #2, but is commonly used when organizations require that all communication on a network connection is encrypted. Messages are forwarded to SMTP servers, typically on port 465. The BIG-IP system can optionally use self-signed TLS/SSL certificates, or certificates with lesser key length, on internal connections.

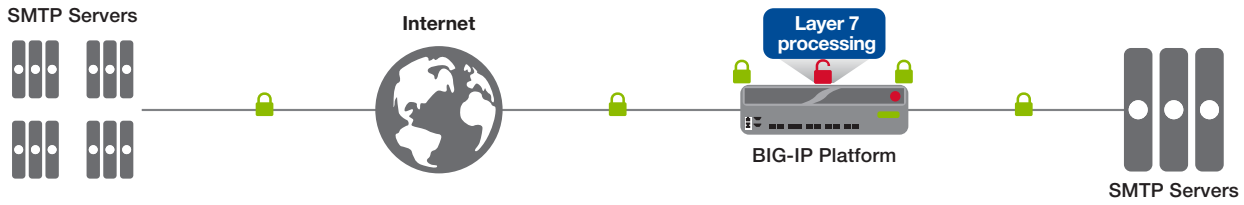

Figure 3: *Encrypted SMTP on the client-side, and re-encrypted to the server side*

4. **SMTP encrypted with TLS/SSL on both client and server sides**
We refer to this scenario as *SSL Passthrough*, because the BIG-IP system does not decrypt the traffic, and acts as a simple Layer 4 load balancer.
Although less common, this scenario is useful when you do not require the BIG-IP system to perform any advanced logging, message handling, or other Layer 7 logic on incoming messages. The BIG-IP system does not provide any handling that is unique to SMTP connectivity; connections are handled at the TCP layer (Layer 4 of the OSI model). All communication is typically on TCP port 465.

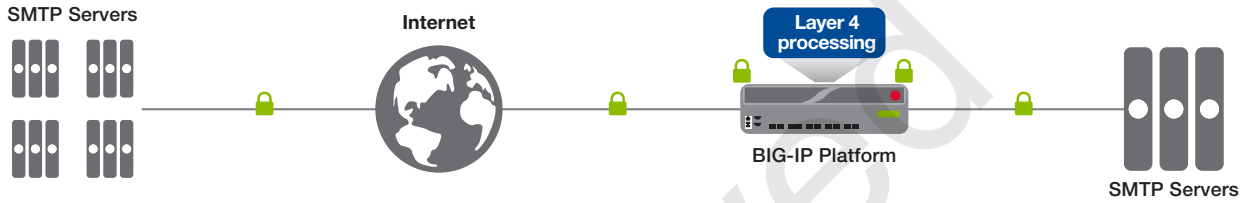

Figure 4: *Encrypted SMTP on both client and server sides*

5. **Client-side: unencrypted SMTP; server-side: SMTP encrypted with TLS/SSL**
This scenario, where traffic arrives unencrypted and then is encrypted before sending to the servers, is uncommon, but could be used at the remote end of a BIG-IP WOM/AAM tunnel deployment as shown in the following diagram.

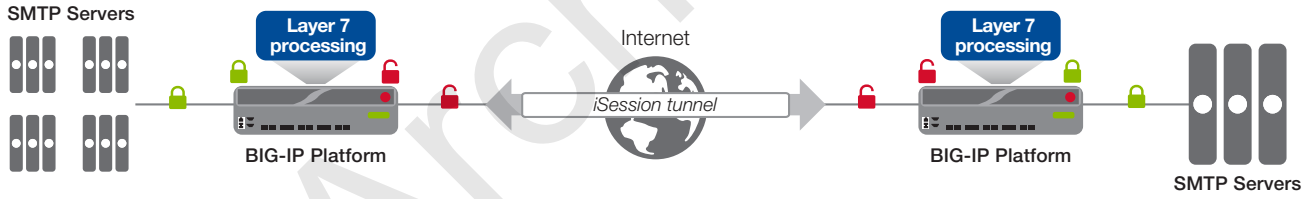

Figure 5: *Unencrypted SMTP on client side, encrypted SMTP to the servers*

6. **Client-side: SMTP with STARTTLS; server-side: unencrypted SMTP**
In this scenario, client-side connections are normally on TCP port 587 or 25, but in this case the clients negotiate encryption using the STARTTLS command. Server-side connections are typically on unencrypted port 25. This is very common in MSAs, for instance when an email client submits a message to a corporate mail server for delivery. Note that STARTTLS capabilities are currently offered via an unsupported iRule in BIG-IP version 11.4; version 11.5 natively supports STARTTLS for SMTP.

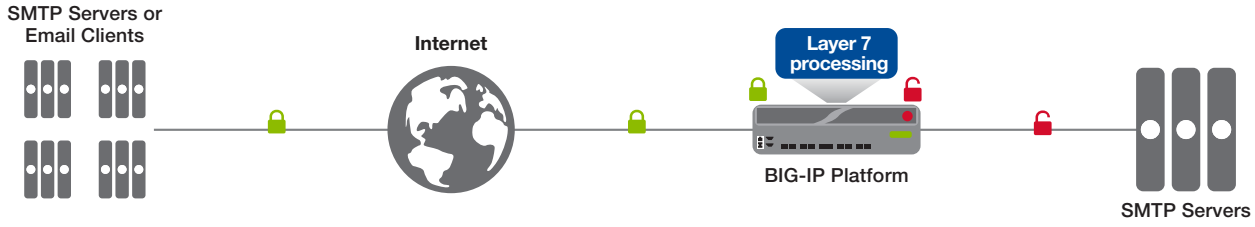

Figure 6: *Client-side SMTP secured with STARTTLS, and unencrypted SMTP on the server-side*

Initial configuration tasks

This section contains configuration tasks that are used in multiple scenarios.

Importing SSL certificates

If you are using the BIG-IP system in a scenario that includes decrypting (and in some cases and re-encrypting) SSL/TLS traffic for processing, you must have imported a valid SSL certificate onto the BIG-IP system. The BIG-IP system uses the SSL certificates in SSL profiles for processing SSL traffic. These scenarios include SSL Offload and SSL Bridging.

When the BIG-IP system encrypts traffic to the servers (for example, in SSL Bridging) , it is acting as an SSL client and by default we assume the servers do not expect the system to present its client certificate on behalf of clients traversing the virtual server. If your servers expect the BIG-IP system to present a client certificate, you must import the appropriate certificate and key and configure a Server SSL profile to use them.

You can import SSL certificates from the Configuration utility, using the **System > File Management > SSL Certificate List**. For specific information on importing or using SSL certificates on the BIG-IP system, see the **SSL Certificates for Local Traffic** chapter of the ***BIG-IP Local Traffic Manager: Concepts*** guide available at *http://support.f5.com*.

SNAT Pool considerations and configuration

This task applies to all scenarios. When a BIG-IP system is configured with SNAT, or secure network address translation, it replaces the original source IP address of each incoming connection with an IP address of its own. By using SNAT, there are usually no routing changes required on the network on servers.

Important *You must NOT use SNAT on a BIG-IP system that processes traffic before sending it to an SMTP server that performs SPAM or other filtering based on the reputation of the source address of the messages, or if you require your SMTP servers to log the source IP address of each message, because all messages will appear to come from the BIG-IP system.*

There are two ways you can use SNAT on the BIG-IP system: Auto Map or a SNAT Pool. With SNAT Auto Map, the BIG-IP system picks one of its own self IP addresses and assigns it to the connections automatically. With a SNAT Pool, you pre-configure a list of one or more IP addresses from which the BIG-IP system uses for address translation. A SNAT pool is only required if you expect more than 65,000 simultaneous SMTP connections for each of your SMTP servers.

Note: *A SNAT pool can be useful when performing traffic analysis. Monitor traffic sent from a BIG-IP will always come from a self IP address of the BIG-IP system; by using a SNAT pool for client-generated traffic, you can easily differentiate monitor traffic from actual client traffic using Wireshark or a similar utility.*

For more information on configuring SNAT on the BIG-IP system, see the **SNATs** chapter of the ***BIG-IP Local Traffic Manager: Concepts*** guide available at *http://support.f5.com*.

This completes the initial configuration tasks. Use the guidance on the following pages to configure the BIG-IP system according to your specific scenario.

Using this guide

This deployment guide is intended to help users deploy the BIG-IP system for SMTP implementations. This document contains guidance configuring the BIG-IP system using the iApp template, as well as manually configuring the BIG-IP system.

Using this guide to configure the iApp template

We recommend using the iApp template to configure the BIG-IP system for SMTP deployments. The majority of this guide describes the iApp template and the different options the template provides for configuring the system for SMTP.

The iApp template configuration portion of this guide walks you through the entire iApp, giving detailed information not found in the iApp or inline help. The questions in the UI for the iApp template itself are all displayed in a table and at the same level. In this guide, we have grouped related questions and answers in a series of lists. Questions are part of an ordered list and are underlined and in italics or bold italics. Options or answers are part of a bulleted list, and in bold. Questions with dependencies on other questions are shown nested under the top level question, as shown in the following example:

1. ***Top-level question found in the iApp template***
   - *Select an object you already created from the list* (such as a profile or pool; not present on all questions. Shown in bold italic)
   - **Choice #1** (in a drop-down list)
   - **Choice #2** (in the list)

     a. *Second level question dependent on selecting choice #2*
        - **Sub choice #1**
        - **Sub choice #2**

          a. *Third level question dependent on sub choice #2*
             - **Sub-sub choice**
             - **Sub-sub #2**

               a. *Fourth level question (and so on)*

Advanced options/questions in the template are marked with the Advanced icon: Advanced. These questions only appear if you select the Advanced configuration mode. The iApp template guidance starts with *Configuring the BIG-IP system using the iApp template on page 7.*

Using this guide to manually configure the BIG-IP system

Users already familiar with the BIG-IP system can use the manual configuration tables to configure the BIG-IP system for the SMTP implementation. These configuration tables only show the configuration objects and any non-default settings recommended by F5, and do not contain procedures on specifically how to configure those options in the Configuration utility. See *Appendix A: Manually configuring the BIG-IP system on page 19.*

Configuring the BIG-IP system using the iApp template

Use this section for configuring the BIG-IP system using the iApp template for SMTP. If you prefer to configure the system manually, see *Appendix A: Manually configuring the BIG-IP system on page 19.*

Downloading and importing the iApp template

The first task is to download and import the SMTP iApp template.

To download and import the iApp

1. Open a web browser and go to *downloads.f5.com*.
2. Click **Find a Download**, and then in the **F5 Product Family > BIG-IP** section, click **iApp Templates**.
3. From the **Select a Product Version and Container** page, click **iApp-Templates**.
4. Accept the EULA, and then download the iapps zip file to a location accessible from your BIG-IP system.
5. Extract (unzip) the **f5.smtp.v1.0.0.<latest version>.tmpl** file. For this release, the template is in the **RELEASE_CANDIDATES** directory of the SMTP folder.
6. Log on to the BIG-IP system web-based Configuration utility.
7. On the Main tab, expand **iApp**, and then click **Templates**.
8. Click the **Import** button on the right side of the screen.
9. Click a check in the **Overwrite Existing Templates** box.
10. Click the **Browse** button, and then browse to the location you saved the iApp file.
11. Click the **Upload** button. The iApp is now available for use.

Getting Started with the iApp

To begin the iApp Template, use the following procedure.

To start the iApp template

1. Log on to the BIG-IP system.
2. On the Main tab, expand **iApp**, and then click **Application Services**.
3. Click **Create**. The Template Selection page opens.
4. In the **Name** box, type a name. In our example, we use **smtp-.**
5. From the **Template** list, select **f5.smtp.v1.0.0rc8** (or a newer version if applicable). The SMTP template opens.

Advanced options

If you select **Advanced** from the **Template Selection** list, you see Sync and Failover options for the application. This feature, new to v11, is a part of the Device Management configuration. This functionality extends the existing High Availability infrastructure and allows for clustering, granular control of configuration synchronization and granular control of failover. For more information on Device Management, see the Online Help or product documentation.

1. ***Device Group***
   To select a specific Device Group, clear the **Device Group** check box and then select the appropriate Device Group from the list.
2. ***Traffic Group***
   To select a specific Traffic Group, clear the **Traffic Group** check box and then select the appropriate Traffic Group from the list.

Template Options

This section contains general questions about the way you configure the iApp template.

1. ***Do you want to see inline help?***
   Choose whether you want to see informational and help messages inline throughout the template, or if you would rather hide this inline help. If you are unsure, we recommend having the iApp display the inline help.
   Important and critical notes are always shown, no matter which selection you make.

   - **Yes, show inline help text**
     Select this option to see all available inline help text.
   - **No, do not show inline help text**
     If you are familiar with this iApp template, or with the BIG-IP system in general, select this option to hide the inline help text.

2. ***Which configuration mode do you want to use?***
   Select whether you want to use F5 recommended settings, or have more granular, advanced options presented.

