



CHAPTER 34

Cisco Common Classification Policy Language

Cisco Common Classification Policy Language ([C3PL](#)) is a structured replacement for feature-specific configuration commands. C3PL allows you to create traffic policies based on events, conditions, and actions. SDM uses C3PL to create the [policy maps](#) and [class maps](#) that the following help topics describe.

Policy Map

Policy maps specify the actions to be taken when traffic matches defined criteria. Traffic types and criteria are defined in class maps associated with a policy map. In order for a router to use the information in a policy map and its associated class maps, the policy map must be associated with a [zone-pair](#). See [Zone-Based Policy Firewall](#) for more information on configuring zones and zone pairs.

Policy Map Windows

Use the policy map windows to review, create and edit policy maps for QoS, HTTP, and other types of traffic. The top portion of the window lists the configured policy maps, and the bottom portion displays the details of the highlighted policy map. If you need to edit a policy map or see more detail, click **Edit** to display a dialog that lets you view information and make changes.

This help topic provides a general description for the policy map windows and some sample data.

Add

Click **Add** to display a dialog in which you can configure a policy map.

Edit

Click **Edit** to display a dialog in which you can edit the selected policy map. The **Edit** button is disabled if no policy maps have been configured.

Delete

Click **Delete** to remove the selected policy map.

Policy Map List Area

This area lists the policy maps configured for the particular protocol or feature. Select a policy map to display details in the lower part of the screen. The following example shows two IM policies.

Policy Map Name	Description
im-pmap-g	guest policy
im-pmap-e	employee policy

Details of Policy Map

The details of the selected policy map shows the policy map configuration. The detail shown varies according to the type of policy map.

[HTTP](#), [IM](#), [P2P](#), [IMAP](#), and [POP3](#) display a match class name, action and log column. The following table shows detail for an IM policy map. The router blocks AOL traffic, but allows all other types of IM traffic.

Match Class Name	Action	Log
aol-cmap	Disabled	Disabled
class-default	Enabled	Disabled

Protocol Inspection, [SMTP](#), and [SUNRPC](#) policy map detail includes Match Class Name and Action columns. The following table shows detail for a SUNRPC policy map.

Match Class Name	Action
cmap-sunrpc1	Allow
cmap-sunrpc2	None

Add or Edit a QoS Policy Map

Use this information to help add or edit a QoS policy map.

Policy Name and Description

If you are create a new policy map, enter a name and a description for it in these fields. If you are editing a policy map, these fields are display only.

Class Map, Queuing, Set DSCP, and Drop Columns

These columns summarize the information about each class map in the policy map. The following example entry is for a voice class map:

```
Voice-FastEthernet0/1 LLQ 70% ef No
```

This class map uses Low Latency Queuing, and 70% of the bandwidth for this interface. The DSCP value is set to ef, and packets of this type are not dropped.

The **Add**, **Edit**, **Delete**, **Move Up**, and **Move Down** buttons can be used to modify the class map information in this list.

Add an Inspection Policy Map

Inspection policy maps specify the action the router is to take for traffic that matches the criteria in the associated class maps. The router can allow the traffic to pass, drop it and optionally log the event, or inspect the traffic.

The name and description that you enter will be visible in the Inspect Policy Maps window. The Class Map and Action columns display the class-maps associated with this policy map, and the action that the router is to take for the traffic that the class-map describes. Click **Add** to add a new class map to the list and configure

the action. Click **Edit** to modify the settings for a class-map. Use the **Move Up**, and **Move Down** buttons to change the order in which the class maps are evaluated.

Layer 7 Policy Map

This window allows you to select a Layer 7 Policy map to use to inspect an application that you have selected. The window displays the policy maps available for that application. Choose a policy map and click **OK**.

Application Inspection

Application inspection policies are applied at Layer 7 of the OSI model, where user applications send and receive messages that allow the applications to offer useful capabilities. Some applications might offer undesired or vulnerable capabilities, so the messages associated with these capabilities must be filtered to limit activities on the application services.

Cisco IOS Software Zone-Policy Firewall offers application inspection and control on the following application services: [HTTP](#), [SMTP](#), [POP3](#), [IMAP](#), [SUNRPC](#), [P2P](#), and [IMAP](#) applications. See the following links for more information

- [Add an HTTP Inspection Class Map](#)
- [Add or Edit an SMTP Class Map](#)
- [Add or Edit a POP3 Class Map](#)
- [Add or Edit an IMAP Class Map](#)
- [Add or Edit a SUNRPC Class Map](#)
- [Add or Edit a Point-to-Point Class Map](#)
- [Add or Edit an Instant Messaging Class Map](#)

Configure Deep Packet Inspection

Layer 7 (Application) Inspection augments Layer 4 Inspection with the capability to recognize and apply service-specific actions, such as selectively blocking or allowing file-search, file-transfer, and text-chat capabilities. Service-specific capabilities vary by service.

