Deployment Guide

Deploying the BIG-IP System with SMTP servers

This document contains guidance on configuring the BIG-IP system version 11.4 and 11.5 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 applicable versions

Product	Version
BIG-IP LTM	11.4.x, 11.5, 11.5.1
BIG-IP AFM	11.5, 11.5.1
SMTP Server	Not generally applicable; see Monitor section for specifics
Deployment guide version	1.0

Important: *Make sure you are using the most recent version of this deployment guide, available at http://www.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*.

Contents

Terminology

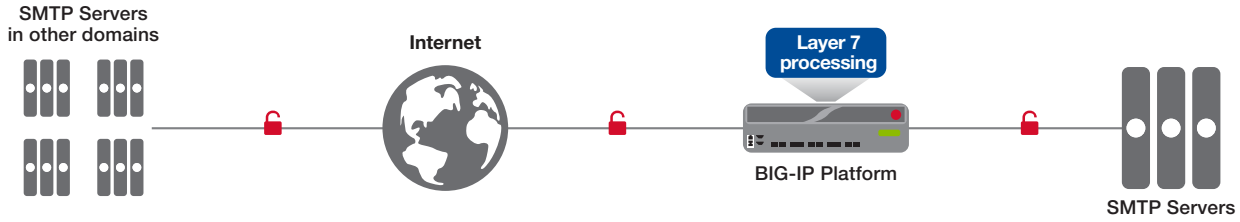
This guide uses the following terminology.

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

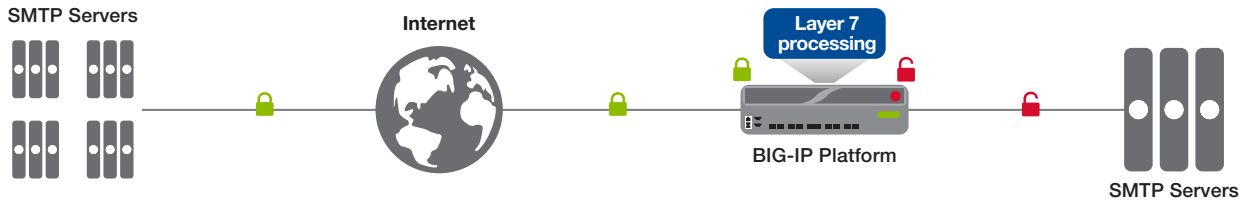
This deployment guide provides guidance on configuring a BIG-IP LTM system to support the following scenarios. All scenarios support the use of the Advanced Firewall Manager (AFM) module.

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.



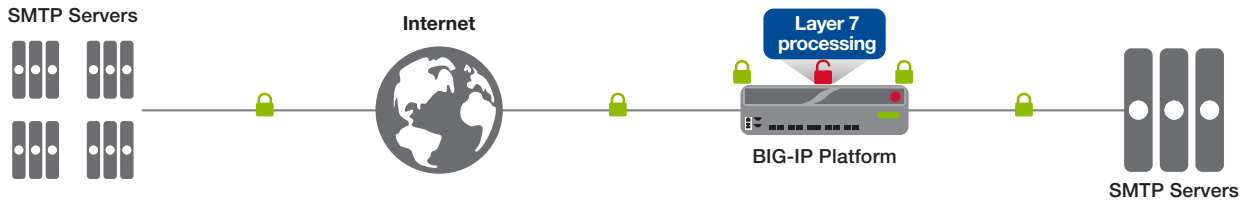
2. **Client-side: SMTP encrypted with TLS/SSL; server-side: unencrypted SMTP**
   We refer to this scenario as *SSL Offload*. Note that encrypted SMTP is often referred to as SMTPS or ESMTPS.
   Clients may send mail using SMTP over an encrypted link, typically on TCP port 587 (or the deprecated port 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.



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.

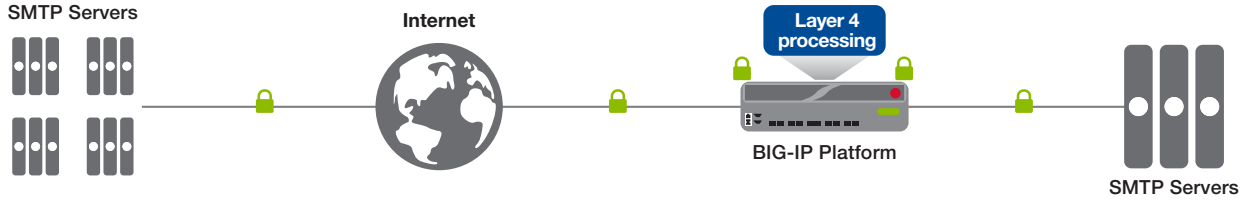
SSL Bridging covers many of the same scenarios as example #2, but is commonly used when organizations require that all communication on a network connection is encrypted. Messages are forwarded to SMTP servers, typically on port 465. The BIG-IP system can optionally use self-signed TLS/SSL certificates,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