   - **Basic - Use F5's recommended settings**
     In basic configuration mode, options like load balancing method and parent profiles are all set automatically. The F5 recommended settings come as a result of extensive testing with web applications, so if you are unsure, choose Basic.
   - **Advanced - Configure advanced options**
     In advanced configuration mode, you have more control over individual settings and objects, such as server-side optimizations and advanced options like Slow Ramp Time and Priority Group Activation. You can also choose to attach iRules you have previously created to the Application Service. The Advanced option provides more flexibility for experienced users.

     As mentioned, advanced options in the template are marked with the Advanced icon: Advanced. If you are using Basic/F5 recommended settings, you can skip the questions with the Advanced icon.

Network

This section contains questions about your networking configuration.

1. ***What type of network connects clients to the BIG-IP system?*** Advanced
   Choose the type of network that connects your clients to the BIG-IP system. If you choose WAN or LAN, the BIG-IP system uses this information to determine the default TCP optimizations (this default can be changed in the optimization sections at the end of the iApp).

   - **Local area network (LAN)**
     Select this option if most clients are connecting to the BIG-IP system on a LAN. This field is used to determine the appropriate TCP profile which is optimized for LAN clients. In this case, the iApp creates a TCP profile using the *tcp-lan-optimized* parent with no additional modifications.
   - **Wide area network (WAN)**
     Select this option if most clients are connecting to the BIG-IP system over a WAN. This field is used to determine the appropriate TCP profile which is optimized for WAN clients. In this case, the iApp creates a TCP profile using the *tcp-wan-optimized* parent with no additional modifications.

2. ***Which VLANs transport client traffic?*** Advanced
   The BIG-IP system allows you to restrict client traffic to specific VLANs that are present on the system. This can provide an additional layer of security, as you can allow traffic only from the VLANs you choose. The VLAN objects must already be configured on this BIG-IP system before you can select them.

   By default, all VLANs configured on the system are enabled and appear in the Selected list. Use the Move buttons (<<) and (>>) to adjust list membership. Only VLANs in the Selected list are allowed.

3. ***Which type of network connects servers to the BIG-IP system?***
   Choose the type of network that connects your servers to the BIG-IP system. Similar to the question about clients connecting to the BIG-IP system, if you choose WAN or LAN, the system uses this information to determine the default TCP optimizations (this default can be changed in the optimization sections at the end of the iApp).

   - **Local area network (LAN)**
     Select this option if the servers connect to the BIG-IP system on a LAN.

- **Wide area network**
  Select this option if the servers connect to the BIG-IP system over a WAN.

4. *Where will the virtual servers be in relation to the SMTP servers?*
   Select whether your BIG-IP virtual servers are on the same subnet as your SMTP servers, or on different subnets. This setting is used to determine the SNAT (secure NAT) and routing configuration.

   - **BIG-IP virtual server IP and SMTP servers are on the same subnet**
     If the BIG-IP virtual servers and SMTP servers are on the same subnet, SNAT is configured on the BIG-IP virtual server and you must specify the number of concurrent connections.

     a. *How many connections to you expect to each SMTP server?*
        Select whether you expect more or fewer than 64,000 concurrent connections to each server. This answer is used to determine what type of SNAT that system uses. A SNAT is an object that maps the source client IP address in a request to a translation address defined on the BIG-IP device. The system configures SNAT Auto Map (fewer than 64,000) or a SNAT pool (more than 64,000).

        - **Fewer than 64,000 concurrent connections**
          Select this option if you expect fewer than 64,000 concurrent connections per SMTP server. With this option, the system applies SNAT Auto Map, doesn't require any additional IP addresses, as an existing self IP address is used for translation. Continue with the next section.
        - **More than 64,000 concurrent connections**
          Select this option if you have a very large deployment and expect more than 64,000 connections at one time. The iApp creates a SNAT Pool, for which you need one IP address for each 64,000 connections you expect.

          a. *Create a new SNAT pool or use an existing one?*
             If you have already created a SNAT pool on the BIG-IP system, you can select it from the list. Otherwise, the system creates a new SNAT pool with the addresses you specify.

             - **Create a new SNAT pool**
               Select this option (the default) to enable the system to create a new SNAT pool. You must specify the appropriate number of IP addresses in the next question.

               a. *What are the IP addresses you want to use for the SNAT pool?*
                  Specify one otherwise unused IP address for every 64,000 concurrent connections you expect, or fraction thereof. Click **Add** for additional rows. Do not use any self IP addresses on the BIG-IP system.
             - **Select a SNAT pool**
               Select the SNAT pool you created for this deployment from the list.

               Important *If you choose more than 64,000 connections, but do not specify enough SNAT pool address(es), after the maximum connection limit of 64,000 concurrent connections per SMTP server is reached, new requests fail.*

   - **BIG-IP virtual servers and SMTP servers are on different subnets**
     If the BIG-IP virtual servers and servers are on different subnets, the following question appears.

     a. *How have you configured routing on your SMTP servers?*
        If you chose different subnets, this question appears asking whether the SMTP servers use this BIG-IP system's self IP address as their default gateway. Select the appropriate answer.

        - **Servers have a route to clients through the BIG-IP system**
          Choose this option if the servers use the BIG-IP system as their default gateway. In this case, no configuration is needed to support your environment to ensure correct server response handling. Continue with the next section.
        - **Servers do not have a route to clients through the BIG-IP system**
          If the SMTP servers do not use the BIG-IP system as their default gateway, SNAT is configured on the BIG-IP virtual server and you must select the expected number of concurrent connections in the next question.

          a. *How many connections to you expect to each SMTP server?*
             Select whether you expect more or fewer than 64,000 concurrent connections to each server. This answer is used to determine what type of SNAT that system uses. A SNAT is an object that maps the source client IP address in a request to a translation address defined on the BIG-IP device. The system configures SNAT Auto Map (fewer than 64,000) or a SNAT pool (more than 64,000).

- **Fewer than 64,000 concurrent connections**
  Select this option if you expect fewer than 64,000 concurrent connections per SMTP server. With this option, the system applies SNAT Auto Map, doesn't require any additional IP addresses, as an existing self IP address is used for translation. Continue with the *SSL Encryption* section.
- **More than 64,000 concurrent connections**
  Select this option if you have a very large deployment and expect more than 64,000 connections at one time. The iApp creates a SNAT Pool, for which you need one IP address for each 64,000 connections you expect.

  a. *Create a new SNAT pool or use an existing one?*
  If you have already created a SNAT pool on the BIG-IP system, you can select it from the list. Otherwise, the system creates a new SNAT pool with the addresses you specify.

  - **Create a new SNAT pool**
    Select this option (the default) to enable the system to create a new SNAT pool. You must specify the appropriate number of IP addresses in the next question.

    a. *Which IP addresses do you want to use for the SNAT pool?*
    Specify one otherwise unused IP address for every 64,000 concurrent connections you expect, or fraction thereof. Click **Add** for additional rows. Do not use any self IP addresses on the BIG-IP system.

  - **Select a SNAT pool**
    Select the SNAT pool you created for this deployment from the list.

    Important *If you choose more than 64,000 connections, but do not specify enough SNAT pool address(es), after the maximum connection limit of 64,000 concurrent connections per SMTP server is reached, new requests fail.*

Advanced Firewall Manager (BIG-IP AFM)

This section gathers information about BIG-IP Advanced Firewall Manager if you want to use it to protect this implementation. For more information on configuring BIG-IP AFM, see http://support.f5.com/kb/en-us/products/big-ip-afm.html, and then select your version. This section only appears if you have BIG-IP AFM licensed and provisioned on your system.

1. *Do you want to use BIG-IP AFM to protect your application?*
   Choose whether you want to use BIG-IP AFM, F5's network firewall, to secure this SMTP deployment. If you choose to use BIG-IP AFM, you can restrict access to the SMTP virtual server to a specific network or IP address. See the BIG-IP AFM documentation for specific details on configuring AFM.

   - **No, do not use AFM to secure your application**
     Select this option if you do not want to enable BIG-IP AFM at this time. You can always re-enter the template at a later date to enable BIG-IP AFM. Continue with the next section.
   - *Select an existing AFM policy from the list*
     If you already created a BIG-IP AFM policy for this implementation, select it from the list. Continue with ***c***.
   - **Yes, use F5's recommended AFM configuration**
     Select this option if you want to enable BIG-IP AFM using F5's recommended configuration.

     a. *Do you want to restrict access to your application by network or IP address?*
     Choose whether you want to restrict access to the SMTP implementation via the BIG-IP virtual server.

     - **No, do not restrict source addresses (allow all sources)**
       By default, the iApp configures the Advanced Firewall module to accept traffic destined for the SMTP virtual server from all sources. If you do not have a need to restrict access to the virtual server, leave this option selected and then continue with ***b***.
     - **Restrict source addresses**
       Select this option to restrict access to the SMTP virtual server by IP address or network address.

       a. *What IP or network addresses should be allowed to access your application?*
       Specify the IP address or network access that should be allowed access to the SMTP virtual server. You can specify a single IP address, a list of IP addresses separated by spaces (not commas or other punctuation), a range of IP addresses separated by a dash (for example **`192.0.2.10-192.0.2.100`**), or a single network address, such as **`192.0.2.200/24`**.

b. *How do you want to control access to your application from sources with a low reputation score?*
The BIG-IP AFM uses an IP intelligence database to categorize IP addresses coming into the system. Choose what you want the system to do for sources that are attempting to access the SMTP virtual server with a low reputation score. For more information, see the BIG-IP AFM documentation.

Important *You must have an active IP Intelligence license for this feature to function. See https://f5.com/products/modules/ip-intelligence-services for information.*

- **Allow all sources regardless of reputation**
  Select this option to allow all sources, without taking into consideration the reputation score.
- **Reject access from sources with a low reputation**
  Select this option to reject access to the SMTP virtual server from any source with a low reputation score.
- **Allow but log access from sources with a low reputation**
  Select this option to allow access to the SMTP virtual server from sources with a low reputation score, but add an entry for it in the logs.

c. *Would you like to stage a policy for testing purposes?*
Choose whether you want to stage a firewall policy for testing purposes. A staged policy allows you to evaluate the effect a policy has on traffic by analyzing the system logs, without actually modifying traffic based on the firewall rules. You must already have a policy on the system in order to select it.

- **Do not apply a staging policy**
  Select this option if you do not want to apply a logging profile at this time. You can always re-enter the template at a later date to add a logging profile. Continue with the next question.
- *Select an existing policy from the list*
  If you have already created a firewall policy for this implementation, select it from the list. Only policies that already exist on the system appear in the list. To create a new policy, on the Main tab, click **Security > Network Firewall > Policies**. Specific instructions for creating a firewall policy is outside the scope of this iApp and deployment guide.

d. *Which logging profile would you like to use?*
Choose whether you or not you want to use a logging profile for this AFM implementation. You can configure the BIG-IP system to log detailed information about BIG-IP system Network Firewall events and store those logs on the BIG-IP system or a remote logging server (supports syslog and Splunk). If you want to use a logging profile, we recommend creating one outside this template. The list only contains profiles with Network Firewall enabled.

- **Do not apply a logging profile**
  Select this option if you do not want to apply a logging profile at this time. You can always re-enter the template at a later date to add a logging profile. Continue with the next question.
- *Select an existing logging profile from the list*
  If you have already created a logging profile for this implementation, select it from the list. You must create a profile before it is available in the list. To create a logging profile, on the Main tab, click **Security > Event Logs > Logging Profiles**. Specific instructions for creating a logging profile is outside the scope of this iApp and deployment guide. See the online help or the *About Local Logging with the Network Firewall* chapter of the ***BIG-IP Network Firewall: Policies and Implementations*** guide for more information.

SMTP Encryption

In this section, you configure the SMTP encryption options. If SMTP traffic will arrive at the BIG-IP system encrypted, before running the template you should have already imported a certificate and key onto the BIG-IP system. While the BIG-IP system does include a self-signed SSL certificate that can be used internally or for testing, we strongly recommend importing a certificate and key issued from a trusted Certificate Authority for processing client-side SSL.

For information on SSL certificates on the BIG-IP system, see the online help or the *Managing SSL Certificates for Local Traffic* chapter in the ***Configuration Guide for BIG-IP Local Traffic Manager*** *available at http://support.f5.com/kb/en-us.html.*

1. ***How should the BIG-IP system handle incoming SMTP traffic?***
   Choose how SMTP traffic is going to arrive at the BIG-IP system, and what the system should do with the traffic once it arrives.

- **Do nothing (no encrypted SMTP traffic)**
  Select this option if your SMTP traffic will be plaintext to and from both clients and servers.
  Continue with *High Availability on page 14.*
- **Terminate encryption from clients, plaintext to servers (SSL Offload)**
  Choose this method if you want the BIG-IP system decrypt the encrypted traffic, and then send the unencrypted traffic to the servers. You need a valid SSL certificate and key for this method. This scenario also supports STARTTLS, which secures unencrypted client connections without modifying the service port.

  a. *Do you want to support STARTTLS for client connections?*
  Choose whether you want the system to support STARTTLS for client connections. STARTTLS enables unencrypted client connections to be secured.