If you are creating a new policy map, enter a name in the **Policy Map Name** field. You can also add a description. Click **Add > New Class Map** to create a new Point-to-Point class map. [Add or Edit a Point-to-Point Class Map](#) contains information on how to create this type of class map. Click **Add > class default** to add the default class map.

When the class map appears in the table, specify the action that you want taken when a match is found, and whether you want matches logged. You can specify **<None>**, **Reset**, or **Allow**. In the following example, there are [P2P](#) class maps for gnutella, and eDonkey.

Match Class Name	Action	Log
gnutellaCMap	Allow	
eDonkeyCMap	Reset	X

Class Maps

Class-maps define the traffic that a Zone-Policy Based Firewall (ZPF) selects for policy application. Layer 4 class-maps sort the traffic based on the following criteria:

- Access-group—A standard, extended, or named Access-Control List can filter traffic based on source and destination IP address and source and destination port
- Protocol—The Layer 4 protocols (TCP, UDP, and ICMP) and application services such as HTTP, SMTP, DNS, etc. Any well-known or user-defined service known to PAM may be specified
- Class-map—A subordinate class-map providing additional match criteria can be nested inside another class-map

- **Not**—The not criterion specifies that any traffic that does not match a specified service (protocol), access-group or subordinate class-map will be selected for the class-map.

Class-maps can apply “match-any” or “match-all” operators to determine how to apply the match criteria. If “match-any” is specified, traffic must meet only one of the match criteria in the class-map. If “match-all” is specified, traffic must match all of the class-map’s criteria to belong to that particular class.

Associate Class Map

To associate a class-map with an inspect policy-map, complete the following tasks.

-
- | | |
|---------------|--|
| Step 1 | Specify a class-map name by clicking the button to the right of the name field and choosing Add a Class Map , Select a Class Map , or class-default . |
| Step 2 | In the Action box, click either Pass , Drop , or Inspect . If you click Drop , you can optionally click Log to have the drop event logged. If you click Inspect , click Advanced Options to specify the parameter maps, inspection policies, or policing that you want for the traffic in this class. |
| Step 3 | Click OK to close this dialog and return to the Add or the Edit an Inspection Policy Map dialog. |
-

Class Map Advanced Options

When you choose the inspect action for traffic, you can specify parameter maps, application inspection, and [ZPF](#) policing.

Inspect Parameter Map

Inspect parameter maps specify TCP, DNS, and UDP timeouts and session control parameters. You can select an existing parameter map. If no parameter map is configured, this field is disabled. Click **View** to display the selected parameter map without leaving this dialog.

URL Filtering Parameter Map

URL filtering parameter maps can specify URL filtering servers and local URL lists. You can select an existing parameter map. If no parameter map is configured, this field is disabled. Click **View** to display the selected parameter map without leaving this dialog.

Enable Application Inspection

An application inspection policy specifies the types of data to inspect in packets of a specified application. You can select an existing application inspection policy. If no application inspection policy is configured, this field is disabled. Click **View** to display the selected application inspection policy without leaving this dialog.

Police Rate and Burst

You can limit traffic to a specified rate, and specify a burst value. The police rate can be a value between 8,000 and 2,000,000,000 bits per second. The burst rate can be a value between 1,000 and 512,000,000 bytes.

QoS Classmap

Use this window to display and edit QoS class map information. QoS class maps are used in QoS policy maps to define types of traffic.

Click on a class map name to display details about that class map in the **Details of Class Map** area.

The details of a class map show which protocols are matched to define the traffic. The following example shows details of a voice signalling class map.

Details of Class Map:SDMSignal-FastEthernet0/1

Item Name	Item Value
Match Protocols	h323,rtcp

H.323 and RTCP are the voice signalling protocols that are to be matched.

Add or Edit a QoS Class Map

Use this information to help add or edit a QoS class map. If you are adding a new QoS class map, click the button on the right of the field and choose either **Add a Classmap** or **Select a Classmap** from the context menu.

See the information in [Action](#) to learn about the **Drop**, **Set DSCP**, and **Queuing** options.

Add or Edit a QoS Class Map

Enter a name and description of the QoS class Map you are creating so that it can be easily identified and used. Click [Classification](#) for a description of the **Any**, **All**, and **Edit** buttons in the Classification box.

Select a Class Map

Click the name of the class map that you want to choose, and click **OK**. The class map entry is added to the window from which you invoked this dialog.

Deep Inspection

Deep inspection allows you to create class maps for parameters specific to an application. For example, you can create class maps for the common [P2P](#) applications such as [eDonkey](#), [gnutella](#), and [kazaa2](#).