4. **SMTP encrypted with TLS/SSL on both client and server sides**

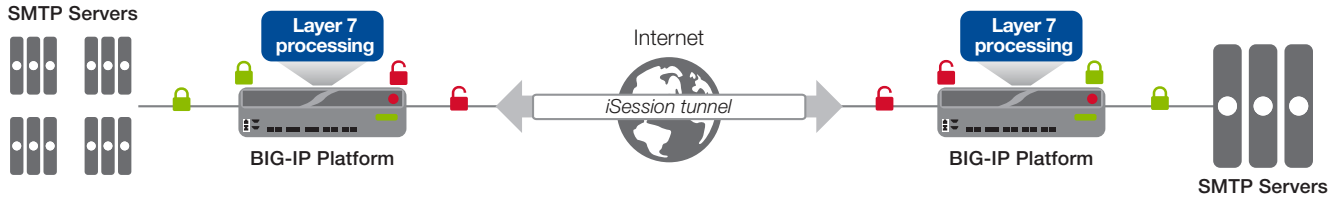
We refer to this scenario as *SSL Passthrough*, because the BIG-IP system does not decrypt the traffic, and acts as a simple Layer 4 load balancer.

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.



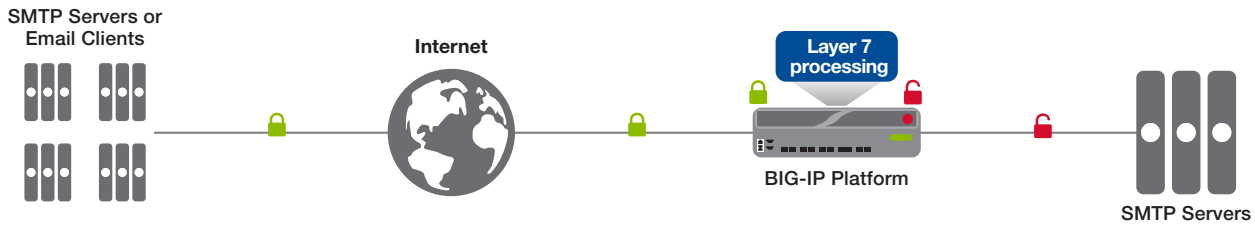
5. **Client-side: unencrypted SMTP; server-side: SMTP encrypted with TLS/SSL**

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.



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.



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.

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 8*
- *Scenario 4: SSL Passthrough on page 9*
- *Scenario 5: Encrypt on server-side only on page 10*
- *Scenario 6: SMTP with STARTTLS on the client-side, and unencrypted SMTP on the server side on page 11*

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.

BIG-IP LTM Object	Non-default settings/Notes	
Health Monitor *(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 18* 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 18* *2) Service check for unencrypted SMTP submitting a message but not requiring authentication on page 19* *3) Service check for unencrypted SMTP submitting a message and requiring authentication on page 20*	
	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 (*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 (*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 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

You can continue with *Configuring the BIG-IP Advanced Firewall Module to secure your SMTP deployment on page 13.*

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.

BIG-IP LTM Object	Non-default settings/Notes	
Health Monitor *(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 18* 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 18* *2) Service check for unencrypted SMTP submitting a message but not requiring authentication on page 19* *3) Service check for unencrypted SMTP submitting a message and requiring authentication on page 20*	
	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 (*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
Client SSL profile (*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 (*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 13.*

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.

BIG-IP LTM Object	Non-default settings/Notes	
Health Monitor *(Local Traffic > Monitors)* *Choose the health monitor appropriate for your deployment*	**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 18* 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 TLS/SSL encrypted SMTP with no authentication or message submission on page 21* *5) Service check for TLS/SSL encrypted SMTP with authentication but without submitting a message on page 22* *6) Service check for TLS/SSL encrypted SMTP submitting a message but no authentication on page 23* *7) Service check for TLS/SSL encrypted SMTP with authentication and submitting a message on page 24*	
	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 (*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
Client SSL profile (*Local Traffic -->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 (*Local Traffic -->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 (*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 13.*

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.

BIG-IP LTM Object	Non-default settings/Notes	
Health Monitor *(Local Traffic > Monitors)* *Choose the health monitor appropriate for your deployment*	**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 18* 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 TLS/SSL encrypted SMTP with no authentication or message submission on page 21* - *5) Service check for TLS/SSL encrypted SMTP with authentication but without submitting a message on page 22* - *6) Service check for TLS/SSL encrypted SMTP submitting a message but no authentication on page 23* - *7) Service check for TLS/SSL encrypted SMTP with authentication and submitting a message on page 24*	
	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 (*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 (*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 13.*

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.

BIG-IP LTM Object	Non-default settings/Notes	
Health Monitor *(Local Traffic > Monitors)* *Choose the health monitor appropriate for your deployment*	**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 18* 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 TLS/SSL encrypted SMTP with no authentication or message submission on page 21* - *5) Service check for TLS/SSL encrypted SMTP with authentication but without submitting a message on page 22* - *6) Service check for TLS/SSL encrypted SMTP submitting a message but no authentication on page 23* - *7) Service check for TLS/SSL encrypted SMTP with authentication and submitting a message on page 24*	
	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 (*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
Server SSL profile (*Local Traffic -->Profiles-->SSL*)	***Name***	Type a unique name
	Parent Profile	**serverssl**
Virtual Servers (*Local Traffic-->Virtual Servers*)	***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 13.*

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.