  - **Yes, allow STARTTLS to secure unencrypted connections**
    Select this option to enable support for STARTTLS to secure encrypted client connections
  - **Yes, require that STARTTLS secures unencrypted connections**
    Select this option to require that STARTTLS is used to secure unencrypted client connections.
  - **No, do not include STARTTLS support for unencrypted connections**
    Select this option if you do not want to enable STARTTLS support. In this case, unencrypted client connections are not modified.

  b. *Which Client SSL profile do you want to use?*
  Select whether you want the iApp to create a new Client SSL profile, or if you have already created a Client SSL profile which contains the appropriate SSL certificate and key.

  Unless you have requirements for configuring specific Client SSL settings, we recommend allowing the iApp to create a new profile. To select a profile from the list, it must already be present on the BIG-IP system. Creating a custom profile is not a part of this template; see **Local Traffic** >> **Profiles** : **SSL** : **Client** to create a Client SSL profile. To select any new profiles you create, you need to restart or reconfigure this template.

  - *Select an existing Client SSL profile*
    If you created a Client SSL profile for this implementation, select it from the list. If you select an existing Client SSL profile, the rest of the questions in this section disappear. Continue with the next section.
  - **Create a new Client SSL profile**
    Select this option for the iApp to create a new Client SSL profile

    a. *Which SSL certificate do you want to use?*
    Select the SSL certificate you imported for this implementation.

    b. *Which SSL private key do you want to use?*
    Select the associated SSL private key.

    c. *Which intermediate certificate do you want to use?* Advanced
    If your deployment requires an intermediate or chain certificate, select the appropriate certificate from the list. Immediate certificates are intended to create a chain of trust between the CA that signed the certificate and the CA that is already trusted by the recipient of the certificate. This allows the recipient to verify the validity of the certificates presented, even when the signing CA is unknown.

- **Terminate SSL from clients, re-encrypt to servers (SSL Bridging)**
  Choose this method if you want the BIG-IP system to terminate SSL to process it, and then re-encrypt the traffic to the servers (SSL Bridging). You need a valid SSL certificate and key for the client-side, and optionally for the server-side (see #d). This scenario supports client-side STARTTLS for securing unencrypted client connections. If you select this option, the assumption is that server-side connections will require SSL/TLS (SMTPS), typically on port 465.

  a. *Do you want to support STARTTLS for securing client connections?*
  Choose whether you want the system to support STARTTLS for securing client connections. STARTTLS enables unencrypted client connections to be secured.

  - **Yes, allow STARTTLS to secure unencrypted connections**
    Select this option to enable support for STARTTLS to secure encrypted client connections
  - **Yes, require that STARTTLS secures unencrypted connections**
    Select this option to require that STARTTLS is used to secure unencrypted client connections.

- **No, do not include STARTTLS support for unencrypted connections**
  Select this option if you do not want to enable STARTTLS support. Unencrypted client connections will not be modified.

b. *Which Client SSL profile do you want to use?* **Advanced**
Select whether you want the iApp to create a new Client SSL profile, or if you have already created a Client SSL profile which contains the appropriate SSL certificate and key.

Unless you have requirements for configuring specific Client SSL settings, we recommend allowing the iApp to create a new profile. To select a profile from the list, it must already be present on the BIG-IP system. Creating a custom profile is not a part of this template; see **Local Traffic** >> **Profiles** : **SSL** : **Client** to create a Client SSL profile. To select any new profiles you create, you need to restart or reconfigure this template.

- *Select an existing Client SSL profile*
  If you created a Client SSL profile for this implementation select it from the list. If you select an existing Client SSL profile, the rest of the questions in this section disappear. Continue with the next section.
- **Create a new Client SSL profile**
  Select this option for the iApp to create a new Client SSL profile

  a. *Which SSL certificate do you want to use?*
  Select the SSL certificate you imported for this implementation.

  b. *Which SSL private key do you want to use?*
  Select the associated SSL private key.

  c. *Which intermediate certificate do you want to use?* **Advanced**
  If your deployment requires an intermediate or chain certificate, select the appropriate certificate from the list.

  Immediate certificates are intended to create a chain of trust between the CA that signed the certificate and the CA that is already trusted by the recipient of the certificate. This allows the recipient to verify the validity of the certificates presented, even when the signing CA is unknown.

c. *Which Server SSL profile do you want to use?*
Select whether you want the iApp to create the F5 recommended Server SSL profile, or if you want to choose a Server SSL profile you already created. In this scenario, the BIG-IP system is acting as an SSL client and by default, we assume the servers do not expect the BIG-IP system to present its client certificate on behalf of clients traversing the virtual server. If your servers expect the BIG-IP system to present a client certificate, you must create a custom Server SSL profile with the appropriate certificate and key.

The default, F5 recommended Server SSL profile uses the serverssl parent profile. For information about the ciphers used in the Server SSL profile, see *http://support.f5.com/kb/en-us/solutions/public/8000/800/sol8802.html*.

- **Forward encrypted traffic without decryption (SSL pass-through)**
  Choose this method if you do not want the BIG-IP system to do anything with encrypted traffic and simply send it to the SMTP servers. This is similar to SSL bridging, although in this case the system does not decrypt then re-encrypt the traffic, it only sends traffic through a Performance (Layer 4) virtual server and then on to the servers without modification.

a. *Do you require STARTTLS for server connections?*
Choose whether you your SMTP server require STARTTLS for server connections. Select Yes if your SMTP servers require STARTTLS, or no if they use TLS or SMTPS without STARTTLS.

- **No, the SMTP servers do not require STARTTLS**
  Select this option if your SMTP servers do not require STARTTLS.

  a. *Do you use TLS (STARTTLS) or SSL (SMTPS) for server-side encryption setup?*
  Choose whether your SMTP servers require TLS or SSL for server connections. Legacy deployments on port 465 usually require SSL (SMTPS), while deployments on port 587 require TLS. Your choice here is used in the health monitor configuration.

  - **The SMTP servers use STARTTLS (recommended)**
    Select this option if your SMTP servers require TLS. Deployments on port 587 require TLS, while legacy deployments on port 465 usually require SSL (SMTPS).
  - **The SMTP servers require SSL (SMTPS)**
    Select this option if your SMTP servers require SSL (SMTPS). This is typically for legacy deployments on port 465.

- **Yes, the SMTP servers require STARTTLS**
  Select this option if your SMTP servers require STARTTLS. Continue with the following section.

High Availability

This section gathers information about your SMTP deployment that is used in the BIG-IP virtual server and load balancing pool if you did not deploy the BIG-IP APM.

1. ***What IP address do you want to use for the virtual server?***
   Type the IP address you want to use for the BIG-IP virtual server. This is the address clients use (or a DNS entry resolves to this address) to access the SMTP deployment via the BIG-IP system.

2. ***What is the associated service port?***
   Type the port number to use for the BIG-IP virtual server. For SMTP deployments, this is typically 25 or 587. The default port listed here depends on how you answered the questions in the SSL Encryption section.

3. ***Do you want to create a new pool or use an existing one?***
   A load balancing pool is a logical set of servers, grouped together to receive and process traffic. When clients attempt to access the application via the BIG-IP virtual server, the BIG-IP system distributes requests to any of the servers that are members of that pool.

   - *Select an existing pool*
     If you have already created a pool for your SMTP servers, you can select it from the list.
     If you do select an existing pool, all of the rest of the questions in this section disappear.
   - **Create a new pool**
     Leave this default option to create a new load balancing pool and configure specific options.

     a. *Which load balancing method do you want to use?* Advanced
     Specify the load balancing method you want to use for this SMTP server pool. We recommend the default, **Least Connections (member)**.

     b. *Should the BIG-IP system queue TCP requests?*
     Select whether you want the BIG-IP system to queue TCP requests. TCP request queuing provides the ability to queue connection requests that exceed the capacity of connections for a pool, as determined by the connection limit. Consequently, instead of dropping connection requests that exceed the capacity of a pool, TCP request queuing enables those connection requests to reside within a queue according to defined conditions until capacity becomes available. For more information on TCP Request Queuing, see the *Preventing TCP Connection Requests From Being Dropped* chapter in the ***BIG-IP Local Traffic Manager: Implementations*** guide, available on support.f5.com.

     Important *TCP Request Queuing is an advanced feature and should be used only if you understand how it will affect your deployment, including application behavior and BIG-IP performance.*
     If you enable TCP Request Queuing, you must have a Connection Limit set on at least one of the nodes when configuring the Address/Port for the nodes.

     - **Do not enable TCP request queuing (recommended)**
       Select this option if you do not want the BIG-IP system to queue TCP requests.
     - **Yes, enable TCP request queuing**
       Select this option if you want to enable TCP request queuing on the BIG-IP system.

       a. *What is the maximum number of TCP requests for the queue?*
       Type the maximum number of requests you want to queue. We do ***not*** recommend using 0, which means unlimited and is only constrained by available memory.

       b. *How many milliseconds should requests remain in the queue?*
       Type a number of milliseconds for the TCP request timeout value.

     c. *Use a Slow Ramp time for newly added servers?* Advanced
     With Slow Ramp, the BIG-IP system gradually adds connections to a newly-enabled or newly-added SMTP server over a time period you specify, rather than sending a full proportion of the traffic immediately. Slow Ramp is essential when using the Least Connections load balancing method (our recommended method for SMTP servers), as the BIG-IP system would otherwise send all new connections to a new server immediately, potentially overwhelming that server.

Select whether you want to use a Slow Ramp time.

- **Use Slow Ramp**
  Select this option for the system to implement Slow Ramp time for this pool.

  a. *How many seconds should Slow Ramp time last?*
  Specify a duration in seconds, for Slow Ramp. The time period you select for Slow Ramp is highly dependent on the speed of your server hardware and the behavior of your web services. The default setting of 300 seconds (5 minutes) is very conservative in most cases.

- **Do not use Slow Ramp**
  Select this option if you do not want to use Slow Ramp. If you select this option, we recommend you do not use the Least Connections load balancing method.

d. *Do you want to give priority to specific groups of servers?* Advanced
Select whether you want to use Priority Group Activation. Priority Group Activation allows you to segment your servers into priority groups. With Priority Group Activation, the BIG-IP system load balances traffic according to the priority number you assign to the pool members. A higher number indicates higher priority. Traffic is only sent to the servers with the highest priority, unless the number of available servers in that priority group falls below the value you specify as the minimum. The BIG-IP then sends traffic to the group of servers with the next highest priority, and so on.

- **Do not use Priority Group Activation (recommended)**
  Select this option if you do not want to enable Priority Group Activation.

- **Use Priority Group Activation**
  Select this option if you want to enable Priority Group Activation.
  You must add a priority to each server in the Priority box described in #c.

  a. *What is the minimum number of active members for each priority group?*
  Specify the minimum number of servers that must be active to continue sending traffic to the priority group. If the number of active servers falls below this minimum, traffic will be sent to the group of servers with the next highest priority group number.

e. *Which servers are a part of this pool?*
Specify the IP address(es) of your SMTP servers. If you have existing nodes on this BIG-IP system, you can select them from the list, otherwise type the addresses. You can optionally add a Connection Limit. If you enabled Priority Group Activation, you must also specify a Priority for each device. Click **Add** to include additional servers.

Application Health

In this section, you answer questions about how you want to implement application health monitoring on the BIG-IP system.

1. ***Create a new health monitor or use an existing one?***
   Application health monitors are used to verify the content that is returned by a request. The system uses these monitors to ensure traffic is only sent to available SMTP servers.

   Unless you have requirements for configuring other options not in the following list of questions, we recommend allowing the iApp to create a new monitor. Creating a custom health monitor is not a part of this template; see **Local Traffic** >> **Monitors**. To select any new monitors you create, you need to restart or reconfigure this template.

   - *Select the monitor you created from the list*
     If you manually created the health monitor, select it from the list. Continue with the next section.

   - **Create a new health monitor**
     If you want the iApp to create a new monitor, continue with the following.

     a. *What is the domain for which your SMTP servers will accept mail?*
     Type the fully-qualified name of the domain for which the SMTP server(s) will accept messages.

     b. *What type of service check should the BIG-IP perform?*
     Specify the authentication and message submission, if any, that the SMTP monitor should use.

     - **No message submitted (no auth)**
       Select this option if you do not want the BIG-IP system to perform a health check that requires authentication, and you do not want the BIG-IP system to submit a message as a part of the health check. Continue with c.