Class Map and Application Service Group Windows

Use the class map windows to review, create and edit class maps for protocols such as [HTTP](#), [SMTP](#), and [POP3](#). The Class Map area of the window lists the configured class maps, and the bottom portion displays the details of the selected class map. If you need to edit a class map or see more detail, click **Edit** to display a dialog that lets you view information and make changes.

Add

Click **Add** to create a new class map of the type you have selected and enter the configuration in the displayed dialog.

Edit

Click **Edit** to change the configuration of the selected class map.

Delete

Click **Delete** to remove the selected class map. Cisco SDM may display dialogs if there are dependencies associated with this configuration, such as subordinate class maps or parameter maps that could be used by other class maps.

Class Map Area

This area displays the class maps configured for the protocol that you selected. It contains the names of the configured class maps and other relevant information.

QoS Class Maps

QoS class maps are displayed in a table with a Class Map Name and a Description column. A sample table follows.

Class Map Name	Description
CMAP-DMZ	FTP and HTTP QoS class map
CMAP-3	Test

Inspection, HTTP, SMTP, SUN RPC, IMAP and POP3 Class Maps

These types of class maps have a Class Map Name and a Used By column. A sample table for HTTP follows.

Class Map Name	Used By
http-rqst	pmap-5
http-rsp-body	pmap-5

Instant Messaging Service Groups and Peer-to-Peer Application Service Groups

Instant Messaging Service group and peer-to-peer (P2P) application service groups have an additional column because class maps are configured for a specific application, such as the Yahoo! Messenger instant messaging application or the [gnutella](#) P2P application. The following table shows sample data for P2P application service groups

Class Map Name	Used By	Class Map Type
cmap-gnutella	pmap-7	gnutella
cmap-edonkey	pmap-7	edonkey
cmap-bittorrent	pmap-7	bittorrent

Details of Class Map

The Details of Class Map area shows the configuration for a particular class map. It has an Item Name and an Item Value column.

Item Name

The name of the configuration setting. For example, an HTTP class map might have settings for Request Header, Port Misuse, and Protocol Violation.

Item Value

The value of the configuration setting. For example, HTTP Request Header setting value might be Length > 500, and the Port Misuse flag might be disabled.

More Information About Class Map Details

For more information about class map details displayed in these windows, click on any of the following links:

- [Add or Edit a QoS Class Map](#)
- [Add or Edit an Inspect Class Map](#)
- [Add an HTTP Inspection Class Map](#)
- [Add or Edit an Instant Messaging Class Map](#)
- [Add or Edit a Point-to-Point Class Map](#)
- [Add or Edit an SMTP Class Map](#)

- [Add or Edit a SUNRPC Class Map](#)
- [Add or Edit an IMAP Class Map](#)
- [Add or Edit a POP3 Class Map](#)

Add or Edit an Inspect Class Map

Creating an inspect class map enables you to make a wide variety of traffic available for inspection. Enter a name to identify this class map in the **Class Name** field. You can also enter a description. If you are editing a class map, you cannot change the name. When you have specified the conditions that you want the class to map, click **OK**.

Specifying whether you want the class to match any or all of the conditions

Click **Any** if the class need only match one or more conditions that you choose. Click **All** if the class must match all conditions.

Choosing what you want the inspect class map to match

Browse what you want the class map to match in the left column. Click the plus (+) sign next to a node to display the child nodes. For example, click **HTTP** to display the child nodes http and https. To choose an item, click it and then click **Add>>**. To remove an item that you have added to the column on the right, click it and then click **<<Remove**.

Changing the match order

If you chose to match any of the conditions, you may want to change the match order of the items in the right column. To move an item up the list, click it and then click **Up**. To move an item down the list, click it and then click **Down**. The **Up** button is disabled when you click the item at the top of the list. The **Down** button is disabled when you click the item at the bottom of the list.

Associate Parameter Map

This dialog displays the parameter maps that you can associate with the class map. Click the **Select** box next to the parameter map you want to associate with the class map.

Add an HTTP Inspection Class Map

HTTP inspection class maps allow you to make a wide variety of HTTP Request, Response, and Request Response data available for inspection.

To create an HTTP inspection class map, do the following:

-
- Step 1** Enter a Class Name to identify the class map. You can also enter a description that will be visible in the HTTP Class Maps window.
 - Step 2** Click on the branch in the HTTP tree that contains the type of data you want to make available for inspection. You can create a class map for HTTP requests, responses, and for request-responses.
 - Step 3** Click on the appropriate sub-branch to further specify the type of data you want to include.
 - Step 4** Configure the class map data in the fields displayed.
 - Step 5** Specify match conditions by clicking **Any conditions below** if the class map need match only one or more conditions. Click **All the specified conditions below** if the class map must match all the conditions that you specify.
-

HTTP Request Header

Enter class map criteria for HTTP request header attributes.

