



# 3

---

---

## Configuring Security for HTTP Traffic

---

---

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

---

## Securing HTTP traffic

When you configure the HTTP security profile, the BIG-IP® Protocol Security Module provides the following security checks for HTTP traffic:

- Validates HTTP protocol compliance
- Detects evasion techniques
- Performs length checks for URIs, query strings, POST data, and requests to help avoid buffer overflow attacks
- Validates HTTP methods
- Validates object types (file types)
- Enforces mandatory headers
- Masks sensitive data in responses with the Data Guard™ feature
- Validates acceptable response codes

For the HTTP security profile, you can also configure a blocking response page. If the system detects a violation according to the security profile settings, and you have enabled the Block flag for the violation, then instead of forwarding the request, the Protocol Security Module sends the blocking response page to the client.

To configure security checks for HTTP traffic, you create an HTTP security profile in the Protocol Security Module, and associate the security profile with a local traffic HTTP 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 HTTP service, see *Creating a security profile for HTTP traffic*, on page 3-2.
- To configure a local traffic HTTP profile and enable the Protocol Security Module, see *Creating a local traffic HTTP profile*, on page 3-14, and *Assigning an HTTP security profile to a local traffic HTTP profile*, on page 3-15.
- To configure a virtual server and pool for HTTP traffic, and associate the local traffic HTTP profile, see *Configuring an HTTP virtual server*, on page 3-16.

### ◆ 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 HTTP traffic

The *HTTP security profile* specifies the security checks that are applicable to the HTTP service, and enforced by the Security Enforcer. 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 HTTP 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. Above the HTTP Security Profiles area, click the **Create** button.  
The New Security Profile screen opens.
3. In the Profile Properties area, in the **Profile Name** box, type a unique name for the profile.
4. 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.*

5. 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.

The available security checks are:

- HTTP protocol checks. See *Configuring HTTP protocol checks*, on page 3-3, for more information.

- Evasion techniques checks. See *Configuring evasion techniques checks*, on page 3-4.
  - Length checks. See *Configuring length checks*, on page 3-5, for more information.
  - Methods checks. See *Configuring method checks*, on page 3-6, for more information.
  - Object types checks. See *Configuring object types checks*, on page 3-7, for more information.
  - Mandatory headers checks. See *Configuring mandatory headers*, on page 3-9, for more information.
  - Response checks. See *Configuring response checks*, on page 3-10, for more information.
6. In the Defense Configuration area, click the Blocking Page tab to configure the blocking response page. See *Configuring the blocking response page*, on page 3-12, for more information.
  7. Click **Create**.  
The screen refreshes, and you see the new security profile in the list.

## Configuring HTTP protocol checks

The first security checks that Protocol Security Module performs are those for RFC compliance for the HTTP protocol. If a request passes the compliance checks, then the system applies the security profile to the remainder of the request. You can also configure whether the system generates alarms, or blocks requests, for requests that trigger the **HTTP protocol compliance failed** violation.

## Understanding how HTTP protocol validation affects security checks

When Protocol Security Module receives a request from a client, the first aspect of the request that the system validates is HTTP protocol compliance. If the request does not comply with the following subset of HTTP protocol validations, the Security Enforcer cannot continue enforcing the security profile, and may pass the request on to the application resources even though it is not a valid request. There are several HTTP protocol validations that may cause this situation:

- **Unparsable request content**  
This security check fails when the Protocol Security Module is unable to parse the incoming request.
- **Null in request**  
This security check fails when the incoming request contains a null character.
- **Several Content-Length headers**  
This security check fails when the incoming request contains more than one Content-Length header.

We recommend that you retain the default properties for the HTTP protocol security checks. As an additional precaution, you may want to enable the Block flag for this security check, even if you enable only the Alarm flag for the other security checks. When you do this, the Security Enforcer blocks all requests that are not compliant with the HTTP protocol standards, and performs the additional security checks only on valid HTTP traffic.

## Configuring HTTP protocol checks

You can review and modify the validation options for the HTTP protocol compliance on the HTTP Protocol Compliance tab of the HTTP security profile defense configuration.

