



# 2

---

---

## Configuring Security for FTP Traffic

---

---

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

## Securing FTP traffic

When you configure the FTP security profile, the BIG-IP® Protocol Security Module inspects FTP traffic for network vulnerabilities. The Protocol Security Module provides the following security checks for FTP traffic:

- Blocks specific FTP commands.
- Blocks anonymous FTP requests.
- Blocks passive or active FTP requests.
- Blocks promiscuous FTP passive connections.
- Blocks promiscuous FTP port connections.
- Blocks FTP traffic when the command line length exceeds the defined length.
- Blocks excessive FTP login attempts.
- Blocks FTP traffic that fails protocol compliance checks.

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

---

**◆ 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 FTP traffic

The *FTP security profile* provides the security checks that are applicable to the FTP service. In the security profile, you also specify whether the Protocol Security Module logs violations to a remote logging server. By default, the Protocol Security Module retains up to 1000 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 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.

### ◆ Important

---

*The following task assumes that you have already set up remote logging.*

#### To create a security profile for FTP traffic

1. On the Main tab of the navigation pane, in the **Advanced Firewall** section, click **Security Profiles**.  
The HTTP Security Profiles screen opens in a new browser session.
2. From the Security Profiles menu, choose FTP.  
The FTP Security Profiles screen opens.
3. Above the FTP 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 **FTP security violations**, on page A-2, 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 FTP profile

Once you have created the FTP security profile in the Protocol Security Module, you create a local traffic FTP profile in the local traffic configuration. The local traffic FTP profile uses the FTP 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**. For information specific to the FTP service protocol, refer to **Configuring FTP profile settings**, in the chapter, **Managing Application Layer Traffic**, in the same guide.*

### To create a local traffic FTP 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 FTP.  
The FTP Profiles screen opens.
3. Above the list area, click the **Create** button.  
The New FTP 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 FTP protocol from which you want the new profile to inherit settings. The default setting is **ftp**.
6. Above the Settings area, check the **Custom** check box.  
The system activates the editing mode for the individual settings.
7. Clear the **Translate Extended** check box to disable IPv6 translation.
8. Leave the **Data Port** setting at the default setting, **20**.
9. Check the **Advanced Firewall** check box to enable the FTP security profile that you created.
10. Click **Finished**.  
The screen refreshes and displays the new local traffic FTP profile in the list.

## Assigning an FTP security profile to a local traffic FTP profile

When you enable the **Advanced Firewall** setting on the local traffic FTP profile, the system automatically assigns the first-listed FTP 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 FTP profile, the virtual server that uses the service profile, and the FTP security profile.

---

◆ **Tip**

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

### To modify the FTP 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 FTP.
3. In the FTP Security Profiles Assignment area, in the Assigned Security Profile column, for each traffic profile select the FTP 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 FTP profile, you will not see any virtual servers listed in the Virtual Servers column.*

---

## Configuring an FTP virtual server

You configure a local traffic virtual server and a default pool for the FTP servers, and associate the local traffic FTP profile that you created. This automatically associates the FTP security profile with the virtual server. The result is that when the virtual server receives FTP traffic, the FTP security profile in the Protocol Security Module scans the FTP 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 FTP 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 **21** in the box, or select **FTP** from the list.
6. Above the Configuration area, select **Advanced**.  
The screen refreshes, and displays additional configuration options.
7. For the **FTP Profile** setting, select the FTP 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. On the New Pool screen, 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 FTP 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. On the New Pool screen, for the **Service Port** setting, select **FTP** 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 FTP traffic for vulnerabilities common to that protocol. See *Reviewing violations statistics for security profiles*, on page 2-7, for information on reviewing the FTP security attacks that the system detects.

---

## Reviewing violations statistics for security profiles

The Protocol Security Module provides statistics and transaction information about FTP traffic that triggers FTP security violations. If you have enabled the Alarm flag for a violation, and incoming FTP traffic triggers the 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 FTP security violations, the Protocol Security Module blocks the request.

### ◆ Important

---

*The Protocol Security Module stores FTP 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 FTP security violations

1. On the Main tab of the Application Security navigation pane, 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 FTP violation, and the event or events that trigger the violation, refer to **FTP security violations**, on page A-2.*