Web Application Security Configuration

This chapter describes how to configure web application security. The following topics are covered:

- Overview
- Global Configuration and Utilities
- Security Feature Configuration
- Web Application Security Regular Expression Syntax

Overview

The web application security feature enables the application appliance to act as an application firewall and provide web application security and intrusion protection.

Note

The web application security module described in this chapter supersedes the AppScreen security feature described in Chapter 7, “AppScreen Configuration,” which is still available and operates as before for backward compatibility. For the highest level of web application security, we recommend that you use the web application security module described in this chapter instead of AppScreen.

Web application security is highly configurable, and can protect against the following kinds of application attacks:

- identity theft
- SQL, OS, and LDAP command injection
- cross site scripting
- meta character and format string attacks
- buffer overflow
- form exploitation
- URL redirects and directory traversal
- error message exploitation
- cookie exploitation
- noncompliant HTTP
- web server fingerprinting
You configure web application security through the management console GUI by using the menu commands under the Web Application Security folder that appears under the Cluster Configuration item under a cluster name. For details on using the management console, creating a cluster, and registering nodes in it, see Chapter 8, “Management Console.”

To configure web application security, follow these basic steps:

1. Use the Traffic Class Maps command to define traffic class maps to classify web application traffic according to various parameters such as hostname, URL, cookie name and value, and so on. A traffic map specifies a set of traffic to which you want to apply a security policy.


3. Use the Policy Maps command to define policy maps that associate a traffic class with a set of security functions. A policy map defines a series of actions (functions) that you want to apply to a set of classified traffic.

4. Use the System Utilities Service Policy command to choose the active policy map.

5. Use the System Utilities Commit Config command to commit the configuration.

6. If you have a cluster of application appliance nodes, use the System Utilities Publish Configuration command to publish the configuration to all nodes in the cluster.

Map Summary Interface

Most of the features in the Web Application Security module use the term “map” for a set of options that configure the feature in a specific way. A map is named and stored, and then it can be viewed, cloned, edited, or deleted. Every feature that uses maps presents a summary list of those that are defined when you first click on the feature command name under the Web Application Security module, as shown in Figure 6-1. If there are no maps yet defined for the feature, then the summary says “No Maps Configured.”

This section describes how to interact with a map summary screen.

Figure 6-1  Map Summary Example
The example in Figure 6-1 shows the map summary that is displayed when you click on the Request Limits command. Every other map summary looks similar and contains similar controls. The following paragraphs describe how to use the controls on a map summary page.

Each row in the summary lists one defined map. Using the controls on a summary row you can view, clone, edit, or delete the map.

To view the definition of a map, click its underlined name at the left end of the row. The displayed page shows a read-only listing of the map definition.

To copy a map to use as the basis of a new map, click the Clone button next to the map that you want to clone. AVS displays a map editing screen that is similar to the one shown when you are adding a new map, except that all the settings are copied from the map that you cloned.

To edit a map, click the Edit button in the summary. AVS displays a map editing screen where you can change the settings in the map.

To delete one or more maps, check the box in the Delete column for each map that you want to delete. Then click the Delete Maps button to delete the checked maps.

To add a new map, click the Add New Map button to display a map editing screen where you can define the map and give it a name. The sections throughout this chapter describe the unique map editing screens for each feature.

You can click the links in the blue bar at the top of the frame to go directly to the screens identified by name.

**Global Configuration and Utilities**

This section describes the following global configuration and utility items that appear under the Web Application Security folder in the lefthand menu of the management console:

- System Utilities
- Traffic Class Maps
- Policy Maps
- Pattern Definitions

**System Utilities**

Various utilities let you manage web application security configuration, logging, and statistics.

Use the System Utilities command to display a page that contains links to the system utilities, as shown in Figure 6-2. To use a utility function, click on its link.
The following sections describe the two groups of items listed on the System Utilities page:

- **Display Utilities**
- **Configuration Utilities**

### Display Utilities

The utilities grouped under the Display Utilities heading let you display various information. The following items are included:

- **Startup Configuration**
- **Running Configuration**
- **New Configuration**
- **System Stats**
- **Traffic Level Stats**
- **Policy Level Stats**
- **Current Log**
- **Saved Log**
- **Show Version**
- **Show Tech Support**
- **Default Config**

### Startup Configuration

The **Startup Configuration** link displays the default web application security configuration. This information is not relevant for users; it is for debugging only.
Running Configuration

The **Running Configuration** link displays the web application security configuration that is currently in effect. This information is not relevant for users; it is for debugging only.

New Configuration

The **New Configuration** link displays the web application security configuration that is being configured, but not yet committed. This information is not relevant for users; it is for debugging only.

System Stats

Click **System Stats** to display statistics related to the web application security operation and features, as shown in **Figure 6-3**.

**Figure 6-3      System Statistics**

![AVS Management Console](image)

The statistics are initially shown for the master node, which is the first AVS 3120 node that is added to the cluster in the management console. To show statistics for a different node, click on the link with the node name in the Nodes field at the top of the screen. You can click the links above the table to jump directly to the section of the table that shows statistics for the feature named in the link. For each item in the table, the statistic shows a number of bytes or the number of times the event has occurred.
Traffic Level Stats

Click **Traffic Level Stats** to display statistics organized by traffic classification map. The display looks similar to that shown in Figure 6-3, but a full set of statistics is listed for each traffic class map. Links to each of the traffic class maps appear across the top of the screen; click one to jump to the statistics for that map. For more information about traffic class maps, see the “Traffic Class Maps” section on page 6-17.

The statistics are initially shown for the master node, which is the first AVS 3120 node that is added to the cluster in the management console. To show statistics for a different node, click on the link with the node name in the Nodes field at the top of the screen.

Policy Level Stats

Click **Policy Level Stats** to display statistics organized by policy map. The display looks similar to that shown in Figure 6-3, but a full set of statistics is listed for each policy map. Links to each of the policy maps appear across the top of the screen; click one to jump to the statistics for that map. For more information about policy maps, see the “Policy Maps” section on page 6-21.

The statistics are initially shown for the master node, which is the first AVS 3120 node that is added to the cluster in the management console. To show statistics for a different node, click on the link with the node name in the Nodes field at the top of the screen.

Current Log

Click **Current Log** to display the current web application security log, as shown in Figure 6-4. The content of the current log varies depending on your system configuration, as follows:

- If you have an AVS 3180 Management Station, then **Current Log** displays the log file of the master node (the first AVS 3120 node that was added to the cluster).
- If you do not have an AVS 3180 Management Station, then **Current Log** displays the log file of the current AVS 3120 node on which you are running the management console.
Figure 6-4 Current Log Display

You can scroll the log window to the right to see additional columns that include the URI, the feature responsible for the log entry, the policy map, traffic class map, feature map, and the log message. The policy map, traffic class map, and feature map names are hyperlinks, which when clicked will take you to a screen where you can edit the named map.

This page displays log entries from all web application security features by default. You can filter the displayed log items by feature by choosing the feature from the Filter By Feature drop-down list. Then click Refresh Saved Logs.

You can clear the current log file by using Clear Current Logs.

Saved Log

Click Saved Log to display the saved log, which looks similar to Figure 6-4. The saved log item works differently, depending on your system configuration, as follows:

- If you have an AVS 3180 Management Station, then Saved Log displays the aggregate log file of all AVS 3120 nodes that are part of the cluster in the management console. (In order to aggregate log files from all nodes in the cluster, you must configure all nodes to send log messages to the AVS 3180 Management Station, as described in the “Log Server Config” section on page 6-16.)
- If you do not have an AVS 3180 Management Station, then Saved Log displays nothing and is not useful.

The log filtering works the same as for Current Log.

Show Version

Click Show Version to display version information about the web application security software.
Show Tech Support

Click **Show Tech Support** to display information about the web application security software that can be helpful for technical support.

Default Config

Click **Default Config** to display a page that controls the defaults for various web application security features, as shown in Figure 6-5.

**Figure 6-5  Default Configuration**

This page lists the web application security features and pattern definitions that can have default configurations. A default configuration is the configuration that appears when you create a new map for a feature.

To view the default configuration for a feature or pattern definition, click the View link next to its name. To enable the feature or pattern definition to have a default configuration, check the Enable check box.

If you make any changes to this screen, click **Apply Changes** at the top to save your changes, or click another AVS command in the lefthand menu to exit this screen without saving your changes.
You can change the default configuration for a feature or pattern definition by creating a new map for it, configuring the settings as needed, and clicking the Set As Default button. Creating a default in this way will automatically enable the default configuration if it is not already enabled.

Configuration Utilities

The utilities grouped under the Configuration Utilities heading let you manage the global web application security configuration and logging. The following items are included:

- System Settings
- Cluster Control
- Publish Configuration
- Service Policy
- Clear System Config
- Commit Config
- Force Commit
- Save Config
- Clear Config
- Clear System Stats
- Clear Traffic Stats
- Clear Policy Stats
- Log Server Config
- Clear Current Logs

System Settings

Click System Settings to display a page that controls overall web application security system operation, as shown in Figure 6-6.
From the Mode of Operation drop-down list, choose one of the following operation modes for the web application security module:

- **Inline**—This mode is used for web application security only; no other AVS features can be used or should be configured, including destination mapping or SSL termination. In this mode, the application appliance acts like a transparent bridge, monitoring traffic on incoming port 3, checking security policies and taking action if necessary, then forwarding the traffic to the web servers on outgoing port 4. Ports 3 and 4 do not have IP addresses and so do not terminate TCP/IP connections. Port 1 is used for management console connectivity and port 2 is not used.

- **Gateway**—This mode is used when you want to operate other AVS features in addition to web application security. For this mode, you must configure at least destination mapping in the application appliance. For details, see the “Destination Mapping Configuration” section on page 5-30. In this mode, traffic enters and leaves the application appliance on port 1, which is also used for management console connectivity. The other three ports are not used.

- **Monitor**—This mode is used for monitoring traffic only; no other AVS features can be used or should be configured. No packets are modified by the web application security module, but instead it only logs events that match security policies. You can use this mode of operation if you want to passively examine your web application traffic for possible security threats. Connect network traffic that you want to monitor to port 2 on the AVS 3120. For example, you can connect port 2 to the

---

**Note**

In gateway mode, SSL-encrypted HTTPS traffic that arrives at the application appliance is decrypted and forwarded to the web servers as unencrypted HTTP traffic if the web application firewall is in use. HTTPS traffic between the application appliance and the web servers is not supported unless the web application firewall is disabled.

---

- **Monitor**—This mode is used for monitoring traffic only; no other AVS features can be used or should be configured. No packets are modified by the web application security module, but instead it only logs events that match security policies. You can use this mode of operation if you want to passively examine your web application traffic for possible security threats. Connect network traffic that you want to monitor to port 2 on the AVS 3120. For example, you can connect port 2 to the
monitor port or Switched Port Analyzer (SPAN) port on a switch. Port 2 does not have an IP address and so does not terminate TCP/IP connections. Port 1 is used for management console connectivity and ports 3 and 4 are not used.

The port assignments for the various operating modes are summarized in Table 6-1.

<table>
<thead>
<tr>
<th>Operating Mode</th>
<th>Port 1</th>
<th>Port 2</th>
<th>Port 3</th>
<th>Port 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inline</td>
<td>management console</td>
<td>not used</td>
<td>incoming client traffic</td>
<td>outgoing server traffic</td>
</tr>
<tr>
<td>Gateway</td>
<td>management console and web traffic</td>
<td>not used</td>
<td>not used</td>
<td>not used</td>
</tr>
<tr>
<td>Monitor</td>
<td>management console</td>
<td>monitored traffic</td>
<td>not used</td>
<td>not used</td>
</tr>
</tbody>
</table>

Note: If you change operating modes, for example from inline to gateway mode, you must restart the web application security module. For details, see the “Cluster Control” section on page 6-11. This is a major change that will likely also require you to reconfigure your network routing.

In all of the operation modes, the application appliance inspects traffic that is going to and coming from the web servers.

In the Software Auto Bypass drop-down list, choose Yes if you want to enable automatic bypass in inline mode. Automatic bypass causes the application appliance to bridge packets between the incoming and outgoing ports if the web application security module fails, which allows clients to continue to access the web servers without security checks. If you choose No and the web application security module fails, client requests will not be forwarded to the web servers.

In the Old Configuration Expires After field, enter the time in seconds to allow any HTTP sessions that are in progress to finish before changing configuration when a new configuration is committed. During this grace period, the old configuration still applies to active HTTP sessions. When this period of time expires, any HTTP sessions that are still in progress are closed and the new configuration is applied.

In the Servers to protect area, you must enter the IP addresses and ports of each web server that you want the web application security module to protect. Enter the IP address of a web server in the IP address field, check the Add box, and click Update Servers. Then you will see a Port field displayed under the IP address. Enter the port to protect, check the Add box next to the port, and click Update Servers. Repeat this procedure to add each port that you want to protect on the web server.

Repeat entering the IP address and ports of each web server that you want to protect. To delete a port or web server IP address, check the Delete check box next to the port or IP address and click Update Servers.

When you are finished with this form, click Apply Changes at the top to save your changes, or click Discard Changes to return to the utilities main page without saving your changes.

Cluster Control

Click Cluster Control to display a page that allows you to stop, start or restart the web application security firewall module on individual application appliance nodes, as shown in Figure 6-5.
This screen shows the status (Running or Stopped) of the web application security firewall module for each node in the cluster.

You can run, stop, or restart the web application firewall module on the nodes in the cluster. Check the check boxes next to the nodes that you want to control, and then click Run, Stop, or Restart to perform that operation on the checked nodes. You can use the Include All Nodes and Exclude All Nodes buttons at the top to check or clear all check boxes.

If you want to control the status of both the Condenser and web application security firewall modules, you can use the Cluster Control command under the cluster name in the lefthand menu. For details, see the “Cluster Control” section on page 8-8.