Length Greater Than

Click this box if you want to specify a global request header length that a packet should not exceed, and enter the number of bytes.

Count Greater Than

Click this box if you want to specify a limit to the total number of request header fields that a packet should not exceed, and enter the number of fields.

Regular Expressions

Click this box to specify regular expressions to be matched against. Choose an existing regular expression class map, or create a new one that will match the strings you are inspecting for. See [Add or Edit Regular Expression](#) for more information on how to create regular expressions. To examine an existing map without leaving this dialog, choose it in the **Select an existing map** list, and click **View**.

Field Name and Configuration Options

You can include fields within the header to the inspection criteria and specify length, count, and strings to inspect for. Click **Add** to include a field, and enter criteria in the dialog displayed.

HTTP Request Header Fields

Choose the type of header field from the list and specify the inspection criteria for it.

Length greater than

Click this box if you want to specify a length that this field should not exceed, and enter the number of bytes. For example, you might block a request whose cookie field exceeded 256 bytes, or whose user-agent field exceeded 128 bytes.

Count greater than

Click this box if you want to specify the number of times that this field can be repeated in the header, and enter a number. For example you might block a request that had multiple content-length header lines by entering the value 1. This example is an effective measure for preventing session smuggling

Regular expressions

Click this box to specify regular expressions to be matched against. Choose an existing regular expression class map, or create a new one that will match the strings you are inspecting for. See [Add or Edit Regular Expression](#) for more

information on how to create regular expressions. To examine an existing map without leaving this dialog, choose it in the **Select an existing map** list, and click **View**.

Match field

Check this box if you want the class map to match the field type that you chose.

Other Fields in this Dialog

Depending on which HTTP header field you choose, additional fields may be displayed in this dialog, enabling you to specify additional criteria. For example, if you choose the **content-type** field, you can inspect for content type mismatches between the request and the response, unknown content types, and protocol violations for the particular content type. If you choose the **transfer-encoding** field, you can inspect for various types of compression and encoding.

HTTP Request Body

You can inspect an HTTP request body for length and character strings.

Length

Check this box and choose **Greater than (>)** to specify an upper limit to the request body length. Choose **Less than (<)** to specify a lower limit.

Regular Expressions

If you want to inspect for strings, click this box and choose an existing regular expression class map, or create a new regular expression class map that will match the strings you are inspecting for. See [Add or Edit Regular Expression](#) for more information on how to create regular expressions. To examine an existing map without leaving this dialog, choose it in the **Select an existing map list**, and click **View**.

HTTP Request Header Arguments

You can inspect for the length of the arguments sent in a request, and inspect for strings that match regular expressions that you have configured.

Length greater than

Click this box and specify the number of bytes that the total length of request header arguments should not exceed.

Regular Expressions

Click this box to specify regular expressions to be matched against. Choose an existing regular expression class map, or create a new one that will match the strings you are inspecting for. See [Add or Edit Regular Expression](#) for more information on how to create regular expressions. To examine an existing map without leaving this dialog, choose it in the **Select an existing map** list, and click **View**.

HTTP Method

HTTP methods indicate the purpose of an HTTP request. Choose the HTTP methods in the **Method List** column that you want to inspect and check the **Select** box next to the method.

Request Port Misuse

HTTP port 80 is sometimes used by [IM](#), [P2P](#), tunnelling, and other applications. Check the types of port misuse that you want to inspect for. You can inspect for any type of port misuse, port misuse by IM applications, P2P application port misuse, and misuse by tunnelling applications.

Request URI

Enter the Universal Resource Identifier ([URI](#)) criteria that you want to include in the class map.

Length Greater than

Click this box if you want to specify a URI length that a packet should not exceed, and enter the number of bytes.

Regular Expressions

Click this box to specify regular expressions to be matched against. Choose an existing regular expression class map, or create a new one that will match the strings you are inspecting for. See [Add or Edit Regular Expression](#) for more information on how to create regular expressions. To examine an existing map without leaving this dialog, choose it in the **Select an existing map** list, and click **View**.

Sample Use Case

Configure an HTTP class map to block a request whose URI matches any of the following regular expressions:

“.*cmd.exe”

“.*sex”

“.*gambling”

Response Header

Enter the criteria for HTTP response headers that you want to include in the class map.

Length Greater Than

Click this box if you want to specify a global response header length that a packet should not exceed, and enter the number of bytes.

Count Greater Than

Click this box if you want to specify a limit to the total number of response header fields that a packet should not exceed, and enter the number of fields.

Regular Expressions

Click this box to specify regular expressions to be matched against. Choose an existing regular expression class map, or create a new one that will match the strings you are inspecting for. See [Add or Edit Regular Expression](#) for more

information on how to create regular expressions. To examine an existing map without leaving this dialog, choose it in the **Select an existing map** list, and click **View**.