BIG-IP LTM Object	Non-default settings/Notes	
Health Monitor *(Local Traffic > Monitors)* *Choose the health monitor appropriate for your deployment*	**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 18* 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 25* - *9) Service check for SMTP with STARTTLS and authentication, but without submitting a message on page 26* - *10) Service check for SMTP with STARTTLS, submitting a message but no authentication on page 27*	
	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 *(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
Client SSL profile *(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 lists.
SMTPS Profile *(Local Traffic > Profiles > Services > SMTPS)*	***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.

BIG-IP LTM Object	Non-default settings/Notes	
Virtual Servers (*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 15*, 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 13)*.
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 *http://www.f5.com/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 *http://www.f5.com/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}
##FOLDER="INBOX"
PIDFILE="/var/run/'basename ${0}'.${IP}_${PORT}.pid",RECV='250'

# 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 "$$" > $PIDFILE
/usr/bin/curl-apd -k -v smtp://${NODE}:${PORT} -u ${USER}:${PASSWORD} 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 *http://www.f5.com/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'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='250'

# 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 "$$" > $PIDFILE
/usr/bin/curl-apd -k -v smtp://${NODE}:${PORT} --mail-from ${FROM} --mail-rcpt ${RCPT} 2>&1 -t MONITORBODY.txt | grep "${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 *http://www.f5.com/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'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}
SUBJECT="BIG-IP monitor"
PIDFILE="/var/run/'basename ${0}'.${IP}_${PORT}.pid"
RECV='250'

# 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 "$$" > $PIDFILE
/usr/bin/curl-apd -k -v smtp://${NODE}:${PORT} -u ${USER}:${PASSWORD} --mail-from ${FROM} --mail-rcpt ${RCPT} -t MONITORBODY.txt 2>&1 | grep "${RECV}" > /dev/null
STATUS=$?
rm -f $PIDFILE
if [ $STATUS -eq 0 ]
then
    echo "UP"
fi
exit
```

4) Service check for TLS/SSL encrypted SMTP with no authentication or message submission

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

This monitor is also available from *http://www.f5.com/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)
#
# 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}
##FOLDER="INBOX"
PIDFILE="/var/run/'basename ${0}'.${IP}_${PORT}.pid"
RECV='250'

# 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 "$$" > $PIDFILE
/usr/bin/curl-apd -k -v smtps://${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 TLS/SSL encrypted SMTP with authentication but without submitting a message

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

This monitor is also available from *http://www.f5.com/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:
#  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}
##FOLDER="INBOX"
PIDFILE="/var/run/'basename ${0}'.${IP}_${PORT}.pid"
RECV='250'

# 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 "$$" > $PIDFILE
/usr/bin/curl-apd -k -v smtps://${NODE}:${PORT} -u {USER}:${PASSWORD} 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 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 *http://www.f5.com/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'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}
SUBJECT="BIG-IP monitor"
PIDFILE="/var/run/'basename ${0}'.${IP}_${PORT}.pid"
RECV='250'

# 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 "$$" > $PIDFILE
/usr/bin/curl-apd -k -v smtps://${NODE}:${PORT} --mail-from ${FROM} --mail-rcpt ${RCPT} -t MONITORBODY.txt 2>&1 | grep "${RECV}" > /dev/null
STATUS=$?
rm -f $PIDFILE
if [ $STATUS -eq 0 ]
then
    echo "UP"
fi
exit
```

7) Service check for TLS/SSL 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 *http://www.f5.com/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'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='250'

# 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 "$$" > $PIDFILE
/usr/bin/curl-apd -k -v smtps://${NODE}:${PORT} -u ${USER}:${PASSWORD} --mail-from ${FROM} --mail-rcpt ${RCPT} -t MONITORBODY.txt 2>&1 | grep "${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 *http://www.f5.com/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)
#
# 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}
##FOLDER="INBOX"
PIDFILE="/var/run/'basename ${0}'.${IP}_${PORT}.pid"
RECV='250'

# 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 "$$" > $PIDFILE
/usr/bin/curl-apd -k -v smtp://${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 *http://www.f5.com/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}
##FOLDER="INBOX"
PIDFILE="/var/run/'basename ${0}'.${IP}_${PORT}.pid"
RECV='250'

# 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 "$$" > $PIDFILE
/usr/bin/curl-apd -k -v smtp://${NODE}:${PORT} -u {USER}:${PASSWORD} 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, 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 *http://www.f5.com/pdf/deployment-guides/smtp-starttls-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:
#  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='250'
SMTPCMDS="EHLO localhost\n\
MAIL FROM: ${FROM}\n\
RCPT TO: ${RCPT}\n\
DATA\n\
Subject: F5 BIG-IP monitor\n\
\n\
This email was generated by a BIG-IP monitor.\n\
.\n\
quit\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
```

Document Revision History

Version	Description	Date
1.0	New Deployment Guide	08-05-2014

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

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

F5 Networks
Asia-Pacific
apacinfo@f5.com

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

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