Publish Configuration

Click Publish Configuration to display a page that allows you to publish a configuration to all nodes in a cluster, as shown in Figure 6-8.
In the Publish Configuration area of the form, click the Publish button to publish the running configuration of the master AVS 3120 node to all other nodes in the same cluster. If there are no other nodes in the cluster, the Publish button is not shown.

The master node is the first AVS 3120 node that is added to the cluster in the management console. If that node is removed, then the next added node becomes the master node, and so on. The master node is identified at the top of the Publish Configuration page.

To cancel the operation and go back to the System Utilities page click Back.

Use the Publish button in situations where the master node is stable and one of the other nodes restarts or a new node is added to the cluster.

Note: All AVS 3120 nodes in a cluster must have the same web application security running configuration. If you are operating a cluster, you must publish the web application security configuration of the master node to all other nodes.

In the Synchronize Configuration area of the form, click the Sync button to publish the configuration that is saved on the management console to all nodes in the same cluster.

Use the Sync button in situations where the master node is restarted with a different configuration and you want to resynchronize it and all other nodes with the saved configuration that is stored in the management console.

To view the saved configuration that will be published to all nodes, click the View Last committed Configuration link.
Service Policy

Click **Service Policy** to display a page that allows you to choose the active policy map, as shown in **Figure 6-9**.

![Service Policy](image1)

**Figure 6-9 Service Policy**

In the Select Policy Map drop-down list, choose the policy map that you want to be active. Then click **Apply Changes** at the top to save your changes, or click **Discard Changes** to discard your changes.

Only one policy map can be active at a time. The setting on this screen interacts with enabling a policy map on the policy map summary screen shown in **Figure 6-13**. Setting a policy to be enabled in that screen will cause it to be the selected service policy in this service policy screen.

Clear System Config

Click **Clear System Config** to clear the saved **System Settings** on the master AVS 3120 node. The master node is the first AVS 3120 node that is added to the cluster in the management console. You are asked in a confirmation dialog if you are sure that you want to clear the configuration. Click **OK** to clear or **Cancel** to cancel.

This command clears only the system settings, not the policy configuration. To clear the policy configuration, use **Clear Config**.

Commit Config

Configuration changes that you make to web application security policies must be committed before they take effect and are applied to web traffic. Before they are committed, they are stored temporarily by the management console but are not saved or applied to the AVS 3120 node where the web application security module operates.

Click **Commit Config** to commit the configuration changes to the master AVS 3120 node and to save them on the management console. The master node is the first AVS 3120 node that is added to the cluster in the management console. You are asked in a confirmation dialog if you are sure that you want to commit the configuration. Click **OK** to commit or **Cancel** to cancel.

If any HTTP sessions are in progress, they are given a grace period in which to finish, before the new configuration takes effect. This grace period is configurable and is described in the “**System Settings**” section on page 6-9. During this period, you normally cannot commit a second new configuration. If you need to commit another configuration before this interval has passed, use **Force Commit**.
After committing a configuration, we recommend that you save the configuration on the master node by using **Save Config**. If you have a cluster of AVS 3120 nodes, you must also publish the configuration to all nodes in the cluster by using **Publish Configuration**. The application appliance does not support a cluster where the nodes have different web application security configurations.

### Force Commit

Click **Force Commit** to immediately commit configuration changes, if you have recently committed another configuration and the grace period for that commit has not yet expired. See the previous section, **Commit Config**, for details.

You are asked in a confirmation dialog if you are sure that you want to force commit the configuration. Click **OK** to commit or **Cancel** to cancel.

After committing a configuration, we recommend that you save the configuration by using **Save Config**. If you have a cluster of AVS 3120 nodes, you must also publish the configuration to all nodes in the cluster by using **Publish Configuration**. The application appliance does not support a cluster where the nodes have different web application security configurations.

### Save Config

Click **Save Config** to save the running configuration on the master AVS 3120 node so that it will be preserved across a reboot of that node. The master node is the first AVS 3120 node that is added to the cluster in the management console. You are asked in a confirmation dialog if you are sure that you want to save the configuration. Click **OK** to save or **Cancel** to cancel.

After committing a configuration by using **Commit Config**, we recommend that you save the configuration by using **Save Config**.

### Clear Config

Click **Clear Config** to clear the saved policy configuration on the master AVS 3120 node. The master node is the first AVS 3120 node that is added to the cluster in the management console. You are asked in a confirmation dialog if you are sure that you want to clear the configuration. Click **OK** to clear or **Cancel** to cancel.

Clearing the configuration clears only the saved copy of the configuration on the master AVS 3120 node. It does not clear the running configuration, so the node will continue to operate with its running configuration. If it is rebooted, that configuration will be lost because it is no longer saved.

### Clear System Stats

Resets the statistics accumulated and displayed by the **System Stats** command.

### Clear Traffic Stats

Resets the statistics accumulated and displayed by the **Traffic Level Stats** command.

### Clear Policy Stats

Resets the statistics accumulated and displayed by the **Policy Level Stats** command.
Log Server Config

The log server configuration page lets you configure remote logging for the web application security firewall. Web application security logs are separate from other AVS logs. Click the Log Server Config link to display the page shown in Figure 6-10, where you can configure remote syslog servers to which logs are sent by the web application security module.

Figure 6-10 Log Server Configuration

In the IP Address field, enter the IP address of a remote server to which AVS should send web application security logs. Check the Add check box and click Update IP Addresses to add the address to the list of remote log servers. Repeat these steps to add additional remote log servers. To delete a log server from the list, check the Delete check box next to it and click Update IP Addresses.

The servers that you specify must have the syslog facility running and configured to receive messages from the network.

If you are managing a cluster of AVS 3120 nodes with the AVS 3180 Management Station, you must configure the AVS 3180 as one of the remote log servers. This allows the management console to display aggregated logs from all nodes in the cluster (see the “Saved Log” section on page 6-7). If you do not have an AVS 3180 Management Station, you may still want to enter the IP address of at least one remote log server where logs will be aggregated, though these will not be accessible through the management console interface.

When you are finished with this form, click Apply Changes at the top to save your changes, or click Discard Changes to discard your changes.

Clear Current Logs

Clears the current log file. The current log file is different, depending on your configuration, as follows:

- If you have an AVS 3180 Management Station, then Clear Current Logs clears the log file of the first AVS 3120 node that is listed in the cluster in the management console.
- If you do not have an AVS 3180 Management Station, then Clear Current Log clears the log file of the current AVS 3120 node on which you are running the management console.

To view the current log file, use Current Log.
Traffic Class Maps

Traffic mapping allows you to classify HTTP request and response traffic according to a set of definable criteria. You must define a traffic map to select a set of traffic before you can apply security features to the traffic in a policy map.

Use the Traffic Class Maps command to display a page that summarizes the traffic classification maps that are defined, as shown in Figure 6-11.

Figure 6-11 Traffic Map Summary

Each row in the summary lists one defined traffic map. From here you can view, clone, edit, or delete a traffic map, or add a new map.

To view the definition of a traffic map, click its underlined name. The displayed page shows a read-only listing of the definition.

The Match column lists the matching policy of the map.

To copy a map to use as the basis of a new map, click the Clone button for the traffic map that you want to copy.

To edit a traffic map, click the Edit button for the map that you want to edit. A form similar to that shown in Figure 6-12 is displayed where you can edit the traffic map.

To delete one or more traffic maps, check the box in the Delete column for each map that you want to delete. Click Delete to delete the checked maps.

To add a new traffic map, use the Add Traffic Class area below the summary table. Give the map a name in the Map Name field. To determine how the criteria in this map are to be applied, choose one of the following radio buttons below this field:

- Match Any Criteria—This traffic map is applied if any one of the criteria is satisfied
- Match All Criteria—This traffic map is applied only if all of the criteria are satisfied
Then click the **Add New Map** button to create the traffic map. You are returned to the map summary page where you will see the new traffic map listed. To continue the process of defining the new map, click the **Edit** button for the map to display the screen shown in *Figure 6-12*. One criteria line has already been added to this traffic map.

*Figure 6-12  Edit New Traffic Classification Map*

You can add criteria lines that describe one or more characteristics of the traffic that you want to classify. From the Type drop-down list, select the traffic type: Request or Response. Next select the type of HTTP data that you want to examine for a match in the Match Criteria drop-down list. The match criteria choices are listed in *Table 6-2*.

*Table 6-2  Traffic Class Match Criteria*

<table>
<thead>
<tr>
<th>Type</th>
<th>Match Criteria</th>
<th>Description of Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request</td>
<td>cookie-name</td>
<td>Name of a request cookie</td>
</tr>
<tr>
<td>Request</td>
<td>cookie-name-value</td>
<td>Name and value of a request cookie</td>
</tr>
<tr>
<td>Request</td>
<td>cookie-value</td>
<td>Value of a request cookie</td>
</tr>
<tr>
<td>Request</td>
<td>host</td>
<td>Value of the Host header</td>
</tr>
<tr>
<td>Request</td>
<td>method</td>
<td>HTTP method used to make the request</td>
</tr>
<tr>
<td>Request</td>
<td>param-name</td>
<td>Name of a query parameter in the URL</td>
</tr>
<tr>
<td>Request</td>
<td>param-name-value</td>
<td>Name and value of a query parameter in the URL</td>
</tr>
<tr>
<td>Request</td>
<td>param-value</td>
<td>Value of a query parameter in the URL</td>
</tr>
<tr>
<td>Request</td>
<td>referer</td>
<td>Value of the Referer header</td>
</tr>
<tr>
<td>Request</td>
<td>request-body</td>
<td>Value of the HTTP request body</td>
</tr>
<tr>
<td>Request</td>
<td>request-date</td>
<td>Value of the Date header</td>
</tr>
<tr>
<td>Request</td>
<td>request-header-name</td>
<td>Name of a request header</td>
</tr>
<tr>
<td>Request</td>
<td>request-header-value</td>
<td>Value of a request header</td>
</tr>
<tr>
<td>Request</td>
<td>request-version</td>
<td>HTTP version of the request</td>
</tr>
<tr>
<td>Request</td>
<td>url</td>
<td>Value of the URL</td>
</tr>
</tbody>
</table>
Next to the match criteria in the Parameter1 and Parameter2 fields, enter the values that are the match criteria. Most match criteria items require only a single value, which you enter into the Parameter1 field. A few of the match criteria items require both a name and a value, such as a cookie name and value or a parameter name and value. Enter the name into the Parameter1 field and the value into the Parameter2 field. If the Parameter2 field is not needed, then it is not shown.

For example, if you choose host for the Match Criteria, then the Parameter1 value would be a host name such as www.cisco.com; the Parameter2 field is not used. If you choose param-name-value for the Match Criteria, then the Parameter1 value would be the name of a request parameter, and the Parameter2 value would be the value of the specified request parameter.

Regular expressions are allowed; for details see the “Web Application Security Regular Expression Syntax” section on page 6-72.

Click the check box in the Negate column if you want to match all traffic that does not meet the criteria. For example, if you check Negate and enter www.cisco.com for host, this criteria matches all requests where the host does not equal www.cisco.com.
Traffic maps that contain response criteria cannot be used to trigger a feature that is operating on a request. For example, if you have a traffic map that uses the content-type criteria (a response criteria), this traffic map cannot be used in a policy where it is associated with a request limits feature map.

Many features can apply to both requests and responses. Such a feature can be associated with a traffic map that contains response criteria only if it does not operate on request data. For example, if you have a traffic map that uses the set-cookie-name criteria (a response criteria), this traffic map can be used in a policy where it is associated with a cookie protection map, as long as the cookie protection map operates only on response cookies. If the cookie protection map includes any request cookie operations, then the policy is invalid.

When you are finished entering one criteria line, click the Update Parameters button to update the page and give you a new line on which to enter another criteria. To delete one or more criteria lines, click the Delete check box on each line that you want to delete and then click Update Parameters to delete all checked lines.

When you are finished with this form, click Apply Changes to save your changes, or click Discard Changes to return to the summary page without saving your changes.

Default Traffic Maps

The system defines some default traffic class maps that you can use in policy maps. The following default maps are defined:

- **class-all**—This traffic map includes all traffic, both requests and responses. Actions and features that are associated with class-all in a policy map are always executed.

- **class-default-request**—This traffic map includes all request traffic that does not match any of the user-defined classes. At the end of an HTTP request, if no user-defined classes have matched, the actions and features in the policy map that is associated with the class-default-request traffic map are executed.

  In a policy map, this traffic map can be associated with feature maps that operate only on request data. A policy map that contains the class-default-request traffic map cannot include other traffic maps that contain the request-body matching criteria (or negation of this criteria).

- **class-default-response**—This traffic map includes all response traffic that does not match any of the user-defined classes. At the end of an HTTP response, if no user-defined classes have matched, the actions and features in the policy map that is associated with the class-default-response traffic map are executed.

  This traffic map can be associated with feature maps that operate only on response data. A policy map that contains the class-default-response traffic map cannot include other traffic maps that contain the response-body matching criteria (or negation of this criteria).

You cannot edit or delete these default traffic maps. No security features are associated with these traffic maps by default. You must use the Policy Maps command to create a policy that associates features with them.
Policy Maps

A policy map allows you to implement specific web application security functions associated with a traffic class. First you must create a traffic class map and one or more application security feature maps, then you can create a policy map that applies the individual security functions to the traffic class. Here is a summary of the steps required to create a policy map:

1. Create one or more traffic class maps and one or more application security feature maps that you want to apply to the traffic classes. For details, see the “Traffic Class Maps” section on page 6-17 and the “Security Feature Configuration” section on page 6-28.

2. Click the Policy Maps command and use the Add New Map button to name a new policy map. For details, see the “Adding a New Policy Map” section on page 6-21.