### ◆ Note

---

*The following procedure assumes you have already created a new security profile. Refer to **Creating a security profile for HTTP traffic**, on page 3-2, for more information.*

### To modify the HTTP protocol validation options

1. On the Main tab of the Application Security navigation pane, click **Security Profiles**.  
The HTTP Security Profiles screen opens.
2. In the HTTP Security Profiles area, in the Profile Name column, click the name of the security profile that you created.  
The Profile Properties screen opens.
3. In the Defense Configuration area, on the HTTP Protocol Checks tab, for the **HTTP Protocol Checks** setting, make any adjustments that are required. For an explanation of the individual security checks, refer to the online help.
4. Click **Update** to retain any changes you may have made.

## Configuring evasion techniques checks

For every HTTP request that the Protocol Security Module receives, the Security Enforcer applies a pre-processor to the requests. The pre-processor detects coding methods for application attacks that are designed to avoid detection. These coding methods are known as *evasion techniques*. Evasion techniques trigger the **Evasion technique detected** violation. The evasion techniques that the Security Enforcer detects are:

- Path traversal
- Multiple slash characters in a URI
- Bad unescape
- Bare byte decoding in a URI

In the HTTP security profile configuration, you can enable or disable the blocking policy for evasion techniques checks, but you cannot disable the evasion techniques detection. The system analyzes every request for evasion techniques, regardless of whether you have enabled the Alarm or Block actions for evasion techniques.

◆ **Note**

---

*The following procedure assumes you have already created a new security profile. Refer to **Creating a security profile for HTTP traffic**, on page 3-2, for more information.*

### **To modify the evasion techniques blocking policy**

1. On the Main tab of the Application Security navigation pane, click **Security Profiles**.  
The HTTP Security Profiles screen opens.
2. In the HTTP Security Profiles area, in the Profile Name column, click the name of the security profile that you created.  
The Profile Properties screen opens.
3. In the Defense Configuration area, on the HTTP Protocol Checks tab, for the **Evasion Techniques Checks** setting, check or clear the **Alarm** or **Block** check boxes as required.
  - Check **Alarm** if you want the system to log any requests that trigger the **Evasion technique detected** violation.
  - Check **Block** if you want the system to block any requests that trigger the **Evasion technique detected** violation.
  - Check both **Alarm** and **Block** if you want the system to perform both actions.
4. Click **Update** to retain any changes you may have made.

## Configuring length checks

In the HTTP security profile, by specifying valid maximum lengths for request components, the Security Enforcer can help prevent buffer overflow attacks. You can configure maximum lengths for URIs, query strings, POST data, and the entire request.

◆ **Note**

---

*The following procedure assumes you have already created a new security profile. Refer to **Creating a security profile for HTTP traffic**, on page 3-2, for more information.*

### **To modify the length checks**

1. On the Main tab of the Application Security navigation pane, click **Security Profiles**.  
The HTTP Security Profiles screen opens.

2. In the HTTP Security Profiles area, in the Profile Name column, click the name of the security profile that you created. The Profile Properties screen opens.
3. In the Defense Configuration area, click the Lengths tab.
4. On the Lengths tab, for the **Length Checks** setting, make any adjustments to the length options as required.
5. Check or clear the **Alarm** or **Block** check boxes as required.
  - Check **Alarm** if you want the system to log any requests that trigger length violations.
  - Check **Block** if you want the system to block any requests that trigger length violations.
  - Check both **Alarm** and **Block** if you want the system to perform both actions.
6. Click **Update** to retain any changes you may have made.

## Configuring method checks

The Protocol Security Module accepts certain HTTP methods by default. The default methods are GET, POST, and HEAD. The system treats any incoming HTTP request that uses an HTTP method other than the allowed methods as an invalid request. If your application uses HTTP methods other than the default allowed methods, you can use the methods security check to manage them.

### ◆ Note

---

*The following procedure assumes you have already created a new security profile. Refer to **Creating a security profile for HTTP traffic**, on page 3-2, for more information.*

### To modify the allowed methods configuration

1. On the Main tab of the Application Security navigation pane, click **Security Profiles**. The HTTP Security Profiles screen opens.
2. In the HTTP Security Profiles area, in the Profile Name column, click the name of the security profile that you created. The Profile Properties screen opens.
3. In the Defense Configuration area, click the Methods tab.
4. On the Methods tab, for the Methods setting, you can perform the following actions:
  - Select a method from the **Available** list, and add it to the **Allowed** list.