Response Header Fields

Choose the type of header field from the list and specify the inspection criteria for it.

Length Greater Than

Click this box if you want to specify a field length that a packet should not exceed, and enter the number of bytes.

Count Greater Than

Click this box if you want to specify a limit to the total number of fields of this type that a packet should not exceed, and enter the number of fields.

Regular Expressions

Click this box to specify regular expressions to be matched against. Choose an existing regular expression class map, or create a new one that will match the strings you are inspecting for. See [Add or Edit Regular Expression](#) for more information on how to create regular expressions. To examine an existing map without leaving this dialog, choose it in the **Select an existing map** list, and click **View**.

Other Fields in this Dialog

Depending on which HTTP header field you choose, additional fields may be displayed in this dialog, enabling you to specify additional criteria. For example, if you choose the **content-type** field, you can inspect for content type mismatches between the request and the response, unknown content types, and protocol violations for the particular content type. If you choose the **transfer-encoding** field, you can inspect for various types of compression and encoding.

Match Field

Check this box if you want the class map to match the field type that you chose.

HTTP Response Body

Specify the HTTP response body criteria to inspect for.

Java Applets in HTTP response

Check this box if you want to inspect for Java applets in the HTTP response. Depending on the actions configured in the policy map

Length

Check this box and choose **Greater than (>)** to specify an upper limit to the response body length. Choose **Less than (<)** to specify a lower limit.

Regular Expressions

Click this box to specify regular expressions to be matched against. Choose an existing regular expression class map, or create a new one that will match the strings you are inspecting for. See [Add or Edit Regular Expression](#) for more information on how to create regular expressions. To examine an existing map without leaving this dialog, choose it in the **Select an existing map** list, and click **View**.

HTTP Response Status Line

Click this box and specify regular expressions to be matched against response status lines. Choose an existing regular expression class map, or create a new one that will match the strings you are inspecting for.

Sample Use Case

Configure the router to log an alarm whenever an attempt is made to access a forbidden page. A forbidden page usually contains a 403 status-code and the status line looks like “HTTP/1.0 403 page forbidden\r\n.”

The regular expression for this is the following:

```
[Hh] [Tt] [Tt] [Pp] [/] [0-9] [.] [0-9] [ \t]+403
```

Logging is specified in the policy map to which the HTTP class map is associated.

See [Add or Edit Regular Expression](#) for more information on how to create regular expressions. To examine an existing map without leaving this dialog, choose it in the **Select an existing map** list, and click **View**.

Request/Response Header Criteria

Enter class map criteria for HTTP request/response headers.

Length Greater Than

Click this box if you want to specify a global request/response header length that a packet should not exceed, and enter the number of bytes.

Count Greater Than

Click this box if you want to specify a limit to the total number of request/response header fields that a packet should not exceed, and enter the number of fields.

Regular Expressions

Click this box to specify regular expressions to be matched against. Choose an existing regular expression class map, or create a new one that will match the strings you are inspecting for. See [Add or Edit Regular Expression](#) for more information on how to create regular expressions. To examine an existing map without leaving this dialog, choose it in the **Select an existing map** list, and click **View**.

HTTP Request/Response Header Fields

Choose the HTTP Request/Response header field that you want to include in the class map.

Length Greater Than

Click this box if you want to specify a field length that a packet should not exceed, and enter the number of bytes.

Count Greater Than

Click this box if you want to specify a limit to the total number of fields of this type that a packet should not exceed, and enter the number of fields.

Regular Expressions

Click this box to specify regular expressions to be matched against. Choose an existing regular expression class map, or create a new one that will match the strings you are inspecting for. See [Add or Edit Regular Expression](#) for more information on how to create regular expressions. To examine an existing map without leaving this dialog, choose it in the **Select an existing map** list, and click **View**.

Other Fields in this Dialog

Depending on which HTTP header field you choose, additional fields may be displayed in this dialog, enabling you to specify additional criteria. For example, if you choose the **content-type** field, you can inspect for content type mismatches between the request and the response, unknown content types, and protocol violations for the particular content type. If you choose the **transfer-encoding** field, you can inspect for various types of compression and encoding.

Match Field

Check this box if you want the class map to match the field type that you chose.

Request/Response Body

The router can inspect for request/response body length and specific text strings inside the body of the request/response.

Length

Check this box and choose **Greater than (>)** to specify an upper limit to the request/response body length. Choose **Less than (<)** to specify a lower limit.

Regular Expressions

Click this box to specify regular expressions to be matched against. Choose an existing regular expression class map, or create a new one that will match the strings you are inspecting for. See [Add or Edit Regular Expression](#) for more information on how to create regular expressions. To examine an existing map without leaving this dialog, choose it in the **Select an existing map** list, and click **View**.