3. In the policy map summary page, click the Edit button to add a traffic class to the policy map. For details, see the “Adding a Traffic Map to a Policy Map” section on page 6-22.

4. In the resulting page that lists traffic maps, click the Edit button next to the newly added traffic map to associate individual security feature maps with the traffic map. For details, see the “Associating Security Feature Maps with a Traffic Map” section on page 6-24.

The following sections describe the policy map GUI in detail.

Adding a New Policy Map

Use the Policy Maps command to display a page that summarizes the policy maps that are defined, as shown in Figure 6-13.

Figure 6-13  Policy Map Summary

Each row in the summary lists one defined policy map. From here you can view, clone, edit, delete, or enable a policy map, or add a new map.

To view the definition of a policy map, click its underlined name. The displayed page shows a read-only listing of the definition.
The Associated Traffic Maps column lists the traffic class maps that are associated with a policy. If no traffic class maps are yet associated, it reads “No Maps Associated.” The Match Criteria column lists the matching policy of the map.

To copy a map to use as the basis of a new map, click the Clone button for the map that you want to copy.

To edit a policy map and add traffic class maps, click the Edit button for the map that you want to edit. A form similar to that shown in Figure 6-14 is displayed where you can edit the policy map.

To delete one or more policy maps, check the box in the Delete column for each map that you want to delete. Click Delete to delete the checked maps.

To enable a policy map (make it active), click the radio button in the Enable column for the map that you want to enable, then click the Enable button at the bottom of the column. You can only enable a policy map that has associated traffic class maps, and you can only enable one policy map at a time. This setting interacts with the policy map selected in the Service Policy screen of the System Utilities, as described in the “Service Policy” section on page 6-14. Selecting a policy to be active in that screen will cause it to be displayed as enabled in this policy map summary screen.

To add a new policy map, use the Add Policy area below the summary table. Give the map a name in the Map Name field. Choose when to execute the policy by clicking one of the following radio buttons:

- First Match—Execute the policy only on the first traffic map that matches the traffic
- Match All—Execute the policy on all traffic maps that match the traffic

Then click Add New Policy Map to add the map to the summary. The new map is not yet configured, and to do that click the Edit button for the map.

Tip

When you choose First Match for the type of traffic map matching, it is important to understand the order in which AVS matches traffic maps. Traffic matching is driven by the order in which the traffic data arrives, which is: HTTP method, HTTP version, host, URL, cookie name, and cookie value. There can be multiple cookies and they can arrive in any order, so the value of one cookie could cause a match before the name of another cookie.

Say that you have a traffic map, url-class, that matches on a specific URL, and another traffic map, cookie-class that matches on a cookie name. In an incoming request, the URL arrives before any cookies, so if the URL matches url-class, then this will cause a First Match policy to fire (if it uses this traffic map). The cookie-class might also match this request, but it is not invoked since the url-class already triggered its policy.

The order in which traffic maps are listed in the traffic maps list (see Figure 6-15) is irrelevant and does not signify the order in which traffic maps are evaluated for a match.

Adding a Traffic Map to a Policy Map

To define a policy map and add traffic class maps, in the map summary table click the Edit button for the map that you want to edit. A form similar to that shown in Figure 6-14 is displayed where you can edit the policy map.
When you first edit a new policy map, there are no traffic maps included in it. To begin defining a policy, choose a traffic map from the Traffic Map Name drop-down list. Then click the Add check box to put a check in it and click the **Update List** button to add the traffic map to the policy. For details on the predefined default traffic maps, see the “Default Traffic Maps” section on page 6-20.

After the update, the screen looks like that shown in *Figure 6-15*.

The newly added traffic map is shown in the first row under the Traffic Map Name heading. Each row summarizes one traffic map that is part of this policy definition. The last row allows you to add a new traffic map by selecting its name from the drop-down list of traffic maps, clicking the Add check box, and clicking the **Update List** button.

Using the controls in the summary row for a traffic map, you can view the policy for the map, delete it, or edit it.

To view the policy for a traffic map, click its underlined name. The displayed page shows a read-only listing of the policy definition.

To delete one or more traffic maps from this policy definition, check the box in the Delete column for each map that you want to delete. Click **Update List** to delete the checked maps.
To edit the policy for a traffic map, click the **Edit** button.

When you are finished adding or editing traffic map policies, click **Apply Changes** to save your changes, or click **Discard Changes** to return to the summary page without saving your changes.

**Associating Security Feature Maps with a Traffic Map**

To edit the policy for a traffic map, click the **Edit** button in the summary. A form similar to that shown in **Figure 6-16** is displayed where you can edit the policy definition by choosing which security feature maps to apply to the traffic class.

**Figure 6-16  Associating Features with a Traffic Class**

On this screen, you choose which security features to apply to the traffic map shown in the Traffic Map Name field. You can choose a general response action and/or apply one or more feature maps to the traffic.

To apply a general response action, choose one of the following actions from the Response Action drop-down list:

- **None**—Take no action
- **Reset client**—Reset the client side of the connection
- **Drop**—Drop the connection silently
- **Reset server client**—Reset both the server and client sides of the connection
- **Reset server**—Reset the server side of the connection
- **Error Page**—Send an error page. Choose the error page to send from the next drop-down list to the right. You define such error pages by using the send page feature described in the “**Error/Redirect Pages**” section on page 6-39

Click the Log check box to log the event.
To apply a feature map to the traffic, choose a feature from the Feature drop-down list and then from the Map Name drop-down list, choose one of the feature maps that you have defined for that feature. Then click the **Update List** button to take you back to the screen shown in Figure 6-15. You can add multiple feature maps to be applied to this traffic map by editing the traffic map again and following the same procedure.

**Note**

Traffic maps that contain response criteria cannot be used to trigger a feature that is operating on a request. For example, if you have a traffic map that uses the content-type criteria (a response criteria), this traffic map cannot be used in a policy where it is associated with a request limits feature map.

Many features can apply to both requests and responses. If such a feature operates only on response data and not on request data, then it can be associated with a traffic map that contains response criteria. For example, if you have a traffic map that uses the set-cookie-name criteria (a response criteria), this traffic map can be used in a policy where it is associated with a cookie protection map, as long as the cookie protection map operates only on response cookies. If the cookie protection map includes any request cookie operations, then the policy is invalid and will not be allowed.

The default traffic map class-default-request can be associated with feature maps that operate only on request data. A policy map that contains the class-default-request traffic map cannot include other traffic maps that contain the request-body matching criteria.

The default traffic map class-default-response can be associated with feature maps that operate only on response data. A policy map that contains the class-default-response traffic map cannot include other traffic maps that contain the response-body matching criteria.

To delete an associated feature map, check the Delete check box for the map and click **Update List**.

If you would rather cancel the changes that you made on this form, click the **Discard Changes** button.

The following features are available in the Feature drop-down list:

- **Cookie Protection**—Protects against cookie tampering by using hashed cookies and provides cookie privacy by encrypting cookies; see the “Cookie Protection” section on page 6-30.
- **HTTP Protocol conformance-MIME Type Controls**—Validates that the content’s MIME type matches the MIME type specified in the HTTP Content-type header; see the “MIME Type Controls” section on page 6-54. This feature operates only on responses.
- **HTTP Protocol conformance-Control HTTP Method**—Filters traffic based on the HTTP method; see the “Control HTTP Methods” section on page 6-57.
- **HTTP Protocol conformance-Generic Pattern Matcher**—Filters traffic based on any user-definable criteria; see the “Generic Pattern Matcher” section on page 6-52.
- **HTTP Protocol conformance-Header Integrity Check**—Checks headers for integrity; see the “Header Integrity Check” section on page 6-59.
- **HTTP Protocol conformance-IM Controls**—Filters instant messenger traffic; see the “IM Controls” section on page 6-49.
- **HTTP Protocol conformance-P2P Controls**—Filters peer-to-peer file sharing traffic; see the “P2P Controls” section on page 6-52.
- **HTTP Protocol conformance-Transfer Encoding**—Filters traffic based on the HTTP Transfer-Encoding header; see the “Transfer Encoding” section on page 6-52.
- **HTTP Protocol conformance-Tunnelling Policies**—Filters traffic that is tunneled over HTTP, such as ShoutCast, GoToMyPC and the like; see the “Tunnelling Policies” section on page 6-52.
Global Configuration and Utilities

- HTTP Protocol conformance-URL Black Listing—Blocks access to specific URLs; see the “URL Black Listing” section on page 6-56.
- IV-OS Command Injection—Validates that input does not contain disallowed command strings; see the “OS Command Injection” section on page 6-64.
- IV-Cross Site Scripting—Validates that input does not contain a cross site scripting attack; see the “Cross Site Scripting” section on page 6-60.
- IV-Format String Attacks—Validates that input does not contain disallowed formatting strings; see the “Format String Attacks” section on page 6-70.
- IV-LDAP Injection—Validates that input does not contain disallowed LDAP strings; see the “LDAP Injection” section on page 6-66.
- IV-Meta Character Detection—Validates that input does not contain disallowed meta characters; see the “Meta Character Detection” section on page 6-68.
- IV-SQL Injection—Validates that input does not contain disallowed SQL command strings; see the “SQL Injection” section on page 6-62.
- ID Theft Protection—Guards against the unsolicited disclosure of social security and credit card numbers in HTTP responses to clients; see the “ID Theft Protection” section on page 6-36. This feature operates only on responses.
- Request Limits—Enforces boundary length checking on all inputs received from the client; see the “Request Limits” section on page 6-37.
- URL Normalization—Secures web applications from attacks that use the URL in HTTP requests, such as directory traversal; see the “URL Normalization” section on page 6-28.
- URL Tagging—Adds information to request URLs that can be used by other downstream devices such as load balancers or application servers; see the “URL Tagging” section on page 6-47.
- Web Cloaking—Hides identifying information about the web server and application; see the “Web Cloaking” section on page 6-45.

Pattern Definitions

Pattern definitions define regular expression sets for matching strings used by other web security features. For example, the identity theft protection feature uses regular expressions that match social security numbers and credit card numbers.

Use the Pattern Definitions command to display a page that summarizes the pattern maps that are defined and to view, delete, clone, edit or add new maps. For details on using the summary page GUI, see the “Map Summary Interface” section on page 6-2.

When you click the button to add a new map, AVS displays the screen shown in Figure 6-17.
Give the new regular expression set a name in the Pattern Definition Name field.

In the Type drop-down list, select the type of regular expression set that you are defining, from the following choices:

- Social Security Number—Regular expressions that describe social security numbers
- Credit Card—Regular expressions that describe credit card numbers
- Custom—Custom regular expression
- Cross Site Scripting—Regular expressions that describe cross site scripting strings
- SQL Injection—Regular expressions that describe SQL command strings
- Command Injection—Regular expressions that describe command strings
- LDAP Injection—Regular expressions that describe LDAP strings
- Meta Character Detection—Regular expressions that describe meta characters
- Format String Attacks—Regular expressions that describe format strings

Select one or more regular expressions that you want to use from the Standard Regular Expressions list and add them to the Included Regular Expressions list on the right side of the page by clicking the right arrow (\(\rightarrow\)) button. The list of standard regular expressions changes depending on the type you choose. You can also add a custom regular expression by typing it into the Custom field and clicking the right arrow (\(\rightarrow\)) button next to that field. For details on the regular expression syntax that is allowed, see the “Web Application Security Regular Expression Syntax” section on page 6-72. If you enter a value into the Custom field, in the Size field you must also enter a maximum number of characters to search for this expression in the target data. Size must be greater than 0 for the custom expression to be added to the Included Regular Expressions list.
You can remove a regular expression from the Included Regular Expressions list by selecting it and clicking the left arrow (<--) button.

When you are finished with this form, click Apply Changes at the top to save your changes, or click Discard Changes to return to the summary page without saving your changes. If you want to use the settings on this form as the default for new maps of this type, click Set As Default.

## Security Feature Configuration

This section describes the following security feature configuration items that appear under the Web Application Security folder in the lefthand menu of the Management Console:

- URL Normalization
- Cookie Protection
- ID Theft Protection
- Request Limits
- Error/Redirect Pages
- Web Cloaking
- URL Tagging
- HTTP Protocol Conformance
- Input Validation Checks

### URL Normalization

The URL normalization feature lets you secure web applications from attacks that use the URL in HTTP requests, such as directory traversal.

To deobfuscate potential attacks, the application appliance first scans the URL in incoming requests and normalizes it by decoding all encoded characters. It can detect the following encoding schemes: escaped encoding, %U encoding, unicode encoding using UTF-8 (up to three bytes in length), and IP address encoding. Additionally, it can handle a combination of encoding schemes and double encoding of the same character.

Use the **URL Normalization** command to display a page that summarizes the URL normalization maps that are defined and to view, delete, clone, edit or add new maps. For details on using the summary page GUI, see the “Map Summary Interface” section on page 6-2.

When you click the button to add a new map, AVS displays the screen shown in Figure 6-18.
Give the new map a name in the Map Name field. In the Normalize Case drop-down list, select True to normalize the case of URLs or False to ignore case.

The following part of the form lists a number of conditions that may indicate a possible attack and lets you determine what action to take if one of the following conditions is detected in a URL:

- Encoding—Any kind of character encoding
- Escape encoding—Escape character encoding
- Percent-U encoding—Percent-U character encoding
- Unicode encoding—Unicode character encoding
- Combination of encoding schemes—A combination of character encoding schemes
- Multiple levels of encoding—Multi-level character encoding
- Unsupported encoding—Unsupported character encoding
- Overlong unicode encoding—Overlong unicode character encoding
- Null encoding—Null character encoding
- Forward directory traversal—Forward directory traversal
- Backward directory traversal—Backward directory traversal

In the Action drop-down list for each item, choose one of the following actions to take if the condition occurs:

- None—Take no action
- Reset server—Reset the server side of the connection
• Reset client—Reset the client side of the connection
• Reset server and client—Reset both the server and client sides of the connection
• Drop—Drop the connection silently
• [SEND-PAGE] pagename—Send the error page identified by pagename. You define such error pages by using the send page feature described in the “Error/Redirect Pages” section on page 6-39.
• [REDIRECT-PAGE] pagename—Send the redirection page identified by pagename. You define such redirection pages by using the redirect page feature described in the “Error/Redirect Pages” section on page 6-39.