- **SMTP message submitted (no auth)**
  Select this option if you want the BIG-IP system to perform a health check that requires authentication, but you do not want the BIG-IP system to submit a message as a part of the health check. In this case, the monitor is successful if the mail server successfully authenticates the connection.

  a. *What text would you like to include in the message body?*
  Type the text you want to use in the body of the message sent to the SMTP server. The message text is not used by the BIG-IP system, but can be useful for filtering or other purposes.

  b. *From what email address should the message be submitted?*
  Type the email address you want the message to be from for the health check. The monitor checks to make sure the message is from this address.

  c. *To what email address should the message be submitted?*
  Type the email address to which you want the message the sent. The monitor checks to make sure the message is going to this address.

c. *Would you like to specify a custom receive string?*
Choose whether you want to specify a custom receive string. The receive string is the response the system expects to be returned from the server in order for the health check to be successful. If you do not specify a receive string, the server is marked Up if any response is returned.

- **No, use the standard monitor receive string**
  Select this option if you do not want to specify a custom receive string. Continue with d.
- **Yes, use a custom monitor receive string**
  Select this option to use a custom receive string. You must specify the string in the following question.

  a. *What would you like the receive string to be?*
  Type the receive string you want to use. The server will only be marked up if this specify string is returned from the health monitor send string.

d. *How many seconds should pass between health checks?*
Specify how long the system should wait between each health check. This is used as the Interval setting for the monitor. We recommend the default of 30 seconds.

Client Optimization

In this section, you answer a question on how you want to optimize client-side connections. This determines the type of TCP profile the iApp assigns to the virtual server. This entire section only appears if you selected the Advanced configuration mode.

1. ***How do you want to optimize client-side connections?*** Advanced
   The client-side TCP profile optimizes the communication between the BIG-IP system and the server by controlling the behavior of the traffic which results in higher transfer rates, improved connection reliability and increased bandwidth efficiency.

   Unless you have requirements for configuring specific TCP optimization settings, we recommend allowing the iApp to create a new profile. Creating a custom profile is not a part of this template; see **Local Traffic** >> **Profiles** : **Protocol : TCP** to create a TCP profile. To select any new profiles you create, you need to restart or reconfigure this template.

   - **New profile based on tcp-wan-optimized (recommended)**
     Select this option to have the system create the recommended TCP profile optimized for WAN connections.
   - *Select the TCP profile you created from the list*
     If you created a custom TCP profile for the client-side connections, select it from the list.

Server Optimization

In this section, you answer a question on how you want to optimize server-side connections. This determines the type of TCP profile the iApp assigns to the virtual server. This entire section only appears if you selected the Advanced configuration mode.

1. ***How do you want to optimize server-side connections?*** Advanced
   The client-side TCP profile optimizes the communication between the BIG-IP system and the server by controlling the behavior of the traffic which results in higher transfer rates, improved connection reliability and increased bandwidth efficiency.

   Unless you have requirements for configuring specific TCP optimization settings, we recommend allowing the iApp to create a new profile. Creating a custom profile is not a part of this template; see **Local Traffic** >> **Profiles** : **Protocol : TCP** to create a TCP profile. To select any new profiles you create, you need to restart or reconfigure this template.

   - **New profile based on tcp-lan-optimized (recommended)**
     Select this option to have the system create the recommended TCP profile optimized for LAN connections.
   - *Select the TCP profile you created from the list*
     If you created a custom TCP profile for server-side connections, select it from the list.

iRules

In this section, you can add custom iRules to the SMTP deployment. This section is available only if you selected Advanced mode.

iRules are a scripting language that allows an administrator to instruct the system to intercept, inspect, transform, direct and track inbound or outbound application traffic. An iRule contains the set of instructions the system uses to process data flowing through it, either in the header or payload of a packet.

1. ***Do you want to add any custom iRules to the virtual server?*** Advanced
   Select if have preexisting iRules you want to add to your SMTP implementation.

   ⚠ ***Warning*** *Improper use or misconfiguration of an iRule can result in unwanted application behavior and poor performance of your BIG-IP system. We recommended you verify the impact of an iRule prior to deployment in a production environment.*

   If you do not want to add any iRules to the configuration, continue with the following section.

   If you have iRules you want to attach to the virtual server the iApp creates for your SMTP servers, from the **Options** box, click the name of the applicable iRule(s) and then click the Add (**<<**) button to move them to the **Selected** box.

Finished

Review the answers to your questions. When you are satisfied, click the **Finished** button. The BIG-IP system creates the relevant objects for the SMTP application.

Next steps

After completing the iApp Template, the BIG-IP Application Services page opens for the SMTP service you just created. To see the list of all the configuration objects created to support the application, on the Menu bar, click **Components**. The complete list of all related objects opens. You can click individual objects to see the settings.

Once the objects have been created, you are ready to use the new deployment.

Modifying DNS settings to use the BIG-IP virtual server address

Before sending traffic to the BIG-IP system, your DNS administrator may need to modify any DNS entries for the SMTP implementation to point to the BIG-IP system's virtual server address.

Modifying the iApp configuration

The iApp Application Service you just created can be quickly and easily modified if you find it necessary to make changes to the configuration. The Strict Updates feature of the iApp prevents users from manually modifying the iApp configuration (Strict Updates can be turned off, but use extreme caution). iApp allows you to re-enter the template, make changes, and then update the template. The modifications are automatically made to any of the associated objects.

To modify the configuration

1. On the Main tab, expand **iApp** and then click **Application Services**.
2. Click the name of your SMTP Service from the list.
3. On the Menu bar, click **Reconfigure**.
4. Make the necessary modifications to the template.
5. Click the **Finished** button.

Viewing statistics

You can easily view a number of different statistics on the BIG-IP system related to the configuration objects created by the iApp template.

Object-level statistics

If you want to view object-level statistics, use the following procedure.

To view object-level statics

1. On the Main tab, expand **Overview**, and then click **Statistics**.
2. From the **Statistics Type** menu, you can select **Virtual Servers** to see statistics related to the virtual servers.
3. You can also choose **Pools** or **Nodes** to get a closer look at the traffic.
4. To see Networking statistics in a graphical format, click **Dashboard**.

For more information on viewing statistics on the BIG-IP system, see the online help or product documentation.

Appendix A: Manually configuring the BIG-IP system

The following tables contains a list of BIG-IP system configuration objects along with any non-default settings you should configure as a part of this deployment scenario. 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.

Configuring the BIG-IP system pools and virtual servers for SMTP

Use this section to configure the remaining objects on the BIG-IP system, depending on your scenario.

- *Scenario 1: Standard unencrypted SMTP on this page*
- *Scenario 2: SSL offload*
- *Scenario 3: SSL Bridging on page 21*
- *Scenario 4: SSL Passthrough on page 22*
- *Scenario 5: Encrypt on server-side only on page 23*
- *Scenario 6: SMTP with STARTTLS on the client-side, and unencrypted SMTP on the server side on page 24*

Scenario 1: Standard unencrypted SMTP

Use the following guidance to configure the BIG-IP for unencrypted SMTP. This table contains a list of configuration objects along with any non-default settings you should configure as a part of this deployment. 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.

Health Monitors (*Main tab > Local Traffic > Monitors*)	Choose the health monitor appropriate for your deployment
SMTP Monitor *(for monitoring server-side unencrpyted SMTP only)*	
Name	Type a unique name
Type	**SMTP**
Interval	**30** (recommended)
Timeout	**91** (recommended)
Domain	The FQDN of your email domain
External monitor: *Use this if you require a monitor that provides authentication or checks for other server responses*	
Important: An External monitor uses a script on the BIG-IP system a part of the check to monitor the health of the servers (see *Configuring the External health monitors on page 31* for complete details). Before creating this type of monitor, you must import the appropriate script onto the BIG-IP system. For this scenario, you can use the following monitors: *1) Service check for unencrypted SMTP requiring authentication but without submitting a message on page 31* *2) Service check for unencrypted SMTP submitting a message but not requiring authentication on page 32* *3) Service check for unencrypted SMTP submitting a message and requiring authentication on page 33*	
Name	Type a unique name
Type	**External**
Interval	**30** (recommended)
Timeout	**91** (recommended)
External Program	Select the script you imported onto the BIG-IP system. See the Important note above for details.
Variables	***Name*** — ***Value***
	USER *(for monitor 1 and 3 only)* — The account name associated with a mailbox.
	PASSWORD *(for monitor 1 and 3 only)* — The password for the user account
	FROM *(for monitor 2 and 3 only)* — The sender's email address
	RCPT *(for monitor 2 and 3 only)* — The recipient's mailbox address
Pools (*Main tab > Local Traffic > Pools*)	
Name	Type a unique name
Health Monitor	Select either the SMTP or External the monitor you created
Load Balancing Method	**Least Connections (member)**
Address	Type the IP Address of your SMTP server
Service Port	**25** Click **Add** to repeat Address and Service Port for all nodes
Virtual Servers (*Main tab > Local Traffic > Virtual Servers*)	
Name	Type a unique name.
Destination Address	Type the IP address for this virtual server.
Service Port	**25**
Source Address Translation	If you created a SNAT Pool, select it here, otherwise, select Auto Map to use SNAT, or leave it at None if your SMTP deployment performs SPAM or other source IP based reputation filtering behind the BIG-IP LTM.
Default Pool	Select the pool you created

You can continue with *Configuring the BIG-IP Advanced Firewall Module to secure your SMTP deployment on page 26.*

Scenario 2: SSL offload

Use the following guidance to configure the BIG-IP for offloading SSL/TLS traffic from the SMTP servers. This table contains a list of configuration objects along with any non-default settings you should configure as a part of this deployment. 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.

Health Monitors (*Main tab > Local Traffic > Monitors*)	
SMTP Monitor *(for monitoring server-side unencrpyted SMTP only)*	
Name	Type a unique name
Type	**SMTP**
Interval	**30** (recommended)
Timeout	**91** (recommended)
Domain	The FQDN of your email domain
External monitor: *Use this if you require a monitor that provides authentication or checks for other server responses*	
Important: An External monitor uses a script on the BIG-IP system a part of the check to monitor the health of the servers (see *Configuring the External health monitors on page 31* for complete details). Before creating this type of monitor, you must import the appropriate script onto the BIG-IP system. For this scenario, you can use the following monitors: *1) Service check for unencrypted SMTP requiring authentication but without submitting a message on page 31* *2) Service check for unencrypted SMTP submitting a message but not requiring authentication on page 32* *3) Service check for unencrypted SMTP submitting a message and requiring authentication on page 33*	
Name	Type a unique name
Type	**External**
Interval	**30** (recommended)
Timeout	**91** (recommended)
External Program	Select the script you imported onto the BIG-IP system. See the Important note above for details.
Variables	***Name*** / ***Value***
	USER *(for monitor 1 and 3 only)* — The account name associated with a mailbox. **PASSWORD** *(for monitor 1 and 3 only)* — The password for the user account **FROM** *(for monitor 2 and 3 only)* — The sender's email address **RCPT** *(for monitor 2 and 3 only)* — The recipient's mailbox address
Pools (*Main tab > Local Traffic > Pools*)	
Name	Type a unique name
Health Monitor	Select either the SMTP or External the monitor you created
Load Balancing Method	**Least Connections (member)**
Address	Type the IP Address of your SMTP server
Service Port	**25** Click **Add** to repeat Address and Service Port for all nodes
Profiles (*Main tab > Local Traffic > Profiles*)	
Name	Type a unique name
Parent Profile	**clientssl**
Certificate and Key	Select the Certificate and Key you imported in *Importing SSL certificates on page 5* from the associated list.
Virtual Servers (*Main tab > Local Traffic > Virtual Servers*)	
Name	Type a unique name.
Destination Address	Type the IP address for this virtual server.
Service Port	**587**
SSL Profile (Client)	Select the Client SSL profile you created.
Source Address Translation	If you created a SNAT Pool using the guidance in *SNAT Pool considerations and configuration on page 5,* select it here, otherwise, select Auto Map to use SNAT, or leave it at None if your SMTP deployment performs SPAM or other source IP based reputation filtering behind the BIG-IP LTM.
Default Pool	Select the pool you created.

This completes the BIG-IP LTM configuration for this scenario. You can continue with *Configuring the BIG-IP Advanced Firewall Module to secure your SMTP deployment on page 26.*

Scenario 3: SSL Bridging

Use the following guidance to configure the BIG-IP for offloading SSL/TLS traffic from the SMTP servers. This table contains a list of configuration objects along with any non-default settings you should configure as a part of this deployment. 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.