- Type the name of a method in the **Method** box, and click the **Add** button to add it to the **Available** list. You can then move the new method to the **Allowed** list, by using the Move [ << ] button. Use this option if the method you want to allow is not in the system-supplied list.
5. Check or clear the **Alarm** or **Block** check boxes as required.
    - Check **Alarm** if you want the system to log any requests that trigger the **Illegal method** violation.
    - Check **Block** if you want the system to block any requests that trigger the **Illegal method** violation.
    - Check both **Alarm** and **Block** if you want the system to perform both actions.
  6. Click **Update** to retain any changes you may have made.

## Configuring object types checks

By default, the HTTP security profile permits all object types, that is, file types. For tighter security, you can create either an allowed object types list, or a disallowed object types list. Note that you cannot create an allowed object types list and a disallowed object types list.

### Creating an allowed object types list

When you create an allowed object types list, the Security Enforcer permits only requests whose file type matches one of those in the list to access the back-end resources. The system alarms, or blocks (if configured), for all other object types. You create the allowed object types list by selecting from the available object types list. You can also add custom object types to the available list.

#### **Important**

*The object types lists are case-sensitive. For example, the Security Enforcer treats **jsp** and **JSP** as separate file types.*

#### **To create an allowed object types list**

1. On the Main tab of the Application Security navigation pane, click **Security Profiles**.  
The HTTP Security Profiles screen opens.
2. In the HTTP Security Profiles area, in the Profile Name column, click the name of the security profile that you created.  
The Profile Properties screen opens.
3. In the Defense Configuration area, click the Object Types tab.
4. On the Object Types tab, for the **Object Types** setting, select **Define Allowed** from the list.

5. To create the actual allowed object types list, you can perform the following actions:
  - Select an object type from the **Available** list, and add it to the **Allowed** list.
  - Type an object type in the **Object type** box, and click the **Add** button to add it to the **Available** list. You can then move the new object type to the **Allowed** list, by using the Move [<<] button. Use this option if the object type you want to allow is not in the system-supplied list.
6. Check or clear the **Alarm** or **Block** check boxes as required.
  - Check **Alarm** if you want the system to log any requests that trigger the **Illegal object type** violation.
  - Check **Block** if you want the system to block any requests that trigger the **Illegal object type** violation.
  - Check both **Alarm** and **Block** if you want the system to perform both actions.
7. Click **Update** to retain any changes you may have made.

## Creating a disallowed object types list

If you create a disallowed object types list, the Security Enforcer permits all requests, except for those object type matches one of those in the list. The system alarms, or blocks (if configured), for the object types that match the disallowed object types list.

### **Important**

---

*The object types lists are case-sensitive. For example, the Security Enforcer treats **jsp** and **JSP** as separate file types.*

### **To create a disallowed object types list**

1. On the Main tab of the Application Security navigation pane, click **Security Profiles**.  
The HTTP Security Profiles screen opens.
2. In the HTTP Security Profiles area, in the Profile Name column, click the name of the security profile that you created.  
The Profile Properties screen opens.
3. In the Defense Configuration area, click the Object Types tab.
4. On the Object Types tab, for the **Object Types** setting, select **Define Disallowed** from the list.
5. To create the actual disallowed object types list, you can perform the following actions:
  - Select an object type from the **Available** list, and add it to the **Disallowed** list.

- Type an object type in the **Object type** box, and click the **Add** button to add it to the **Available** list. You can then move the new object type to the **Disallowed** list, by using the Move [<<] button. Use this option if the object type you want to disallow is not in the system-supplied list.
6. Check or clear the **Alarm** or **Block** check boxes as required.
    - Check **Alarm** if you want the system to log any requests that trigger the **Illegal object type** violation.
    - Check **Block** if you want the system to block any requests that trigger the **Illegal object type** violation.
    - Check both **Alarm** and **Block** if you want the system to perform both actions.
  7. Click **Update** to retain any changes you may have made.

## Configuring mandatory headers

If your application uses custom headers that must occur in every request, you can use the mandatory headers option to include them in the security profile. If you specify mandatory headers in the security profile, then the Security Enforcer verifies that requests contain those headers. If a request does not contain the mandatory header, the system issues the **Mandatory HTTP header is missing** violation, and applies the blocking policy to the request.