For each item you can also click the Log check box to log the event.

When you are finished with this form, click Apply Changes at the top to save your changes, or click Discard Changes to return to the summary page without saving your changes. If you want to use the settings on this form as the default for new maps of this type, click Set As Default.

Cookie Protection

Web applications store a variety of information in plain text cookies. The application appliance protects against cookie tampering by using hashed cookies and provides cookie privacy by encrypting cookies. The application appliance also supports adding and removing cookie attributes, and filtering cookies based on user configurable attributes such as HTTP-only cookies, maximum age, number of cookies, and others. The cookie protection features operate both on server cookies sent to clients in HTTP responses and on client cookies that are sent back to servers in HTTP requests.

Use the Cookie Protection command to display a page that summarizes the cookie protection maps that are defined and to view, delete, clone, edit or add new maps. For details on using the summary page GUI, see the “Map Summary Interface” section on page 6-2.

When you click the button to add a new map, AVS displays the screen shown in Figure 6-19.
Give the new map a name in the Map Name field.

The next three Tamper Proof fields set the key and algorithm used for hashing cookies. In the Tamper Proof Key Length drop-down list, choose the key length in bits that you want to use. In the Tamper Proof Key field, enter a key of the chosen length. You must enter 16 characters for a 128-bit key or 32 characters for a 256-bit key. Spaces are not allowed in keys. In the Tamper Proof Algorithm drop-down list, choose the hashing algorithm to use. Currently, AVS supports only SHA-1.
The next three Encrypt fields set the key and algorithm used for encrypting cookies. In the Encrypt Key Length drop-down list, choose the key length in bits that you want to use. In the Encrypt Key field, enter a key of the chosen length. You must enter 16 characters for a 128-bit key or 32 characters for a 256-bit key. Spaces are not allowed in keys. In the Encrypt Algorithm drop-down list, choose the encryption algorithm to use. Currently, AVS supports only AES.

In the Process Response Cookies drop-down list, choose the cookie protection actions to take on all response cookies (cookies sent from the server to the client). The following actions are defined:

- Allow individual cookie processing—Allow response rule map processing whereby you can enable encryption and/or tamper proofing on selected cookies, based on cookie/attribute names and values; see the section “Response Rule Maps” section on page 6-33
- Encrypt all cookies—Encrypt all cookies
- Tamper proof all cookies—Hash all cookies to prevent tampering
- Encrypt and tamper proof all cookies—Encrypt and hash all cookies

The next part of the form lists a number of cookie problems and lets you determine what action to take if one of the following events occurs:

- Alien Cookie—A cookie is observed that is not one processed by the AVS cookie protection feature
- Old Cookie—A cookie sent from the client uses an old version of the hash or encryption key. In this case, the cookie cannot be unhashed or decrypted.
- Encrypt Fail—Cookie decryption failed
- Tamper Proof Verification Fail—Verification that the cookie was not tampered with failed, so this may indicate possible cookie tampering
- Server Cookie Range not between—The number of server cookies is not within the specified range. Enter a range of integers, with the smaller number in the first field and the larger number in the second field.
- Client Cookie Range not between—The number of client cookies is not within the specified range. Enter a range of integers, with the smaller number in the first field and the larger number in the second field.

In the Action drop-down list for each item, choose one of the following actions to take if the event occurs:

- Allow—Allow the request unchanged
- Remove cookie—Remove the cookie that triggered the event
- Drop—Drop the connection silently
- Reset—Reset the connection
- [SEND-PAGE] pagename—Send the error page identified by pagename. You define such error pages by using the send page feature described in the “Error/Redirect Pages” section on page 6-39.
- [REDIRECT-PAGE] pagename—Send the redirection page identified by pagename. You define such redirection pages by using the redirect page feature described in the “Error/Redirect Pages” section on page 6-39.

For each item you can also click the Log check box to log the event.

By using the next parts of the form, you can add rule-based processing to cookies that is based on their values and attributes. These next form parts are described in the following sections:

- Response Attribute Rule Maps
- Response Rule Maps
• Request Rule Maps

When you are finished with this form, click Apply Changes at the top to save your changes, or click Discard Changes to return to the summary page without saving your changes. If you want to use the settings on this form as the default for new maps of this type, click Set As Default.

Response Attribute Rule Maps

In the Response Attribute Rule Maps section, you can define operations to set, insert, or remove specific cookie attributes from response cookies (cookies sent from the server to the client). You can delete one or more operations by clicking the Delete check box next to each operation that you want to delete and then clicking the Delete button.

To add a new attribute operation, click the Add New button to open the window shown in Figure 6-20.

Figure 6-20 Add Attribute Operation

From the Operation drop-down list, select the type of operation you want to perform, as follows:

• Insert—Insert an attribute with the specified name and value. If the attribute already exists, its value is replaced with the specified value.
• Remove—Remove the attribute with the specified name and value. If the attribute exists but the value is different from the specified value, it is not removed.
• Set—Set an existing attribute with the specified name to the specified value. If the attribute does not exist, it is not added. To insert a new attribute, use Insert.

Enter the attribute name in the Attribute Name field and its value in the Attribute Value field. When you are finished, click Create to add the operation or Close Window to cancel the operation.

When you add a new operation, it will be listed in the Response Attribute Rule Maps section of the cookie protection map form.

Response Rule Maps

In the Response Rule Maps section, you can define rule maps for response cookies (cookies sent from the server to the client). In a response rule map, you can specify specific cookies to which to apply encryption and/or tamper proofing actions. This response rule map processing applies only if the Process Response Cookies element is set to Allow individual cookie processing in the cookie protection map.

If there are already rule maps listed here, you can view them by clicking on the underlined identifier in the RuleMaps column. You can edit a rule map by clicking the Edit button next to the map name. You can delete one or more rule maps by clicking the Delete check box next to each rule map that you want to delete and then the clicking the Delete button.
To add a new rule map, click the **Add New** button to open the window shown in **Figure 6-21**.

**Figure 6-21 Add Response Rule Map**

![Add Response Rule Map](image)

Enter a unique name for the rule map in the Rule Map Name field. You can specify a numeric priority (from 1 to 65535) in the Numeric Priority field, which is used to order the rule maps. Rule maps are applied to cookies in descending order of priority (highest number priority first). If the criteria in the next priority rule map do not match the cookie, then the rule map with the next highest priority that matches is applied.

Identify the cookie to which this rule map is to be applied by name and/or value in the Cookie Name and Cookie Value fields. You can use regular expressions in these fields; for details see the “Web Application Security Regular Expression Syntax” section on page 6-72.

You can also identify cookies by attribute name and/or value by specifying one or more regular expressions in the Attribute Name and Attribute Value fields. If you specify more than one name/value pair, all specified attributes must be present in order for this rule to match a cookie.

In the Action drop-down list, select the action to apply to matched cookies, as follows:

- Encrypt—Encrypt all cookies
- Tamper proof—Hash all cookies to prevent tampering
- Encrypt and tamper proof—Encrypt and hash all cookies
If you want to log the event, click the Log check box next to the Action field. When you are finished, click **Create** to add the rule map or **Close Window** to cancel the operation.

### Request Rule Maps

In the Request Rule Maps section, you can define rule maps for request cookies (cookies sent from the client to the server). In a request rule map, you can specify cookies to drop or to cause a connection reset.

**Note**

Request rule map processing occurs regardless of the setting of the Process Response Cookies drop-down list, but operates only on request cookies that were initially processed by the cookie protection feature in the server to client direction. Any cookies that do not meet this criteria are implicitly allowed, though they are processed by other cookie protection features and may be removed as a result of that processing.

If there are already rule maps listed here, you can view them by clicking on the underlined identifier in the RuleMaps column. You can edit a rule map by clicking the **Edit** button next to the map name. You can delete one or more rule maps by clicking the Delete check box next to each rule map that you want to delete and then the clicking the **Delete** button.

To add a new rule map, click the **Add New** button to open the window shown in **Figure 6-22**.

**Figure 6-22**  
**Add Request Rule Map**

Enter a unique name for the rule map in the Rule Map Name field. You can specify a numeric priority (from 1 to 65535) in the Numeric Priority field, which is used to order the rule maps. Rule maps are applied to cookies in descending order of priority (highest number priority first). If the criteria in the next priority rule map do not match the cookie, then the rule map with the next highest priority that matches is applied.

Identify the cookie to which this rule map is to be applied by name and/or value in the Cookie Name and Cookie Value fields. You can use regular expressions in these fields; for details see the “Web Application Security Regular Expression Syntax” section on page 6-72.

In the Action drop-down list, select the action to apply to matched cookies, as follows:

- **Drop**—Drop the connection silently
- **Reset**—Reset the connection
If you want to log the event, click the Log check box next to the Action field.
When you are finished, click **Create** to add the rule map or **Close Window** to cancel the operation.

**ID Theft Protection**

Identity theft protection guards against the unsolicited disclosure of social security and credit card numbers in HTTP responses to clients. The web application firewall searches for numbers that resemble social security or credit card numbers and performs a configurable action when it finds them.

Use the **ID Theft Protection** command to display a page that summarizes the identity protection maps that are defined and to view, delete, clone, edit or add new maps. For details on using the summary page GUI, see the “**Map Summary Interface**” section on page 6-2.

When you click the button to add a new map, AVS displays the screen shown in **Figure 6-23**.

**Figure 6-23      Add Identity Theft Map**

![AVS Management Console](image)

Give the new map a name in the Map Name field.
You can protect social security numbers, credit card numbers, and custom types of numbers by using the SSN, Credit Card, and Custom controls. In the SSN drop-down list, choose one of the defined SSN regular expression sets. In the Credit Card drop-down list, choose one of the defined credit card number regular expression sets. In the Custom drop-down list, choose one of the defined custom regular expression sets. These regular expression sets are defined by using the **Pattern Definitions** command.

In the Action drop-down lists that are to the right of the other fields, choose the action to perform when the firewall finds a number that matches one of these sets of regular expressions. The following actions are defined:

- **None**—Take no action
- **Reset server**—Reset the server side of the connection
- **Reset client**—Reset the client side of the connection
- **Reset server client**—Reset both the server and client sides of the connection
- **Blank out**—Substitute an “x” character for each number in the string that matches the regular expression. This action is not available for Custom expressions.

If you want to log the event, click the Log check box next to the Action field.
When you are finished with this form, click **Apply Changes** at the top to save your changes, or click **Discard Changes** to return to the summary page without saving your changes.

## Request Limits

Many web sites use user-supplied input to create dynamic web pages. Improper validation of inputs such as URL, URL query string, and HTTP headers, can lead to buffer overflow attacks. A buffer overflow attack is when a program writes data beyond its allocated space. These attacks can cause denial of service by crashing the server and/or injecting malicious code to alter program execution. Execution of the malicious code facilitates exploit of downstream resources. Such attacks can be prevented by enforcing boundary length checking on all inputs received from the client.

Use the **Request Limits** command to display a page that summarizes the request limit maps that are defined and to view, delete, clone, edit or add new maps. For details on using the summary page GUI, see the “**Map Summary Interface**” section on page 6-2.

When you click the button to add a new map, AVS displays the screen shown in **Figure 6-24**.
Give the new map a name in the Map Name field.

In the URL length checks area you can enter the maximum lengths, in bytes, for various parts of the URL, as follows:

- **URI Length**—Maximum length of the URI not including the query portion
- **Query Length**—Maximum length of the query portion of the URI
- **URI+Query Length**—Maximum length of the full URI including the query portion

In the Action drop-down list, choose the action to apply if one of the above lengths is exceeded. Actions include these:

- **None**—Take no action
- **Drop**—Drop the connection silently
- **Reset client**—Reset the client side of the connection
• [SEND-PAGE] pagename—Send the error page identified by pagename. You define such error pages by using the send page feature described in the “Error/Redirect Pages” section on page 6-39.

• [REDIRECT-PAGE] pagename—Send the redirection page identified by pagename. You define such redirection pages by using the redirect page feature described in the “Error/Redirect Pages” section on page 6-39.

If you want to log the event when a URL length parameter is exceeded, click the Log check box next to the Action drop-down list.

To limit header length, in the Default Header Length field you can enter the maximum length allowed for any single HTTP header. In the Action drop-down list, choose the action to apply if any header exceeds this limit. The actions are the same as those for the URL length settings. If you want to log the event when a header length limit is exceeded, click the Log check box below the Action drop-down list.

To limit the number of headers, in the Number of Headers field you can enter the maximum number of HTTP headers allowed. In the Action drop-down list, choose the action to apply if the number of headers exceeds this limit. The actions are the same as those for the URL length settings. If you want to log the event when the header limit is exceeded, click the Log check box next to the Action drop-down list.

In the Advanced Checks area, you can check if a particular header value exceeds a length limit. Choose the header to check from the Parameter Name drop-down list. If the header you want to check is not listed, select custom and enter the header name in field below the drop-down list. Enter the maximum length of the header’s value in the Parameter Value field. Then check the Add check box and click Update Parameters to add this header value check to the map. You can repeat this procedure to add more header value checks to the map. In the Action drop-down list, choose the action to apply if any of the header values exceeds the specified limits. The actions are the same as those for the URL length settings. If you want to log the event when a header value length limit is exceeded, click the Log check box next to the Action drop-down list.

To delete a header value length check, click the Delete check box next to the header check that you want to delete and then click Update Parameters.

