



4

Configuring Security for SMTP Traffic

- Securing SMTP traffic
- Creating a security profile for SMTP traffic
- Configuring a local traffic SMTP profile
- Assigning an SMTP security profile to a local traffic SMTP profile
- Configuring an SMTP virtual server
- Reviewing violations statistics for SMTP security profiles

Securing SMTP traffic

When you configure the SMTP security profile, the system provides the following security checks for SMTP traffic:

- Enforces SMTP protocol compliance as defined in RFC 2821.
- Rejects the first message from a sender, because legitimate senders retry sending the message, and spam senders typically do not. The system does not reject subsequent messages from the same sender to the same recipient.
- Blocks mail from domains or IP addresses in the Disallowed Senders list.
- Blocks mail from IP addresses or domains that cannot be resolved with a DNS server (typically, spam senders on the Internet).
- Blocks mail from any senders whose **MAIL FROM:** domain is in the Disallowed Users list.
- Blocks mail from senders whose **MAIL FROM:** domain cannot be resolved with a DNS server (spam senders use fake domain names).
- Blocks mail from senders whose **RCPT TO:** domain is not configured as an allowed receiving domain.
- Blocks attempted directory attacks.
- Blocks certain SMTP methods, such as VRFY, EXPN, and ETRN, that spam senders use to attack mail servers.
- Applies rate limits to the number of messages from a particular domain, which helps prevent an attack from a spam sender.
- Applies rate limits, per domain, to the number of messages sent to the mail servers.
- Validates DNS SPF records.

To configure security checks for the SMTP traffic, you create an SMTP security profile in the Protocol Security Module, and associate the security profile with a local traffic SMTP profile for a virtual server. For detailed information and specific configuration tasks, refer to the remaining sections of this chapter.

- To configure a security profile, see *Creating a security profile for SMTP traffic*, on page 4-2.
- To configure a local traffic SMTP profile and enable the Protocol Security Module, see *Configuring a local traffic SMTP profile*, on page 4-3, and *Assigning an SMTP security profile to a local traffic SMTP profile*, on page 4-4.
- To configure a virtual server and pool for SMTP traffic, and associate the local traffic SMTP profile, see *Configuring an SMTP virtual server*, on page 4-5.

◆ Note

*For more information on configuring local traffic management features, refer to the **Configuration Guide for BIG-IP® Local Traffic Management**.*

Creating a security profile for SMTP traffic

The SMTP security profile provides the security settings that are applicable to the SMTP service. In the security profile, you also specify whether the Protocol Security Module sends violation log messages to a remote logging server. By default, the Protocol Security Module retains up to 500 log entries per security profile in memory. If you want to retain additional log data, then we recommend that you configure remote logging. If you want to use remote logging, we recommend that you set up the remote logging configuration before you create any security profiles. The remote logging configuration applies to all security profiles. For more information, refer to *Configuring remote logging*, on page 5-2.

To create a security profile for SMTP traffic

1. On the Main tab of the Application Security navigation pane, click **Security Profiles**.
The SMTP Security Profiles screen opens.
2. From the Security Profiles menu, choose SMTP.
The SMTP Security Profiles screen opens.
3. Above the SMTP Security Profiles area, click the **Create** button.
The New Security Profile screen opens.
4. In the Profile Properties area, in the **Profile Name** box, type a unique name for the profile.
5. For the **Remote Logging** setting, check the box to enable remote logging for this security profile. If you have not yet configured remote logging, then click the **Remote Logging configuration** link.
The Remote Logging Configuration screen opens.

Note: The system does not return you to the New Security Profile screen if you configure remote logging in this manner. Therefore, you must return to step 1 to create the security profile after you set up the remote logging configuration.

6. In the Defense Configuration area, you can enable the blocking policy settings for the security profile violations. If you do not check either **Alarm** or **Block** for a violation, the system does not perform the corresponding security check.
 - Check **Alarm** if you want the system to log any requests that trigger the security profile violation.
 - Check **Block** if you want the system to block requests that trigger the security profile violation.
 - Check both **Alarm** and **Block** if you want the system to perform both actions.

Tip: See *SMTP security violations*, on page A-4, for an explanation of the individual violations.

7. Click **Create**.
The screen refreshes, and you see the new security profile in the list.

Configuring a local traffic SMTP profile

Once you have created the SMTP security profile in the Protocol Security Module, you create a local traffic SMTP profile in the local traffic configuration. The local traffic SMTP profile uses the SMTP security profile to scan for vulnerabilities specific to the protocol.

◆ **Note**

*For more information about local traffic profiles in general, refer to the chapter, **Understanding Profiles**, in the **Configuration Guide for BIG-IP® Local Traffic Management**.*

To create a local traffic SMTP profile

1. On the Main tab of the navigation pane, expand **Local Traffic**, and then click **Profiles**.
The HTTP Profiles screen opens.
2. From the Services menu, choose SMTP.
The SMTP Profiles screen opens.
3. Above the list area, click the **Create** button.
The New SMTP Profile screen opens.
4. In the General Properties area, for the **Name** setting, type a unique name for the profile.
5. For the **Parent Profile** setting, select the existing SMTP protocol from which you want the new profile to inherit settings. The default setting is **smtp**.
6. Above the Settings area, check the **Custom** check box.
The system activates the editing mode for the individual settings.
7. Check the **Advanced Firewall** check box to enable the SMTP security profile that you created.
8. Click **Finished**.
The screen refreshes and displays the new local traffic SMTP profile in the list.