Health Monitors (*Main tab > Local Traffic > Monitors*)		
Important: An External monitor uses a script on the BIG-IP system a part of the check to monitor the health of the servers (see *Configuring the External health monitors on page 31* for complete details). Before creating this type of monitor, you must import the appropriate script onto the BIG-IP system. For this scenario, you can use the following monitors: *4) Service check for SSL(SMTPS) encrypted SMTP with no authentication or message submission on page 34* *5) Service check for SSL (SMTPS) encrypted SMTP with authentication but without submitting a message on page 35* *6) Service check for TLS/SSL (SMTPS) encrypted SMTP submitting a message but no authentication on page 36* *7) Service check for TLS/SSL (SMTPS) encrypted SMTP with authentication and submitting a message on page 37*		
Name	Type a unique name	
Type	**External**	
Interval	**30** (recommended)	
Timeout	**91** (recommended)	
External Program	Select the script you imported onto the BIG-IP system. See the Important note above for details.	
	Name	***Value***
Variables *(Not applicable to monitor 7)*	**USER** *(for monitor 4 and 6 only)* **PASSWORD** *(for monitor 4 and 6 only)* **FROM** *(for monitor 5 and 6 only)* **RCPT** *(for monitor 5 and 6 only)*	The account name associated with a mailbox. The password for the user account The sender's email address The recipient's mailbox address
Pools (*Main tab > Local Traffic > Pools*)		
Name	Type a unique name	
Health Monitor	Select the External the monitor you created	
Load Balancing Method	**Least Connections (member)**	
Address	Type the IP Address of your SMTP server	
Service Port	**587** Click **Add** to repeat Address and Service Port for all nodes	
Profiles (*Main tab > Local Traffic > Profiles*)		
Client SSL profile (*Profiles-->SSL*)	***Name***	Type a unique name
	Parent Profile	**clientssl**
	Certificate and Key	Select the Certificate and Key you imported in *Importing SSL certificates on page 5* from the associated list.
Server SSL profile (*Profiles-->SSL*)	***Name***	Type a unique name
	Parent Profile	**serverssl** For information about the ciphers used in the Server SSL profile, see *http://support.f5.com/kb/en-us/solutions/public/8000/800/sol8802.html*.
Virtual Servers (*Main tab > Local Traffic > Virtual Servers*)		
Name	Type a unique name.	
Destination Address	Type the IP address for this virtual server.	
Service Port	**587**	
SSL Profile (Client)	Select the Client SSL profile you created	
SSL Profile (Server)	Select the Server SSL profile you created	
Source Address Translation	If you created a SNAT Pool using the guidance in *SNAT Pool considerations and configuration on page 5,* select it here, otherwise, select Auto Map to use SNAT, or leave it at None if your SMTP deployment performs SPAM or other source IP based reputation filtering behind the BIG-IP LTM.	
Default Pool	Select the pool you created above	

This completes the BIG-IP LTM configuration for this scenario. You can continue with *Configuring the BIG-IP Advanced Firewall Module to secure your SMTP deployment on page 26.*

Scenario 4: SSL Passthrough

Use the following guidance to configure the BIG-IP system for passing encrypted SMTP traffic without processing it. This table contains a list of configuration objects along with any non-default settings you should configure as a part of this deployment. 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.

Health Monitors (*Main tab > Local Traffic > Monitors*)	
Important: An External monitor uses a script on the BIG-IP system a part of the check to monitor the health of the servers (see *Configuring the External health monitors on page 31* for complete details). Before creating this type of monitor, you must import the appropriate script onto the BIG-IP system. For this scenario, you can use the following monitors: - *4) Service check for SSL(SMTPS) encrypted SMTP with no authentication or message submission on page 34* - *5) Service check for SSL (SMTPS) encrypted SMTP with authentication but without submitting a message on page 35* - *6) Service check for TLS/SSL (SMTPS) encrypted SMTP submitting a message but no authentication on page 36* - *7) Service check for TLS/SSL (SMTPS) encrypted SMTP with authentication and submitting a message on page 37*	
Name	Type a unique name
Type	**External**
Interval	**30** (recommended)
Timeout	**91** (recommended)
External Program	Select the script you imported onto the BIG-IP system. See the Important note above for details.
Variables *(Not applicable to monitor 7)*	***Name*** / ***Value*** **USER** *(for monitor 4 and 6 only)* — The account name associated with a mailbox. **PASSWORD** *(for monitor 4 and 6 only)* — The password for the user account **FROM** *(for monitor 5 and 6 only)* — The sender's email address **RCPT** *(for monitor 5 and 6 only)* — The recipient's mailbox address
Pools (*Main tab > Local Traffic > Pools*)	
Name	Type a unique name
Health Monitor	Select the External the monitor you created
Load Balancing Method	**Least Connections (member)**
Address	Type the IP Address of your SMTP server
Service Port	**587** Click **Add** to repeat Address and Service Port for all nodes
Virtual Servers (*Main tab > Local Traffic > Virtual Servers*)	
Name	Type a unique name.
Destination Address	Type the IP address for this virtual server.
Service Port	**587**
Source Address Translation	If you created a SNAT Pool using the guidance in *SNAT Pool considerations and configuration on page 5,* select it here, otherwise, select Auto Map to use SNAT, or leave it at None if your SMTP deployment performs SPAM or other source IP based reputation filtering behind the BIG-IP LTM.
Default Pool	Select the pool you created

This completes the BIG-IP LTM configuration for this scenario. You can continue with *Configuring the BIG-IP Advanced Firewall Module to secure your SMTP deployment on page 26.*

Scenario 5: Encrypt on server-side only

Use the following guidance to configure the BIG-IP for accepting unencrypted SMTP traffic and encrypting it before sending to the SMTP servers. As mentioned in the introduction, this is not a common configuration, however it is used when configuring the remote end of BIG-IP AAM symmetric optimization deployment. Configuring symmetric optimization is outside the scope of this document, see the BIG-IP AAM manuals for specific information.

The following table contains a list of configuration objects along with any non-default settings you should configure as a part of this deployment. 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.

Health Monitors (*Main tab > Local Traffic > Monitors*)

Important: An External monitor uses a script on the BIG-IP system a part of the check to monitor the health of the servers (see *Configuring the External health monitors on page 31* for complete details). Before creating this type of monitor, you must import the appropriate script onto the BIG-IP system. For this scenario, you can use the following monitors:

- *4) Service check for SSL(SMTPS) encrypted SMTP with no authentication or message submission on page 34*
- *5) Service check for SSL (SMTPS) encrypted SMTP with authentication but without submitting a message on page 35*
- *6) Service check for TLS/SSL (SMTPS) encrypted SMTP submitting a message but no authentication on page 36*
- *7) Service check for TLS/SSL (SMTPS) encrypted SMTP with authentication and submitting a message on page 37*

Name	Type a unique name
Type	**External**
Interval	**30** (recommended)
Timeout	**91** (recommended)
External Program	Select the script you imported onto the BIG-IP system. See the Important note above for details.

Variables (*Not applicable to monitor 7*)	***Name***	***Value***
	USER *(for monitor 4 and 6 only)*	The account name associated with a mailbox.
	PASSWORD *(for monitor 4 and 6 only)*	The password for the user account
	FROM *(for monitor 5 and 6 only)*	The sender's email address
	RCPT *(for monitor 5 and 6 only)*	The recipient's mailbox address

Pools (*Main tab > Local Traffic > Pools*)

Name	Type a unique name
Health Monitor	Select the External the monitor you created
Load Balancing Method	**Least Connections (member)**
Address	Type the IP Address of your SMTP server
Service Port	**587** Click **Add** to repeat Address and Service Port for all nodes

Virtual Servers (*Main tab > Local Traffic > Virtual Servers*)

Name	Type a unique name
Parent Profile	**serverssl**
Name	Type a unique name.
Destination Address	Type the IP address for this virtual server.
Service Port	**587**
SSL Profile (Server)	Select the Client SSL profile you created
Source Address Translation	If you created a SNAT Pool using the guidance in *SNAT Pool considerations and configuration on page 5,* select it here, otherwise, select Auto Map to use SNAT, or leave it at None if your SMTP deployment performs SPAM or other source IP based reputation filtering behind the BIG-IP LTM.
Default Pool	Select the pool you created above

This completes the BIG-IP LTM configuration for this scenario. You can continue with *Configuring the BIG-IP Advanced Firewall Module to secure your SMTP deployment on page 26.*

Scenario 6: SMTP with STARTTLS on the client-side, and unencrypted SMTP on the server side

In this scenario, client-side connections are on port 25, but the clients negotiate encryption using the STARTTLS command. On the server-side, connections are on unencrypted port 25.

This table contains a list of configuration objects along with any non-default settings you should configure as a part of this deployment. 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.

Health Monitors (*Main tab > Local Traffic > Monitors*)		
SMTP Monitor *(simple for monitoring server-side unencrpyted SMTP only)*		
Name	Type a unique name	
Type	**SMTP**	
Interval	**30** (recommended)	
Timeout	**91** (recommended)	
Domain	The FQDN of your email domain	
External monitor: *Use this if you require a monitor that provides authentication or checks for other server responses*		
Important: An External monitor uses a script on the BIG-IP system a part of the check to monitor the health of the servers (see *Configuring the External health monitors on page 31* for complete details). Before creating this type of monitor, you must import the appropriate script onto the BIG-IP system. For this scenario, you can use the following monitors: - *8) Service check for SMTP with STARTTLS with no authentication or message submission on page 38* - *9) Service check for SMTP with STARTTLS and authentication, but without submitting a message on page 39* - *10) Service check for SMTP with STARTTLS (required), submitting a message but no authentication on page 40*		
Name	Type a unique name	
Type	**External**	
Interval	**30** (recommended)	
Timeout	**91** (recommended)	
External Program	Select the script you imported onto the BIG-IP system. See the Important note above for details.	
Variables *(Not applicable to monitor 8)*	***Name***	***Value***
	USER *(for monitor 9 only)*	The account name associated with a mailbox.
	PASSWORD *(for monitor 9 only)*	The password for the user account
	FROM *(for monitor 10 only)*	The sender's email address
	RCPT *(for monitor 10 only)*	The recipient's mailbox address
Pools (*Main tab > Local Traffic > Pools*)		
Name	Type a unique name	
Health Monitor	Select either the SMTP or External the monitor you created	
Load Balancing Method	**Least Connections (member)**	
Address	Type the IP Address of your SMTP server	
Service Port	**25** Click **Add** to repeat Address and Service Port for all nodes	
Profiles (*Main tab > Local Traffic > Profiles*)		
Client SSL profile (*Profiles-->SSL*)	***Name***	Type a unique name
	Parent Profile	**clientssl**
	Certificate and Key	Select the Certificate and Key you imported in *Importing SSL certificates on page 5* from the lists.
SMTPS profile (*Profiles-->SSL*)	***Note:*** *The SMTPS profile for STARTTLS support is only available in BIG-IP v11.5 and later. For an unsupported workaround for v11.4, see Using STARTTLS in BIG-IP v11.4 following this table.*	
	Name	Type a unique name
	Parent Profile	**smtps**
	STARTTLS Activation Mode	**Require** (recommended). If necessary, you can change the activation mode, however in most cases, you should leave the value at Require (default) which forces clients to only connect using STARTTLS.

Virtual Servers (*Main tab > Local Traffic > Virtual Servers*)	
Name	Type a unique name.
Destination Address	Type the IP address for this virtual server.
Service Port	**25**
SSL Profile (Client)	Select the Client SSL profile you created
SMTPS Profile	If using v11.5, select the SMTPS profile you created ***Important:*** *You cannot select the SMTPS profile until you have selected the Client SSL profile.*
Source Address Translation	If you created a SNAT Pool using the guidance in *SNAT Pool considerations and configuration on page 5,* select it here, otherwise, select Auto Map to use SNAT, or leave it at None if your SMTP deployment performs SPAM or other source IP based reputation filtering behind the BIG-IP LTM.
Default Pool	Select the pool you created above

Using STARTTLS in BIG-IP v11.4

If you are using BIG-IP version 11.4 and want to support STARTTLS on the BIG-IP system, you need to create an iRule and attach it to the virtual server. It is important to note that using STARTTLS on BIG-IP version 11.4 is not a supported configuration. See *https://devcentral.f5.com/articles/iruleology-ndashsmtp-start-tls* for specific details.

Configuring the BIG-IP Advanced Firewall Module to secure your SMTP deployment

This section describes how to use BIG-IP AFM, F5's Network Firewall module, to secure your SMTP deployment. BIG-IP AFM is particularly useful if you want to restrict SMTP access to specific clients or networks.

Network Firewall settings

When configuring the BIG-IP Advanced Firewall Manager, you may want to configure your BIG-IP system to drop all traffic that you have not specifically allowed with firewall rules. This in known as ***firewall mode***. By default, your BIG-IP system is set to default-accept, or ***ADC mode***. Instructions for configuring your BIG-IP system, and the implications to consider, can be found at *http://support.f5.com/kb/en-us/products/big-ip-afm/manuals/product/network-firewall-policies-implementations-11-5-0/1.html*

In general, public-facing SMTP servers will not have firewall restrictions, although if you have licensed IP Intelligence on the BIG-IP system, you may want to prohibit connections from sources with low reputation.

SMTP servers that relay internal traffic might have firewall rules to prevent them from being used as open relays, to allow traffic only from management or security devices and systems, or otherwise prevent unauthorized or undesirable traffic.

Dedicated business-to-business or similar SMTP connections will typically be configured to only allow connections from a single IP address, or a small range of addresses, known and verified to be the trusted remote email servers.