Request/Response Protocol Violation

To inspect for protocol violations in HTTP request/responses, click **Protocol Violation**.

Add or Edit an IMAP Class Map

Creating a class map for Internet Message Access Protocol ([IMAP](#)) inspection can help ensure that users are using secure authentication mechanisms to prevent compromise of user credentials.

Enter a name to identify this class map in the **Class Name** field. You can also enter a description. If you are editing a class map, you cannot change the name.

Click **Login string in clear text** to have the router inspect IMAP traffic for nonsecure logins.

Click **Invalid protocol command** to have the router inspect IMAP traffic for invalid commands.

Add or Edit an SMTP Class Map

Simple Mail Transfer Protocol ([SMTP](#)) class maps enable you to limit content length and enforce protocol compliance.

Enter a name to identify this class map in the **Class Name** field. You can also enter a description in the field provided.

Enter the **Maximum data transfer allowed** in the **Match Criteria** box.

Add or Edit a SUNRPC Class Map

SUN Remote Procedure Call ([SUNRPC](#)) class maps allow you to specify the number of the program whose traffic you want the router to inspect.

Enter a name to identify this class map in the **Class Name** field. You can also enter a description. If you are editing a class map, you cannot change the name.

Click **Add** in the **Match Program Number** box to add a program number.

Add or Edit an Instant Messaging Class Map

Instant Messaging ([IM](#)) class maps allow you to specify the type of instant messaging and whether you want traffic for all IM services inspected, or only traffic for the text chat service.

In the **Class Map Type** field, choose **aol** for America Online, **msnmsgr** for Microsoft Networks Messenger, or choose **ymsgr** for Yahoo! Messenger.

In the Match Criteria box, click **All services**, or click **Text chat services** if you only want text chat traffic to be inspected.

Add or Edit a Point-to-Point Class Map

A [P2P](#) class map specifies a P2P application, and the match criteria. Only one application can be specified per class map.

Class Name

Enter a new class name to create a new class map. Clicking the button on the right of the field allows you to select existing class maps to edit. You can edit the match criteria for a class map, but you cannot change the class map type.

Class Map Type

You can create a P2P class map for the following types of P2P services:

- [eDonkey](#)
- [fasttrack](#)
- [gnutella](#)
- [kazaa2](#)

Match Criteria and Value

Click **Add** to enter match criteria to specify the type of connections that are to be identified by the traffic class.

Enter match criteria to specify the type of connections that are to be identified by the traffic class. You can specify that file transfer connections be identified by the traffic class for fasttrack, gnutella, and kazaa2. For eDonkey, you can specify that file transfer connections, filename requests (search-file-name), and text chats be identified by the traffic class. The value for the match criteria can be any regular expression. For example, to specify that all file transfer connections be identified, enter `*`.

Add P2P Rule

Enter match criteria to specify the type of connections that are to be identified by the traffic class. You can specify that file transfer connections be identified by the traffic class for fasttrack, gnutella, and kazaa2. For eDonkey, you can specify that file transfer connections, filename requests (search-file-name), and text chats be identified by the traffic class. The value for the match criteria can be any regular expression. For example, to specify that all file transfer connections be identified, enter `*`.

Add or Edit a POP3 Class Map

Creating a class map for Post Office Protocol version 3 (**POP3**) inspection can help ensure that users are using secure authentication mechanisms to prevent compromise of user credentials.

Enter a name to identify this class map in the **Class Name** field. You can also enter a description. If you are editing a class map, you cannot change the name.

Click **Login string in clear text** to have the router inspect POP3 traffic for nonsecure logins.

Click **Invalid protocol command** to have the router inspect POP3 traffic for invalid commands.

Parameter Maps

Parameter-maps specify inspection behavior for Zone-Policy Firewall, for parameters such as Denial-of-Service Protection, session and connection timers, and logging settings. Parameter-maps are also applied with Layer 7 class- and policy-maps to define application-specific behavior, such as HTTP objects, POP3 and IMAP authentication requirements, and other application-specific information.

Parameter Map Windows

The parameter map windows list the configured parameter maps for Protocol Information, URL Filtering, Regular Expressions, and other types of parameter maps. If the parameter map has been associated with a class map, the class-map name appears in the Used By column. The details of the selected parameter map are displayed in the bottom half of the window. You can add, edit and delete parameter maps. SDM informs you if you attempt to delete a parameter map that is being used by a class map.

For more information about the parameter maps displayed in these windows, click on any of the following links:

- [Timeouts and Thresholds for Inspect Parameter Maps and CBAC](#)
- [Add or Edit a Parameter Map for Protocol Information](#)
- [General Settings for URL Filtering](#)
- [Add or Edit an URL Filter Server](#)
- [Local URL List](#)
- [Add or Edit Regular Expression](#)

Add or Edit a Parameter Map for Protocol Information

It may be necessary to identify servers for specific types of applications, such as [IM](#) applications so that you can restrict use to a particular activity, such as text chat.