### To configure a mandatory header

1. On the Main tab of the Application Security navigation pane, click **Security Profiles**.  
The HTTP Security Profiles screen opens.
2. In the HTTP Security Profiles area, in the Profile Name column, click the name of the security profile that you created.  
The Profile Properties screen opens.
3. In the Defense Configuration area, click the Mandatory Headers tab.
4. For the **Mandatory Headers** setting, in the **Headers** box, type the name of the mandatory header, and click the **Add** button to add it to the **Available** list.
5. Move the new mandatory header from the **Available** list to the **Mandatory** list, by using the Move [<<] button.
6. Check or clear the **Alarm** or **Block** check boxes as required.
  - Check **Alarm** if you want the system to log any requests that trigger the **Mandatory HTTP header is missing** violation.
  - Check **Block** if you want the system to block any requests that trigger the **Mandatory HTTP header is missing** violation.

- Check both **Alarm** and **Block** if you want the system to perform both actions.
7. Click **Update** to retain any changes you may have made.

## Configuring response checks

The HTTP security profile uses response checks to discover common vulnerabilities in server responses. The Data Guard response check detects sensitive user information in the server response. The allowed response codes list specifies which HTTP response codes are acceptable in the server response.

## Configuring the Data Guard feature

Depending on the application, a response may contain sensitive user information, such as credit card numbers, or social security numbers (U.S. only). You can configure the Data Guard™ feature to prevent responses from exposing this sensitive information. This process is known as *response scrubbing*. In addition to protecting credit card numbers and social security numbers, you can configure custom patterns, by using PCRE-compliant regular expressions, to match other types of sensitive information.

When the system detects sensitive information in a response, and you have enabled the Data Guard feature, the system generates the **Information leakage detected** violation. Additionally, if you have enabled the Block action, the system does not send the response to the client.

### Important

---

*When you enable the **Mask Data** option, in the server response, the system replaces sensitive data with asterisk characters (\*\*\*\*). We recommend that you enable this setting if you enable only the Alarm action for the Data Guard feature. Otherwise, when the system returns the response, the sensitive data is exposed to the client.*

### To configure response scrubbing

1. On the Main tab of the Application Security navigation pane, click **Security Profiles**.  
The HTTP Security Profiles screen opens.
2. In the HTTP Security Profiles area, in the Profile Name column, click the name of the security profile that you created.  
The Profile Properties screen opens.
3. In the Defense Configuration area, click the Response Checks tab.
4. For the **Data Guard** setting, check the sensitive data that you want the system to identify in responses. The online help describes the options.
5. Check the **Mask data** box if, in the response, you want the system to replace the sensitive data with asterisk characters.

6. Check or clear the **Alarm** or **Block** check boxes as required.
  - Check **Alarm** if you want the system to log any requests that trigger the **Information leakage detected** violation.
  - Check **Block** if you want the system to block any requests that trigger the **Information leakage detected** violation.
  - Check both **Alarm** and **Block** if you want the system to perform both actions.
7. Click **Update** to retain any changes you may have made.

## Configuring allowed response codes

For the HTTP security profile, the allowed response codes determine which response codes are acceptable within a server response. If the HTTP response code is in the 4XX range or the 5XX range, then only responses with a response code that appears in this list are returned as-is to the client. If a response contains a response code other than those specified in the allowed response code list, and the response code is in the 4XX range or the 5XX range, then the system issues the **Illegal HTTP status in response** violation, and, if blocking is enabled for this violation, blocks the response.

### ◆ Note

*The allowed response codes configuration does not apply to response codes in the 1XX, 2XX, or 3XX ranges.*

### To modify allowed response codes

1. On the Main tab of the Application Security navigation pane, click **Security Profiles**.  
The HTTP Security Profiles screen opens.
2. In the HTTP Security Profiles area, in the Profile Name column, click the name of the security profile that you created.  
The Profile Properties screen opens.
3. In the Defense Configuration area, click the Response Checks tab.
4. For the **Allowed Response Codes** setting, in the **New Response Code** box, type a response code and click the **Add** button to add the response code to the list. By default, the Allowed Response Codes list contains these response codes: **400, 401, 404, 401, 417, 503**.
5. Check or clear the **Alarm** or **Block** check boxes as required.
  - Check **Alarm** if you want the system to log any requests that trigger the **Illegal HTTP status in response** violation.
  - Check **Block** if you want the system to block any requests that trigger the **Illegal HTTP status in response** violation.
  - Check both **Alarm** and **Block** if you want the system to perform both actions.