The following instructions cover a basic firewall configuration that is effective for the most common scenario of wanting to allow connections from a single trusted network. If you have complex requirements, such as the need to schedule different policies for different times of the day, or you want to create complicated rule or address lists, consult the BIG-IP AFM documentation. The basic steps for Policy and Rule creation apply to all scenarios.

To configure the BIG-IP AFM to allow connections from a single trusted network

1. Create a Network Firewall Policy:
    a. From the Configuration utility, click **Security > Network Firewall > Policies**, and then click **Create**.
    b. In the **Name** field, type a unique name for the policy, such as SMTP Policy.
    c. Click **Finished**.
2. Create a rule to allow authorized hosts or networks to connect:
    a. Click **Security > Network Firewall > Policies**.
    b. Click the name of the policy you just created.
    c. In the Rule section (below the General Properties section), click the **Add** button.
    d. Leave the **Type** list set to Rule.
    e. From the **Order** list, select **First**. The Order list only appears in version 11.5 and later. In 11.4.x, you must reorder the rules from the Policy General Properties page.
    f. In the **Name** field, type a unique name, for instance **SMTP Allowed**.
    g. Ensure the **State** list is set to **Enabled**.
    h. From the **Protocol** list, select **TCP**. Leave the box to the right of TCP set to **6**.
    i. In the **Source** section, from the **Address/Region** list, select **Specify**.
    You are now able to list the trusted source addresses for your connection.
    In the following example, we will configure a single subnet as trusted.
        - Select **Address**.
        - In the box, type the network address you want to allow, including netmask if more than a single host. Specify a network using CIDR notation, such as **10.0.0.0/24**.
        - Do not configure a source port.
        - Optional: If you want to limit inbound connections to a specific VLAN or Tunnel, from the **VLAN / Tunnel** list, select **Specify**, and then move the VLANs or tunnels that are allowed access to the Selected box.

- Click **Add**.
- Repeat these steps for additional hosts or networks. Use **Address List** or **Address Range** when appropriate.

j. In the **Destination** section, leave the **Address/Region** and **Port** set to **Any**. Because you will be applying your policy to a virtual server that listens only on a single desired address and port, do not specify that information here.

k. If necessary, from the **Action** list, select **Accept**.

l. *Optional:* If you have configured a logging profile and want to log connections, from the **Logging** list, select **Enabled**. Typically, allowed connections do not need to be logged.

m. Click **Finished**.

3. Creating a firewall rule to block all other traffic

The next task is to create a firewall rule to block all other traffic that you have not allowed. Although this is not a required step if your BIG-IP system is set to default deny (**Firewall mode**), it is required in default-accept (**ADC mode**), and is a good practice to always configure such a rule.

a. Click **Security > Network Firewall > Policies**.

b. Click the name of the policy you created in step 1.

c. In the Rule section (below the General Properties section), click the **Add** button.

d. Leave the **Type** list set to **Rule**.

e. Leave the **Order** list, select **Last**.

f. In the **Name** field, type a unique name, for example **SMTP Prohibited**.

g. Ensure the **State** list is set to **Enabled**.

h. From the **Protocol** list, select **TCP**. Leave the box to the right of TCP set to **6**.

i. In the **Source** section, leave all the lists set to **Any**

j. From the **Action** list, select either **Drop** (to silently discard incoming connections) or **Reject** (to send a Destination Unreachable message to the sender).

k. If you configured a logging profile as described in *Optional: Configuring the BIG-IP system to log network firewall events on page 28*, from the **Logging** list, select **Enabled**.

l. Click **Finished**. You return to the Policy Properties page.

m. On the Policy Properties page, in the Rules section, ensure the rule with the Action of Accept comes before the Drop or Reject rule you just created. If it does not, use the **Reorder** button and drag the rules into the correct order.

4. Apply Your Firewall Policy to your Virtual Server

a. Click **Security > Network Firewall > Active Rules**.

b. In the Rule section (below the General Properties section), click the **Add** button.

c. From the **Context** list, select **Virtual Server**, and then select the virtual server you created for your SMTP traffic.

d. From the **Type** list, select **Policy**, and then select the firewall policy you created.

e. From the **Policy Type** list, select **Enforced**.

f. Click **Finished**.

Optional: Assigning an IP Intelligence Policy to your SMTP Virtual Server

If you want to restrict access to your SMTP virtual server based on the reputation of the remote sender, you can enable and assign an IP Intelligence policy. This requires an IP intelligence license; contact your F5 Sales representative for more information.

It is outside the scope of this document to provide instructions on configuring an IP Intelligence Policy. Full documentation on enabling and configuring the IP Intelligence feature can be found at *https://support.f5.com/kb/en-us/products/big-ip-afm/manuals/product/network-firewall-policies-implementations-11-5-0/5.html*

After you have enabled and configured an IP Intelligence policy, use the following procedure to assign the policy to your SMTP virtual server:

To assign the IP intelligence policy to the SMTP virtual server

1. On the Main tab, click **Local Traffic > Virtual Servers**. The Virtual Server List screen opens.
2. Click the name of your SMTP virtual server.
3. From the **Security** menu, choose **Policies**.
4. Next to **IP Intelligence**, select **Enabled**, then select the IP intelligence policy to apply to traffic on the virtual server.
5. Click **Update**. The list screen and the updated item are displayed.

   The specified IP Intelligence policy is applied to traffic on the selected virtual server.

Optional: Configuring the BIG-IP system to log network firewall events

If you are using BIG-IP AFM, you have the option of logging network firewall events to one or more remote syslog servers (recommended) or to log events locally. You can either use an iApp template to create the logging profile, or create the logging profile manually.

For specific information on logging on the BIG-IP system, see the appropriate guide for your version. For example, for 11.5.0:

- Remote High-Speed Logging: *https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-implementations-11-5-0/22.html*
- Local logging: *https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-concepts-11-5-0/11.html*

Creating the logging profile using the iApp template

Use this section to create the logging profile using the logging profile iApp template. If you have not already downloaded the iApp template, see *https://devcentral.f5.com/wiki/iApp.F5-Remote-Logging-iApp.ashx*.

To configure the logging profile iApp

1. Log on to the BIG-IP system.
2. On the Main tab, click **iApp > Application Services**.
3. Click **Create**. The Template Selection page opens.
4. In the **Name** box, type a name. In our example, we use **logging-iapp_.**
5. From the **Template** list, select **f5.remote_logging.v*<latest-version>***. The template opens
6. Use the following table for guidance on configuring the iApp template. Questions not mentioned in the table can be configured as applicable for your implementation.

Question	Your selection
Do you want to create a new pool of remote logging servers, or use an existing one?	Unless you have already created a pool on the BIG-IP system for your remote logging servers, select **Create a new pool**.
Which servers should be included in this pool?	Specify the IP addresses of your logging servers. Click **Add** to include more servers.
What port do the pool members use?	Specify the port used by your logging servers, typically **514**.
Do the pool members expect UDP or TCP connections?	Specify whether your logging servers expect incoming connections to be TCP or UDP.
Do you want to create a new monitor for this pool, or use an existing one?	Unless you have already created a health monitor for your pool of logging servers, select **Use a simple ICMP (ping) monitor**.
Do your log pool members require a specific log format?	If your logging servers require a specific format, select the appropriate format from the list.

7. Click **Finished**.

8. On the Main tab, click **Local Traffic > Virtual Servers**. The Virtual Server List screen opens.
9. Click the name of your SMTP virtual server.
10. From the **Security** menu, choose **Policies**.
11. Next to **Log Profile**, select **Enabled**, then select the Logging profile you created.
12. Click **Update**. The list screen and the updated item are displayed.

Note

The iApp template creates a log publisher and attaches it to the logging profile. If the publisher does not appear in the BIG-IP Configuration utility (GUI), you can verify the configuration by running the following command from the Traffic Management shell (tmsh): **`list security log profile`** *`<your profile name>`.*

Creating logging profile manually

If you do not want to use the iApp template to create a logging profile, use this section for guidance on configuring the logging profile manually. You must have access to the tmsh command line to use this method.

To manually configure a logging profile

1. Use the following guidance for configuring a health monitor and load balancing pool for the logging servers.

BIG-IP LTM Object	Non-default settings/Notes	
Health Monitor (*Local Traffic -->Monitors*)	***Name***	Type a unique name
	Type	**ICMP**
	Interval	**30** (recommended)
	Timeout	**91** (recommended)
Pool (*Local Traffic -->Pools*)	***Name***	Type a unique name
	Health Monitor	Select the appropriate monitor you created
	Slow Ramp Time	**300**
	Load Balancing Method	Choose a load balancing method. We recommend **Least Connections (Member)**
	Address	Type the IP Address of a server.
	Service Port	Type the appropriate port, such as UDP port **514**, the port on which logging typically occurs. Click **Add**, and then repeat Address and Port for all nodes

2. Log into the BIG-IP system using the command line. Enter the tmsh shell, by typing **tmsh** from the prompt.
3. Create a Remote High Speed Log (HSL) destination:

```
(tmos)# create / sys log-config destination remote-high-speed-log [name] pool-name [specified pool] protocol [udp or tcp]
```

4. If you have a specific log format requirement, create a format-specific log destination, and forward that to the previously-created HSL destination:

```
(tmos)# create / sys log-config destination [splunk|arcsight|remote-high-speed-log] [name] forward-to [HSL name]
```

5. Create a log publisher:

```
(tmos)# create / sys log-config publisher [name] destinations add { [logdestination name] }
```

6. Create the logging profile to tie everything together.
If you chose to log allowed connections, include the green text (as in step 2 substep l in *To configure the BIG-IP AFM to allow connections from a single trusted network on page 26)*.
If you set the rule to drop incoming connections, include the text in blue.

If you chose to log IP intelligence events, include the text in red to add the parameter that sets the log publisher.

```
(tmos)# create / security log profile [name] network add { [name] { filter { log-acl-match-accept enabled
log-acl-match-drop enabled log-acl-match-reject enabled } format { field-list { date_time action drop_reason
protocol src_ip src_port dest_ip dest_port } type field-list } publisher [logpublisher name] } } ip-
intelligence { log-publisher [logpublisher name] }
```

Assigning the logging profile to the virtual server

The final task is to assign the logging profile to the virtual server.

To assign the logging profile to the SMTP virtual server

1. On the Main tab, click **Local Traffic > Virtual Servers**. The Virtual Server List screen opens.
2. Click the name of your SMTP virtual server.
3. From the **Security** menu, choose **Policies**.
4. Next to **Log Profile**, select **Enabled**, then select the Logging profile you created.
5. Click **Update**. The list screen and the updated item are displayed.

Configuring the External health monitors

As described in the configuration tables, you have the option of creating an external health monitor on the BIG-IP system which calls a script which can more accurately determine the health of the servers than the default SMTP monitor. Before you can create the health monitor in the Configuration utility, you must import the script onto the BIG-IP system. Each scenario described in this guide has multiple scripts that could be used; use the script most appropriate for your configuration.

Each monitor in this section includes a link to download the script code, and shows the actual code contained in the downloadable file. If you would prefer to download all the scripts in one file, go to *https://www.f5.com/content/dam/f5/corp/global/pdf/deployment-guides/smtp-eav-monitors_all.zip*.

1) Service check for unencrypted SMTP requiring authentication but without submitting a message

Use the following script if you want the BIG-IP system to perform a health check to the SMTP servers that requires authentication. This monitor does not submit a message as a part of the health check. The monitor is successful if the mail server successfully authenticates the connection.

This monitor is also available from *https://www.f5.com/content/dam/f5/corp/global/pdf/deployment-guides/unencrypted-smtp-auth-no-message.zip*.

You must make sure to enter the Name/Value pairs as described in the configuration tables.
To import the file, go to **System > File Management > External Monitor Program File List** and then click **Import**. On the Import File page, choose the monitor script file, and give the file a unique name. You choose this name when configuring the monitor. Click **Import**.

```
#!/bin/sh
# These arguments supplied automatically for all external monitors:
# $1 = IP (nnn.nnn.nnn.nnn notation)
# $2 = port (decimal, host byte order)
#
# This script expects the following Name/Value pairs:
# USER = the username associated with a mailbox
# PASSWORD = the password for the user account
#
#
#
# Remove IPv6/IPv4 compatibility prefix (LTM passes addresses in IPv6 format)

NODE=`echo ${1} | sed 's/::ffff://'`
if [[ $NODE =~ ^[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}$ ]]; then
# node is v4
NODE=${NODE}
else
# node is v6
NODE=[${NODE}]
fi
PORT=${2}
PIDFILE="/var/run/`basename ${0}`.${IP}_${PORT}.pid"
RECV='235'

# kill off the last instance of this monitor if hung and log current pid
if [ -f $PIDFILE ]
then
echo "EAV exceeded runtime needed to kill ${NODE}:${PORT}" | logger -p local0.error
kill -9 'cat $PIDFILE' > /dev/null 2>&1
fi
echo "$$" > $PIDFILE
/usr/bin/curl-apd -k -v smtp://${NODE}:${PORT} -u ${USER}:${PASSWORD} --mail-from bigip_smtp_test_monitor@mail.testing.com --mail-rcpt bigip_smtp_test_monitor@mail.testing.com 2>&1 | grep "${RECV}" > /dev/null
STATUS=$?
rm -f $PIDFILE
if [ $STATUS -eq 0 ]
then
echo "UP"
fi
exit
```

2) Service check for unencrypted SMTP submitting a message but not requiring authentication

Use the following script if you want the BIG-IP system to perform a service check to the SMTP servers that does not require authentication, but submits a message to the servers as part of the health check. The server is considered available if it accepts and queues the message for delivery.