Parameter Map Name

Enter a name that conveys the use of this parameter map. For example, if you are creating a server list for Yahoo! Instant Messenger text chat servers, you can use the name `ymgr-pmap`.

Server Details

This area of the screen is a list of server names, server IP addresses, or IP address ranges.

Add or Edit a Server Entry

You can provide the hostname or IP address of an individual server, or a range of IP addresses assigned to a group of servers.

You can enter a hostname in the **Name** field if the router is able to contact a DNS server on the network to resolve the server's IP address. If you want to enter the IP address for one server, enter it in the **Single IP Address** field. If there are several servers that use an IP address range, use the **IP range** field. Enter the lowest IP address in the left-hand field and the highest IP address in the right hand field. For example to enter the range 103.24.5.67 through 99, enter `103.24.5.67` in the left-hand field and `103.24.5.99` in the right-hand field.

Add or Edit Regular Expression

A regular expression matches text strings either literally as an exact string, or by using *metacharacters* so you can match multiple variants of a text string. You can use a regular expression to match the content of certain application traffic; for example, you can match body text inside an HTTP packet.

Regular expressions you create can be used anywhere a regular expression is needed in the Zone-Based Policy Firewall screens. [Regular Expression Metacharacters](#) contains a list of regular expression metacharacters and how they are used.

Name

Enter a name to identify the regular expression. If you are editing the regular expression, the name field is read only.

Pattern List

A regular expression can contain multiple patterns. Click **Add** to display a dialog in which you can enter a new regular expression pattern. Each pattern that you create is automatically added to the list. If you need to copy a pattern from another regular expression, click **Copy Pattern**, click the plus (+) sign next to regular expression name, click the pattern that you want, and then click **OK**.

```
parameter-map type regex ref_regex
pattern "\.delfinproject\.com"
pattern "\.looksmart\.com"
parameter-map type regex host_regex
pattern "secure\.keenvalue\.com"
pattern "\.looksmart\.com"
parameter-map type regex usragnt_regex
pattern "Peer Points Manager"
```

Replace this with table.

Add a Pattern

The pattern that you enter in this window is added to the bottom of the regular expression parameter map that you are editing. If you need to reorder the patterns in the parameter map, you can do so in the Edit Regular Expression window.

Pattern

Enter the pattern that you want to add to the regular expression.

Guide Button

Click to display the [Build Regular Expression](#) dialog which can assist you in constructing a regular expression. If you click **Guide**, any text that you entered in the **Pattern** field appears in the [Regular Expression](#) field of the Build Regular Expression dialog.

Build Regular Expression

The Build Regular Expression dialog box lets you construct a regular expression out of characters and metacharacters. Fields that insert metacharacters include the metacharacter in parentheses in the field name.

Build Snippet

This area lets you build text snippets of regular text or lets you insert a metacharacter into the Regular Expression field.

- Starts at the beginning of the line (^)—Indicates that the snippet should start at the beginning of a line, using the caret (^) metacharacter. Be sure to insert any snippet with this option at the beginning of the regular expression.
- Specify Character String—Enter a text string manually.
 - Character String—Enter a text string.
 - Escape Special Characters—If you entered any metacharacters in your text string that you want to be used literally, check this box to add the backslash (\) escape character before them. For example, if you enter “example.com,” this option converts it to “example\com”.
 - Ignore Case—If you want to match upper and lower case characters, this check box automatically adds text to match both upper and lower case. For example, entering “cats” is converted to “[cC][aA][tT][sS]”.

Specify Character

Lets you specify a metacharacter to insert in the regular expression.

- Negate the character—Specifies not to match the character you identify.
- Any character (.)—Inserts the period (.) metacharacter to match any character. For example, **d.g** matches dog, dag, dtg, and any word that contains those characters, such as doggonnit.
- Character set—Inserts a character set. Text can match any character in the set. Sets include:

[0-9A-Za-z]

[0-9]

[A-Z]

[a-z]

[aeiou]

[\n\r\t] (which matches a new line, form feed, carriage return, or a tab)

For example, if you specify [0-9A-Za-z], then this snippet will match any character from A to Z (upper or lower case) or any digit 0 through 9.

- **Special character**—Inserts a character that requires an escape, including \, ?, *, +, |, ., [, (, or ^. The escape character is the backslash (\), which is automatically entered when you choose this option.
- **Whitespace character**—Whitespace characters include \n (new line), \f (form feed), \r (carriage return), or \t (tab).
- **Three digit octal number**—Matches an ASCII character as octal (up to three digits). For example, the character \040 represents a space. The backslash (\) is entered automatically.
- **Two digit hexadecimal number**—Matches an ASCII character using hexadecimal (exactly two digits). The backslash (\) is entered automatically.
- **Specified character**—Enter any single character.