Assigning an SMTP security profile to a local traffic SMTP profile

When you enable the **Advanced Firewall** setting on the local traffic SMTP profile, the system automatically assigns the first-listed SMTP security profile to the service profile. If you have more than one security profile configured, you can change the associations on the Profiles Assignment screen in the Protocol Security Module. On the Profiles Assignment screen, you can review the current associations, including the local traffic SMTP profile, the virtual server that uses the service profile, and the SMTP security profile.

◆ **Tip**

You can use the same SMTP security profile for many local traffic SMTP profiles.

To modify the SMTP security profiles assignment

1. On the Main tab of the Application Security navigation pane, click **Profiles Assignment**.
The Profile Assignment screen opens.
2. From the Profile Assignment menu, choose SMTP.
3. In the SMTP Security Profiles Assignment area, in the Assigned Security Profile column, for each traffic profile select the SMTP security profile that you want the service profile to use.
4. Click **Save** to retain any changes you may have made.

◆ **Note**

If you have not yet created a virtual server that uses the local traffic SMTP profile, you will not see any virtual servers listed in the Virtual Servers column.

Configuring an SMTP virtual server

You configure a local traffic virtual server and a default pool for the SMTP servers, and associate the local traffic SMTP profile that you created. This automatically associates the SMTP security profile with the virtual server. The result is that when the virtual server receives SMTP traffic, the SMTP security profile in the Protocol Security Module scans the SMTP traffic for security vulnerabilities, and then the local traffic virtual server load balances any traffic that passes the scan.

◆ Note

*For more information about local traffic profiles in general, refer to the chapter, **Configuring Virtual Servers**, in the **Configuration Guide for BIG-IP® Local Traffic Management**.*

To create a local traffic virtual server for SMTP traffic

1. On the Main tab of the navigation pane, expand **Local Traffic**, and then click **Virtual Servers**.
The Virtual Servers screen opens.
2. Above the list, click the **Create** button.
The New Virtual Server screen opens.
3. In the General Properties area, for the **Name** setting, type a unique name for the virtual server.
4. For the **Destination** setting, select the type, and type an address, or an address and mask, as appropriate for your network.
5. For the **Service Port** setting, either type **25** in the box, or select **SMTP** from the list.
6. Above the Configuration area, select **Advanced**.
The screen refreshes, and displays additional configuration options.
7. For the **SMTP Profile** setting, select the SMTP service protocol that you created.
8. For the **SNAT Pool** setting, if your network configuration requires address translation, select **Auto Map**.
9. In the Resources area, for the **Default Pool** setting, click the Create (+) button.
The New Pool screen opens.
10. On the New Pool screen, in the Configuration area, for the **Name** setting, type a unique name for the pool.
11. In the Resources area, for the **New Members** setting, you can add members to the pool by typing the IP addresses and ports, or by selecting addresses from a list.
 - Select **New Address** to type the address and port of any SMTP servers that you want to add to the configuration. (Note that the system automatically adds them as nodes, too.)

- Select **Node List** to select addresses from a list of servers that already exist in the local traffic configuration.
12. For the **Service Port** setting, select **SMTP** from the list.
 13. Click the **Add** button to add each node or address to the **New Members** list.
 14. Click **Finished**.
The screen refreshes, and returns you to the New Virtual Server screen. The new pool should be listed in the **Default Pool** setting.
 15. Click **Finished** on the New Virtual Server screen.
The screen refreshes, and you see the new virtual server in the list.

The system is now ready to scan SMTP traffic for vulnerabilities common to that protocol. See *Reviewing violations statistics for SMTP security profiles*, on page 4-7, for information on reviewing the SMTP security attacks that the system detects.

Reviewing violations statistics for SMTP security profiles

The Protocol Security Module provides statistics and other information about requests that trigger SMTP security violations. If you have enabled the Alarm flag for a violation, and an incoming request triggers a violation, the Protocol Security Module logs the request, which you can review from the Statistics screen of the Protocol Security Module. If you have enabled the Block flag for any of the SMTP security violations, then the Protocol Security Module blocks the request.

◆ Important

*The Protocol Security Module stores security violations in the system memory rather than on the hard disk. As a result, if you are using a redundant system, the violations data does not replicate to the other unit when you perform the **ConfigSync** operation.*

To review SMTP security violations

1. On the Main tab of the Application Security navigation pane, in the **Advanced Firewall** section, click **Statistics**.
The Statistics screen opens.
2. If the system has detected a violation, then the violation name becomes a hyperlink. Click the link to see details about the offending requests.
3. On the Statistics screen, you can also review information regarding the traffic volume for each service.

◆ Note

*For a description of each SMTP violation, and the event or events that trigger the violation, refer to **SMTP security violations**, on page A-4.*