This monitor is also available from *https://www.f5.com/content/dam/f5/corp/global/pdf/deployment-guides/unencrypted-smtp-message-no-auth.zip*.

For this monitor, you must import two files: the monitor script file, and the message file the script uses to test the servers. You must also make sure to enter the Name/Value pairs as described in the configuration tables.

To import the file, go to **System > File Management > External Monitor Program File List** and then click **Import**. On the Import File page, choose the monitor script file, and give the file a unique name. You choose this name when configuring the monitor. Click **Import**.

Message code

```
## MONITORBODY.txt is a separate file with the following format:
Subject: BIG-IP Monitor

# Optional body text could go here
.
```

Monitor code

```
#!/bin/sh
# These arguments supplied automatically for all external monitors:
# $1 = IP (nnn.nnn.nnn.nnn notation)
# $2 = port (decimal, host byte order)
#
# This script expects the following Name/Value pairs:
#
#
# FROM = sender email address
# RCPT = recipient mailbox address
#
# Remove IPv6/IPv4 compatibility prefix (LTM passes addresses in IPv6 format)

NODE=`echo ${1} | sed 's/::ffff://'`
if [[ $NODE =~ ^[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}$ ]]; then
# node is v4
NODE=${NODE}
else
# node is v6
NODE=[${NODE}]
fi
PORT=${2}
PIDFILE="/var/run/`basename ${0}`.${IP}_${PORT}.pid"
RECV='354'

# kill off the last instance of this monitor if hung and log current pid
if [ -f $PIDFILE ]
then
echo "EAV exceeded runtime needed to kill ${NODE}:${PORT}" | logger -p local0.error
kill -9 'cat $PIDFILE' > /dev/null 2>&1
fi
echo "$$" > $PIDFILE
/usr/bin/curl-apd -k -v smtp://${NODE}:${PORT}  --mail-from ${FROM} --mail-rcpt ${RCPT} -T /config/monitors/smtp_
test_MONITORBODY.txt 2>&1 | grep "${RECV}" > /dev/null
STATUS=$?
rm -f $PIDFILE
if [ $STATUS -eq 0 ]
then
echo "UP"
fi
exit
```

3) Service check for unencrypted SMTP submitting a message and requiring authentication

Use the following script if you want the BIG-IP system to perform a service check to the SMTP servers that requires authentication and submits a message to the servers as part of the health check. The server is considered available if it authenticates the connection, then accepts and queues the message for delivery.

This monitor is also available from *https://www.f5.com/content/dam/f5/corp/global/pdf/deployment-guides/unencrypted-smtp-message-auth.zip*.

For this monitor, you must import two files: the monitor script file, and the message file the script uses to test the servers. You must also make sure to enter the Name/Value pairs as described in the configuration tables.

To import the file, go to **System > File Management > External Monitor Program File List** and then click **Import**. On the Import File page, choose the monitor script file, and give the file a unique name. You choose this name when configuring the monitor. Click **Import**.

Message code

```
## MONITORBODY.txt is a separate file with the following format:
Subject: BIG-IP Monitor

# Optional body text could go here
.
```

Monitor code

```
#!/bin/sh
# These arguments supplied automatically for all external monitors:
# $1 = IP (nnn.nnn.nnn.nnn notation)
# $2 = port (decimal, host byte order)
#
# This script expects the following Name/Value pairs:
# USER = the username associated with a mailbox
# PASSWORD = the password for the user account
# FROM = sender email address
# RCPT = recipient mailbox address
#
# Remove IPv6/IPv4 compatibility prefix (LTM passes addresses in IPv6 format)

NODE=`echo ${1} | sed 's/::ffff://'`
if [[ $NODE =~ ^[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}$ ]]; then
# node is v4
NODE=${NODE}
else
# node is v6
NODE=[${NODE}]
fi
PORT=${2}
PIDFILE="/var/run/`basename ${0}`.${IP}_${PORT}.pid"
RECV='354'

# kill off the last instance of this monitor if hung and log current pid
if [ -f $PIDFILE ]
then
echo "EAV exceeded runtime needed to kill ${NODE}:${PORT}" | logger -p local0.error
kill -9 'cat $PIDFILE' > /dev/null 2>&1
fi
echo "$$" > $PIDFILE
/usr/bin/curl-apd -k -v smtp://${NODE}:${PORT} -u ${USER}:${PASSWORD} --mail-from ${FROM} --mail-rcpt ${RCPT} -T /
config/monitors/smtp_test_MONITORBODY.txt 2>&1 | grep "${RECV}" > /dev/null
STATUS=$?
rm -f $PIDFILE
if [ $STATUS -eq 0 ]
then
echo "UP"
fi
exit
```

4) Service check for SSL(SMTPS) encrypted SMTP with no authentication or message submission

Use the following script if clients are connecting to the BIG-IP system with encryted SMTP. In this case, the monitor does not account for authentication or message submission.

This monitor is also available from *https://www.f5.com/content/dam/f5/corp/global/pdf/deployment-guides/encrypted-smtp-no-message-no-auth.zip*.

To import the file, go to **System > File Management > External Monitor Program File List** and then click **Import**. On the Import File page, choose the monitor script file, and give the file a unique name. You choose this name when configuring the monitor. Click **Import**.

Monitor code

```
#!/bin/sh
# These arguments supplied automatically for all external monitors:
# $1 = IP (nnn.nnn.nnn.nnn notation)
# $2 = port (decimal, host byte order)
#
# This script expects the following Name/Value pairs(These may be auto-generated):
# FROM = sender's email address
# RCPT = recipient mailbox address
#
# Remove IPv6/IPv4 compatibility prefix (LTM passes addresses in IPv6 format)

NODE=`echo ${1} | sed 's/::ffff://'`
if [[ $NODE =~ ^[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}$ ]]; then
# node is v4
NODE=${NODE}
else
# node is v6
NODE=[${NODE}]
fi
PORT=${2}
PIDFILE="/var/run/`basename ${0}`.${IP}_${PORT}.pid"

RECV='221'
SMTPCMDS="EHLO localhost\nMAIL FROM: ${FROM}\nRCPT TO: ${RCPT}\nquit\n"

# kill of the last instance of this monitor if hung and log current pid
if [ -f $PIDFILE ]
then
echo "EAV exceeded runtime needed to kill ${NODE}:${PORT}" | logger -p local0.error
kill -9 'cat $PIDFILE' > /dev/null 2>&1
fi
echo "$$" > $PIDFILE
echo -e ${SMTPCMDS} | openssl s_client  -crlf -quiet -connect ${NODE}:${PORT} 2>&1 | grep "${RECV}" > /dev/null
STATUS=$?
rm -f $PIDFILE
if [ $STATUS -eq 0 ]
then
echo "UP"
fi
exit
```

5) Service check for SSL (SMTPS) encrypted SMTP with authentication but without submitting a message

Use the following script if clients are connecting to the BIG-IP system with encrypted SMTP. In this case, the monitor does perform authentication, but does not submit a message.

This monitor is also available from *https://www.f5.com/content/dam/f5/corp/global/pdf/deployment-guides/encrypted-smtp-auth-no-message.zip*.

You must make sure to enter the Name/Value pairs as described in the configuration tables.

To import the file, go to **System > File Management > External Monitor Program File List** and then click **Import**. On the Import File page, choose the monitor script file, and give the file a unique name. You choose this name when configuring the monitor. Click **Import**.

Monitor code

```
#!/bin/sh
# These arguments supplied automatically for all external monitors:
# $1 = IP (nnn.nnn.nnn.nnn notation)
# $2 = port (decimal, host byte order)
#
# This script expects the following Name/Value pairs(These may be auto-generated):
# FROM = sender's email address
# RCPT = recipient mailbox address
# USER = the username associated with a mailbox
# PASSWORD = the password for the user account
#
# Remove IPv6/IPv4 compatibility prefix (LTM passes addresses in IPv6 format)

NODE=`echo ${1} | sed 's/::ffff://'`
if [[ $NODE =~ ^[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}$ ]]; then
# node is v4
NODE=${NODE}
else
# node is v6
NODE=[${NODE}]
fi
PORT=${2}
PIDFILE="/var/run/`basename ${0}`.${IP}_${PORT}.pid"

USER_ENC=`echo -ne ${USER} | base64`
PWD_ENC=`echo -ne ${PASSWORD} | base64`
RECV='235'
SMTPCMDS="EHLO localhost\nAUTH LOGIN\n$USER_ENC\n$PWD_ENC\nMAIL FROM: ${FROM}\nRCPT TO: ${RCPT}\nquit\n"

# kill of the last instance of this monitor if hung and log current pid
if [ -f $PIDFILE ]
then
echo "EAV exceeded runtime needed to kill ${NODE}:${PORT}" | logger -p local0.error
kill -9 'cat $PIDFILE' > /dev/null 2>&1
fi
echo "$$" > $PIDFILE
echo -e ${SMTPCMDS} | openssl s_client  -crlf -quiet -connect ${NODE}:${PORT} 2>&1 | grep "${RECV}" > /dev/null
STATUS=$?
rm -f $PIDFILE
if [ $STATUS -eq 0 ]
then
echo "UP"
fi
exit
```

6) Service check for TLS/SSL (SMTPS) encrypted SMTP submitting a message but no authentication

Use the following script if clients are connecting over TLS/SSL and you want the BIG-IP system to perform a service check to the SMTP servers that requires a message to the servers as part of the health check but does not include authentication. The server is considered available if it accepts and queues the message for delivery.

This monitor is also available from *https://www.f5.com/content/dam/f5/corp/global/pdf/deployment-guides/encrypted-smtp-message-no-auth.zip*.

For this monitor, you must import two files: the monitor script file, and the message file the script uses to test the servers. You must also make sure to enter the Name/Value pairs as described in the configuration tables.

To import the file, go to **System > File Management > External Monitor Program File List** and then click **Import**. On the Import File page, choose the monitor script file, and give the file a unique name. You choose this name when configuring the monitor. Click **Import**.

Message code

```
## MONITORBODY.txt is a separate file with the following format:
Subject: BIG-IP Monitor

# Optional body text could go here
.
```

Monitor code

```
#!/bin/sh
# These arguments supplied automatically for all external monitors:
# $1 = IP (nnn.nnn.nnn.nnn notation)
# $2 = port (decimal, host byte order)
#
# This script expects the following Name/Value pairs:
#
#
# FROM = sender email address
# RCPT = recipient mailbox address
#
# Remove IPv6/IPv4 compatibility prefix (LTM passes addresses in IPv6 format)

NODE=`echo ${1} | sed 's/::ffff://'`
if [[ $NODE =~ ^[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}$ ]]; then
# node is v4
NODE=${NODE}
else
# node is v6
NODE=[${NODE}]
fi
PORT=${2}
PIDFILE="/var/run/`basename ${0}`.${IP}_${PORT}.pid"
RECV='354'

# kill off the last instance of this monitor if hung and log current pid
if [ -f $PIDFILE ]
then
echo "EAV exceeded runtime needed to kill ${NODE}:${PORT}" | logger -p local0.error
kill -9 'cat $PIDFILE' > /dev/null 2>&1
fi
echo "$$" > $PIDFILE
/usr/bin/curl-apd -k -v smtps://${NODE}:${PORT}  --mail-from ${FROM} --mail-rcpt ${RCPT} -T /config/monitors/
smtp_test_MONITORBODY.txt 2>&1 | grep "${RECV}" > /dev/null
STATUS=$?
rm -f $PIDFILE
if [ $STATUS -eq 0 ]
then
echo "UP"
fi
exit
```

7) Service check for TLS/SSL (SMTPS) encrypted SMTP with authentication and submitting a message

Use the following script if clients are connecting over TLS/SSL and you want the BIG-IP system to perform a service check to the SMTP servers that requires authentication and submits a message to the servers as part of the health check. The server is considered available if it authenticates the connection, then accepts and queues the message for delivery.

This monitor is also available from *https://www.f5.com/content/dam/f5/corp/global/pdf/deployment-guides/encrypted-smtp-message-auth.zip*.

For this monitor, you must import two files: the monitor script file, and the message file the script uses to test the servers. You must also make sure to enter the Name/Value pairs as described in the configuration tables.

To import the file, go to **System > File Management > External Monitor Program File List** and then click **Import**. On the Import File page, choose the monitor script file, and give the file a unique name. You choose this name when configuring the monitor. Click **Import**.