Snippet Preview

Display only. Shows the snippet as it will be entered in the regular expression.

- **Append Snippet**—Adds the snippet to the end of the regular expression.
- **Append Snippet as Alternate**—Adds the snippet to the end of the regular expression separated by a pipe (|), which matches either expression it separates. For example, **dog|cat** matches dog or cat.
- **Insert Snippet at Cursor**—Inserts the snippet at the cursor.

Regular Expression

This area includes regular expression text that you can enter manually and build with snippets. You can then select text in the Regular Expression field and apply a quantifier to the selection.

- **Selection Occurrences**—Select text in the Regular Expression field, click one of the following options, and then click **Apply to Selection**. For example, if the regular expression is “test me,” and you select “me” and apply **One or more times**, then the regular expression changes to “test (me)+”.
 - **Zero or one times (?)**—A quantifier that indicates that there are 0 or 1 of the previous expression. For example, **lo?se** matches lse or lose.
 - **One or more times (+)**—A quantifier that indicates that there is at least 1 of the previous expression. For example, **lo+se** matches lose and loose, but not lse.

- One or more times (+)—A quantifier that indicates that there is at least 1 of the previous expression. For example, **lo+se** matches lose and loose, but not lse.
- Any number of times (*)—A quantifier that indicates that there are 0, 1 or any number of the previous expression. For example, **lo*se** matches lse, lose, loose, etc.
- At least—Repeat at least x times. For example, **ab(xy){2,}z** matches abxyxyz, abxyxyxyz, etc.
- Exactly—Repeat exactly x times. For example, **ab(xy){3}z** matches abxyxyxyz.
- Apply to Selection—Applies the quantifier to the selection.
- Test—Tests a regular expression against some sample text.

Regular Expression Metacharacters

The following table lists the metacharacters that have special meanings.

Character	Description	Notes
.	Dot	Matches any single character. For example, d.g matches dog, dag, dtg, and any word that contains those characters, such as doggonnit.
(<i>exp</i>)	Subexpression	A subexpression segregates characters from surrounding characters, so that you can use other metacharacters on the subexpression. For example, d(ola)g matches dog and dag, but dolag matches do and ag. A subexpression can also be used with repeat quantifiers to differentiate the characters meant for repetition. For example, ab(xy){3}z matches abxyxyxyz.
	Alternation	Matches either expression it separates. For example, dog cat matches dog or cat.

Parameter Maps

Character	Description	Notes
?	Question mark	<p>A quantifier that indicates that there are 0 or 1 of the previous expression. For example, lo?se matches lse or lose.</p> <p>Note You must enter Ctrl+V and then the question mark or else the help function is invoked.</p>
*	Asterisk	A quantifier that indicates that there are 0, 1 or any number of the previous expression. For example, lo*se matches lse, lose, loose, etc.
+	Plus	A quantifier that indicates that there is at least 1 of the previous expression. For example, lo+se matches lose and loose, but not lse.
{x}	Repeat quantifier	Repeat exactly <i>x</i> times. For example, ab(xy){3}z matches abxyxyxyz.
{x,}	Minimum repeat quantifier	Repeat at least <i>x</i> times. For example, ab(xy){2,}z matches abxyxyz, abxyxyxyz, etc.
[abc]	Character class	Matches any character in the brackets. For example, [abc] matches a, b, or c.
[^abc]	Negated character class	Matches a single character that is not contained within the brackets. For example, [^abc] matches any character other than a, b, or c. [^A-Z] matches any single character that is not an uppercase letter.
[a-c]	Character range class	<p>Matches any character in the range. [a-z] matches any lowercase letter. You can mix characters and ranges: [abcq-z] matches a, b, c, q, r, s, t, u, v, w, x, y, z, and so does [a-cq-z].</p> <p>The dash (-) character is literal only if it is the last or the first character within the brackets: [abc-] or [-abc].</p>
""	Quotation marks	Preserves trailing or leading spaces in the string. For example, " test" preserves the leading space when it looks for a match.
^	Caret	Specifies the beginning of a line.

Character	Description	Notes
\	Escape character	When used with a metacharacter, matches a literal character. For example, \[matches the left square bracket.
<i>char</i>	Character	When character is not a metacharacter, matches the literal character.
\r	Carriage return	Matches a carriage return 0x0d.
\n	Newline	Matches a new line 0x0a.
\t	Tab	Matches a tab 0x09.
\f	Formfeed	Matches a form feed 0x0c.
\xNN	Escaped hexadecimal number	Matches an ASCII character using hexadecimal (exactly two digits).
\NNN	Escaped octal number	Matches an ASCII character as octal (exactly three digits). For example, the character 040 represents a space.