When you are finished with this form, click Apply Changes at the top to save your changes, or click Discard Changes to return to the summary page without saving your changes. If you want to use the settings on this form as the default for new maps of this type, click Set As Default.

Error/Redirect Pages

Error obfuscation makes it more difficult for hackers to discover identifying information about the web server and application by masking or mapping error messages that might normally be returned to the user. Many security vulnerabilities are dependent on specific software versions and hiding this information can increase the security of the system.

AVS implements the following techniques for error obfuscation:

• Mapping errors by sending custom configured error pages to clients; see the “Send Page Configuration” section on page 6-40

• Masking errors by redirecting the client when an error occurs; see the “Redirect Page Configuration” section on page 6-43

Error obfuscation can be triggered as the action to perform when one of the following web application security features encounters an error: URL Normalization, Cookie Protection, Request Limits, Input Validation Checks, and HTTP Protocol Conformance.

Use the Error/Redirect Pages command to configure this feature. Click this command to display a page that summarizes the error obfuscation maps that you have configured, as shown in Figure 6-25.
Each of the four summary sections of the page lists the maps configured for a subfeature of error obfuscation. Each defined map is summarized on one line. From here you can view, clone, edit, or delete a map, or add a new map.

To view the definition of a map, click its underlined name. The displayed page shows a read-only listing of the definition.

To copy a map to use as the basis of a new map, click the **Clone** button next to the map that you want to clone.

To edit a map, click the **Edit** button in the summary. A form similar to that shown when adding a map is displayed where you can edit the map.

To delete one or more maps, check the box in the Delete column for the map. Click **Delete Maps** to delete the checked maps.

To add a new map or template, click the **Add New Map** or **Add New Template** button for the item that you want to add. For details on adding a send page header map and a send page map, see the following section, “Send Page Configuration.” For details on adding a redirect page header map and a redirect page map, see the “Redirect Page Configuration” section on page 6-43.

### Send Page Configuration

Before you can configure a send page map you must first define a send page header template, which is a template of HTTP headers that can be sent on error pages.
To define a send page header template, on the summary page, click on the **Add New Template** button to display the form shown in **Figure 6-26**.

**Figure 6-26 Add Send Page Header Template**

Give the template a name in the **Template Name** field.

Add one or more headers to the template by choosing a header name from the **Header Name** drop-down list. If you want to add a header that is not in the list, choose **Custom** and enter the name of the header in the field below the list. Enter the value of the header in the **Header Value** field next to the name. Then click the **Add** check box and click the **Update Headers** button to add the header to the template. You can add multiple headers by following the same procedure for each one.

To delete a header from the template, click the Delete check box next to it and click the **Update Headers** button.

When you are finished with this form, click **Apply Changes** at the top to save your changes, or click **Discard Changes** to return to the summary page without saving your changes. If you want to use the settings on this form as the default for new maps of this type, click **Set As Default**.

After at least one send page header template is defined, you can define a send page map, which defines the error page that you want to send to the client. Click the **Add New Map** button on the summary page to display the form shown in **Figure 6-27**.
Give the error page map a name in the Map Name field.

You can define two different sets of error codes, error phrases, and header templates that are to be sent in response to HTTP requests that use HTTP versions 1.0 and 1.1. If you want to define an error page that is to be sent in response to HTTP version 1.0 requests, check the HTTP Version 1.0 check box and complete the fields on that line. To send this error page in response to HTTP version 1.1 requests, check the HTTP Version 1.1 check box and complete the fields on that line. To respond to both versions of HTTP requests, check both check boxes. This error page is sent only if the HTTP version setting matches the HTTP version of the request.

In the Error Code drop-down list, choose the error code that this error page should show to the client. In the Error Phrase field, enter the phrase that should be used to describe this error. By default, the Error Phrase field initially shows the standard error phrase that corresponds to the selected error code, but you can change it.

In the Header Template drop-down list, select the name of the send page header template map that you want to use for this error page. If no header templates are defined, only --Select-- is shown in this list, and you must define a send page header template before you can define a send page map. Go back to the summary page and use the Add New Template button to define a header template.

In the Include Date Header drop-down list, select Yes or No to include a date header or not in the error page.

In the HTTP Body field, enter the HTML for the body of the error page.

In the Content Type drop-down list, select the MIME type of the page content: either text/plain or text/html.

When you are finished with this form, click Apply Changes at the top to save your changes, or click Discard Changes to return to the summary page without saving your changes. If you want to use the settings on this form as the default for new maps of this type, click Set As Default.
Redirect Page Configuration

Before you can configure a redirect page map, you must first define a redirect page header template, which is a template of HTTP headers that can be sent on redirect pages. To define a redirect page header template, on the summary page, click on the Add New Template button to display the form shown in Figure 6-28.

**Figure 6-28  Add Redirect Page Header Template**

![AVS Management Console](image)

Give the template a name in the Template Name field.

Add one or more headers to the template by choosing a header name from the Header Name drop-down list. If you want to add a header that is not in the list, choose Custom and enter the name of the header in the field below the list. Enter the value of the header in the Header Value field next to the name. Then click the Add New check box and click the Update Headers button to add the header to the template. You can add multiple headers by following the same procedure for each one.

To delete a header from the template, click the Delete check box next to it and click the Update Headers button.

When you are finished with this form, click Apply Changes at the top to save your changes, or click Discard Changes to return to the summary page without saving your changes. If you want to use the settings on this form as the default for new maps of this type, click Set As Default.

After at least one redirect page header template is defined, you can define a redirect page map, which defines the redirect page that you want to send to the client. Click the Add New Map button on the summary page to display the form shown in Figure 6-29.
Give the redirect page map a name in the Map Name field.

You can define two different sets of error codes, error phrases, and header templates that are to be sent in response to HTTP requests that use HTTP versions 1.0 and 1.1. If you want to define a redirect page that is to be sent in response to HTTP version 1.0 requests, check the HTTP Version 1.0 check box and complete the fields on that line. To send this redirect page in response to HTTP version 1.1 requests, check the HTTP Version 1.1 check box and complete the fields on that line. To respond to both versions of HTTP requests, check both check boxes. This redirect page is sent only if the HTTP version setting matches the HTTP version of the request.

In the Error Code drop-down list, choose the error code that this error page should show to the client. In the Error Phrase field, enter the phrase that should be used to describe this error. By default, the Error Phrase field initially shows the standard error phrase that corresponds to the selected error code, but you can change it.

In the Header Template drop-down list, select the name of the redirect page header template map that you want to use for this redirect page. If no header templates are defined, only "Select" is shown in this list, and you must define a redirect page header template before you can define a send page map. Go back to the summary page and use the Add New Template button to define a header template.

In the Location Header field, enter the absolute URI of the location to which the client should be redirected.

In the Include Date Header drop-down list, select Yes or No to include a date header or not in the redirect page.

In the HTTP Body field, enter the HTML for the body of the redirect page.

In the Content Type drop-down list, select the MIME type of the page content: either text/plain or text/html.
Web Cloaking

Web cloaking makes it more difficult for hackers to discover identifying information about the web server and application. Many security vulnerabilities are dependent on specific software versions and hiding this information can increase the security of the system.

AVS focuses on the HTTP response headers and implements the following techniques for web server cloaking:

- Changing the sequence of individual header fields in the response (web servers can be fingerprinted based on the sequence of header fields in the response)
- Changing the case of header names (web servers can be fingerprinted based on the capitalization of header names)
- Changing the value of a header based on its name and value
- Removing a header based on its name and value
- Adding false headers to confuse attackers

Use the Web Cloaking command to display a page that summarizes the web cloaking maps that are defined and to view, delete, clone, edit or add new maps. For details on using the summary page GUI, see the “Map Summary Interface” section on page 6-2.

When you click the button to add a new map, AVS displays the screen shown in Figure 6-30.
Give the new map a name in the Map Name field.
If you want to log web cloaking actions, click the Enable Log check box.
In the Available Headers/Header Sequence area you can change the sequence of individual HTTP headers in responses. Select the header that you want to be first from the Standard list and click the right arrow (>) to add it to the Header Sequence list on the right side of the page. Then select the header that you want to be second, and so on, adding each one in turn to the Header Sequence list. When you add a header, it is always added at the bottom of the list. You can also add a custom header that is not listed by typing its name into the Custom field and clicking the right arrow (>) next to that field.
To reorder the headers listed in the Header Sequence list, select a header and click the up arrow next to the list to move the header up one position in the list, or click the down arrow to move it one position down. Repeat the process each time that you want to move the header one more position up or down.
In the Add/Modify/Remove Response Headers area you can add, modify, or remove HTTP headers in responses. You can add multiple functions in this area; one operation is summarized on each line.
To add an operation, in the Operation drop-down list choose the type of operation: ADD, MODIFY, or REMOVE. In the Response Header drop-down list, choose the name of the header that you want to add, modify, or remove. If the header name is not listed, choose custom from the list and type the name of the header in the Response Header field below the drop-down list. Next, enter values in the Old Value and New Value fields, as follows:

- If you are adding a header, enter a value in the New Value field only and leave Old Value empty.
- If you are modifying a header, enter the existing value to match in the Old Value field and enter the value to change it to in the New Value field. Only headers whose value matches the Old Value will be changed to New Value.
- If you are removing a header, enter a value in the Old Value field only, to remove only headers that have this value.

Finally, click the Add check box to add the header operation to this web cloaking map. The operation is added after you click Update Parameters, and a new blank operation line is shown below the newly added one, where you can add another operation. Also, a Delete check box is shown at the right end of each operation line, which you can use to delete an operation by checking it and clicking Update Parameters.

In the Header Name Normalization area, you can force specific header names to be all uppercase or all lowercase. To normalize the case of a header name, select it in the list at the left side of the page and click the Uppercase right arrow (>) button to make it uppercase, or click the Lowercase right arrow button to make it lowercase. Do the same for each header name that you want to normalize. If you want to normalize a custom header name, choose Custom in the list and type the name in the Custom field below the list. Then click the appropriate right arrow button. To remove a header name from a normalization list at the right side, select it and click the left arrow (<) button next to the list.

When you are finished with this form, click Apply Changes at the top to save your changes, or click Discard Changes to return to the summary page without saving your changes. If you want to use the settings on this form as the default for new maps of this type, click Set As Default.

**Interaction with AVS Acceleration in Gateway Mode**

When you use web cloaking and operate the web application firewall in gateway mode, the AVS acceleration features interact with the response and can change HTTP response headers. AVS acceleration processing occurs after web application firewall processing, so the response might contain headers different from those set by web cloaking.

Specifically, AVS acceleration features may add, remove, or change the following headers:

- Add—Content-Encoding, Transfer-Encoding, Set-Cookie
- Remove—Content-Length
- Change—Connection

If Web Cloaking normalizes, sequences, adds, removes, or modifies any of these headers, the AVS acceleration processing may undo or change these actions in the response.

**URL Tagging**

The URL tagging feature lets you add information to request URLs that can be used by other downstream devices such as load balancers or application servers. You can search for a string in the URL and if there is a match you can either replace the complete URL with another URL or replace only the matched string. Additionally, you can insert or remove parameter name/value pairs.
Use the **URL Tagging** command to display a page that summarizes the URL tagging maps that are defined and to view, delete, clone, edit or add new maps. For details on using the summary page GUI, see the “Map Summary Interface” section on page 6-2.

When you click the button to add a new map, AVS displays the screen shown in Figure 6-31.

---

**Figure 6-31   Add URL Tagging Map**

---

Give the new map a name in the Map Name field.

Using the following areas of the form you can configure these functions:

- **Parameter rewrite**—By using the Parameter Rules area, you can insert or remove parameter name/value pairs in the query portion of matched URLs. Enter a parameter name in the Parameter field and its value in the Value field. Choose either Add or Remove from the Operation drop-down list. If you choose Remove, the parameter name and value must match exactly for it to be removed. Click the **Update Parameter Rule** button to add the rule.

  **Note**      Regular expressions and the following characters are not allowed in the Parameter and Value fields when you are adding a parameter: ?*{}[()]^$,

  When you are removing a parameter, regular expressions are allowed and there are no character restrictions in the Parameter and Value fields.

- **URL rewrite**—By using the URL Rules area, you can search for a string in the URL and if there is a match you can either replace the complete URL with another URL or replace only the matched string with another string. Enter the string to search for in the Find field and enter the replacement string or URL in the Replace field. From the Type drop-down list, choose either Replace URL (to replace the whole URL with the URL entered in the Replace field) or Replace matched string (to replace just the matched string in the URL with the string entered in the Replace field). Click the **Update URL Rule** button to add the rule. Rewritten URLs are escape encoded before being sent out.
Regular expressions and the following characters are mostly not allowed in the Find and Replace fields: \*\{1,\}\*\$.
When you are replacing a complete URL, then regular expression are allowed and there are no character restrictions in the Find field.

For details on the regular expression syntax that is allowed, see the “Web Application Security Regular Expression Syntax” section on page 6-72.

To delete an existing parameter or URL rewriting rule, click the Delete check box on the same line as the rule, and when you click Update Parameter Rule (to delete parameter rules) or Update URL Rule (to delete URL rewrite rules), the rule will be deleted.

When you are finished with this form, click Apply Changes at the top to save your changes, or click Discard Changes to return to the summary page without saving your changes. If you want to use the settings on this form as the default for new maps of this type, click Set As Default.

HTTP Protocol Conformance

HTTP protocol conformance provides deep analysis of web traffic, enabling granular control over HTTP sessions for improved protection from a wide range of web-based attacks. In addition, this feature allows administrative control over instant messaging applications, peer-to-peer file sharing applications, and applications that attempt to tunnel over port 80 or any port used for HTTP transactions. Capabilities provided include RFC compliance enforcement, HTTP command authorization and enforcement, response validation, Multipurpose Internet Mail Extension (MIME) type validation and content control, URL blacklisting, and more.