Message code

```
## MONITORBODY.txt is a separate file with the following format:
Subject: BIG-IP Monitor

# Optional body text could go here
.
```

Monitor code

```
#!/bin/sh
# These arguments supplied automatically for all external monitors:
# $1 = IP (nnn.nnn.nnn.nnn notation)
# $2 = port (decimal, host byte order)
#
# This script expects the following Name/Value pairs:
# USER = the username associated with a mailbox
# PASSWORD = the password for the user account
# FROM = sender email address
# RCPT = recipient mailbox address
#
# Remove IPv6/IPv4 compatibility prefix (LTM passes addresses in IPv6 format)

NODE=`echo ${1} | sed 's/::ffff://'`
if [[ $NODE =~ ^[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}$ ]]; then
# node is v4
NODE=${NODE}
else
# node is v6
NODE=[${NODE}]
fi
PORT=${2}
PIDFILE="/var/run/`basename ${0}`.${IP}_${PORT}.pid"
RECV='354'

# kill off the last instance of this monitor if hung and log current pid
if [ -f $PIDFILE ]
then
echo "EAV exceeded runtime needed to kill ${NODE}:${PORT}" | logger -p local0.error
kill -9 'cat $PIDFILE' > /dev/null 2>&1
fi
echo "$$" > $PIDFILE
/usr/bin/curl-apd -k -v smtps://${NODE}:${PORT} -u ${USER}:${PASSWORD} --mail-from ${FROM} --mail-rcpt ${RCPT} -T
/config/monitors/smtp_test_MONITORBODY.txt 2>&1 | grep "${RECV}" > /dev/null
STATUS=$?
rm -f $PIDFILE
if [ $STATUS -eq 0 ]
then
echo "UP"
fi
exit
```

8) Service check for SMTP with STARTTLS with no authentication or message submission

Use the following script if clients are connecting to the BIG-IP system with SMTP encrypted using the STARTTLS command. In this case, the monitor does not account for authentication or message submission.

This monitor is also available from *https://www.f5.com/content/dam/f5/corp/global/pdf/deployment-guides/smtp-starttls-no-auth-no-message.zip*.

To import the file, go to **System > File Management > External Monitor Program File List** and then click **Import**. On the Import File page, choose the monitor script file, and give the file a unique name. You choose this name when configuring the monitor. Click **Import**.

Monitor code

```
#!/bin/sh
# These arguments supplied automatically for all external monitors:
# $1 = IP (nnn.nnn.nnn.nnn notation)
# $2 = port (decimal, host byte order)
#
# This script expects the following Name/Value pairs(These may be auto-generated):
# FROM = sender's email address
# RCPT = recipient mailbox address
#
# Remove IPv6/IPv4 compatibility prefix (LTM passes addresses in IPv6 format)

NODE=`echo ${1} | sed 's/::ffff://'`
if [[ $NODE =~ ^[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}$ ]]; then
# node is v4
NODE=${NODE}
else
# node is v6
NODE=[${NODE}]
fi
PORT=${2}
PIDFILE="/var/run/`basename ${0}`.${IP}_${PORT}.pid"


RECV='221'
SMTPCMDS="EHLO localhost\nMAIL FROM: ${FROM}\nRCPT TO: ${RCPT}\nquit\n"

# kill of the last instance of this monitor if hung and log current pid
if [ -f $PIDFILE ]
then
echo "EAV exceeded runtime needed to kill ${NODE}:${PORT}" | logger -p local0.error
kill -9 'cat $PIDFILE' > /dev/null 2>&1
fi
echo "$$" > $PIDFILE
echo -e ${SMTPCMDS} | openssl s_client -starttls smtp -crlf -quiet -connect ${NODE}:${PORT} 2>&1 | grep
"${RECV}" > /dev/null
STATUS=$?
rm -f $PIDFILE
if [ $STATUS -eq 0 ]
then
echo "UP"
fi
exit
```

9) Service check for SMTP with STARTTLS and authentication, but without submitting a message

Use the following script if clients are connecting to the BIG-IP system with SMTP encrypted using the STARTTLS command. In this case, the monitor performs authentication as a part of the health check but does not submit a message.

This monitor is also available from *https://www.f5.com/content/dam/f5/corp/global/pdf/deployment-guides/smtp-starttls-auth-no-message.zip*.

You must make sure to enter the Name/Value pairs as described in the configuration tables.

To import the file, go to **System > File Management > External Monitor Program File List** and then click **Import**. On the Import File page, choose the monitor script file, and give the file a unique name. You choose this name when configuring the monitor. Click **Import**.

Monitor code

```
#!/bin/sh
# These arguments supplied automatically for all external monitors:
# $1 = IP (nnn.nnn.nnn.nnn notation)
# $2 = port (decimal, host byte order)
#
# This script expects the following Name/Value pairs:
# USER = the username associated with a mailbox
# PASSWORD = the password for the user account
#
# Remove IPv6/IPv4 compatibility prefix (LTM passes addresses in IPv6 format)

NODE=`echo ${1} | sed 's/::ffff://'`
if [[ $NODE =~ ^[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}$ ]]; then
# node is v4
NODE=${NODE}
else
# node is v6
NODE=[${NODE}]
fi
PORT=${2}
PIDFILE="/var/run/`basename ${0}`.${IP}_${PORT}.pid"
RECV='235'

# kill off the last instance of this monitor if hung and log current pid
if [ -f $PIDFILE ]
then
echo "EAV exceeded runtime needed to kill ${NODE}:${PORT}" | logger -p local0.error
kill -9 'cat $PIDFILE' > /dev/null 2>&1
fi
echo "$$" > $PIDFILE
/usr/bin/curl-apd -k -v smtp://${NODE}:${PORT} -u ${USER}:${PASSWORD} --mail-from bigip_smtp_test_monitor@mail.testing.com --mail-rcpt bigip_smtp_test_monitor@mail.testing.com 2>&1 | grep "${RECV}" > /dev/null
STATUS=$?
rm -f $PIDFILE
if [ $STATUS -eq 0 ]
then
echo "UP"
fi
exit
```

10) Service check for SMTP with STARTTLS (required), submitting a message but no authentication

Use the following script if clients are connecting to the BIG-IP system with SMTP encrypted using the STARTTLS command. In this case, the monitor does not account for authentication but submits a message as a part of the health check.

This monitor is also available from *https://www.f5.com/content/dam/f5/corp/global/pdf/deployment-guides/smtp-starttls-required-message-no-auth.zip*.

You must make sure to enter the Name/Value pairs as described in the configuration tables.

To import the file, go to **System > File Management > External Monitor Program File List** and then click **Import**. On the Import File page, choose the monitor script file, and give the file a unique name. You choose this name when configuring the monitor. Click **Import**.

Monitor code

```
#!/bin/sh
# These arguments supplied automatically for all external monitors:
# $1 = IP (nnn.nnn.nnn.nnn notation)
# $2 = port (decimal, host byte order)
#
# This script expects the following Name/Value pairs:
# USER = the username associated with a mailbox
# PASSWORD = the password for the user account
#
# Remove IPv6/IPv4 compatibility prefix (LTM passes addresses in IPv6 format)

NODE=`echo ${1} | sed 's/::ffff://'`
if [[ $NODE =~ ^[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}$ ]]; then
# node is v4
NODE=${NODE}
else
# node is v6
NODE=[${NODE}]
fi
PORT=${2}
PIDFILE="/var/run/`basename ${0}`.${IP}_${PORT}.pid"
RECV='235'

# kill off the last instance of this monitor if hung and log current pid
if [ -f $PIDFILE ]
then
echo "EAV exceeded runtime needed to kill ${NODE}:${PORT}" | logger -p local0.error
kill -9 'cat $PIDFILE' > /dev/null 2>&1
fi
echo "$$" > $PIDFILE
/usr/bin/curl-apd -k -v smtp://${NODE}:${PORT} -u ${USER}:${PASSWORD} --mail-from bigip_smtp_test_monitor@mail.testing.com --mail-rcpt bigip_smtp_test_monitor@mail.testing.com 2>&1 | grep "${RECV}" > /dev/null
STATUS=$?
rm -f $PIDFILE
if [ $STATUS -eq 0 ]
then
echo "UP"
fi
exit
```

11) Service check for SMTP with STARTTLS (required), not submitting a message and with no authentication

Use the following script if clients are connecting to the BIG-IP system with SMTP encrypted using the STARTTLS command. In this case, the monitor does not account for authentication but submits a message as a part of the health check.

This monitor is also available from *https://www.f5.com/content/dam/f5/corp/global/pdf/deployment-guides/smtp-starttls-required-no-message-no-auth.zip*

You must make sure to enter the Name/Value pairs as described in the configuration tables.

To import the file, go to **System > File Management > External Monitor Program File List** and then click **Import**. On the Import File page, choose the monitor script file, and give the file a unique name. You choose this name when configuring the monitor. Click **Import**.

Monitor code

```
#!/bin/sh
# These arguments supplied automatically for all external monitors:
# $1 = IP (nnn.nnn.nnn.nnn notation)
# $2 = port (decimal, host byte order)
#
# This script expects the following Name/Value pairs(These may be auto-generated):
# FROM = sender's email address
# RCPT = recipient mailbox address
#
# Remove IPv6/IPv4 compatibility prefix (LTM passes addresses in IPv6 format)

NODE=`echo ${1} | sed 's/::ffff://'`
if [[ $NODE =~ ^[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}$ ]]; then
# node is v4
NODE=${NODE}
else
# node is v6
NODE=[${NODE}]
fi
PORT=${2}
PIDFILE="/var/run/`basename ${0}`.${IP}_${PORT}.pid"

RECV='221'
SMTPCMDS="EHLO localhost\nMAIL FROM: ${FROM}\nRCPT TO: ${RCPT}\nquit\n"

# kill of the last instance of this monitor if hung and log current pid
if [ -f $PIDFILE ]
then
echo "EAV exceeded runtime needed to kill ${NODE}:${PORT}" | logger -p local0.error
kill -9 'cat $PIDFILE' > /dev/null 2>&1
fi
echo "$$" > $PIDFILE
echo -e ${SMTPCMDS} | openssl s_client -starttls smtp -crlf -quiet -connect ${NODE}:${PORT} 2>&1 | grep
"${RECV}" > /dev/null
STATUS=$?
rm -f $PIDFILE
if [ $STATUS -eq 0 ]
then
echo "UP"
fi
exit
```

This completes the external monitor configuration.

Document Revision History

Version	Description	Date
1.0	New Deployment Guide	08-05-2014
1.1	Added support for BIG-IP v11.6	08-25-2014
1.2	Added guidance for configuring the BIG-IP system using the new SMTP iApp template.	04-16-2015
1.3	Added support for BIG-IP v12.0 Updated the guide for v1.0.0rc5 of the iApp template. This release fixes an issue with incorrectly formatted external monitor scripts. Also updated the downloadable script files with the same fix.	01-26-2016
1.4	Added support for BIG-IP v12.1	05-18-2016
1.5	- Updated this guide for iApp version f5.smtp.v1.0.0rc6. There are no changes to the iApp content, however the iApp can now be found on downloads.f5.com in the RELEASE_CANDIDATE directory of the iApp package. See *Downloading and importing the iApp template on page 7.* - Added support for BIG-IP v12.1.1	08-30-2016
1.6	Updated this guide for iApp version f5.smtp.v1.0.0rc7, found on downloads.f5.com in the RELEASE_CANDIDATE directory of the iApp package. See *Downloading and importing the iApp template on page 7.* This version contains the following changes: - Added support for BIG-IP v13.0 - Fixed an issue with monitors used in the SSL Bridging and Pass-Through scenarios. As a result the openSSL EAV monitor is used in the 'no msg submitted' monitor scenarios. - Added a fifth monitor option to split the 'authentication but no message' option into Basic and NTLM so the external monitor can use OpenSSL if Basic (auth login) is selected. - You can now specify a custom receive string for monitors if using Advanced mode.	03-29-2017
1.7	Updated this guide for iApp version f5.smtp.v1.0.0rc8, found on downloads.f5.com in the RELEASE_CANDIDATE directory of the SMTP folder in the iApp package. See *Downloading and importing the iApp template on page 7.* This version contains the following changes: - Added support for entering a custom message body in the monitor if **STARTTLS required** is selected. - Fixed an issue in the template where incorrect options were presented in the SSL bridging scenario.	12-14-2017
1.8	Updated this guide for iApp version f5.smtp.v1.0.0rc9, found on downloads.f5.com in the RELEASE_CANDIDATE directory of the SMTP folder in the iApp package. See *Downloading and importing the iApp template on page 7.* This version contains the following changes: - Corrected an issue that caused TCL iApps using client-ssl profiles to break when the iApp was reconfigured. This issue only affected iApps running on BIG-IP 14.1.	01-31-2019
1.9	Updated the links for External health monitors.	08-28-2019

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