6. Click **Save** to save any changes you may have made to the security policy properties.

## Configuring the blocking response page

The Protocol Security Module has a default response page that it returns to the client when the client request, or the web server response, is blocked by the security profile. This page is the *blocking response page*.

### ◆ Important

---

*The system issues the response pages only when the enforcement mode is **Blocking**.*

The following options are available for the response page:

- You can use the default response page.
- You can customize the default blocking response page.
- You can upload a custom blocking response page.
- You can provide a URL for redirection.

### To customize the blocking response page

1. On the Main tab of the Application Security navigation pane, click **Security Profiles**.  
The HTTP Security Profiles screen opens.
2. In the HTTP Security Profiles area, in the Profile Name column, click the name of the security profile that you created.  
The Profile Properties screen opens.
3. In the Defense Configuration area, click the Blocking Page tab.
4. For the **Response Type** setting, select one of the following options:
  - **Default Response**: Specifies that the system returns the system-supplied blocking response page. Note that you cannot edit HTML code on the default response page.
  - **Custom Response**: Specifies that the system returns a user-defined response page.
  - **Redirect URL**: Specifies that the system returns a redirect URL to the client.

*Note: The settings on the screen change depending on the selection that you make for the **Response Type** setting.*

5. If you selected the **Custom Response** option in step 4, you can either modify the default text, or upload an HTML file.
  - To modify the default text:

- For the **Response Header** setting, click the **Paste Default Response Header** button, and make any changes as required. Note that you should use standard HTML syntax for this setting and the **Response HTML Code** setting.
  - For the **Response HTML Code** setting, click the **Paste Default Response HTML Code** button, and make any changes as required.
  - To upload an HTML file:
    - For the **Upload HTML File** setting, either type a path to an HTML response page in the box, or click **Browse** and navigate to an HTML response page.
    - Click **Upload** when you are finished.
6. If you selected the **Redirect URL** option in step 4, then in the **Redirect URL** box, type the URL to which the system redirects the client. The URL that you configure should be for a page that is not within the web application itself.
  7. Click **Update** to save any changes you may have made.

## Creating a local traffic HTTP profile

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

◆ **Note**

---

*For more information about local traffic profiles in general, refer to the **Understanding Profiles** chapter in the **Configuration Guide for BIG-IP® Local Traffic Management**. For information specific to the HTTP service protocol, refer to **Configuring HTTP standard profile settings**, in the **Managing Application Layer Traffic** chapter in the same guide.*

### To create a local traffic HTTP profile

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

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

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

---

### ◆ Tip

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

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

## Configuring an HTTP virtual server

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

### ◆ Note

---

*For detailed information about local traffic virtual servers, refer to the **Configuring Virtual Servers** chapter in the **Configuration Guide for BIG-IP® Local Traffic Management**, which is available from the Ask F5 web site, <https://support.f5.com>.*

### To create a local traffic virtual server for HTTP 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, type either **80** (for HTTP) or **443** (for HTTPS) in the box. Alternately, select **HTTP** or **HTTPS** from the list.
6. Above the Configuration area, select **Advanced**.  
The screen refreshes, and displays additional configuration options.
7. For the **HTTP Profile** setting, select the HTTP 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 HTTP 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 **HTTP** 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 HTTP traffic for vulnerabilities common to that protocol. See *Reviewing violations statistics for HTTP security profiles*, on page 3-18, for information on reviewing the HTTP security attacks that the system detects.

## Reviewing violations statistics for HTTP security profiles

The Protocol Security Module provides statistics and other information about requests that trigger HTTP 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 HTTP security violations, the Protocol Security Module blocks the request and sends the blocking response page, which includes the Support ID, to the offending client.

### ◆ 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 HTTP 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. Optionally, use the **Search by Support ID (HTTP)** setting to find a violation by the Support ID.
4. On the Statistics screen, you can also review information regarding the traffic volume for each service.

### ◆ Note

---

*For a description of each HTTP violation, and the event or events that trigger the violation, refer to **HTTP security violations**, on page A-3.*