The following sections describe the HTTP Protocol Conformance menu commands:

- IM Controls
- P2P Controls
- Tunnelling Policies
- Generic Pattern Matcher
- Transfer Encoding
- MIME Type Controls
- URL Black Listing
- Control HTTP Methods
- Header Integrity Check

IM Controls

The IM controls feature allows you to control incoming and outgoing instant messaging traffic by logging or denying it.

Use the IM Controls command to display a page that summarizes the instant messaging maps that are defined and to view, delete, clone, edit or add new maps. For details on using the summary page GUI, see the “Map Summary Interface” section on page 6-2.

When you click the button to add a new map, AVS displays the screen shown in Figure 6-32.
Use this form to define criteria for identifying instant messaging traffic in either requests or responses. Give the instant messaging map a name in the Map Name field.

If you are creating a new map, only the New Criteria section of the form is shown. As each criteria for identifying instant messaging traffic is added, it is listed in a criteria section at the top of the form.

In the New Criteria section, click the Add check box to indicate that you are adding a new criteria. Then in the Message Type drop-down list, choose the message type that you want to examine: either Request or Response messages. In the Search Type drop-down list, choose the part of the request or response that you want to examine, and in the next three fields (Name, Value, and Max No of bytes to search), enter the criteria that must be matched to consider the traffic to be instant messenger related. For each message type/search type pair, only certain criteria fields are used, and these are described in Table 6-3.

The Obfuscation Option check box is available in certain cases. Checking this box deobfuscates the URL before performing regular expression matching with the specified criteria. Deobfuscation decodes encoded URLs. For example, a URL might contain the string “%20”, which is decoded to a space character.
The Value field can be a regular expression; for details see the “Web Application Security Regular Expression Syntax” section on page 6-72.

When you are done entering the criteria, make sure the Add check box is checked and click the Update Criteria button to add the criteria to the map. You can add more criteria by following the same procedure for each one. To delete a criteria from the map, click the Delete check box next to it and click the Update Criteria button.

After you have defined the criteria to identify instant messenger traffic, you can configure the action to apply when such traffic is observed. In the first Action drop-down list, choose one of the following items:

- Match All—All criteria must be matched to apply the action
- Match Any—Any single criteria must be matched to apply the action

Click the Not check box if you want to match all traffic that does not meet the criteria. If Not is checked, the match criteria are interpreted as follows:

- Match All—Fewer than all criteria must be matched to apply the action
- Match Any—None of the criteria must be matched to apply the action

In the second drop-down list, choose one of the following actions:

- None—Take no action
- Deny—Block the traffic

<table>
<thead>
<tr>
<th>Message Type/Search Type</th>
<th>Criteria Fields Used</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request/Method</td>
<td>Name</td>
<td>Enter the HTTP request method name in the Name field.</td>
</tr>
<tr>
<td>Request/Url</td>
<td>Value, Obfuscation Option check box</td>
<td>In the Value field, enter a string to match in the URL and check the Obfuscation Option check box to deobfuscate the URL before matching. You can enter either a full URL or a partial string. If any part of the value is found in the URL, then the match is successful. Only the URL is searched for a match, not the query parameters.</td>
</tr>
<tr>
<td>Request/Arg</td>
<td>Value, Obfuscation Option check box</td>
<td>In the Value field, enter a string to match in the query portion of the URL and check the Obfuscation Option check box to deobfuscate the URL before matching. If any part of the value is found in the query parameters, then the match is successful. Only the query parameter portion of the URL is searched.</td>
</tr>
<tr>
<td>Request/Header</td>
<td>Name, Value</td>
<td>Enter the name of the HTTP request header in the Name field and the header value in the Value field.</td>
</tr>
<tr>
<td>Request/Body</td>
<td>Value, Max No of bytes to search</td>
<td>Enter the string to search for in the body of the request in the Value field, and enter the maximum number of bytes to search in the body in the Max No of bytes to search field. The match is successful if the specified string is found anywhere in the body, ending at the byte specified in Max No of bytes to search.</td>
</tr>
<tr>
<td>Response/StatusCode</td>
<td>Value</td>
<td>Enter the numeric response status code to search for in the Value field.</td>
</tr>
<tr>
<td>Response/Header</td>
<td>Name, Value</td>
<td>Enter the name of the HTTP response header in the Name field and the header value in the Value field.</td>
</tr>
<tr>
<td>Response/Body</td>
<td>Value, Max No of bytes to search</td>
<td>Enter the string to search for in the body of the response in the Value field, and enter the maximum number of bytes to search in the body in the Max No of bytes to search field. The match is successful if the specified string is found anywhere in the body, ending at the byte specified in Max No of bytes to search.</td>
</tr>
</tbody>
</table>
- [SEND-PAGE] pagename—Send the error page identified by pagename. You define such error pages by using the send page feature described in the “Error/Redirect Pages” section on page 6-39.
- [REDIRECT-PAGE] pagename—Send the redirection page identified by pagename. You define such redirection pages by using the redirect page feature described in the “Error/Redirect Pages” section on page 6-39.

If you want to log the event, click the Log check box next to the Action drop-down lists.

When you are finished with this form, click Apply Changes at the top to save your changes, or click Discard Changes to return to the summary page without saving your changes.

**P2P Controls**

The P2P controls feature allows you to control incoming and outgoing peer-to-peer application traffic by logging or denying it. Use the P2P Controls command to configure peer-to-peer application control. This command works exactly like the IM Controls command, so for details, see the “IM Controls” section on page 6-49.

**Tunnelling Policies**

The tunnelling policies feature allows you to control incoming and outgoing tunnelled application traffic by logging or denying it. Use the Tunnelling Policies command to configure tunnelling application control. This command works exactly like the IM Controls command, so for details, see the “IM Controls” section on page 6-49.

**Generic Pattern Matcher**

The generic pattern matcher feature allows you to configure a policy based on any user-definable criteria in the traffic, to control incoming and outgoing traffic by logging or denying it. Use the Generic Pattern Matcher command to configure such control. This command works exactly like the IM Controls command, so for details, see the “IM Controls” section on page 6-49.

**Transfer Encoding**

The transfer encoding feature allows you to control incoming and outgoing traffic that has a specific Transfer-Encoding header by logging or denying it.

Use the Transfer Encoding command to display a page that summarizes the transfer encoding maps that are defined and to view, delete, clone, edit or add new maps. For details on using the summary page GUI, see the “Map Summary Interface” section on page 6-2.

When you click the button to add a new map, AVS displays the screen shown in Figure 6-33.
Give the transfer encoding map a name in the Map Name field.

In the next part of the form, you can add criteria lines that describe one or more transfer encodings of the traffic that you want to act on. First choose the type of transfer encoding in the Transfer Encoding drop-down list. The following choices are available:

- Custom—an encoding other than those listed; enter the encoding type in the field below the list
- Identity—no transfer encoding used
- Gzip—gzip encoding
- Chunked—chunked encoding
- Deflate—deflate encoding
- Compress—compress encoding

In the Type drop-down list, choose whether you want to act on request or response traffic. In the Action drop-down list, choose one of the following actions:

- None—Take no action
- Deny—Block the traffic
- [SEND-PAGE] pagename—Send the error page identified by pagename. You define such error pages by using the send page feature described in the “Error/Redirect Pages” section on page 6-39.
- [REDIRECT-PAGE] pagename—Send the redirection page identified by pagename. You define such redirection pages by using the redirect page feature described in the “Error/Redirect Pages” section on page 6-39.

If you want to log the event, click the Log check box next to the Action drop-down list. Finally, check the Add check box and click Update to add the criteria to this form and give you a new line on which to enter another criteria. To delete one or more criteria lines, click the Delete check box on each line that you want to delete and then click Update to delete all checked lines.
There is another Action drop-down list at the bottom of the form, labeled Action for Nonmatching Traffic. This action applies to all traffic that has a transfer encoding that does not match any of the criteria on this form. You can choose the same actions as on the other Action list. Also, you can click the Log check box next to this drop-down list if you want to log such traffic.

When you are finished with this form, click Apply Changes at the top to save your changes, or click Discard Changes to return to the summary page without saving your changes.

**MIME Type Controls**

The MIME type controls feature allows you to validate that the MIME type specified in the HTTP Content-Type header matches the content type’s magic number in the body of the message. (Magic numbers are byte sequences that are always present in a particular MIME type and thus can be used to identify entities as being of a given media type.)

Use the MIME Type Controls command to display a page that summarizes the content type verification maps that are defined and to view, delete, clone, edit or add new maps. For details on using the summary page GUI, see the “Map Summary Interface” section on page 6-2.

When you click the button to add a new map, AVS displays the screen shown in Figure 6-34.
Figure 6-34  Add Content Type Verification Map

![Add Content Type Verification Map](image-url)
Give the content type verification map a name in the Map Name field. The content types that are validated are listed below this field. Ensure that the Select check box is checked for each MIME type that you want to verify. All MIME types listed are checked initially.

In the Action drop-down list, choose one of the following actions:

- None—Take no action
- Deny—Block traffic with one of the listed content types
- SEND-PAGE | pagename—Send the error page identified by pagename. You define such error pages by using the send page feature described in the “Error/Redirect Pages” section on page 6-39.
- REDIRECT-PAGE | pagename—Send the redirection page identified by pagename. You define such redirection pages by using the redirect page feature described in the “Error/Redirect Pages” section on page 6-39.

If you want to log the event, click the Log check box next to the Action drop-down list.

When you are finished with this form, click Apply Changes at the top to save your changes, or click Discard Changes to return to the summary page without saving your changes.

**URL Black Listing**

The URL black listing feature allows you to block incoming requests for particular URLs.

Use the URL Black Listing command to display a page that summarizes the URL blacklist maps that are defined and to view, delete, clone, edit or add new maps. For details on using the summary page GUI, see the “Map Summary Interface” section on page 6-2.

When you click the button to add a new map, AVS displays the screen shown in Figure 6-35.

*Figure 6-35 Add URL Blacklist Map*

Give the URL black listing map a name in the Map Name field.
In the next part of the form, you can add regular expressions for URLs that you want to block traffic to. In the URL field, enter a regular expression that is used to match part of a URL string in incoming requests. The regular expression is matched against only the URL and not the query parameters. If the regular expression matches any part of the URL, the match is considered successful. For details on the regular expression syntax, see the “Web Application Security Regular Expression Syntax” section on page 6-72.

Check the Obfuscation check box to deobfuscate the URL before performing regular expression matching. Deobfuscation decodes encoded URLs. For example, a URL might contain the string “%20”, which is decoded to a space character.

Check the Add check box and click Update to add the URL to this form and give you a new line on which to enter another URL. To delete one or more URL lines, click the Delete check box on each line that you want to delete and then click Update to delete all checked lines.

After you have defined the URLs to blacklist, you can configure the action to apply when such traffic is observed. In the first Action drop-down list, choose one of the following items:

- Match All—All criteria must be matched to apply the action
- Match Any—Any single criteria must be matched to apply the action

Click the Not check box if you want to match all traffic that does not meet the criteria. If Not is checked, the match criteria are interpreted as follows:

- Match All—Fewer than all criteria must be matched to apply the action
- Match Any—None of the criteria must be matched to apply the action

In the second drop-down list, choose one of the following actions:

- None—Take no action
- Deny—Block the traffic
- [SEND-PAGE] pagename—Send the error page identified by pagename. You define such error pages by using the send page feature described in the “Error/Redirect Pages” section on page 6-39.
- [REDIRECT-PAGE] pagename—Send the redirection page identified by pagename. You define such redirection pages by using the redirect page feature described in the “Error/Redirect Pages” section on page 6-39.

If you want to log the event, click the Log check box next to the Action drop-down lists.

When you are finished with this form, click Apply Changes at the top to save your changes, or click Discard Changes to return to the summary page without saving your changes.

**Note**

URL blacklisting can also be done directly in a policy map by defining the traffic to blacklist in a traffic map, then setting a general policy to drop the connection when such traffic is encountered.

**Control HTTP Methods**

The HTTP method control feature allows you to control incoming traffic that uses a specific HTTP method by logging or denying it.

Use the **Control HTTP Methods** command to display a page that summarizes the HTTP content method maps that are defined and to view, delete, clone, edit or add new maps. For details on using the summary page GUI, see the “Map Summary Interface” section on page 6-2.

When you click the button to add a new map, AVS displays the screen shown in **Figure 6-36**.
Give the HTTP content methods map a name in the Map Name field.

In the next part of the form, you can add one or more HTTP methods to act on. In the Methods drop-down list choose an HTTP method. Check the Add check box and click Update to add the method to this form and give you a new line on which to enter another method. To delete one or more method lines, click the Delete check box on each line that you want to delete and then click Update to delete all checked lines.

After you have defined the HTTP methods to look for, you can configure the action to apply when such traffic is observed. In the first Action drop-down list, choose one of the following items:

- Match All—All criteria must be matched to apply the action
- Match Any—Any single criteria must be matched to apply the action

Click the Not check box if you want to match all traffic that does not meet the criteria. If Not is checked, the match criteria are interpreted as follows:

- Match All—Fewer than all criteria must be matched to apply the action
- Match Any—None of the criteria must be matched to apply the action

In the second drop-down list, choose one of the following actions:

- None—Take no action
- Deny—Block the traffic
- [SEND-PAGE] pagename—Send the error page identified by pagename. You define such error pages by using the send page feature described in the “Error/Redirect Pages” section on page 6-39.
- [REDIRECT-PAGE] pagename—Send the redirection page identified by pagename. You define such redirection pages by using the redirect page feature described in the “Error/Redirect Pages” section on page 6-39.

If you want to log the event, click the Log check box next to the Action drop-down lists.

When you are finished with this form, click Apply Changes at the top to save your changes, or click Discard Changes to return to the summary page without saving your changes.
Header Integrity Check

The header integrity check feature allows you to check the integrity of HTTP headers and take action if problems are found.

Use the **Header Integrity Check** command to display a page that summarizes the header integrity check maps that are defined and to view, delete, clone, edit or add new maps. For details on using the summary page GUI, see the “Map Summary Interface” section on page 6-2.

When you click the button to add a new map, AVS displays the screen shown in Figure 6-37.

**Figure 6-37  Add Header Integrity Check Map**

Give the header integrity check map a name in the Map Name field.

In the next part of the form, you can configure actions to take when the following problems are found in a header:

- Null Encoding—Transfer-encoding header has no encodings listed
- Non ASCII Characters—Non-ASCII characters are found in a header
- Illegal Content Length—Content-length header contains non-numeric characters
- Illegal Chunk Encoding—Chunk encoding is not valid
- Multiple Length Headers—Multiple content-length headers appear in the request

For each listed header integrity problem, select one of the following actions from the Action drop-down list:

- None—Take no action
- Reset server—Reset the server side of the connection
- Reset client—Reset the client side of the connection
- Reset server client—Reset both the server and client sides of the connection
- Drop—Drop the connection silently
- [SEND-PAGE] pagename—Send the error page identified by pagename. You define such error pages by using the send page feature described in the “Error/Redirect Pages” section on page 6-39.
Input Validation Checks

The input validation module inspects incoming HTTP messages from clients and web servers to protect against a variety of attacks that use form input submitted by the GET or POST methods. The following sections describe these input validation checks:

- Cross Site Scripting
- SQL Injection
- OS Command Injection
- LDAP Injection
- Meta Character Detection
- Format String Attacks

All input validation checks use regular expression sets that have been defined with the Pattern Definitions command; for details, see the “Pattern Definitions” section on page 6-26.

Cross Site Scripting

A cross site scripting attack takes advantage of dynamically generated web pages in which data is usually gathered in the form of a hyperlink. An attacker, when prompted to enter information like a user name, will instead pass a script to be executed. A web server that does not properly perform input validation will execute the script and wait for an innocent user to click the link provided by the attacker. The victim may unknowingly release information to the attacker.

Use the Cross Site Scripting command to display a page that summarizes the cross site scripting maps that are defined and to view, delete, clone, edit or add new maps. For details on using the summary page GUI, see the “Map Summary Interface” section on page 6-2.

When you click the button to add a new map, AVS displays the screen shown in Figure 6-38.
Give the map a name in the Map Name field.

In the map, you can configure protection in three ways:

- **Scan all of the form input data.**
  
  Set the Type to Scan All Parameters. Choose a regular expression pattern set from the Pattern Set drop-down list that lists regular expressions that you want to exclude from form input. The regular expression patterns that are listed here are those that are defined in the Pattern Definitions page where the type is Cross Site Scripting. If you see the message “No Pattern Set of this type is defined,” you must define at least one pattern map of the Cross Site Scripting type before you can complete this form. Any form input that contains a string that matches one of the regular expressions in the specified pattern set is flagged for the action specified in the Action drop-down list. Leave the Parameter field empty and make no selection from the Allow Pattern Set drop-down list.

- **Scan all of the form input data except for the values of one or more specific form parameters, in which certain expressions are allowed.**

  Set the Type to Scan All Parameters. Choose a regular expression pattern set from the Pattern Set drop-down list that lists regular expressions that you want to exclude from form input. The regular expression patterns that are listed here are those that are defined in the Pattern Definitions page where the type is Cross Site Scripting. If you see the message “No Pattern Set of this type is defined,” you must define at least one pattern map of the Cross Site Scripting type before you can complete this form. In the Parameter field enter the name of an exception parameter in which you want to allow input that might otherwise be flagged by the Pattern Set regular expression set. In the Allow Pattern Set drop-down list, choose a regular expression pattern set that lists regular expressions that you want to allow in the value of the exception parameter. Check the Add check box to the right of the Allow Pattern Set drop-down list and click Update Parameters. You can enter as many exception parameters as you want by repeating this procedure. Each parameter can have its own associated regular expression that defines the values that are allowed. To delete a parameter, click the Delete check box to the right of the Allow Pattern Set drop-down list and click Update Parameters.
Any form input that contains a string that matches one of the regular expressions in the Pattern Set is flagged for the action specified in the Action drop-down list. If an exception parameter value contains a string that matches both the Pattern Set and Allow Pattern Set regular expressions, then it is allowed rather than being flagged for action.

- Scan the values of a one or more specific form parameters within the input data.

Set the Type to Scan Specific Parameters. Choose a regular expression pattern set from the Pattern Set drop-down list and enter the name of a form parameter to scan in the Parameter field. Check the Add check box to the right of the parameter name and click **Update Parameters**. You can enter as many parameters as you want by repeating this procedure. To delete a parameter, click the Delete check box to the right of the parameter name and click **Update Parameters**. If any of the specified parameter values contain a string that matches one of the regular expressions in the specified pattern set, the request is flagged for the action specified in the Action drop-down list.

Check the Ignore Case check box if you do not need to match the case of a parameter specified in the Parameter field. If you do need to match the case exactly, leave this check box unchecked.

In the Action drop-down list, choose the action to apply if a form input string that matches this map is detected. Actions include these:

- None—Take no action
- Reset server client—Reset both the server and client sides of the connection
- Drop—Drop the connection silently
- [SEND-PAGE] pagename—Send the error page identified by pagename. You define such error pages by using the send page feature described in the “Error/Redirect Pages” section on page 6-39.
- [REDIRECT-PAGE] pagename—Send the redirection page identified by pagename. You define such redirection pages by using the redirect page feature described in the “Error/Redirect Pages” section on page 6-39.

If you want to log the event, click the Log check box below the Action drop-down list.

When you are finished with this form, click **Apply Changes** at the top to save your changes, or click **Discard Changes** to return to the summary page without saving your changes.

**SQL Injection**

A SQL injection attack appends or modifies SQL commands in form input with the intention of gathering information regarding the application and obtaining access to unauthorized data.

Use the **SQL Injection** command to display a page that summarizes the SQL injection maps that are defined and to view, delete, clone, edit or add new maps. For details on using the summary page GUI, see the “Map Summary Interface” section on page 6-2.

When you click the button to add a new map, AVS displays the screen shown in Figure 6-39.
Give the map a name in the Map Name field.

In the map, you can configure protection in three ways:

- **Scan all of the form input data.**
  
  Set the Type to Scan All Parameters. Choose a regular expression pattern set from the Pattern Set drop-down list that lists regular expressions that you want to exclude from form input. The regular expression patterns that are listed here are those that are defined in the Pattern Definitions page where the type is SQL Injection. If you see the message “No Pattern Set of this type is defined,” you must define at least one pattern map of the SQL Injection type before you can complete this form. Any form input that contains a string that matches one of the regular expressions in the specified pattern set is flagged for the action specified in the Action drop-down list. Leave the Parameter field empty and make no selection from the Allow Pattern Set drop-down list.

- **Scan all of the form input data except for the values of one or more specific form parameters, in which certain expressions are allowed.**
  
  Set the Type to Scan All Parameters. Choose a regular expression pattern set from the Pattern Set drop-down list that lists regular expressions that you want to exclude from form input. The regular expression patterns that are listed here are those that are defined in the Pattern Definitions page where the type is SQL Injection. If you see the message “No Pattern Set of this type is defined,” you must define at least one pattern map of the SQL Injection type before you can complete this form. In the Parameter field enter the name of an exception parameter in which you want to allow input that might otherwise be flagged by the Pattern Set regular expression set. In the Allow Pattern Set drop-down list, choose a regular expression pattern set that lists regular expressions that you want to allow in the value of the exception parameter. Check the Add check box to the right of the Allow Pattern Set drop-down list and click Update Parameters. You can enter as many exception parameters as you want by repeating this procedure. Each parameter can have its own associated regular expression that defines the values that are allowed. To delete a parameter, click the Delete check box to the right of the Allow Pattern Set drop-down list and click Update Parameters.
Any form input that contains a string that matches one of the regular expressions in the Pattern Set is flagged for the action specified in the Action drop-down list. If an exception parameter value contains a string that matches both the Pattern Set and Allow Pattern Set regular expressions, then it is allowed rather than being flagged for action.

- Scan the values of a one or more specific form parameters within the input data.

Set the Type to Scan Specific Parameters. Choose a regular expression pattern set from the Pattern Set drop-down list and enter the name of a form parameter to scan in the Parameter field. Check the Add check box to the right of the parameter name and click Update Parameters. You can enter as many parameters as you want by repeating this procedure. To delete a parameter, click the Delete check box to the right of the parameter name and click Update Parameters. If any of the specified parameter values contain a string that matches one of the regular expressions in the specified pattern set, the request is flagged for the action specified in the Action drop-down list.

Check the Ignore Case check box if you do not need to match the case of a parameter specified in the Parameter field. If you do need to match the case exactly, leave this check box unchecked.

In the Action drop-down list, choose the action to apply if a form input string that matches this map is detected. Actions include these:

- None—Take no action
- Reset server client—Reset both the server and client sides of the connection
- Drop—Drop the connection silently
- [SEND-PAGE] pagename—Send the error page identified by pagename. You define such error pages by using the send page feature described in the “Error/Redirect Pages” section on page 6-39.
- [REDIRECT-PAGE] pagename—Send the redirection page identified by pagename. You define such redirection pages by using the redirect page feature described in the “Error/Redirect Pages” section on page 6-39.

If you want to log the event, click the Log check box below the Action drop-down list.

When you are finished with this form, click Apply Changes at the top to save your changes, or click Discard Changes to return to the summary page without saving your changes.

**OS Command Injection**

An OS command injection attack inserts OS commands into form input with the intention to gain elevated privileges to access a web server.

Use the OS Command Injection command to display a page that summarizes the command injection maps that are defined and to view, delete, clone, edit or add new maps. For details on using the summary page GUI, see the “Map Summary Interface” section on page 6-2.

When you click the button to add a new map, AVS displays the screen shown in Figure 6-40.
Give the map a name in the Map Name field.

In the map, you can configure protection in three ways:

- **Scan all of the form input data.**
  
  Set the Type to Scan All Parameters. Choose a regular expression pattern set from the Pattern Set drop-down list that lists regular expressions that you want to exclude from form input. The regular expression patterns that are listed here are those that are defined in the Pattern Definitions page where the type is Command Injection. If you see the message “No Pattern Set of this type is defined,” you must define at least one pattern map of the Command Injection type before you can complete this form. Any form input that contains a string that matches one of the regular expressions in the specified pattern set is flagged for the action specified in the Action drop-down list. Leave the Parameter field empty and make no selection from the Allow Pattern Set drop-down list.

- **Scan all of the form input data except for the values of one or more specific form parameters, in which certain expressions are allowed.**
  
  Set the Type to Scan All Parameters. Choose a regular expression pattern set from the Pattern Set drop-down list that lists regular expressions that you want to exclude from form input. The regular expression patterns that are listed here are those that are defined in the Pattern Definitions page where the type is Command Injection. If you see the message “No Pattern Set of this type is defined,” you must define at least one pattern map of the Command Injection type before you can complete this form.

  In the Parameter field enter the name of an exception parameter in which you want to allow input that might otherwise be flagged by the Pattern Set regular expression set. In the Allow Pattern Set drop-down list, choose a regular expression pattern set that lists regular expressions that you want to allow in the value of the exception parameter. Check the Add check box to the right of the Allow Pattern Set drop-down list and click **Update Parameters.** You can enter as many exception
parameters as you want by repeating this procedure. Each parameter can have its own associated regular expression that defines the values that are allowed. To delete a parameter, click the Delete check box to the right of the Allow Pattern Set drop-down list and click **Update Parameters**.

Any form input that contains a string that matches one of the regular expressions in the Pattern Set is flagged for the action specified in the Action drop-down list. If an exception parameter value contains a string that matches both the Pattern Set and Allow Pattern Set regular expressions, then it is allowed rather than being flagged for action.

- Scan the values of a one or more specific form parameters within the input data.

Set the Type to Scan Specific Parameters. Choose a regular expression pattern set from the Pattern Set drop-down list and enter the name of a form parameter to scan in the Parameter field. Check the Add check box to the right of the parameter name and click **Update Parameters**. You can enter as many parameters as you want by repeating this procedure. To delete a parameter, click the Delete check box to the right of the parameter name and click **Update Parameters**. If any of the specified parameter values contain a string that matches one of the regular expressions in the specified pattern set, the request is flagged for the action specified in the Action drop-down list.

Check the Ignore Case check box if you do not need to match the case of a parameter specified in the Parameter field. If you do need to match the case exactly, leave this check box unchecked.

In the Action drop-down list, choose the action to apply if a form input string that matches this map is detected. Actions include these:

- None—Take no action
- Reset server client—Reset both the server and client sides of the connection
- Drop—Drop the connection silently
- [SEND-PAGE] pagename—Send the error page identified by pagename. You define such error pages by using the send page feature described in the “Error/Redirect Pages” section on page 6-39.
- [REDIRECT-PAGE] pagename—Send the redirection page identified by pagename. You define such redirection pages by using the redirect page feature described in the “Error/Redirect Pages” section on page 6-39.

If you want to log the event, click the Log check box below the Action drop-down list.

When you are finished with this form, click **Apply Changes** at the top to save your changes, or click **Discard Changes** to return to the summary page without saving your changes.

### LDAP Injection

Lightweight Directory Access Protocol (LDAP) is widely used to query and manipulate X.500 directory services. Web applications may use form input to create custom LDAP statements for dynamic web page requests. An LDAP injection attack modifies an LDAP statement, letting the process run with the same permissions as the component that executed the command, and can let the attacker obtain unauthorized information from the database.

Use the **LDAP Injection** command to display a page that summarizes the LDAP injection maps that are defined and to view, delete, clone, edit or add new maps. For details on using the summary page GUI, see the “Map Summary Interface” section on page 6-2.

When you click the button to add a new map, AVS displays the screen shown in Figure 6-41.
Give the map a name in the Map Name field.

In the map, you can configure protection in three ways:

- **Scan all of the form input data.**
  
  Set the Type to Scan All Parameters. Choose a regular expression pattern set from the Pattern Set drop-down list that lists regular expressions that you want to exclude from form input. The regular expression patterns that are listed here are those that are defined in the Pattern Definitions page where the type is LDAP Injection. If you see the message “No Pattern Set of this type is defined,” you must define at least one pattern map of the LDAP Injection type before you can complete this form. Any form input that contains a string that matches one of the regular expressions in the specified pattern set is flagged for the action specified in the Action drop-down list. Leave the Parameter field empty and make no selection from the Allow Pattern Set drop-down list.

- **Scan all of the form input data except for the values of one or more specific form parameters, in which certain expressions are allowed.**
  
  Set the Type to Scan All Parameters. Choose a regular expression pattern set from the Pattern Set drop-down list that lists regular expressions that you want to exclude from form input. The regular expression patterns that are listed here are those that are defined in the Pattern Definitions page where the type is LDAP Injection. If you see the message “No Pattern Set of this type is defined,” you must define at least one pattern map of the LDAP Injection type before you can complete this form.
  
  In the Parameter field enter the name of an exception parameter in which you want to allow input that might otherwise be flagged by the Pattern Set regular expression set. In the Allow Pattern Set drop-down list, choose a regular expression pattern set that lists regular expressions that you want to allow in the value of the exception parameter. Check the Add check box to the right of the Allow Pattern Set drop-down list and click **Update Parameters**. You can enter as many exception
parameters as you want by repeating this procedure. Each parameter can have its own associated
regular expression that defines the values that are allowed. To delete a parameter, click the Delete
check box to the right of the Allow Pattern Set drop-down list and click Update Parameters.

Any form input that contains a string that matches one of the regular expressions in the Pattern Set
is flagged for the action specified in the Action drop-down list. If an exception parameter value
contains a string that matches both the Pattern Set and Allow Pattern Set regular expressions, then
it is allowed rather than being flagged for action.

- Scan the values of a one or more specific form parameters within the input data.

Set the Type to Scan Specific Parameters. Choose a regular expression pattern set from the Pattern
Set drop-down list and enter the name of a form parameter to scan in the Parameter field. Check the
Add check box to the right of the parameter name and click Update Parameters. You can enter as
many parameters as you want by repeating this procedure. To delete a parameter, click the Delete
check box to the right of the parameter name and click Update Parameters. If any of the specified
parameter values contain a string that matches one of the regular expressions in the specified pattern
set, the request is flagged for the action specified in the Action drop-down list.

Check the Ignore Case check box if you do not need to match the case of a parameter specified in the
Parameter field. If you do need to match the case exactly, leave this check box unchecked.

In the Action drop-down list, choose the action to apply if a form input string that matches this map is
detected. Actions include these:

- None—Take no action
- Reset server client—Reset both the server and client sides of the connection
- Drop—Drop the connection silently
- [SEND-PAGE] pagename—Send the error page identified by pagename. You define such error
  pages by using the send page feature described in the “Error/Redirect Pages” section on page 6-39.
- [REDIRECT-PAGE] pagename—Send the redirection page identified by pagename. You define
  such redirection pages by using the redirect page feature described in the “Error/Redirect Pages”
  section on page 6-39.

If you want to log the event, click the Log check box below the Action drop-down list.

When you are finished with this form, click Apply Changes at the top to save your changes, or click
Discard Changes to return to the summary page without saving your changes.

**Meta Character Detection**

A meta character attack inserts meta characters in the form input. Meta characters include characters
such as semicolons (;), pipes (|), tildes (~), and so on.

Use the Meta Character Detection command to display a page that summarizes the meta character
maps that are defined and to view, delete, clone, edit or add new maps. For details on using the summary
page GUI, see the “Map Summary Interface” section on page 6-2.

When you click the button to add a new map, AVS displays the screen shown in Figure 6-42.
Give the map a name in the Map Name field.

In the map, you can configure protection in three ways:

- **Scan all of the form input data.**
  
  Set the Type to Scan All Parameters. Choose a regular expression pattern set from the Pattern Set drop-down list that lists regular expressions that you want to exclude from form input. The regular expression patterns that are listed here are those that are defined in the Pattern Definitions page where the type is Meta Character Detection. If you see the message “No Pattern Set of this type is defined,” you must define at least one pattern map of the Meta Character Detection type before you can complete this form. Any form input that contains a string that matches one of the regular expressions in the specified pattern set is flagged for the action specified in the Action drop-down list. Leave the Parameter field empty and make no selection from the Allow Pattern Set drop-down list.

- **Scan all of the form input data except for the values of one or more specific form parameters, in which certain expressions are allowed.**
  
  Set the Type to Scan All Parameters. Choose a regular expression pattern set from the Pattern Set drop-down list that lists regular expressions that you want to exclude from form input. The regular expression patterns that are listed here are those that are defined in the Pattern Definitions page where the type is Meta Character Detection. If you see the message “No Pattern Set of this type is defined,” you must define at least one pattern map of the Meta Character Detection type before you can complete this form.

  In the Parameter field enter the name of an exception parameter in which you want to allow input that might otherwise be flagged by the Pattern Set regular expression set. In the Allow Pattern Set drop-down list, choose a regular expression pattern set that lists regular expressions that you want to allow in the value of the exception parameter. Check the Add check box to the right of the Allow Pattern Set drop-down list and click **Update Parameters**. You can enter as many exception
parameters as you want by repeating this procedure. Each parameter can have its own associated regular expression that defines the values that are allowed. To delete a parameter, click the Delete check box to the right of the Allow Pattern Set drop-down list and click **Update Parameters**.

Any form input that contains a string that matches one of the regular expressions in the Pattern Set is flagged for the action specified in the Action drop-down list. If an exception parameter value contains a string that matches both the Pattern Set and Allow Pattern Set regular expressions, then it is allowed rather than being flagged for action.

- Scan the values of a one or more specific form parameters within the input data.

Set the Type to Scan Specific Parameters. Choose a regular expression pattern set from the Pattern Set drop-down list and enter the name of a form parameter to scan in the Parameter field. Check the Add check box to the right of the parameter name and click **Update Parameters**. You can enter as many parameters as you want by repeating this procedure. To delete a parameter, click the Delete check box to the right of the parameter name and click **Update Parameters**. If any of the specified parameter values contain a string that matches one of the regular expressions in the specified pattern set, the request is flagged for the action specified in the Action drop-down list.

Check the Ignore Case check box if you do not need to match the case of a parameter specified in the Parameter field. If you do need to match the case exactly, leave this check box unchecked.

In the Action drop-down list, choose the action to apply if a form input string that matches this map is detected. Actions include these:

- **None**—Take no action
- **Reset server client**—Reset both the server and client sides of the connection
- **Drop**—Drop the connection silently
- **[SEND-PAGE] pagename**—Send the error page identified by *pagename*. You define such error pages by using the send page feature described in the “Error/Redirect Pages” section on page 6-39.
- **[REDIRECT-PAGE] pagename**—Send the redirection page identified by *pagename*. You define such redirection pages by using the redirect page feature described in the “Error/Redirect Pages” section on page 6-39.

If you want to log the event, click the Log check box below the Action drop-down list.

When you are finished with this form, click **Apply Changes** at the top to save your changes, or click **Discard Changes** to return to the summary page without saving your changes.

### Format String Attacks

A format string attack passes format string characters as form input, which may result in the unwarranted change of the stack, which can cause segmentation faults or an unanticipated program to run.

Use the **Format String Attacks** command to display a page that summarizes the format string attack maps that are defined and to view, delete, clone, edit or add new maps. For details on using the summary page GUI, see the “Map Summary Interface” section on page 6-2.

When you click the button to add a new map, AVS displays the screen shown in Figure 6-43.
Give the map a name in the Map Name field.

In the map, you can configure protection in two ways:

- **Scan all of the form input data.**
  
  Set the Type to Scan All Parameters. Choose a regular expression pattern set from the Pattern Set drop-down list that lists regular expressions that you want to exclude from form input. The regular expression patterns that are listed here are those that are defined in the Pattern Definitions page where the type is Format String Attacks. If you see the message “No Pattern Set of this type is defined,” you must define at least one pattern map of the Format String Attacks type before you can complete this form. Any form input that contains a string that matches one of the regular expressions in the specified pattern set is flagged for the action specified in the Action drop-down list. Leave the Parameter field empty and make no selection from the Allow Pattern Set drop-down list.

- **Scan the values of a one or more specific form parameters within the input data.**
  
  Set the Type to Scan Specific Parameters. Choose a regular expression pattern set from the Pattern Set drop-down list and enter the name of a form parameter to scan in the Parameter field. Check the Add check box to the right of the parameter name and click **Update Parameters**. You can enter as many parameters as you want by repeating this procedure. To delete a parameter, click the Delete check box to the right of the parameter name and click **Update Parameters**. If any of the specified parameter values contain a string that matches one of the regular expressions in the specified pattern set, the request is flagged for the action specified in the Action drop-down list.

  **Note**

  Scanning all form input data except for the values of one or more specific form parameters is not allowed in the Format String Attacks form. If Type is set to Scan All Parameters, and you enter an exception parameter in the Parameter field, you will receive an error when you click **Apply Changes**.

  Check the Ignore Case check box if you do not need to match the case exactly of a parameter specified in the Parameter field. If you do need to match the case exactly, leave this check box unchecked.
In the Action drop-down list, choose the action to apply if a form input string that matches this map is detected. Actions include these:

- None—Take no action
- Reset server client—Reset both the server and client sides of the connection
- Drop—Drop the connection silently
- [SEND-PAGE] pagename—Send the error page identified by pagename. You define such error pages by using the send page feature described in the “Error/Redirect Pages” section on page 6-39.
- [REDIRECT-PAGE] pagename—Send the redirection page identified by pagename. You define such redirection pages by using the redirect page feature described in the “Error/Redirect Pages” section on page 6-39.

If you want to log the event, click the Log check box that is below the Action drop-down list.

When you are finished with this form, click Apply Changes at the top to save your changes, or click Discard Changes to return to the summary page without saving your changes.

## Web Application Security Regular Expression Syntax

The web application security module uses a regular expression syntax that is different from the regular expression syntax used by other AVS features (and that is described in the Appendix F, “Regular Expressions”). The regular expression syntax used by the web application security module is summarized in Table 6-4.

Table 6-4 Web Application Security Regular Expression Syntax

<table>
<thead>
<tr>
<th>Metacharacter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.</td>
<td>Matches any single character, except for the new line character (0x0A). For example, the regular expression r.t matches the strings rat, rut, r t, but not root.</td>
</tr>
<tr>
<td>^</td>
<td>Matches the beginning of a line. For example, the regular expression ^When in matches the beginning of the string “When in the course of human events” but not the string “What and When in the”</td>
</tr>
<tr>
<td>*</td>
<td>Matches zero or more occurrences of the character immediately preceding. For example, the regular expression .* means match any number of any characters.</td>
</tr>
<tr>
<td>\</td>
<td>This is the quoting character; use it to treat the following metacharacter as an ordinary character. For example, ^ is used to match the caret character (^) rather than the beginning of a line. Similarly, the expression . is used to match the period character rather than any single character.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Matches any one of the characters between the brackets. For example, the regular expression r[aou]t matches rat, rot, and rut, but not ret. Ranges of characters are specified by a beginning character (c1), a hyphen, and an ending character (c2). For example, the regular expression [0-9] means match any digit. Multiple ranges can be specified as well. The regular expression [A-Za-z] means match any upper or lower case letter. To match any character except those in the range (that is, the complement range), use the caret as the first character after the opening bracket. For example, the expression [^269A-Z] matches any characters except 2, 6, 9, and uppercase letters.</td>
</tr>
<tr>
<td>( )</td>
<td>Treat the expression between ( and ) as a group, limiting the scope of other metacharacters.</td>
</tr>
<tr>
<td></td>
<td>Logical OR two conditions together. For example (him</td>
</tr>
<tr>
<td>+</td>
<td>Matches one or more occurrences of the character or regular expression immediately preceding. For example, the regular expression 9+ matches 9, 99, and 999.</td>
</tr>
</tbody>
</table>
Table 6-4  Web Application Security Regular Expression Syntax (continued)

<table>
<thead>
<tr>
<th>Metacharacter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>Matches 0 or 1 occurrence of the character or regular expression immediately preceding.</td>
</tr>
<tr>
<td>{i}</td>
<td>Matches a specific number (i) or minimum number (i,) of instances of the preceding character. For example, the expression A[0-9]{3} matches “A” followed by exactly 3 digits. That is, it matches A123 but not A1234. The expression [0-9]{4,} matches any sequence of 4 or more digits.</td>
</tr>
<tr>
<td>\r</td>
<td>Matches the carriage return character (0x0D).</td>
</tr>
<tr>
<td>\n</td>
<td>Matches the new line character (0x0A).</td>
</tr>
<tr>
<td>\t</td>
<td>Matches the tab character (0x09).</td>
</tr>
<tr>
<td>\f</td>
<td>Matches the form feed character (0x0C).</td>
</tr>
<tr>
<td>\xNN</td>
<td>Matches the character with the hexadecimal code NN, where N is between 0 and F.</td>
</tr>
<tr>
<td>\NNN</td>
<td>Matches the character with the octal code NNN, where N is between 0 and 8.</td>
</tr>
</tbody>
</table>

The web application security regular expression evaluator matches the shortest pattern possible.